UNIVERZITET U BEOGRADU
ELEKTROTEHNIČKI FAKULTET

Boriša Ž. Jovanović

EFIKASAN MEHANIZAM KRIPTOGRAFSKE SINHRONIZACIJE U ALGORITMIMA SELEKTIVNOG ŠIFROVANJA MULTIMEDIJALNIH SISTEMA NOVE GENERACIJE

doktorska disertacija

Beograd, 2018.

UNIVERSITY OF BELGRADE
SCHOOL OF ELECTRICAL ENGINEERING

Boriša Ž. Jovanović

AN EFFICIENT MECHANISM OF CRYPTOGRAPHIC SYNCHRONIZATION WITHIN SELECTIVE ENCRYPTION ALGORITHMS OF THE NEW GENRATION MULTIMEDIA SYSTEMS

Doctoral Dissertation

Belgrade, 2018

Mentor:
dr Slavko Gajin, docent
Univerzitet u Beogradu - Elektrotehnički fakultet

Članovi komisije:
dr Zoran Jovanović, redovni profesor
Univerzitet u Beogradu - Elektrotehnički fakultet

dr Pavle Vuletić, docent
Univerzitet u Beogradu - Elektrotehnički fakultet

dr Vladan Devedžić, redovni profesor
Univerzitet u Beogradu - Fakultet organizacionih nauka

Datum odbrane: _____

Izjava zahvalnosti:

Želeo bih da se zahvalim svojoj supruzi Mariji bez čije bezrezervne podrške, ohrabrivanja, ljubavi, razumevanja, i ogromnog strpljenja ovaj rad verovatno nikada ne bi bio napisan. Zahvalnost dugujem i našoj ćerki Dani na sreći, radosti i veselju koji je unela u naš dom i naše živote u vremenu mog napornog angažovanja na sprovođenju istraživanja i pisanja ovog rada.

Zahvalnost dugujem i mentoru, docentu dr Slavku Gajinu, na sveobuhvatnoj podršci koju mi je pružao sve vreme dok sam realizovao istraživanje opisano u ovom radu.

Na kraju, zahvaljujem se i Ministarstvu odbrane Republike Srbije koje je stipendiralo moje akademske doktorske studije.

Naslov doktorske disertacije: Efikasan mehanizam kriptografske sinhronizacije u algoritmima selektivnog šifrovanja multimedijalnih sistema nove generacije.

Rezime: Brzi razvoj digitalne multimedije, dostupnost većih propusnih opsega u komunikacionim mrežama i porast procesorske snage prouzrokovali su svakodnevno korišćenje digitalnih multimedijalnih podataka na različitim uređajima i u različitim sferama života. Velika količina kako ličnih tako i poslovnih multimedijalnih podataka postaje javno dostupno i mogu biti lako ukradeni, kopirani ili modifikovani.

HEVC (High Efficiency Video Coding) je najnoviji standard kompresije video podataka koji su zajedno razvile institucije ITU-T i ISO/IEC u toku 2013. godine. Ovaj standard kodovanja video podataka je razvijen kao odgovor na rastuće potrebe za većim rezolucijama video podataka, većim stepenom kompresije pokretnih slika i boljim iskorišćenjem računarskih arhitektura za paralelnu obradu podataka. Dizajn najnovijeg standarda kompresije video podataka obezbeđuje približno 30% -50% redukcije bitskog protoka (bitske brzine) u odnosu na ekvivalentni perceptualni kvalitet koji se postiže prethodnim standardom video kompresije - H.264/AVC High Profile. Ovakva karakteristika čini HEVC standard pogodnim za različite primene kao što su Internet striming, komunikacione tehnologije, konverzacija u realnom vremenu koja obuhvata i video ćaskanje, video konferencije i telepresence sisteme komunikacije. Osim navedenog, HEVC standard se može efikasno koristiti za skladištenje digitalnih video podataka i za emitovanje televizijskog signala visoke definicije (engl. HD TV - High deffinition) preko satelitskih, kablovskih ili zemaljskih sistema prenosa. Prethodno navedeno čini HEVC standard atraktivnim rešenjem za širok opseg mogućih primena video sadržaja kako i okviru različitih Internet servisa u komercijalnom sektoru tako i u vojnim komunikacionim sistemima.

Navedeni standard predstavlja najefikasniji sistem kompresije video podataka koji postoji. Međutim, ovaj standard ne obezbeđuje bezbednosne mehanizme kojima se implementiraju kriptografski servis očuvanja tajnosti podataka. Postoji nekoliko javno dostupnih algoritama selektivnog šifrovanja za prethodni H.264/AVC standard kompresije i nekoliko novih za novi H.265/HEVC standard. Algoritmi selektivnog šifrovanja se koriste za zaštitu tajnosti video toka podataka. Mali deo video toka je

kriptografski obrađen, sa minimalnim utroškom resursa (procesorska snaga, vreme obrade) i još uvek dovoljnim nivoom sigurnosti za različite oblasti primene. Selektivnim šifrovanjem video toka postižu se značajne uštede u vremenu obrade podataka. Ovakav način očuvanja procesorske snage je poželjan u komunikacionim sistemima sa ograničenim resursima (mrežne aplikacije koje rade u realnom vremenu, razmena slika i video sadržaja visokog kvaliteta i rezolucije, mobilni sistemi sa uređajima koji imaju ograničenu procesorsku snagu i ograničen vek baterije).

Šifrovanje malog dela video toka na predajnoj strani sprečava ili ometa slučajni pristup u okviru selektivno šifrovanog HEVC video toka na prijemnoj strani. Slučajan pristup u okviru selektivno šifrovanog HEVC video toka na prijemnoj strani, podrazumeva da algoritam selektivnog šifrovanja i HEVC dekoder mogu da pokrenu proces dešifrovanja i dekodiranja u bilo kojoj tački slučajnog pristupa video toka podataka. To znači da su oni u mogućnosti da pristupe proizvoljnoj poziciji u okviru video fajla, proizvoljnoj poziciji u okviru video toka podataka, do obave operaciju spajanja video tokova ili operaciju promene kanala (promena izvora video toka podataka) u bilo kom vremenskom trenutku. Na prijemnoj strani, algoritam selektivnog šifrovanja treba da zna koji deo sintaksnih elemenata HEVC video toka podataka treba da dešifruje i koje je početno stanje od koga počinje operaciju dešifrovanja. Drugim rečima, prijemna strana (strana dekodera) mora biti kriptografski sinhronizovana sa predajnom stranom (enkoderom). Delovi sintaksnih elemenata koji trebaju da se dešifruju definisani su primenjenim algoritmom selektivnog šifrovanja dok je inicijalno stanje od koga počinje proces dešifrovanja definisano primenjenim simetričnim kriptografskim algoritmom.

Suštinske karakteristike algoritama selektivnog šifrovanja su: sintaksni elementi video toka podataka koji su šifrovani i primenjeni simetrični kriptografski algoritam. Navedene karakteristike se razlikuju među različitim algoritmima selektivnog šifrovanja. Ovakva različitost među algoritmima selektivnog šifrovanja zahteva postojanje efikasnog mehanizma kriptografske sinhronizacije koji je nezavistan od primenjenog algoritma selektivnog šifrovanja.

Glavni doprinos ove disertacije je definicija originalnog i efikasnog mehanizma kriptografske sinhronizacije u okviru selektivno šifrovanog HEVC video toka podataka koji je nezavistan od primenjenog algoritma selektivnog šifrovanja. Ovako efikasan

mehanizam postignut je definisanjem sintakse i semantike novog sintaksnog elementa u okviru HEVC video toka čijom primenom se implementira kriptografska sinhronizacija i omogućava slučajan pristup u okviru selektivno šifrovanog HEVC video toka. Efikasnost ponuđenog rešenja ogleda se u minimalnoj količini dodatih bita u HEVC video tok podataka. Veličina dodatnih sinhronizacionih podataka je direktno proporcionalna veličini bloka primenjenog simetričnog kriptografskog algoritma. Veličina sinhronizacionih podataka ne zavisi od parametara video toka podataka koji je selektivno šifrovan. Centralni deo ove disertacije je definicija dodatnog sintaksnog elementa u HEVC video toku, što predstavlja proširenje navedenog standarda video kompresije, sa ciljem da se dizajniraju efikasni H.265/HEVC enkoder i dekoder sa mogućnošću slučajnog pristupa.

Ključne reči: Video kodovanje visoke efikasnosti, HEVC/H.265, kriptografska sinhronizacija, selektivno šifrovanje, slučajni pristup, kriptografski algoritam, algoritam selektivnog šifrovanja, AES kriptografski algoritam.

Naučna oblast: Elektrotehnika i računarstvo
Uža naučna oblast: Softversko inženjerstvo
UDK broj: 621.3

Title: An efficient mechanism of cryptographic synchronization within selective encryption algorithm of the new generation multimedia systems.

Abstract: Following advancement and rapid development of digital multimedia, larger bandwidths available within the communication network and increased processing power led to the everyday utilization of digital multimedia on different devices and in different areas of life. A large amount of both personal and business multimedia data has consequently become publicly available, and in turn can be more easily copied or modified.

High Efficiency Video Coding (HEVC) is the newest video coding standard of ITU-T and ISO/IEC, proposed in 2013. This coding standard was developed in response to the growing need for increased video resolution support, higher compression of moving picture and greater use of parallel processing architectures. The design of the HEVC video coding standard provides approximately 30% - 50% bit-rate reduction for the equivalent perceptual quality relative to the performance of the previous standard H.264/AVC High Profile. This feature makes HEVC suitable for various applications such as Internet streaming, communication, real-time conversation comprising video chat, video conferencing and telepresence systems. Furthermore, HEVC can be efficiently used for digital storage media, and broadcasting of high definition (HD) television signal via satellite, cable and terrestrial transmission systems. This makes HEVC an attractive solution for a wide range of video applications, including various Internet services, commercial sectors, as well as military purposes.

This standard represents the most efficient video compression system available nowadays. However, the standard does not provide security mechanisms that would ensure confidentiality and authenticity. There are several publicly available selective encryption algorithms for the previous H.264/AVC standard and for the new H.265/HEVC standard. Selective encryption algorithms are used to protect video stream – a small part of the video stream is encrypted, with minimal resource overhead and still a sufficient security level for most applications. Selective encryption of video stream achieved significant savings in time of data processing. This way of preserving CPU power is desirable in communication systems with limited resources (real time network

application, exchange of images and video stream of high quality and resolution, mobile devices that have limited processing power and battery life).

Encryption of a small part of the video stream at the transmiting side prevents or hinders random access within selectively encrypted HEVC video stream on the receiving side. Random access within selectively encrypted HEVC video stream, at the receiving side, means that selective encryption algorithm and HEVC decoder can start the deciphering and decoding process at any point of the video stream. This means that they are possible to jump to a particular position within the file, a particular position within the video stream, perform splicing operation or channel switching (change source of video stream) at any time. At the receiving side, selective encryption algorithm needs to know which parts of HEVC syntax elements necessary to decrypt and that the initial state from which starts when decrypt. In other words, the receiving side (decoder) must be cryptographically synchronized with a transmitting side (encoder). Parts that need to be decrypted are defined by selectively encryption algorithm and the initial state are defined by the selected symmetric cryptographic algorithm.

The essential characteristics of a selective encryption algorithm are: video stream syntax elements that are encrypted and applied symmetric cryptographic algorithm. These characteristics are different among different selectively encryption algorithms. Such diversity between the selective encryption algorithms, requires the existence of the cryptographic synchronization mechanism that is independent from the applied selectively encryption algorithm.

The main contribution of this disertation is defining an original and efficient cryptographic synchronization mechanism within the selectively encrypted HEVC video stream that is independent from the applied selective encryption algorithm. This mechanism is achieved by defining the syntax and semantics of the new syntax element in the HEVC bitstream that provides cryptographic synchronization and allows random access to the selectively encrypted HEVC video stream. The efficiency of the offered solutions is reflected in the resulting data overhead. The size of the synchronization parameter is directly proportional to the size of the block of the applied cryptographic algorithm. It also does not depend on the parameters of the encoded video. Defining an

additional syntax element is the central part of the disertation and it is dedicated to the design of an efficient H.265/HEVC crypto encoder with random access capability.

Keywords: High Efficiency Video Coding, HEVC/H.265, cryptographic synchronization, selective encryption, random access, cryptographic algorithm, selective encryption algorithm, AES algorithm.

Scientific area: Electrical and Computer Engineering
Scientific subarea: Software Engineering
UDC number: 621.3

SADRŽAJ

1. UVOD

Širokopojasni Internet, savremene komunikacione tehnologije, smart telefoni, prenosni i tablet računari, televizijski signal visoke rezolucije (engl. *HDTV - High Deffinition TV*) i društvene mreže postali su nezaobilazni element ljudskog života. Njihova svakodnevna upotreba prouzrokuje da digitalni video podaci igraju sve važniju ulogu u modernom društvu. Zajedno sa brzim razvojem različitih multimedijalnih tehnologija, sve više ličnih ali i poslovnih video podataka generiše se i razmenjuje u različitim sferama života: medicini, komercijalnom sektoru, vojnim komunikacionim sistemima, u okviru interakcije na društvenim mrežama. Većina navedenih video podataka sadrži osetljive informacije koje treba da budu dostupne samo onome kome su namenjene. Prema tome, bezbednost i privatnost video podataka postaje važna i sve više dobija na značaju.

Tokom poslednjih nekoliko godina razvijeno je više algoritama za šifrovanje video sadržaja sa ciljem da se zaštiti tajnost video podataka. Navedeni algoritmi mogu se podeliti u dve grupe: tradicionalni algoritmi i algoritmi selektivnog šifrovanja. Kod tradicionalnih algoritama zaštite tajnosti video podataka, video sadržaj se najpre u celosti kompresuje pa se tako dobijeni kompresovani video tok kriptografski obradi nekim od standardnih kriptografskih algoritama (AES, IDEA i td.). Specifične karakteristike podataka ovog tipa, velika bitska brzina prenosa podatka i ograničena dozvoljena širina propusnog opsega, čine tradicionalne algortime neadekvatnim za zaštitu tajnosti video podataka. Drugo ograničenje tradicionalnih algoritama za zaštitu tajnosti podataka ovog tipa je to što se njihovom primenom menja struktura i sintaksa samog video toka čime se onemogućavaju određene funkcionalnosti kodera koji generišu taj video tok ali i dekodera koji, na prijemnoj strani, interpretiraju primljeni video. Novi trend u oblasti kriptografske zaštite video sadržaja je primena algoritama selektivnog šifrovanja. Kako samo ime kaže, ovi mehanizmi se sastoje od kriptografske obrade samo određenog, precizno definisanog, podskupa video toka podataka. Cilj primene mehanizama selektivnog šifrovanja je da se smanji količina podataka koju

treba kriptografski obraditi a da istovremeno bude očuvan dovoljan nivo bezbednosti. Ovakav način očuvanja procesorske snage je veoma poželjan u komunikacionim sistemima sa ograničenim resursima: mrežne aplikacije koje rade u realnom vremenu, razmena slika i video sadržaja visokog kvaliteta i rezolucije, mobilni sistemi sa uređajima koji imaju ograničenu procesorsku snagu i ograničen vek baterije itd. Uopšteno gledano, postupak selektivnog šifrovanja svodi se na podelu video sadržaja, koji se prenosi putem komunikacionog sistema, na dva dela. Prvi deo je javni deo, deo podataka koji se ne šifruje i ostaje dostupan svim korisnicima u sistemu prenosa podataka. Drugi deo je zaštićeni deo i na njega se primenjuju odgovarajuće kriptografske tehnike najčešće primenom simetričnih blokovskih kriptografskih algoritama. Na taj način se postiže da samo autorizovani korisnici imaju pristup zaštićenom delu podataka.

Bez obzira na primenjeni algoritam za šifrovanje video sadržaja, ne postoji adekvatan mehanizam kriptografske sinhronizacije prilikom operacije slučajnog pristupa odabranom delu šifrovanog video toka. Slučajni pristup šifrovanom video toku podrazumeva sposobnost dekodera da pristupi (otpočne dešifrovanje i dekodiranje) proizvoljnoj tački slučajnog pristupa u okviru šifrovanog video toka podataka približno lako i efikasno kao i svakoj drugoj, bez obzira na to koliko tačaka slučajnog pristupa postoji u video toku. Da bi dekoder bio sposoban da ostvari pristup proizvoljnoj tački slučajnog pristupa, algoritam dešifrovanja na prijemnoj strani (strana dekodera) mora biti kriptografski sinhronizovan sa algoritmom šifrovanja na predajnoj strani (strana enkodera). Ukoliko algoritam dešifrovanja na prijemnoj strani nije pravilno kriptografski sinhronizovan sa algoritmom na predajnoj strani, dešifrovani podaci će biti netačni. Posledično, rezultat operacije dešifrovanja i dekodiranja video toka podataka neći biti ispravan.

Kod tradicionalnih algoritama za šifrovanje video podataka, celokupni video tok podataka je kriptografski obrađen te se kod njih koriste tradicionalne tehnike kriptografske sinhronizacije. Kada su u pitanju savremeni algoritmi selektivnog šifrovanja video toka podatka, nijedan od ponuđenih i javno dostupnih algoritama ne obrađuje problem kriptografske sinhronizacije prilikom operacije slučajnog pristupa određenom delu selektivno šifrovanog video toka. Shodno tome, postoji potreba da se dizajnira i implementira adekvatan mehanizam kriptografske sinhronizacije. Na dizajn i

implementaciju mehanizma kriptografske sinhronizacije značajan uticaj imaju specifičnosti algoritama selektivnog šifrovanja. Ono što je specifično svakom novom algoritmu selektivnog šifrovanja video toka su sledeće dve karakteristike: koji elementi sintakse video toka podataka su kriptografski obrađeni i koji simetrični kriptografski algoritam je primenjen za njihovu kriptografsku obradu. Broj sintaksnih elemenata, koji su izabrani za kriptografsku obradu, i njihov položaj u video toku podataka indirektno utiču na dizajn mehanizma kriptografske sinhronizacije. Uticaj se ogleda u nemogućnosti da se na lak i vremenski jednostavan način dođe do prethodnog kriptografski obrađenog sintaksnog elementa. Takođe, primenjeni simetrični blokovski kriptografski algoritam i kriptografski mod rada u kome se on koristi, utiču na mehanizme kriptografske sinhronizacije svojim sinhronizacionim karakteristikama. Naime, svaki od različitih kriptografskih modova rada se različito ponaša u slučajevima slučajnog pristupa i propagacije greške prilikom šifrovanja odnosno dešifrovanja. Navedene specifičnosti i različitosti algoritama selektivnog šifrovanja nameću potrebu za postojanjem efikasnog mehanizma kriptografske sinhronizacije koji je nezavistan od primenjenog algoritma selektivnog šifrovanja.

Naučni doprinos ove disertacije je definicija originalnog i efikasnog mehanizma kriptografske sinhronizacije nezavisnog od primenjenog algoritma selektivnog šifrovanja. Navedeni mehanizam kriptografske sinhronizacije realizovan je kroz definiciju sintakse i semantike novog elementa HEVC video toka podataka, koji predstavlja proširenje navedenog standarda. Efikasnost ovako definisanog mehanizma kriptografske sinhronizacije ogleda se u minimalnoj količini podataka dodatih u HEVC video tok. Ovako definisan, efikasan mehanizam kriptografske sinhronizacije predstavlja potreban i dovoljan uslov za implementaciju operacije pristupa proizvoljnoj tački slučajnog pristupa u okviru selektivno šifrovanog HEVC video toka. Osim toga, ova disertacija doprinosi boljem razumevanju algoritama selektivnog šifrovanja HEVC video toka i daje teorijska razmatranja mogućnosti primene ponuđenog rešenja u vojnim komunikacionim sistemima.

Teza je organizovana u sedam poglavlja. Posle uvoda, u drugom poglavlju je dat kratak pregled najnovijeg HEVC standarda kompresije video podataka sa osvrtom na karakteristike i specifičnosti implementacije slučajnog pristupa u okviru HEVC video toka. U trećem poglavlju je data teorijska osnova algoritama selektivnog šifrovanja sa

kratkom analizom postojećih algoritama selektivnog šifrovanja za novi HEVC video tok podataka. U četvrtom poglavlju dat je opis kriptografske osnove ponuđenog rešenja kroz opis AES kriptografskog algoritma, kao najčešće upotrebljavanog simetričnog blokovskog kriptografskog algoritma. Posebno su analizirani modovi rada u kojima se blokovski kriptografski algoritmi mogu koristiti i kako navedeni modovi rada mogu da utiču na kriptografsku sinhronizaciju. U petom poglavlju detaljno je opisana sintaksa i semantika ponuđenog efikasnog mehanizma kriptografske sinhronizacije u algoritmima selektivnog šifrovanja HEVC video toka i na sestematičan način obrađeni i prikazani dobijeni rezultati njegove implementacije, testirane nad referentnim test sekvencama. Šesto poglavlje predstavlja teorijske osnove moguće primene ponuđenog rešenja u vojnim komunikacionim sistemima. U sedmom poglavlju predstavljen je zaključak u kome su data završna razmatranja.

2. HEVC/H.265 - NOVI STANDARD KOMPRESIJE VIDEO PODATAKA

Konceptualno gledano HEVC standard predstavlja dvoslojno dizajnirani sistem koji se sastoji od sloja kodovanja videa (engl. *VCL - Video Coding Layer*) i sloja apstrakcije mreže (engl. *NAL - Network Abstraction Layer*). Sloj kodovanja videa obuhvata celokupnu obradu slika na najnižem nivou uključujući podelu slika na blokove, inter i intra predikciju, kodovanje transformacije, kodovanje entropije i filtriranje unutar petlji enkodera/dekodera. Sloj apstrakcije mreže obuhvata enkapsulaciju kodiranih video podataka i pratećih informacija u NAL jedinice koje predstavljaju logičke formate paketa koji omogućavaju prenos video podataka putem različitih transportnih slojeva, uključujući RTP/IP, ISO MP4 i H.222.0/MPEG2 sisteme[1].

2.1. HEVC tehnika video kodovanja

Kao i svi prethodni ITU-T i ISO/IEC JTC standardi, počev od H.261 standarda, dizajn HEVC standarda se zasniva na klasičnom hibridnom kodovanju video podataka zasnovanom na blokovima. U osnovi algoritma kodovanja video podataka nalazi se hibrid koji sadrži intra i inter predikcije slika i 2D transformacije. Intra predikcija slika eksploatiše vremensku statističku zavisnost dok na drugoj strani inter predikcija slika eksploatiše prostornu statističku zavisnost. 2D transformacijom vrši se kodiranje indeksa ostataka predikcije da bi se u budućnosti eksploatisala prostorna statistička zavisnost.

Algoritam kompresije video podataka koji proizvodi HEVC kompatibilan video tok podataka radi na sledeći način. Svaka slika se deli na blokovski oblikovane regione, i istovremeno se unapred definisanim mehanizmom identične podele na regione dostavlja dekoderu. Prva slika u video sekvenci (ali i prva slika u svakoj tački čisto slučajnog pristupa u video sekvenci) je kodirana koristeći samo intra predikciju slika. Intra predikcija slika koristi neku od predikcija podataka prostorno od regiona do regiona u

okviru iste slike, ali nema zavisnosti od drugih slika. Za sve ostale slike u okviru video sekvence ili za slike između dve tačke slučajnog pristupa, koristi se inter predikcija slika za većinu od blokova. Inter predikcija predstavlja vremensku predikciju slika na osnovu susednih slika video sekvence. Dok intra predikcija slika za cilj ima uklanjanje prostorne redudanse, inter predikcija za cilj ima uklanjanje vremenske redudanse.

Slike iste video sekvence su jako slične i predikcija bloka se vrši tako što se proceni njegova translacija u odnosu na neku prethodnu ili narednu sliku video sekvence (engl. *ME - Motion Estimation*). Tako se odredi vektor pomeraja (engl. *MV - Motion Vector*). Zatim se vrši kompenzacija pokreta (engl. *MC - Motion Compesation*) tako što se oduzme orginalni blok slike od predviđenog i dobije njihova razlika (engl. *residual*). Ova razlika se transformiše pomoću linearne prostorne transformacije i značajni koeficijenti se skaliraju, kvantizuju i šalju ka koderu entropije zajedno sa informacijama o predikciji.

2.1.1. Predstavljanje slika bazirano na odbircima

Za predstavljanje prostora boja i vrednosti piksela koristi se YUV (ili YCbCr) prostor boja. On se sastoji od tri kanala: Y je kanal osvetljenja (engl. *luminance-luma*), U (ili Cb - *chrominance*[1] *blue, chroma blue*) je kanal intenziteta plave boje i V (ili Cr - *chrominance red, chroma red*) je kanal intenziteta crvene boje. Tačnije, intenzitet crvene i plave boje predstavljen je stepenom odstupanja boje od sive do crvene ili plave respektivno. Pri dizajniranju YUV prostora boja uzeta je u obzir ljudska percepcija. Propusni opseg intenziteta boje se smanjuje, jer je ljudski vizuelni sistem manje osetljiv na intenzitet boje u odnosu na osvetljenje. Budući da je ljudski vizuelni sistem mnogo osetljiviji na nivo osvetljenja nego na intenzitet boje, tipično se koristi 4:2:0 struktura odabiranja, u kome na svaki odbirak intenziteta boje dolazi jedna četvrtina odbiraka osvetljenja. Svaki odbirak za svaki od kanala tipično se predstavlja sa 8 ili 10 bita preciznosti, ali se u praksi za sada koristi 8 bitska preciznost.

Uzimanje odbiraka kod slika u okviru video podataka se obično realizuje progresivnim odabiranjem pravouganih slika veličine *WxH*, gde *W* predstavlja širinu a *H* predstavlja visinu slike izraženu celobrojnom vrednošću broja odbiraka osvetljenja.

[1] chrominance - kolorimetrijska razlika između date boje u nekoj slici koja je sastavni deo videa i standardne boje pri jednakom osvetljenju.

To za posledicu ima da svaki niz komponenti intenziteta boje, u slučaju kada je struktura odabiranja 4:2:0, ima dimnezije *W/2xH/2*.

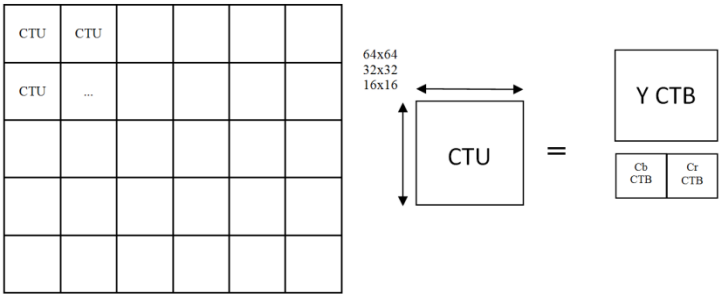
2.1.2. Podela na blokove bazirana na „quadtree“ strukturama

U hibridnom video kodovanju zasnovanom na blokovima, svaka slika se deli na blokove odbiraka, a više blokova unutar slike su agregirani tako da formiraju odsečak koji predstavlja nezavistan samostalno dekodabilni entitet. U svim prethodnim standardima video kodovanja, razvijenim od strane ITU-T ili ISO/IEC organizacija, svaka slika sekvence se deli na takozvane makroblokove. Jedan makroblok sadrži 16x16 odbiraka intenziteta svetlosti i, u 4:2:0 strukturi odabiranja, i dva pridružena 8x8 odbiraka intenziteta boje. Kod ovih standarda, makroblok predstavlja osnovnu jedinicu kodiranja. U zavisnosti od karakteristika koje podržava aktuelni standard, može biti dodatno predviđena podela makroblokova u podblokove koji se koriste za kompenzaciju pokreta ili za intra predikciju slika. Veličini makrobloka od 16x16 odbiraka intenziteta svetlosti predstavlja najveću veličinu bloka koja se može koristiti za signalizaciju parametara predviđanja, kao što su podaci o kretanju.

Iako se standardi video kodovanja kao što su H.262/MPEG-2 [2] ili H.264/AVC [3] danas koriste za skladištenje i prenos video podataka visoke definicije (engl. *HD - High-Deffinition*), sa tipičnim rezolucijama slike od 1280x720 ili 1920x1080 odbirka intenziteta svetlosti, oni su primarno dizajnirani za video sa rezolucijama koje se kreću od QCIF rezolucije (176x144 odbirka intenziteta svetlosti) do video rezolucije standardne definicije (engl. *SD - standard definition*) (720x480 ili 720x576 odbirka intenziteta svetlosti). Zahvaljujući popularnosti HD videa i rastućem interesovanju za Ultra HD (UHD) formate [4] sa rezolucijama video od, na primer, 3840x2160 ili 7680x4320 odbirka intenziteta svetlosti, HEVC standard [5] je dizajniran sa fokusom na video sa visokim rezolucijama. Međutim, za ovako velike rezolucije slika, ograničavanje najveće veličine bloka koje se mogu koristiti za signaliziranje predmeta predviđanja na 16x16 odbirka intenziteta osvetljenja (kao što je to slučaj sa prethodnim standardima) je neefikasno u smislu stepena distorzije[6]. Za tipičan HD i UHD video sadržaj, mnogi regioni slike koji mogu biti opisani sa istim parametrima pokreta su mnogo veći nego što je to region od 16x16 odbirka. Iako je povećanje najveće podržane veličine bloka pogodno za video zapise visoke rezolucije, sa druge strane može imati

negativan uticaj na efikasnost kompresije video zapisa u niskim rezolucijama. Iz tog razloga HEVC standard uključuje fleksibilan mehanizam podele slika u okviru video sekvence u osnovne jedinice kodiranja promenljive veličine.

HEVC standard kao osnovnu jedinicu kodiranja koristi mnogo adaptivniju „*quadtree*“ strukturu stabla, koja je nazvana CTU (engl. *CTU - Coding Tree Unit*). Svaka slika (frejm) se deli na osnovne jedinice kodiranja – CTU-ove. Moguće veličine za osnovne jedinice kodiranja su 64x64, 32x32 ili 16x16 odbirka. U principu, „*quadtree*“ struktura kodovanja se opisuje pomoću "blokova" i "jedinica"[2]. Blok definiše niz odbirka i veličine istih, dok jedinica enkapsulira jedan luma i odgovarajuće hroma blokove zajedno sa sintaksom potrebnom za njihovo kodiranje. Osnovne jedinice kodiranja su sastavljene od jednog bloka osvetljenja (Y - luma) i dva bloka intenziteta plave i crvene boje (Cb i Cr), kao što je prikazano na slici 1. Navedeni blokvi se nazivaju blokovi stabla kodiranja (engl. *CTB – Coding Tree Blocks*). Shodno tome, osnovna jedinica kodiranja - CTU, obuhvata blokove stabla kodiranja (CTB blokove) i sintaksu koja specificira kodiranje podataka i buduću podpodelu. Svaki blok stabla kodiranja (CTB) ima istu veličinu kao i osnovna jedinica kodiranja (CTU).

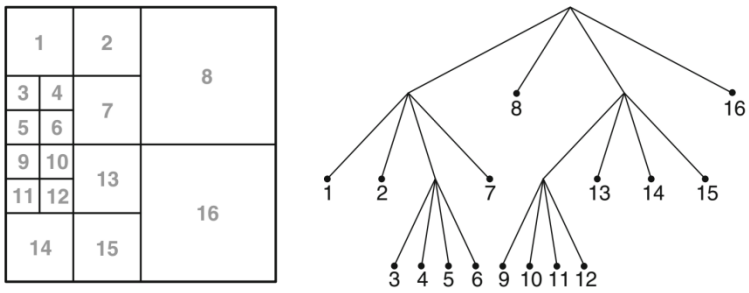


Slika 1. CTU i CTB

U zavisnosti od dela video frejma koji se kodira, blok stabla kodiranja (CTB) može biti prevelik da se na osnovu njega odluči da li treba vršiti intra ili inter predikciju. Svaki blok stabla kodiranja (CTB) se može rekurzivno podeliti na novu *quadtree* strukturu, sve do veličine 8x8 odbirka. Tako na primer jedan 64x64 CTB može sadržati

[2] Ovde postoji jedna važna konvencija imenovanja u HEVC standardu. Ako se nešto označava sa "xxxxUnit" to označava logičku jedinicu kodovanja koja se sukcesivno kodira u HEVC video tok podataka. Sa druge strane, ako se nešto označava sa "xxxxBlock" on ukazuje na deo bafera video frejma na koji je proces kodiranja usmeren.

dva 32x32, šest 16x16 i osam 8x8 regiona, kao što je prikazano na slici 2. Ovi regioni se zovu jedinice kodiranja (engl. *CU - Conding Units*) i predstavljaju osnovne jedinice predikcije u HEVC standardu. Slično kao i CTU, CU se sastoji od kvadratnog bloka odbirka intenziteta osvetljenja, dva odgovarajuća bloka intenziteta boje i sintaksnih elemenata koji su im pridruženi. Nizovi odbirka intenziteta osvetljenja i intenziteta boje koji se nalaze u okviru CU nazivaju se blokovi kodiranja (engl. *CB - Coding Block*).



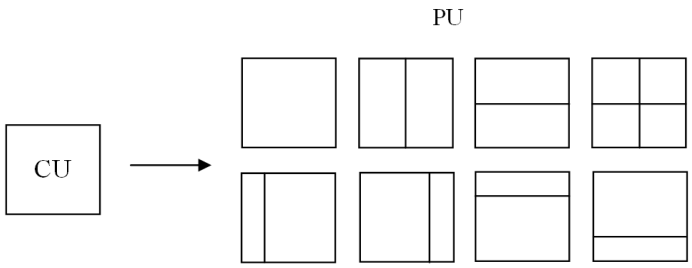
Slika 2. Deljenje CTU na CU

Jedinice kodiranja se, u okviru stabla kodiranja, kodiraju po redosledu prikazanom brojevima na prethodnoj slici 2. Ovakav redosled kodiranja se označava Z-skeniranje. Ovakav način kodiranja obezbeđuje da su za svaku jedinicu kodiranja, osim onih koje se nalaze na samom vrhu ili levoj granici odsečka, svi odbirci iznad i levo od date jedinice kodiranja već kodirani, tako da odgovarajući uzorci mogu biti korišćeni za intra predikciju i pridruženi parametri kodiranja mogu biti korišćeni za predikciju parametara kodiranja tekućeg odbirka.

Svaka jedinica kodiranja (CU) sadrži više entiteta koji su namenjeni za proces predikcije, takozvane jedinice predviđanja (engl. *PU - Prediction Unit*) i za potrebe transformacije, takozvane jedinice transformacije (engl. *TU - Tarnsformation Unit*). Na sličan način, svaki blok kodiranja se deli na blok predviđanja (engl. *PB - Prediction Block*) i blok transformacije (engl. *TB - Transform Block*).

Jedinice kodiranja (CU), a samim tim i blokovi kodiranja (CB), dovoljno su dobre da se odluči koji tip predikcije će biti primenjen, ali su sa druge strane veoma velike da sačuvaju vektore pokreta u nekom od oblika predikcije. Na primer, veoma mali objekti kao što je pahuljica snega može da se kreće u sredini bloka 8x8 odbirka, pa je stoga potrebno koristiti različite vektore pokreta u zavisnosti od dela jedinice kodiranja (CU). Iz tog razloga, jedinica kodiranja (CU) deli se na jedinice predviđanja (PU). Analogno ovome blok kodiranja (CB) deli se na blokove predviđanja (PB). Podela jedinica

kodiranja (CU) vrši se primenom jednog od osam postojećih modova. Ovih osam modova imaju sledeće mnemonike: *2Nx2N*, *2NxN*, *Nx2N*, *NxN*, *2NxnU*, *2NxnD*, *nLx2N*, *nRx2N*. Gde veliko slovo *N* predstavlja polovinu dužine stranice jedinice kodiranja (CU), a malo slovo *n* predstavlja njenu četvrtinu. Sa slike 3 se može videti da ova podela nije rekurzivna.



Slika 3. Podela CU na PU

Prema tome, jedna jedinica kodiranja (CU) sadrži jednu, dve ili četiri jedinice predviđanja (PU). Analogno ovome jedan blok kodiranja (CB) sadrži jedan, dva ili četiri blokova predviđanja (PB). Jedinica kodiranja (CU) može biti intra ili inter kodirana, tako da ukoliko je jedinica kodiranja (CU) podeljena na dve jedinice predviđanja (PU) obe od njih su ili intra ili inter kodirane. Intra kodirane jedinice kodiranja mogu da koriste samo modove 2Nx2N ili NxN, tako da su Intra jedinice predviđanja uvek samo kvadratnog oblika.

Nakon što je završen proces predikcije, potrebno je kodovati residual (razliku između prediktovane slike i stvarne slike) primenom neke transformacije. CU može biti veoma velika za realizaciju ove operacije jer jedna CU (jedan CB) može sadržati istovremeno deo sa velikom količinom detalja (*high frequency*) i deo sa malom količinom detalja (*low frequency*). Prema tome svaki CU (CB) može dalje da se podeli na TU (tj. na TB). Ovde se radi o rekurzivnoj podeli po principu „*quadtree*“ strukture na isti način kako se CTU deli na CU odnosno isto kao što se CTB deli na CB. HEVC ima nekoliko veličina transformacija: 32x32, 16x16, 8x8, i 4x4. Veće jedinice transformacije su u stanju da bolje kodiraju stacionarne signale dok su manji TU bolji za kodiranje manjih "impulsivnih" signala.

2.1.3. Intra predikcija slika

Sa ciljem postizanja visoke efikasnosti kodiranja uz istovremeno smanjivanje vremenskih i memorijskih zahteva, intra predikcija slika sastoji od tri koraka: konstrukcije niza referentnih odbirka, predikcije odbirka i postprocesiranja. Metode intra predikcije slike u HEVC standardu se mogu podeliti u dve kategorije. Prvu kategoriju predikcije čine ugaone metode[7] koje daju enkoderu mogućnost preciznog procesiranja struktura sa usmerenim ivicama. U drugu kategoriju spadaju planarna predikcija i DC predikcija koje enkoderu pružaju mogućnost predikciju glatkog sadržaja slike[8]. Ukupan broj metoda intra predikcije u HEVC standardu je 35, za razliku od svega 8 koliko ih je bilo kod prethodnog H.264 standarda.

Intra predikcija u jedinicama kodiranja u potpunosti prati stablo jedinica transformacije. Kada je intra jedinica kodiranja kodirana u režimu podele NxN, stablo transformacije se prisilno razdvaja najmanje jednom obezbeđujući na taj način da se intra i stablo transfomracije podudaraju. To znači da se intra predikcija uvek odvija na odbircima veličine 4x4, 8x8, 16x16 ili 32x32.

Sve metode intra predikcije koriste referentne odbirke iz susednih rekonstruisanih blokova. U zavisnosti od položaja bloka intra predikcije, bilo koji od navedenih susednih odbirka možda neće biti dostupan. Na primer, oni mogu biti van slike, na drugom delu slike ili da pripadaju jedinici kodiranja koja će biti obrađena u budućnosti. Svi odbirci koji nisu dostupni popunjavaju se unapred definisanim vrednostima, nakon čega su oni ispunjeni važećim odbircima.

U ekstremnom slučaju kada nijedan referentni odbirak nije dostupan, svi referentni odbirci se zamenjuju nominalnom prosečnom vrednošću odbirka za datu bitsku reprezentaciju (na primer, vrednošću 128 ako se koristi 8 bitska preciznost). Ako postoji najmanje jedan referentni odbirak označen kao dostupan za inter predikciju, nedostupni referentni uzorci se zamenjuju korišćenjem dostupnih uzoraka. Nedostupni referentni odbirci se zamenjuju skeniranjem dostupnih odbiraka u smeru kretanja kazaljke na časovniku na taj način što se uzima vrednost najnovijeg dostupnog odbirka da bi se zamenio prvi nedostupni odbirak. Na ovako kreirane nizove referentnih odbiraka mogu se uslovno primeniti filteri za uglačavanje. Ovakvim filtriranjem se postiže poboljšanje vizuelnog izgleda bloka predikcije izbegavanjem vrednosti referentnih odbiraka koji mogu potencijalno generisati neželjene ivice u okviru bloka predikcije.

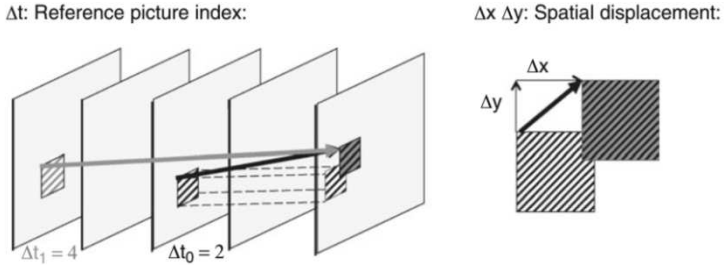
Nakon što su kreirani nizovi referentnih odbiraka pristupa se samom procesu inter predikcije. Kao što je prethodno rečeno, HEVC standard ima 35 metoda intra predikcije. Ugaone metode intra predikcije namenjene su za modelovanje različitih usmerenih struktura koje su tipično prisutne na slikama. Sa druge strane planarna i DC metoda intra predikcije pružaju mogućnost predikcije za oblasti slike sa glatkim i postepeno promenljivim sadržajem.

U cilju daljeg poboljšanja kvaliteta predikcije, neke od ugaonih i DC metoda predikcije uključuju laganu operaciju postprocesiranja koja se ogleda u filtriranju radi povećanja kontinuiteta signala predikcije na granicama blokova.

2.1.4. Inter predikcija slika

Inter predikcija u HEVC standardu se može posmatrati kao stalno unapređivanje i generalizacija svih tehnika i pristupa poznatih iz prethodnih standarda video kodovanja. U novom standardu se sreće unapređena predikcija vektora pokreta bazirana na nadmetanju vektora pokreta, dok je tehnika sjedinjavanja blokova inter predikcije značajno pojednostavila signalizaciju podataka o blokovima predikcije tako što je nasledila sve podatke o pokretu iz blokova koji su već enkodovani.

Dok inter predikcija iskorišćava korelaciju između prostorno susednih odbiraka, inter predikcija koristi vremensku korelaciju između slika sa ciljem da kreira predikciju kompenzacije pokreta (engl. *MCP - Motion-Compensated Prediction*) za blok odbiraka slike. Kod ovakvog pristupa predikcije kompenzacije pokreta bazirane na blokovima, slika u okviru video toka se deli na pravougaone blokove. Uz pretpostavku da je unutar nekog bloka homogeno kretanje i da su pokretni objekti veći od jednog bloka, za svaki blok se može naći odgovarajući blok u prethodno enkodovanoj slici koji može da služi kao prediktor[9]. Opšti koncept predikcije kompenzacije pokreta zasnovan na modelu translacionog kretanja ilustrovan je na slici 4.



Slika 4. Ilustracija postupka Inter predikcije (preuzeto iz [9])

Kod modela translacionog kretanja, pozicija bloka u okviru prethodno enkodovane slike označen je vektorom pokreta (Δx, Δy), gde Δx određuje horizontalni a Δy vertikalni pomeraj u odnosu na položaj trenutnog bloka. Vektori pokreta (Δx, Δy) mogu biti delimične tačnosti uzorka da preciznije prikažu kretanje objekta. Na referentnim slikama se primenjuje interpolacija sa ciljem da se izvede signal predikcije u situacijama kada vektor pokreta ima delimičnu tačnost odabiranja. Prethodno dekodovana slika se naziva referentna slika i označava referentnim indeksom Δ_t u listi referentnih slika. Ovi parametri modela translacionog kretanja, tj. vektori pokreta i referentni indeks, u daljem tekstu će biti kratko označavani kao podaci o kretanju. Podaci o kretanju se izračunavaju u enkoderu i procesu procene kretanja (engl. *Motion estimation*). Sam proces procene kretanja nije specificiran standardom tako da različiti enkoderi mogu da koriste različite kompromise u njihovim implementacijama koji se odnose na kompleksnosti izračunavanja i dobijeni kvalitet.

U modernim standardima video kodovanja sreću se dve vrste inter predikcije, uni-predikcija i bi-predikcija. U slučaju bi-predikcije, dva skupa podataka o kretanju (Δx_0, Δy_0, Δt_0 *i* Δx_1, Δy_1, Δt_1) se koriste za kreiranje predikcije kompenzacije pokreta (po mogućnosti sa različitih slika), koji se zatim kombinuju da se dobije konačna predikcija kompenzacije pokreta. Podrazumevano, kombinovanje se realizuje usrednjavanjem vrednosti, dok se u slučaju ponderisane predikcije na svaku predikciju kompenzacije pokreta primenjuju različiti težinski parametri. Referentne slike koje se mogu koristiti u procesu bi-predikcije čuvaju se u dve odvojene liste, nazvane lista 0 i lista 1.

Podaci o kretanju jednog bloka su u korelaciji sa susednim blokovima. Da bi iskoristili ovu korelaciju, podaci i kretanju nisu direktno kodovani u video tok, već se vrši prediktivno kodovanje zasnovano na podacima o kretanju susednih blokova. Za prediktivno kodovanje, u HEVC standardu, koriste se dva pristupa. Jedan od njih je novi alat koji je uveden sa HEVC standardom koji je nazvan napredna predikcija vektora pokreta (engl. *AMVP - Advanced Motion Vector Prediction*) kod koga se za svaki blok dekoderu signalizira najbolji prediktor. Pored toga, nova tehnika nazvana inter prediktivno spajanje blokova izvodi sve podatke o kretanju datog bloka iz podataka o kretanju svih susednih blokova[10].

2.1.5. Transformacija i kvantizacija

HEVC standard specificira dvodimenzionalne transformacije različitih veličina od 4x4 do 32x32 koje predstavljaju konačne precizne aproksimacije diskretne kosinusne transformacije (engl. *DCT - Discrete Cosine Transform*). Pored toga, HEVC takođe specificira alternativnu transformaciju 4x4 zasnovanu na diskretnoj sinusnoj transformaciji (engl. *DST - Discrete Sine Transform*) za upotrebu sa 4x4 blokovima intenziteta osvetljenja kod intra predikcije. Kvantizacija u HEVC standardu je slična onoj definisanoj za H.264 standard, gde je parametar kvantizacije (QP) može da uzima vrednosti od 0-51 (za 8-bitne video sekvence) mapiran na veličinu koraka kvantizatora koji se duplira svaki put kada se prednost parametra kvantizacije poveća za 6.

Kao rezultat intra ili inter predikcije dobija se signal razlike predviđenog bloka u odnosu na originalni. Na tako dobijenu razliku primenjuje se transformacija i kvantizacija sa ciljem dalje eksploatacije prostornih statističkih zavisnosti. Na strani enkodera, signal razlike se deli na kvadratne blokove veličine $N \times N$ gde je $N = 2^M$ a M je celobrojna veličina. Na svaki blok razlike se onda primeni dvodimenzionalna $N \times N$ transformacija. Dobijeni koeficijenti transformacije tada podležu kvantizaciji (što je ekvivalentno deljenju veličinom stepena kvantizacije *Qstep* i naknadnim zaokruživanjem) kako bi se dobili kvantizovani koeficijenti transformacije. Na strani dekodera se radi obrnuti proces, najpre dekvantizacija a potom i inverzna transformacija

2.1.6. Filteri u petlji enkodera/dekodera

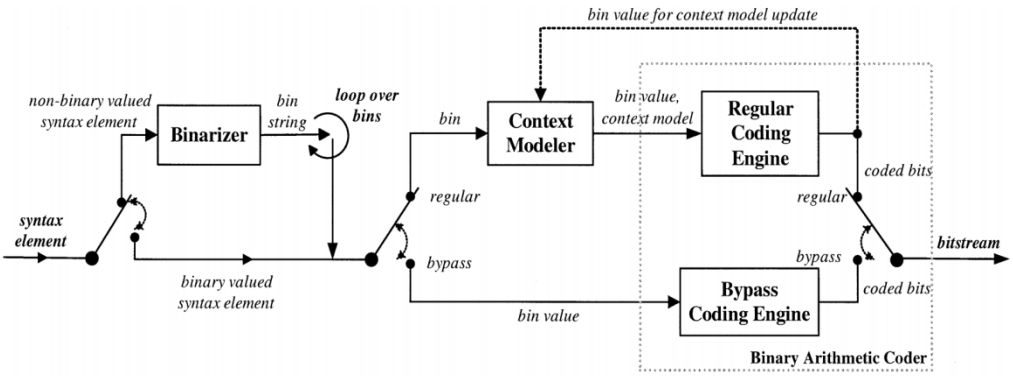
Filteri u petlji enkodera/dekodera predstavljaju važan deo HEVC standarda kompresije video podataka. Kao što se može videti iz njihovog imena, filteri u petlji se primenjuju u petlji enkodera i dekodera nakon procesa kvantizacije a pre skladištenja tekuće slike u neki od bafera. HEVC standard specificira upotrebu dva filtera, prvo se na izlazne podatke procesa kvantizacije/dekvatizacije primenjuje filter za uklanjanje blokovskih efekata (engl. *deblocking filter*), dok se nakon toga na tako dobijene podatke primenjuje adaptivni ofset uzoraka (engl. *SAO - Sample Adaptive Offset*)[5]. Filter za uklanjanje blokovskih efekata smanjuje diskontinuitete na granicama blokova transformacije i blokva predikcije[11]. SAO filter dalje poboljšava kvalitet dekodovane slike smanjenjem artefakta zvona i promenama intenziteta odbiraka u datom regionu rekonstruisane slike. Kako navedeni filteri umanjuju različite artefakte prednosti njihove

upotrebe su kumulativni ako se koriste istovremeno. HEVC enkoder može samostalno da uključi ili isključi bilo koji od navedenih filtera[9].

2.1.7. Kodovanje entropije

HEVC standard specificira samo jedan metod kodovanja entropije, kontekstno adaptivno binarno aritmetičko kodovanje (engl. *CABAC - Context Adaptive Binary Arithmetic Coding*)[12]. Kodovanje netropije je šema kompresije podataka bez gubitaka koja koristi statistička svojstva za obradu podataka tako da je broj bitova koji se koriste za prikaz podataka logaritamski proporcionalna njihovoj verovatnoći[13]. Na primer, kada se vrši kompresija niza karaktera, češće korišćeni karakteri se predstavljaju sa (manjim brojem) nekoliko bitova, dok se ređe korišćeni karakteri predstavljaju sa većim brojem bita. Iz Šenonove teorije informacija[14], ako se kompresovani podaci predstavljaju i bitskoj reprezentaciji {0,1}, optimalna prosečna dužina koda kojim će biti predstavljen karakter čija je verovatnoća pojavljivanja p jednaka je $log_2 p$.

Kodovanje entropije se izvodi u poslednjem koraku kodovanja video podataka (ili u prvom koraku dekodovanja), nakon što je video signal redukovan na nizove sintaksnih elemenata. Namena sintaksnih elemenata je da opišu kako se video podaci mogu rekonstruisati na strani dekodera. To uključuje i metod predikcije (intra ili inter predikcija), zajedno sa pridruženim parametrima predikcije i signalom razlike. Treba napomenuti da se, u HEVC standardu, samo sintaksni elementi koji pripadaju podacima iz odsečaka slike kodiraju primenom CABAC kodera entropije. Svi drugi sintaksni elementi sa viših nivoa se kodiraju ili primenom eksponencijalnih Golomb kodovima sa nultim redosledom ili fiksnim bitskim šablonima[13].



Slika 5. CABAC koder entropije (preuzeto iz [12])

U osnovi dizajna CABAC kodera entropije nalaze se tri koraka: binarizacija, modelovanje konteksta i binarno aritmetičko kodovanje. Model CABAC kodera entropije prikazan je na slici 5.

Generalno, binarizacija definiše jedinstveno mapiranje vrednosti sintaksnih elemenata u sekvence binarnih simbola, takozvanih bina, koji se takođe mogu predstaviti u formi binarnog kodnog stabla. Dizajn šeme binarizacije baziran je na nekoliko prototipova čija struktura omogućava brze implementacije i koji su reprezentativi nekog od pogodnih modela raspodele verovatnoće.

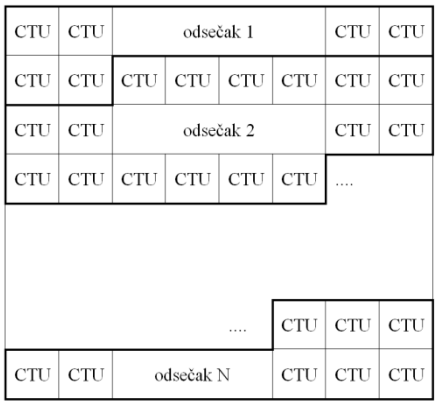
Nakon mapiranja svake vrednosti nebinarnog sintaksnog elementa u sekvencu binova, dalja obrada svake vrednosti bina zavisi od pridružene odluke da se bin regularno kodira aritmetičkim binarnim koderom ili da se jednostavno koder zaobilazi i bin prosleđuje takav kakav jeste. Prosleđivanje bina u formatu takav kakav jeste bira se za binove za koje se smatra da su uniformo raspoređeni. Za preostale binove primenjuje se regularno aritmetičko kodovanje, gde je pridruženi model verovatnoće ili određen fiksnim izborom baziranim na tipu sintaksnog elementa i na položaju bina u binarizovanoj reprezntaciji datog sintaksnog elementa ili adaptivno izabran od dve ili više verovatnoće u zavisnosti od srodnih sporednih informacija. Navedeni izbor modela verovatnoće naziva se modelovanje konteksta. Na taj način, CABAC omogućava selektivno modelovanje adaptivnih verovatnoća na nivou podsimbola, te stoga pruža efikasan instrument za iskorišćavanje redudanse među simbolima i značajno smanjuje ukupne troškove učenja i modelovanja konteksta.

Konačno, binarno aritmetičko kodovanje kompresuje bine u bite prema procenjenoj verovatnoći. Binarno aritmetičko kodovanje je bazirano na rekurzivnoj podeli na intervale. Opseg sa početnom vrednošću od 0 do 1, podeljen je na dva podintervala na osnovu verovatnoće datog bina. Kodovani biti obezbeđuju pomeraj koji, kada se konvertuje u binarnu frakciju, bira jedan od dva podintervala, što ukazuje na vrednost dekodiranog bina. Nakon svakog dekodiranog bina, pomeraj se ažurira tako da odgovara izabranom podintervalu a postupak podele se ponavlja.

2.1.8. Podela slike za pakovanje u pakete i paralelnu obradu

Na najvišem nivou, u HEVC standardu, slike se dele na odsečke (engl. *slices*). Primenom odsečaka obezbeđuje se podela slika na takav način da se svaki odsečak

može dekodovati nezavisno od svih preostalih odsečaka iste slike. Jedino filteri u petlji dekodera mogu zahtevati informacije vezane za više odsečaka iste slike. Jedna slika može biti podeljena na jedan ili više odsečaka, kao što je prikazano na slici 6. Generalno gledano, jedan odsečak može da sadrži samo jednu osnovnu jedinicu kodovanja (CTU) ali je najčešće njihov broj u okviru jednog odsečka veći i zavisi od dinamičnosti video scene. Osnovne jedinice kodovanja se u okviru odsečka procesiraju u rasterskom redosledu skeniranja, te se na taj način postiže da se svaki odsečak slike može nezavisno parsirati i dekodovati.



Slika 6. Podela slike na odsečke (engl. *slices*)

Podela slike na odsečke donosi sledeće pogodnosti:

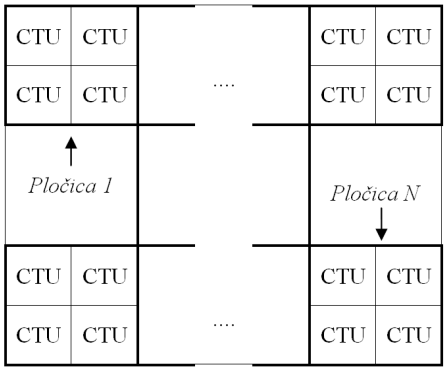
1. **Paralelno procesiranje (kodovanje)**. Ovakva pogodnost je posledica činjenice da se sve operacije kodovanja i dekodovanja, uključujući i rekonstrukciju pre filtera u petlji dekodera, mogu izvršavati na nivou odsečaka samostalno i međusobno nezavisno.
2. **Otpornost na greške**. Particionisanjem slike na manje samostalne entitete postiže se otpornost na greške kao posledica mogućnosti da se resinhronizuje proces parsiranja i dekodovanja video podataka u slučaju gubitka podataka.
3. **Podešavanje veličine maksimalne jedince prenosa (MTU)**. Promenljiva i podesiva veličina odsečaka doprinosi mogućnosti prilagođavanja ograničenju komunikacionih mreža zasnovanih na IP protokolu, zasnovanom na maksimalnoj veličini paketa koji se prenosi. Ovakav način pakovanja u pakete tačno određene veličine ograničava maksimalan broj bita korisnih video podataka u okviru odsečka, bez obzira na veličinu slike koja se koduje.

Postoje tri tipa odsečaka i to:

- ***I* odsečak** - kod koga su sve osnovne jedinice kodovanja kodovane koristeći samo intra predikciju;
- **P odsečak** - kod koga neke kodne jedinice mogu da koriste inter predikciju ali u jednom smeru i to pomoću jedne referentne slike;
- **B odsečak** - kod koga neke kodne jedinice mogu da koriste inter predikciju i to pomoću dve referentne slike.

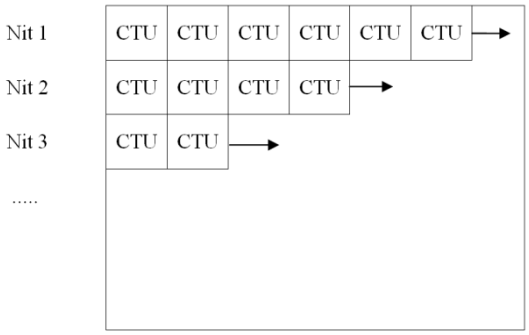
Da bi prevazišao ograničenja primenjenih strategija paralelizacije u prethodnim standardima, HEVC obezbeđuje alate za kodovanje na nivou video podataka koji su specijalno dizajnirani da omoguće procesiranje na paralelnim arhitekturama. Dva nova alata za olakšavanje paralelne obrade uključena su u HEVC standard [5][9]:

- **Pločice** (engl. *Tiles*). Mehanizam podele slike sličan odsečcima, koji se bazira na fleksibilnoj podeli slika na pravougaone regione osnovnih jedinica kodiranja tako da su međusobne zavisnosti jedinica kodiranja iz različitih regiona slike nedopustive. Dakle, svaka pločica se sastoji od pravougaone uređene grupe osnovnih jedinica kodiranja (CTU) pri čemu obično, ali ne i obavezno, svaka od njih ima jednak broj osnovnih jedinica kodiranja. Načelna podela na pločice prikazana je na slici 7.



Slika 7. Mehanizam podele slike na pločice

- **Wavefront Parallel Processing (WPP)**. Vid paralelnog procesiranja analogan wavefront principu raspoređivanja, koji se zasniva na podeli slike na redove osnovnih jedinica kodiranja tako da su zavisnosti između jedinica kodiranja iz različitih particija, u smislu predikcije i kodovanja entropije, u najvećoj meri očuvane, slika 8. Svaki red osnovnih jedinica procesiranja obrađuje posebna programska nit.



Slika H_8. Wavefront parallel processing

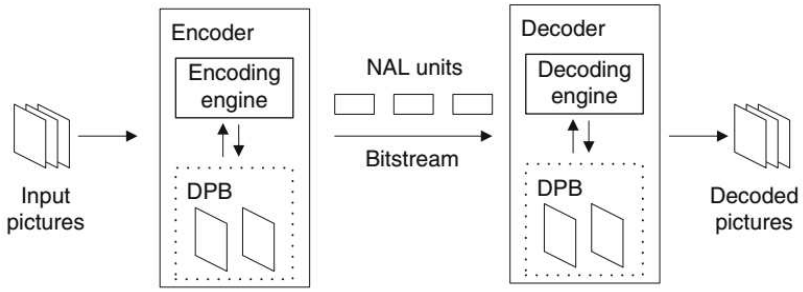
Oba navedena alata omogućavaju podelu svake slike na više delova koji se mogu paralelno obrađivati. Svaki deo sadrži celi broj osnovnih jedinica kodiranja koji mogu ili ne moraju imati zavisnost od jedinica kodiranja iz ostalih delova. Za sada, u HEVC standardu, samo jedan od navedenih alata može biti korišćen u jednom trenutku.

2.2. HEVC sloj apstrakcije mreže

Deo HEVC standarda koji uključuje strukturu video toka podataka kao i signalizaciju informacija na visokom nivou koje se odnose na jedan ili više odsečaka slike ili više slika u okviru video toka, naziva se sintaksa visokog nivoa[15]. Na primer, elementi sintakse visokog nivoa ukazuju na prostornu rezoluciju video zapisa, identifikuju alate koji su korišćeni za kodiranje, opisuje funkcionalnost slučajnog pristupa video toku. Takođe, sintaksa visokog nivoa uključuje parametre koji su bitni pri procesu dekodovanja video toka kao što su upravljanje referentnim slikama i redosled prikaza dekodovanih slika.

Na slici 9 prikazan je konceptualni model rada HEVC enkodera i dekodera. Ulazne slike se učitavaju u enkoder koji kodira slike u video tok podataka. HEVC video tok se sastoji od više pristupnih jedinica (engl. *access units*) od kojih svaka sadrži kodirane podatke i metapodatke povezane sa jednom slikom koja ima različita vremena snimanja i prikazivanja. Svaka jedinica pristupa je podeljena na NAL jedinice uključujući jednu ili više NAL jedinica koje pripadaju sloju kodovanja videa (VCL NAL jedinice) i nijednu, jednu ili više NAL jedinica koje ne pripadaju sloju kodovanja videa (ne-VCL NAL jedinice). VCL NAL jedinice se sastoje od kodovanih odsečaka (engl. *slices*) koji predstavljaju grupisane blokove odbiraka video slike. Ne-VCL NAL jedinice sadrže prateće podatke kao što su, na primer, NAL jedinice koje sadrže skupove parametara ili

NAL jedinice koje sadrže dodatne informacije za unapredjenja video sadržaja (engl. *SEI - Supplemental Enhancement Information*). Skupovi parametara sadrže podatke koji su bitni za proces dekodiranja dok SEI NAL jedinice sadrže opcionu podršku sa dodatnim skupovima podataka. Skup parametara može biti jedan od sledećih: skup parametara o sekvenci (engl. *SPS - Sequence Parameter Set*), skup parametara o slici (engl. *PPS - Picture Parameter Set*) ili skup parametara o videu (engl. *VPS - Video Parameter Set*).



Slika 9. Koncptualni model rada HEVC enkodera i dekodera (preuzeto iz [9])

NAL jedinice se, na strani dekodera, dekodiraju i kao izlaz se dobija sekvenca dekodiranih slika u redosledu prikazivanja. I na strani enkodera i na strani dekodera slike se čuvaju u baferu za dekodirane slike (engl. *DPB - Decoding Picture Buffer*). Navedeni bufer se uglavnom koristi za privremeno čuvanje slika tako da se prethodno kodovane slike mogu koristiti za generisanje parametara predikcije potrebnih za kodiranje drugih slika. Ovako memorisane slike nazivaju se referentne slike.

2.2.1. Struktura NAL jedinice

Svaka NAL jedinica se sastoji od zaglavlja NAL jedinice i korisnih podatka NAL jedinice. Zaglavlje NAL jedinice, veličine dva bajta, sadrži informacije o tipu korisnih podataka, o identifikatoru sloja kao i vremenski identifikator koji ukazuje na nivo u vremenskoj strukturi hijerarhijske predikcije.

Prvi bit zaglavlja NAL jedinice se uvek postavlja na '0', da bi se izbeglo generisanje sekvence bita koja može biti interpretirana kao MPEG-2 startna sekvenca u starim MPEG-2 sistemskim okruženjima[15]. Sledećih šest bita sadrže informaciju o tipu NAL jedinice, identifikujući i tip podataka koji se nalazi unutar NAL jedinice. Sa šest bita moguće je predstaviti 64 različitih tipova NAL jedinica. Sledećih šest bitova sadrži identifikator nivoa koji ukazuje kom nivou NAL jedinica pripada i namenjen je za

upotrebu u budućim slojevitim i skalabilnim ekstenzijama standarda. Poslednja tri bita predstavljaju vremenski identifikator. Vremenske identifikatore koriste mrežni media konvertori za inteligentne operacije nad video tokovima, kao na primer, redigovanje video toka podataka koristeći vremensku skalabilnost.

2.2.2. Tipovi VCL NAL jedinica

U tabeli 1, vrednostima od 0 do 31 identifikovani se tipovi NAL jedinice koje su rezervisane za VCL NAL jedinice. Sve VCL NAL jedinice koje pripadaju istoj pristupnoj jedinici moraju da imaju istu vrednost identifikatora tipa NAL jedinice a samim tim i tipa slike koja je kodirana u okviru nje. Na primer, kada sve VCL NAL jedinice u okviru pristupne jedinice imaju identifikator tipa NAL jedinice jednak 21, ta pristupna jedinica se zove pristupna jedinica čistog slučajnog pristupa (engl. *CRA - Clean Random Access*) a slika koja je kodirana naziva se slika čistog slučajnog pristupa. U HEVC standardu postoje tri osnovne klase slika: intra kodovane tačke slučajnog pristupa (enlg. *IRAP - Inra Random Access Point*), vodeće slike i prateće slike.

Tabela 1. Celobrojni identifikator tipa NAL jedinice, značenje i klasa NAL jedinice

ID tipa NAL jedinice	Značenje	Klasa NAL jedinice
0, 1	Segment odsečka obične prateće slike	VCL
2, 3	Segment odsečka TSA slike	VCL
4, 5	Segment odsečka STSA slike	VCL
6, 7	Segment odsečka RADL slike	VCL
8, 9	Segment odsečka RASL slike	VCL
10-15	Rezervisani za buduća proširenja	VCL
16-18	Segment odsečka BLA slike	VCL
19, 20	Segment odsečka IDR slike	VCL
21	Segment odsečka CRA slike	VCL
22-31	Rezervisani za buduća proširenja	VCL
32	Skup parametara o videu (VPS)	ne-VCL
33	Skup parametara o sekvenci (SPS)	ne-VCL
34	Skup parametara o slici (PPS)	ne-VCL
35	Delimiter jedinice prisutpa	ne-VCL
36	Kraj sekvence	ne-VCL
37	Kraj toka bita	ne-VCL
38	Podaci za popunjavanje	ne-VCL
39, 40	SEI poruke	ne-VCL
41-47	Rezervisani za buduća proširenja	ne-VCL
48-63	Nespecifikovani (dostupni za upotrebu)	ne-VCL

IRAP slike identifikovane su vrednostima tipa NAL jedinice u opsegu od 16-23. U okviru ovog opsega nalaze se IDR (engl. *IDR – Instantaneous Decoding Refresh*), CRA (engl. *CRA – Clean Random Access*) i BLA (engl. *BLA – Broken Link Access*) slike. IDR slika je slika koja u potpunosti resetuje proces dekodovanja i otpočinje novi sekvencu kodovanog videa (engl. *CVS – Coded Video Sequence*). To znači da ni IDR slika niti ijedna slika koja prati datu IDR sliku u redosledu dekodiranja nemaju zavisnost od bilo koje slike koja prethodi datu IDR sliku u redolsedu dekodiranja. CRA slika predstavlja intra kodovanu sliku koja, za razliku od IDR slike, ne resetuje proces dekodiranja i ne počinje novu sekvencu kodovanog videa. To daje mogućnost vodećim slikama date CRA slike da u smislu predikcije zavise od slika koje u redosledu dekodiranja prethode CRA slici. Dozvoljavajući ovakvu zavisnost povećava efikasnost kompresije do 6%, u odnosu na sekvence koje sadrže IDR slike[16]. Slučajni pristup u CRA slici se odvija tako što se najpre dekodira CRA slika, zatim se dekodiraju njene vodeće slike koje nemaju zavisnost od nijedne slike koja prethodi CRA slici u redosledu dekodiranja i na kraju se dekodiraju slike koje slede datu CRA sliku i po redosledu dekodiranja i po redosledu prikazivanja. Najčešće CRA slika nema pridruženih vodećih slika[9]. Pored toga što se CRA slika može koristiti za slučajan pristup video toku podataka, CRA slika se takođe može koristiti za spajanje video tokova. Spajanje video tokova je operacija kod koje se određena IRAP jedinica pristupa i sve naredne jedinice pristupa originalnog video toka zamene sa IRAP jedinicom pristupa i svim narednim jedinicama pristupa iz novog video toka. Kako CRA slika ne počinje novu kodovanu video sekvencu nakon operacije spajanja video tokova u CRA slici potrebno je izvršiti modifikaciju svih vrednosti brojača redosleda slika. Alternativna opcija spajanja video tokova u HEVC standardu je „prekinuti link“ koji nagoveštava da je brojač redosleda slika prekinut i mora biti resetovan nakon što se operacija spajanja video tokova realizuje. U HEVC standardu BLA slika se koristi za operacije spajanja video tokova u CRA slikama. U toku spajanja video tokova, CRA slika se jednostavno preimenuje i BLA sliku. Kao i u slučaju IDR slike, BLA slika resetuje dekoder i otpočinje novu sekvencu kodovanog videa.

Sve IRAP slike moraju biti kodovane bez upotrebe bilo koje druge slike kao referentne (tj. moraju biti kodovane upotrebom samo tehnika intra predikcije). Pozicija IRAP slike u video toku predstavlja tačku čisto slučajnog pristupa, tj. tačku od koje je

moguće otpočeti proces dekodovanja video podataka nezavisno od bilo koje prethodne slike iz video toka podataka. Prema tome, IRAP slika sama po sebi ne sme biti zavisna od bilo koje druge slike.

Prva slika u video toku podataka mora biti IRAP slika, dok u preostalom delu video toka može postojati neograničen broj IRAP slika. IRAP slika pruža mogućnost priključivanja (mogućnost uključenja) u video tok, na primer trenutak uključivanja TV-a ili trenutak prelaska sa jednog TV kanala na drugi. Takođe, IRAP slika se može koristiti da se omogući privremeno traženje pozicije u video sadržaju – na primer da se pomeri tekuća pozicija prikaza video sadržaja u okviru programa za reprodukciju video sadržaja. Najzad, IRAP slika se može koristiti za neprimetno prebacivanje sa jednog video toka na drugi video tok u domenu kompresije. Ova operacija je poznata pod imenom zamena ili spajanje video tokova i ona se može odvijati između dva video toka u realnom vremenu, između video toka u realnom vremenu i video toka iz fajla uskladištenog u trajnoj memoriji i između video podataka iz dva video fajla uskladištena u trajnoj memoriji. Uvek je moguće otpočeti proces dekodovanja video toka počevši od IRAP slike i progresivno dekodovati i prikazati na izlazu sve slike koje slede po redosledu prikazivanja čak iako su sve slike koje prethode datoj IRAP u redosledu dekodiranja odstranjene iz video toka[9]. Redosled dekodiranja je redosled po kome se slike dekoduju i on je identičan redosledu o kome su slike poređane u video toku. Redosled prikazivanja je redosled u kome će slike biti prikazane i on je najčešće različit od redosleda dekodiranja. Redosled prikazivanja za svaku sliku se eksplicitno signalizira u video toku koristeći vrednost brojača redosleda slike (engl. *POC – Picture Order Count*).

Kada se vrši kompresija (kodiranje) video podataka za skladištenje u trajnu memoriju ili za emitovanje putem nekog vida prenosa (bežične mreže, kablovska televizija, satelitske komunikacije), IRAP slike su tipično ravnomerno distribuirane kako bi obezbedile ravnomernu učestalost tačaka slučajnog pristupa u okviru video toka. Ovakav mod rada HEVC enkodera se naziva *random acces* mod. Sa druge strane, u aplikacijama u kojima slučajan pristup nije toliko važan ili kod kojih često slanje IRAP slike predstavlja opterećenje (aplikacije koje rade u realnom vremenu), u smislu većeg broja bita koje je potrebno poslati, frekfencija slanja IRAP slike može biti veoma mala ili se IRAP slika može poslati samo onda kada se dobije povratni signal da je video tok

podataka oštećen i da video scena mora biti osvežena[9]. Ovakav mod rada HEVC enkodera se naziva *real-time* mod rada.

Vodeća slika je slika koja sledi određenu IRAP sliku u redosledu dekodovanja a prethodi joj u redosledu prikazivanja. Prateća slika je slika koja sledi određenu IRAP sliku i u redosledu dekodovanja i u redosledu prikazivanja. Prateća slika kao referentnu sliku može imati samo svoju IRAP sliku ili neku drugu prateću sliku svojoj IRAP slici. Takođe, sve vodeće slike date IRAP slike moraju da u redosledu dekodiranja prethode sve prateće slike date IRAP slike. To znači da je redosled dekodiranja pridruženih slika sledeći: prvo se dekodira IRAP slika, zatim se dekodiraju pridružene vodeće slike i na kraju pridružene prateće slike.

Različiti tipovi pratećih slika su identifikovani vrednostima tipa NAL jedinice od 0 do 5, do su tipovi vodećih slika identifikovane vrednostima 6 do 9. Pojedini specifični tipovi vodećih ili pratećih slika nemaju nikakav značaj za navedenu temu te stoga njihova uloga i namena neće biti posebno objašnjavana u ovom radu.

Pored VCL NAL identifikatora koji su dodeljeni određenim tipovima NAL jedinica, u prethodnoj tabeli mogu se videti i nekoliko rezervisanih VCL NAL identifikatora koji su podeljeni u dve kategorije, IRAP i ne IRAP. Ove rezervisane vrednosti nije dozvoljeno koristiti u video tokovima koji su kompatibilni sa verzijom 1 specifikacije HEVC standarda, i namenjene su za buduća proširenja. Dekoder koji je kompatibilan sa verzijom 1 specifikacije HEVC standarda, mora jednostavno da odbaci ovakve NAL jedinice ako u svom radu naiđe na neku od njih. Neki od tipova NAL jedinica su označene kao „nespecifikovan“, što znači da one mogu biti korišćene za potrebe signaliziranja indikacija ili prenošenje informacija koje ne utiču direktno na proces dekodovanja video podataka. Razlika između rezervisane i nespecifikovane vrednosti tipa NAL jedinice je u tome što rezervisana vrednost može biti upotrebljena u budućim proširenjima HEVC standarda dok se za nespecifikovane vrednosti garantuje da u budućnosti nikada neće biti specificirane za potrebe kodiranja video podataka tako da mogu da se koriste za druge svrhe koja nije definisana standardom[17].

2.2.3. Tipovi ne VCL NAL jedinica

U tabeli 1 vrednosti identifikatora tipa NAL jedinice od 32 do 63 rezervisane su za ne-VCL NAL jedinice. NAL jedinica koja u zaglavlju ima identifikator tipa jednak 32

naziva se skup parametara o video toku (engl. *VPS - Video Parameter Set*). VPS sadrži informacije koje se odnose na sve slojeve u okviru kodirane video sekvence i namenjene su za korišćenje u predstojećim proširenjima HEVC standarda sa ciljem da omoguće skalabilno i višestruko kodiranje. Vrednost 33 identifikuje skup parametara o sekvenci (engl. *SPS - Sequence Paramter Set*). SPS sadrži podatke koji su primenljivi na sve slike u istoj kodovanoj sekvenci video podataka. Neki od parametara, u okviru SPS, daju ključne opise kodirane sekvence što predstavlja korisnu informaciju za različite sistemske interfejse. Drugi parametri opisuju način upotrebe alata za kodiranje ili pak sadrže parametre alata kodiranja što utiče na povećanje bitske brzine. Vrednost 34 identifikuje skup parametara o slici (engl. *PPS - Picture Parameter Set*). PPS obuhvata parametre koji mogu biti promenljivi od slike do slike u okviru kodovane video sekvence. Pored identifikatora skupa parametara o slici, PPS sadrži parametre o alatu koji je korišćen za kodiranje date slike, uključujući podatke o povezanim odsečcima, ograničenja intra predikcije, parametre ponderisane predikcije, modifikacije liste referentnih slika. Ovaj skup parametara takođe sadrži i referentni indeks slike, inicijalnu vrednost parametra kvantizacije i dozvoljeni ofset parametra kvantizacije.

Svaki odsečak ima referencu na po jedan aktivan skup parametara (PPS, SPS i VPS) kako bi pristupio informacijama potrebnim za njegovo dekodiranje. Iako se PPS može razlikovati za sve različite slike, uobičajeno je za mnoge ili skoro za sve slike u kodovanoj video sekvenci da imaju referencu na isti PPS. Ponovna upotreba skupa parametara je po pitanju bitske brzine efikasna jer se na taj način izbegava višestruko slanje istih informacija[18].

Da bi se za neki odsečak identifikovano aktivan skup parametara na svakom nivou hijerarhije skupa parametara, svako zaglavlje odsečka sadrži identifikator skupa PPS koji referencira tačno određeni PPS. Unutar PPS nalazi se identifikator koji referencira tačno određeni SPS, dok se unutar SPS parametara nalazi identifikator koji referencira određeni VPS.

Ne VCL NAL jedinice sa identifikatorima tipa u zatvorenom opsegu od 35 do 37 spadaju u grupu delimitera. Delimiter jedinice pristupa (identifikator tipa 35), se može opciono koristiti za označavanje granice između pristupnih jedinica. U svom korisnom sadržaju ima samo jednu kodnu reč i ona predstavalja tip odsečaka koji se mogu naći u datoj jedinici pristupa. Vrednosti 36 i 37 respektivno identifikuju delimiter kraja

sekvence i delimiter kraja video toka podataka. Identifikator tipa sa vrednošću 38 koristi se da identifikuje podatke za popunjavanje. Ovi podaci nemaju uticaja na proces dekodiranja a koriste se za popunjavanje kanala prenosa do željene brzine prenosa u slučaju da nema dovoljno VLC podataka. NAL jedince iz opsega vrednosti tipa NAL jedinice od 41 do 47 su rezervisane za buduću upotrebu dok se vrednosti tipa NAL jedinice u opsegu od 48 do 63 nespecifikovane.

2.3. Profili, nivoi i slojevi

Profili, nivoi i slojevi predstavljaju tačke usklađivanja implementacija HEVC standarda i postizanja interoperabilnosti između raznovrsnih aplikacija koje imaju slične funkcionalne zahteve[1]. Međutim, raznovrsnost odvojenih potencijalnih "ostrva" interoperabilnosti u verziji 1 HEVC standarda je prilično skromna i direktno zavisi od planirane primene.

Profil definiše skup kodnih alata i algoritama koji, ako se koriste, obezbeđuju kompatibilnost izlaznog toka video podataka. Nivo se odnosi na ograničenja nad video tokom podataka koja određuju resursne i memorijske zahteve dekodera. U navedena ograničenja spadaju: maksimalan broj odbiraka, maksimalan broj odbiraka po sekundi koji se može dekodovati, maksimalna veličina slike, maksimalna bitska brzina, minimalni stepen kompresije, i kapaciteti bafera kodovanih i dekodovanih slika za potrebe upravljanja protokom podataka. U HEVC standardu najniži nivo ima samo najnižu rezoluciju i najnižu vrednost broja frejmova u sekundi. Tipično, nivo 1 ima rezoluciju 176x144 i svega 15 frejma u sekundi. Nivo 4.1, na primer, ima mogućnost obrade video toka rezolucije 1920x1080 (HDTV) sa 60 frejma po sekundi. U verziji 1 HEVC standarda, nivoi su definisani do nivoa 6.1 koji ima mogućnost obrade video toka rezolucije 8192x4320 sa 120 frejmova u sekundi.

Kod definisanja nivoa u HEVC standardu, pojavio se problem između zahteva za običnu i profesionalnu upotrebu video podataka koji imaju sličnu rezoluciju slike i broj frejmova u sekundi. U profesionalnim okruženjima, mnogo veće bitske brzine su potrebne za odgovarajući kvalitet od onog koji je potreban za običnu upotrebu[9]. Ovaj problem je rešen uvođenjem slojeva. Na osnovu bitske brzine rukovanja video tokom podataka, u HEVC standardu definisani su dva sloja: osnovni (Main) i viši (High) nivo.

U prvoj verziji standarda definisana su samo tri profila:

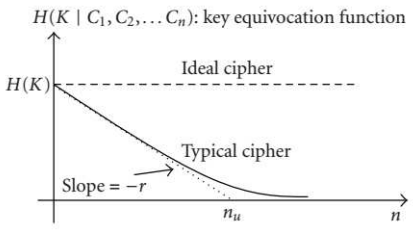
- **Glavni profil** - za upotrebu u tipičnim aplikacijama koje su većini korisnika trenutno poznate. Ovaj profil predstavlja video podatke sa 8 bita po odbirku i tipičnom 4:2:0 struktura odabiranja, u kome na svaki odbirak intenziteta boje dolazi jedna četvrtina odbiraka osvetljenja.
- **Glavni profil za slike** - za dobijanje fotografija sa kamere ili za ekstrakciju slika iz video sekvence. Ovaj profil je podskup glavnog profila.
- **Glavni 10 bitni profil** - podržava preciznost do 10 bita po dekodiranom odbirku slike. Ovaj profil obezbeđuje povećanu bitsku dubinu za povećanje dinamičkog opsega osvetljenja, produženi sadržaj boje ili za jednostavno bolje i preciznije prikazivanje nijansi boje. Ovaj profil je nadskup glavnog profila.

3. TEORIJSKE OSNOVE SELEKTIVNOG ŠIFROVANJA VIDEO PODATAKA

3.1. Veza između kompresije i šifrovanja video podataka

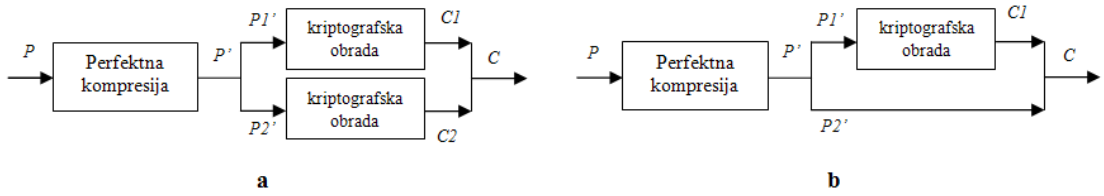
Čvrstu vezu između kompresije i šifrovanja prvi je istakao Klod Šenon u svom radu iz 1949. godine [19] o teoriji prenosa informacija u sistemima za očuvanje tajnosti. Poznato je da se statistički podaci vezani za slike i video sadržaje u mnogo čemu razlikuju od klasičnih tekstualnih podataka. I zaista, slike i video sadržaji su uzajamno čvrsto povezani i u svom digitalnom zapisu imaju mnogobrojna vremenska i prostorna ponavljanja. Osim toga, za razliku od podataka koji se razmenjuju u bankarskom sektoru ili drugih vidova veoma osetljivih informacija, slike i video sadržaji imaju veliku brzinu prenosa informacija koji su sa bezbednosne tačke gledišta na nešto nižem nivou. Šenon u svom radu ističe usku vezu između statističkih karakteristika izvora podataka i bezbednosti kriptološki zaštićenog sadržaja. Pouzdane kriptološke tehnike bi trebale da odstrane sva ponavljanja iz originalnih informacija tako da se u kriptološki zaštićenim informacijama ne mogu uočiti nikakve korisne korelacije. On definiše funkciju ekvivokacije koja pokazuje meru nesigurnosti kriptoanalitičara u sadržaj otvorenog teksta ako posmatra skup šifrata. Na slici 10 predstavljen je parametar n_u kao minimalni broj blokova šifrata koji su potrebni da daju jedinstveno rešenje u postupku kriptoanalize kada je poznat samo otvoreni tekst i dat je relacijom (1) gde je *H(k)* entropija ključa a *r* predstavlja redudansu otvorenog teksta.

$$n_u = \frac{H(k)}{r} \tag{1}$$



Slika 10. Shanonova funkcija (preuzeto iz [19])

Na osnovu ovoga se može izvući zaključak da bi kriptološki zaštićeni sadržaj bio sigurniji neophodno je da izvor sadržaja ima što je moguće manje redudanse. Šenon u svom radu pridaje veliki značaj tradicionalnim sistemima u kojima se najpre primeni algoritam „savršene“ kompresije koji ima zadatak da ukloni sva ponavljanja iz originalnog sadržaja. Zatim se tako dobijeni podaci u celosti kriptološki obrade. Šenon dalje govori da bi algoritam kompresije trebao da bude savršen, tj. da ako je ***P*** originalna poruka, onda je ***P'*** „savršeno“ kompresovana poruka. Tako dobijenu poruku ***P'*** možemo podeliti na dva dela, ***P1'*** i ***P2'*** (slika 11a) gde su ***C1*** i ***C2*** kriptološki obrađeni sadržaji poruka ***P1'*** i ***P2'*** respektivno. Savršena kompresija podrazumeva da ako nam je poznat sadržaj poruke ***P1'*** onda se sadržaj poruke ***P2'*** ne može predvideti. Ovakva konstatacija se može potvrditi dokazivanjem putem kontradiktornosti. Ako je prethodni izraz netačan, onda je potrebno postojanje jednog dodatnog bloka koji je rezultat dodatne kompresije poruke ***P2'*** koja je zasnovana na poruci ***P1'***. Ovakav scenario je nemoguć jer smo kao polaznu pretpostavku imali da je primenjen algoritam „perfektne“ kompresije[20]. Ovakav rezultat je veoma interesantan. Pretpostavimo sledeći scenario: neka je samo određenom podskupu toka kompresovanih podataka potrebna kriptološka obrada (na primer blok ***P1'***), onda možemo da ovaj, algoritmom kompresije obrađeni blok podataka, zamenimo blokom podataka koji je selektivno šifrovan. Na taj način samo određeni podskup podataka se kriptološki obrađuje (slika 11b), dok je sigurnost cele poruke obezbeđena prethodno diskutovanim i dokazanim postupcima, uz pretpostavku da su sva ponavljanja iz izvora poruka uklonjena. Poruka ***P1'*** je kriptografski zaštićena i njen sadržaj se ne može predvideti na osnovu ***P2'*** jer se koristi perfektan algoritam kompresije[21].



Slika 11. (a) tradicinalni sistem, (b) sistem selektivnog šifrovanja

Na osnovu ovoga se može zaključiti da je dobra kompresija neophodan preduslov efikasnog algoritma selektivnog šifrovanja. Jedino pitanje koje preostaje je kako izabrati i koji deo toka podataka selektivno šifrovati kako bi time bio postignut željeni nivo

vizuelne degradacije. U Šenonovoj teoriji, snaga „perfektno“ kompresovanog otvorenog sadržaja je u ravnomernoj distribuciji, pa prema tome kriptografska obrada delova kompresovane originalne poruke bi trebalo da proizvede isto izobličenje u kriptografski obrađenom toku podataka. Međutim, mnogi standardni algoritmi kompresije nisu „perfektni“ i koncentrišu informacije neravnomerno u okviru toka otvorene poruke. Na primer, kod JPEG algoritma kompresije biti kojima se kodiraju DC koeficijenti imaju veći uticaj na kvalitet rekonstrukcije od bita kojima se kodiraju AC koeficijenti (DC i AC koeficijenti su koeficijenti diskretne kosinusne transformacije koja je deo procesa kompresije JPEG slika). Jedna prednost ovakvih algoritama kompresije koji koncentrišu informacije neravnomerno ogleda se u tome što oni na taj način istovremeno i pomažu pri izboru dela toka podataka koji treba kriptološki obraditi. Mnogi algoritmi selektivnog šifrovanja se upravo zasnivaju na ovim karakteristikama algoritama kompresije.

3.2. Efekti selektivnog šifrovanja video podataka

Koji su efekti šifrovanja samo jednog dela kompresovanog video toka podataka? Postoje dva odgovora od kojih je jedan prilično očigledan dok je drugi manje uočljiv. Prema prilično očiglednom odgovoru na prethodno pitanje, selektivno šifrovanje smanjuje ukupnu složenost izračunavanja prilikom obrade multimedijalnih podataka koji treba kompresovati i šifrovati. Tačnije, šifrovanjem samo dela video podataka ušteda se postiže uštedom procesorskih ciklusa obrade koji bi bili potrebni za šifrovanje celog video toka. Svedoci smo sveprisutnosti različitih multimedijalnih formi podataka (slike, audio i video) koji treba kriptografski zaštiti bilo zbog očuvanja privatnosti bilo zbog zaštite prava vlasnika multimedijalnog sadržaja. Navedeni multimedijalni sadržaj se sve češće koristi na prenosivim uređajima sa ograničenjima u pogledu procesorske obrade i životnog veka baterije. Upotreba algoritama selektivnog šifrovanja za zaštitu tajnosti multimedijalnih podataka, doprinosi i očuvanju baterije i uštedi resursa procesora.

Prema manje uočljivom odgovoru, selektivno šifrovanje može omogućiti nove funkcionalnosti sistema. Jedna od aplikacija u okviru potrošačke elektronike je i efikasan mehanizam preklapanja više od jednog sistema kriptografski zaštićenog prenosa u okviru jednog kompresovanog video toka. Na primer, imamo jednog

operatera kablovske televizije koji koristi otvoreni standard kompresije video podataka i sopstveni mehanizam kriptografske zaštite. U nekom trenutku želimo da razmatramo alternativnog kablovskog operatera, ali bi bilo neisplativo zameniti celokupnu opremu kako bi omogućili drugačiji sistem zaštite video podataka. Sa druge strane ne želimo da potrošimo propusni opseg za dupliranje televizijskih kanala koji se šalju pomoću sigurnosnih sistema starog i novog operatera. Navedeni problem se u praksi rešava primenom selektivnog šifrovanja. Selektivno se šifruje samo malo deo, recimo nekoliko procenata, na svakom kanalu i to korišćenjem sigurnosnih sistema svakog od operatera. Preostali deo sadržaja svakog od kanala se šalje jednom i to otvoreno. Na ovaj način, sa svega nekoliko procenata povećanja na propusnom opsegu, omogućili smo novu funkcionalnost sistema (omogućili smo upotrebu opreme i starih i novih kablovskih operatera istovremeno u mreži). Konkretan sistem iz prakse je Sony-jev *Passage* sistem namenjen kablovskim operaterima u SAD[22]. Ovakva funkcionalnost bi mogla da bude korisna prilikom zamene starog sistema prenosa novim ili da podstakne konkurenciju između dva proizvođača opreme od kojih svaki pruža sopstveni mehanizam zaštite[23].

Mehanizam preklapanja više od jednog sistema kriptografski zaštićenog prenosa u okviru jednog kompresovanog toka video podataka pruža mogućnost kombinovanja različitih taktika primene navedene tehnologije u vojnim komunikacijama.

3.3. Elementi ocene performansi algoritama selektivnog šifrovanja

Za potrebe vrednovanja kvaliteta različitih algoritama selektivnog šifrovanja kao i za njihovo međusobno poređenje definisan je skup kriterijuma[20][24]:

- **Podesivost**. Mnogi od javno dostupnih algoritama selektivnog šifrovanja koriste statičko definisanje dela koji se kriptološki obrađuje kao i statičke definicije kriptoloških parametara (ključ, kriptografski algoritam). Ovakve karakteristike ograničavaju upotrebljivost takve vrste algoritama na ograničeni skup oblasti primena. Kod algoritama selektivnog šifrovanja video toka podataka poželjno je da korisnik ima mogućnost da dinamički definiše deo koji će se kriptografski obrađivati kao i kriptološke parametre koji će se pri tome koristiti i sve to u zavisnosti od oblasti primene i zahteva koje primena nameće.

- **Vizuelna degradacija**. Ovaj kriterijum predstavlja meru perceptualnog izobličenja šifrovanog video toka podataka (ili slike) u odnosu na originalni video tok (ili sliku). On podrazumeva da se kriptografski obrađeni video tok (ili slika) može dekodovati i pregledati bez potreba da se dešifruje. Ovu pretpostavku ne zadovoljavaju svi postojeći algoritmi selektivnog šifrovanja. U nekim oblastima primene, poželjno je da nivo vizuelne degradacije bude takav da potencijalni napadač još uvek razume sadržaj ali ipak donosi odluku da plati i na taj način dobije pristup originalnom sadržaju. Međutim, u sistemima za prenos veoma osetljivih video poruka, kao što su vojni komunikacioni sistemi, često se javlja zahtev da nivo vizuelne degradacije bude na zadovoljavajuće visokom nivou tako da se sadržaj poruke u potpunosti sakriva i nije dostupan neovlašćenim korisnicima. Shodno ovom zahtevu, veliki značaj ima svojstvo podesivosti jer se njime postižu različiti nivoi vizuelne degradacije kriptološki obrađenog sadržaja i u potpunosti zavisi od zahteva i oblasti primene algoritma selektivnog šifrovanja. Kao mera vizuelne degradacije u literaturi se najčešće koristi odnos signal šum. Na osnovu toga se može reći da je vizuelna degradacija subjektivni kriterijum pa je zbog toga veoma teško definisati nivo vizuelnog izobličenja prihvatljivog za određenu primenu.
- **Kriptografska bezbednost.** Mnogi istraživački radovi ocenu kvaliteta algoritma selektivnog šifrovanja baziraju samo na stepenu vizuelne degradacije. Kako je prethodno navedeno, vizuelna degradacija je subjektivni kriterijum tako da nije moguće samo njega koristiti pri oceni kriptološke snage određenog algoritma selektivnog šifrovanja. Pored toga, pokazano je da neki algoritmi selektivnog šifrovanja koji postižu značajnu vizuelnu degradaciju mogu imati ozbiljne bezbednosne propuste [25][26]. Kriptoanaliza algoritama selektivnog šifrovanja zasniva se na otkrivanju kriptografskog ključa (ukoliko prostor ključeva nije preveliki) ili na predviđanju dela video toka koji je kriptografski obrađen. Prema tome, kriptografska bezbednost algoritama selektivnog šifrovanja zasniva se na dva elementa: na izvoru ključa i na nepredvidivosti izabranog dela podataka koji se kriptološki obrađuje.

  Mali broj istraživačkih radova obrađuje problem nepredvidivosti kriptološki obrađenog dela. Bezbednost algoritma selektivnog šifrovanja zavisi od toga koliko delova i koje delove video podataka treba kriptološki obraditi sa ciljem da se osigura

da se napad isprobavanjem svih mogućih ključeva u polju ključeva (***brute-force attack***) učini lakšim od identičnog napada na otvorene video podatke. Inače, potencijalni napadač bi mogao da zaobiđe šifrovanje i sav svoj napor koncentriše na predviđanje otvorenih video podataka[24].

Teško je definisati i pronaći apsolutnu meru bezbednosti algoritama selektivnog šifrovanja video toka. Umesto toga u [27] su definisana indirektna merila koja mogu aproksimativno da definišu kriptografsku bezbednost algoritma selektivnog šifrovanja. Primeri takvih merila su: entropija, jedinstvena distanca, nagađanje i α-radni faktor. Entropiju kao merilo kriptografske bezbednosti definisao je Šenon u svojoj teoriji [19], kao meru neizvesnosti date poruke. Entropija definiše slučajnost date poruke. Iz definicije entropije izvodi se i definicija jedinstvene distance koja predstavlja minimalnu dužinu originalnog šifrata koji je potreban da bi se postigao uspeh u brute-force napadu i dobilo jedinstveno rešenje. Nagađanje kao merilo definiše očekivani broj pokušaja pogađanja u okviru brute-force napada na šifrovani tekst kako bi se pronašao otvoreni tekst, uz pretpostavku da potencijalni napadač ima potpuno znanje o rasporedu verovatnoće pojavljivanja simbola u šifratu. U [28] i [29] autori su pokazali da nije moguće naći jednostavne granice za postupak pogađanja, a samim tim i α-radni faktor, na osnovu entropije. Oni su pokazali da nagađanje može biti proizvoljno veliko ako entropija teži nuli.

Iz prethodnog navedenog može se zaključiti da univerzalno merilo kriptografske bezbednosti algoritma selektivnog šifrovanja ne postoji. Ovo je posledica činjenice da algoritam "perfektne" kompresije u multimedijalnim podacima još uvek ne postoji. Za svaki od navedenih algoritama koji su javno dostupni autori u svojim radovima teorijski i praktično pokazuju dali su (ili nisu) oni otporni na poznate napade u okviru kriptoanalize.

- **Kriptografski koeficijent**. Predstavlja odnos između veličine kriptografski obrađenog dela poruke i ukupne veličine originalne poruke. Cilj algoritma selektivnog šifrovanja je da se postigne što je moguće manji kriptografski koeficijent.

  Razmatrajmo idealan slučaj kada je upotrebljen algoritam "perfektne" kompresije i neka je M poruka koja se sastoji od n simbola. Proizvoljno se izabere n_e simbola koji će biti kriptografski obrađeni ($n_e \leq n$), i oni predstavljaju skup X koji označava

šifrovani deo poruke *M*. Preostali deo poruke ostaje u izvornom formatu, nešifrovan. Tada je kriptografski koeficijent definisan formulom:

$$KK = \frac{n_e}{n} \tag{2}$$

U [24] data je procena koliko je teško potencijalnom napadaču da pogodi *X*, kriptografski obrađeni deo poruke, u napadu upotrebom grube sile (napad isprobavanjem svih mogućih kombinacija) i pokuša da pronađe uslove pod kojim se isprobavanje svih mogućih ključeva u polju ključeva (***brute-force attack***) čini lakšim od identičnog napada na nešifrovane podatke. Ova procena je data pod pretpostavkom da potencijalni napadač zna dužinu i lokaciju kriptografski zaštićenog dela poruke *M* i ima mogućnost da prepozna kada je pogađanje otvorenog teksta ispravno.

Algoritam perfektne kompresije podrazumeva da su eliminisane sve redudanse u izvornoj poruci i da su svi simboli u kompresovanoj poruci *M* nezavisni i ravnomerno distribuirani. Prema tome, kriptografski obrađeni deo poruke *X* se može smatrati diskretnom slučajnom promenljivom koja svoje vrednosti uzima u jeziku L^{n_e}:

$$X \in \{X_1, X_2, X_3, \dots, X_{|L|^{n_e}}\} \tag{3}$$

gde je L prostor simbola, a |L| predstavlja njegovu kardinalnost. Potencijalni napadač bi mogao da pokuša da pogodi vrednost kriptografski zaštićenog dela *X* pokušavajući (isprobavajući) sve moguće vrednosti u redosledu koji je jednak opadajućem redosledu njihovih verovatnoća: $p_1 \geq p_2 \geq p_3 \geq \dots \geq p_{|L|^{n_e}}$, tada je postupak pogađanja dat relacijom:

$$W(X) = \sum_{i=1}^{|L|^{n_e}} i * p_i \tag{4}$$

Kako je početna pretpostavka da se koristi algoritam perfektne kompresije, tada su svi simboli jednako verovatni, pa su verovatnoće pojavljivanja simbola jednake:

$$p_i = \frac{1}{|L|^{n_e}} \tag{5}$$

Na osnovu formula 4 i 5, postupak pogađanja se može dalje predstaviti relacijom:

$$W(X) = \frac{1}{|L|^{n_e}} \sum_{i=1}^{|L|^{n_e}} i = \frac{|L|^{n_e}+1}{2} \tag{6}$$

Sa druge strane, neka je dužina ključa kriptografskog algoritma *k* bita onda se proces pogađanja ključa u prostoru ključeva može predstaviti relacijom:

$$W(K) = \sum_{i=1}^{2^k} \frac{i}{2^k} = \frac{2^k+1}{2} \tag{7}$$

Na osnovu formula 6 i 7, može se zaključiti da bi napad isprobavanja svih mogućih poruka bio teži od napada isprobavanja svih mogućih ključeva iz prostora ključa onda mora da bude zadovoljena relacija:

$$W(X) \geq W(K) \tag{8}$$

što se matematičkim operacijama može svesti na:

$$|L|^{n_e} \geq 2^k \tag{9}$$

Prethodna relacija daje mogućnost da se izračuna minimalan broj bajtova koji je potrebno kriptografski obraditi u okviru algoritma selektivnog šifrovanja da bi se postigla zadovoljavajuća kriprografska bezbednost uz minimalni kriptografski koeficijent:

$$n_{e(\min)} \geq \frac{k}{\log_2(|L|)} \tag{10}$$

U praksi je ova vrednost malo drugačija jer, kako smo prethodno rekli, još uvek u praktičnoj primeni ne postoji algoritam idealne kompresije video podataka.

- **Uticaj na kompresiju podataka**. Neki algoritmi selektivnog šifrovanja mogu da utiču na mogućnost kvalitetne kompresije podataka ili pak da uvode dodatne podatke koji su neophodni u procesu kriptološke obrade podataka na prijemnoj strani. Poželjno je da ovaj uticaj bude ograničen, odnosno da sam algoritam selektivnog šifrovanja ne dodaje nikakve podatke i narušava sam algoritam kompresije.
- **Otpornost na greške**. Ovaj kriterijum je posebno značajan u mrežama koje nisu otporne na greške. Standardni kritpografski algoritmi u svom radu postižu veoma izražen efekat lavine tako da ukoliko dođe do greške u samo jednom bitu podataka, ta greška će se propagirati na veći broj uzastopnih bita. Ovakva pojava prouzrokuje grešku u procesu dekodiranja ili značajna izobličenja podataka na prijemnoj strani. To kao posledicu ima potrebu da se naprave ustupci između kriptografske sigurnosti i otpornosti na greške. Cilj postojećih istraživačkih radova je da se dizajnira siguran algoritam selektivnog šifrovanja koji istovremeno održava dovoljno dobar efekat lavine ali ima zadovoljavajuću otpornost na greške. To se u praksi postiže tako što se

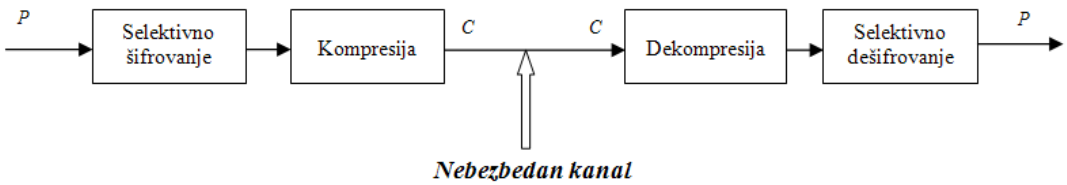
izbegavaju modovi rada kriptografskih algoritama koji rad zasnivaju na ulančavanju blokova[30]. Upotreba AES kriptografskog algoritma u CTR modu rada ili bilo kog drugog algoritma koji šifruje blokove podataka međusobno nezavisno, predstavlja i nudi dobar balans između kriptografske bezbednosti i otpornosti na greške.

3.4. Podela algoritama selektivnog šifrovanja

Jedna moguća podela algoritama selektivnog šifrovanja je izvršena na osnovu trenutka izvršavanja kriptografske obrade podataka u odnosu na kompresiju podataka. Ovakav način klasifikacije je veoma interesantan jer sam redosled primene kriptografske obrade toka podataka i algoritma kompresije ima veliki uticaj na ponašanje kompletnog algoritma selektivnog šifrovanja. Analizom definisanog kriterijuma podele utvrđena su tri tipa algoritama selektivnog šifrovanja.

3.4.1. Prekompresioni algoritmi

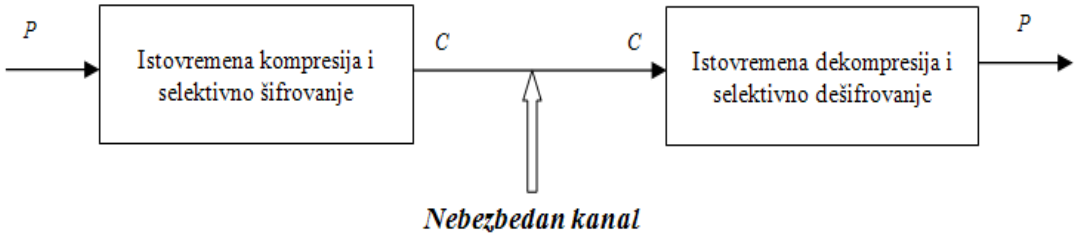
Algoritmi selektivnog šifrovanja iz ove grupe algoritama na predajnoj strani najpre primenjuju kriptološku obradu podatka pa onda primene algoritam kompresije, dok je na prijemnoj strani taj redosled obrnut (slika 12). Na osnovu samog opisa ponašanja može se zaključiti da algoritmi iz ove grupe sigurno zadovoljavaju kriterijum održivost formata ali isto tako nisu primenljivi u sistemima gde algoritam kompresije utiče na slabljenje kvaliteta podataka ili na gubitak određenog dela podataka (kao u sistemima za prenos video sadržaja gde algoritam kompresije oslabi kvalitet originalnog sadržaja). Ova klasa algoritama ima nepovoljan uticaj na samu kompresiju podatka jer sama primena kriptografske obrade podataka pre kompresije utiče na povećanje širine propusnog opsega i istovremeno utiče na slabljenje kvaliteta primenjenog algoritma kompresije.



Slika 12. Šematski prikaz prekompresionih algoritama selektivnog šifrovanja

3.4.2. Algoritmi istovremene kompresije i kriptografske obrade

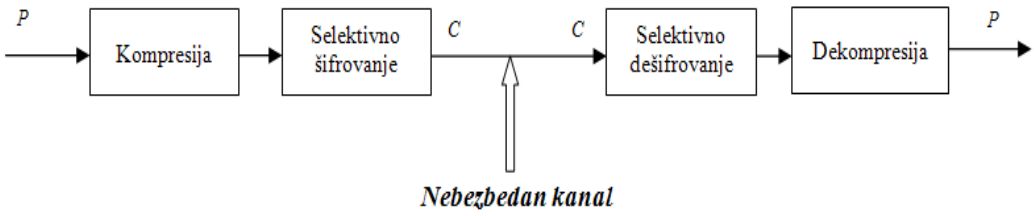
Kod ove klase algoritama selektivnog šifrovanja kriptografska obrada podataka je objedinjena, integrisana, zajedno sa algoritmom kompresije (slika 13). Algoritmi iz ove klase podrazumevaju određene modifikacije i na koderu i na dekoderu tako da se ne može reći da se njima postiže održivost formata i mali uticaj na kompresiju podataka. Međutim, danas su dostupni algoritmi iz ove grupe koji imaju održiv format i minimalni, skoro nikakav, uticaj na kompresiju podataka.



Slika 13. Šematski prikaz algoritama istovremene kompresije i kriptografske obrade

3.4.3. Postkompresioni algoritmi

Algoritmi selektivnog šifrovanja iz ove grupe algoritama najpre primene algoritam kompresije pa onda primenjuju kriptološku obradu podataka na predajnoj strani dok je na prijemnoj strani taj redosled obrnut (slika 14). Ova klasa algoritama ima mali uticaj na kompresiju podataka dok kriptološka obrada podataka na prijemnoj i na predajnoj strani ne zahteva nikakve modifikacije na koderu odnosno dekoderu. Generalno, na osnovu slike se može zaključiti da algoritmi iz ove klase ne zadržavaju format sadržaja koji se prenosi. Sa bezbednosne tačke gledišta, postkompresioni algoritmi selektivnog šifrovanja imaju najveći kriptografsku snagu zato što kompresija eliminiše korelaciju podataka čime se smanjuje predvidivost dela podataka koji je selektivno šifrovan.



Slika 14. Šematski prikaz postkompresionih algoritama selektivnog šifrovanja

3.5. Algoritmi selektivnog šifrovanja HEVC video toka podataka

U periodu od nastanka novog standarda kompresije video podatka pa do izrade ove disertacije, u okviru naučne zajednice se pojavio određeni broj stručnih i naučnih radova u kojima autori definišu nove algoritme selektivnog šifrovanja HEVC video toka. U narednom delu biće data kratak pregled dostupnih algoritama selektivnog šifrovanja HEVC video toka podataka sa osvrtom na njihove osnovne karakteristike.

3.5.1. Algoritam autora Zafar Shahid i William Puech

Algoritam navedenih autora predstavlja jedan od prvih javno publikovanih algoritama selektivnog šifrovanja HEVC video toka podataka. Vizuelna degradacija se postiže selektivnom šifrovanjem binstringova u okviru CABAC kodera entropije u HEVC enkoderu. U navedenom algoritmu, selektivno šifrovanje, sa usaglašenim formatom, obavlja se nad podskupom CABAC binstringova na takav način da zadovoljava ograničenja za rad u realnom vremenu[31]. Binstringovi su nebinarni elementi HEVC sintakse koji se i procesu binarizacije CABAC kodera entropije pretvaraju u binarni oblik. U navedenom algoritmu su odabrani binstringovi tako da šifrovani binstring mora biti iste dužine kao i originalni binstring, šifrovani binstring mora biti validan i dekoder entropije treba da može da ga dekodira, svaki tip odabranog binstring u svakom trenutku binarizacije mora biti predstavljen jednakim celobrojnim brojem bita. Binstringovi iz navedenih podskupova se nadovezuju i kreira se otvoreni tekst koji se šifruje primenom AES kriptografskog algoritma u CFB (engl. *CFB - Cipher FeedBack*) modu rada.

Predloženi algoritam selektivnog šifrovanja zahteva veoma malo procesorske snage i idealan je za reprodukciju na ručnim uređajima. Navedeni algoritam je prihvatljiv za široki spektar različitih oblasti primene, jer su kriptografski obrađene informacije o konturi i kretanju, zajedno sa teksturom. Za eksperimentalnu evaluaciju predloženog algoritma korišćeno je nekoliko referentnih video sekvenci različitih rezolucija i različitih sadržaja. Detaljna sigurnosna analiza predloženog algoritma selektivnog šifrovanja HEVC video toka podataka (obrađena u [31]) potvrđuje validnost i primenljivost predloženog algoritma za kriptografsku zaštitu tajnosti video podataka u širokom spektru oblasti primena. Sa navedenim karakteristikama, ovaj algoritam selektivnog šifrovanja može se primenjivati i u vojnim komunikacionim sistemima.

Ocena performansi navedenog algoritma selektivnog šifrovanja, prema prethodno definisanim kriterijumima:

- Podesivost - nije podesiv, selektivno šifruje fiksno definisanom podskup CABAC binstringova,
- Vizuelna degradacija - vizuelna degradacija je na visokom nivou. U [31] tabelarno je prikazan odnos signal šum (sa i bez selektivnog šifrovanja) za različite sekvence i različite vrednosti parametra kvantizacije. Iz navedenih podataka se može zaključiti da je stepen vizuelne degradacije visok i da algoritam dobro funkcioniše za različite kombinacije kretanja, tekstura i objekata.
- Kriptografska bezbednost - u radu je pokazana otpornost navedenog algoritma selektivnog šifrovanja na različite poznate tehnike kriptoanalize. Kriptografska bezbednost se faktički svodi na kriptografsku bezbednost primenjenog simetričnog blokovskog kriptografskog algoritma. U navedenom slučaju to je trenutno važeći standardni algoritam šifrovanja podataka, AES u CFB modu rada.
- Kriptografski koeficijent - kriptografski koeficijent se kreće u granicama od 16,96% do 20,08% što se i poklapa sa visokim nivoom vizuelne degradacije.
- Uticaj na kompresiju podataka - nema uticaja na kompresiju podataka. Šifrovanje sintaksnih elemenata se izvršava u vreme kodiranja video toka podataka.
- Usaglašenost formata - po formatu je potpuno usaglašen sa standardnim HEVC video tokom podataka.
- Otpornost na greške - nije otporan na greške, jer primenjeni CFB mod rada blokovskog kriptografskog algoritma nije otporan na greške. Tačnije, greška nastala prilikom dešifrovanja jednog bloka podataka propagira se na ostale blokove.

3.5.2. Algoritam autora Glen Van Wallendael i saradnika

Ovaj algoritam je razvijan i publikovan paralelno sa procesom izrade novog H.265/HEVC standarda video kodovanja. Primena kriptografske obrade nad celokupnim video tokom podataka može biti računarski skupa (procesorsko vreme) i može da onemogući napredne modifikacije video toka podataka od strane neproverenih (nepouzdanih) uređaja u mreži kao što su: spajanje dva video toka podataka, monitorisanje kvaliteta video podataka, proces kreiranja digitalnih vodenih žigova

(watermarking[3]) i direktna digitalno-digitalna konverzija video toka iz jednog načina kodovanja u drugi ili iz jedne bitske brzine u drugu (engl. *transcoding and/or transrating*). Navedena grupa autora u svom radu istražuje višestruke tehnike za selektivno šifrovanje HEVC video toka podatka na način koji je usaglašen po formatu. Posebnu pažnju posvećuju izboru sintaksnih elementa koji mogu biti selektivno šifrovani a da i dalje budu omogućene gore navedene napredne modifikacije video toka podataka. Tako na primer, da bi bile moguće operacije digitalno-digitalne konverzije (*transcoding i transrating*) podaci o primenjenom parametru kvantizacije i informacije o razlici između prediktovane slike i stvarne slike (engl. *residual information*) moraju da budu dostupne u otvorenom obliku u video toku podataka (ne smeju biti šifrovane).

Sa njihove tačke gledišta, održavanje usaglašenosti formata nakon selektivnog šifrovanja zahteva da šifrovani sintaksni elementi ne menjaju ponašanje dekodera prilikom parsiranja[32]. U njihovom radu je dat tabelarni prikaz šest različitih sintaksnih elemenata čijim bi se šifrovanjem postiglo selektivno šifrovanje HEVC video toka, pod prethodno navedenim uslovima koji se tiču ponašanja dekodera. Među identifikovanim sintaksnim elementima nalaze se: kratkoročni skup referentnih slika, informacije o parametru kvantizacije, informacije o inter kodiranoj slici (indeksi referentne slike, indikatori predikcije vektora pokreta, indeksi spajanja kretanja, razlike vektorskih pokreta), informacije o razlici između prediktovane slike i stvarne slike (engl. *residual information*), parametri filtera za uklanjanje blokovskih efekata (engl. *deblocking filter*) i parametri filtera adaptivnih ofseta uzoraka (*SAO filter*). Ovako identifikovani sintaksni elementi, ili samo neki od navedenih elemenata u zavisnosti od oblasti primene predloženog algoritma, šifruju se AES kriptografskim algoritmom u ECB modu rada. Eksperimentalni rezultati dati u[32], u pogledu efikasnosti kompresije i performansama skremblovanja, mogu služiti kao dobra uputstva pri donošenju odluke o tome koji element treba šifrovati i s kojim gubitkom efikasnosti kompresije.

Ocena performansi navedenog algoritma selektivnog šifrovanja, prema prethodno definisanim kriterijumima:

[3] Watermarking - proces skrivanja digitalnih informacija u signalu nosioca. Skrivene informacije mogu ali i ne moraju da sadrže vezu sa signalom nosioca. Digitalni vodeni žigovi se mogu koristiti za proveru autentičnosti ili integriteta signala nosioca ili za prikaz identiteta njegovog vlasnika. Oni se uglavnom koriste za monitoring kršenja autorskih prava i za autentikaciju novčanica.

- Podesivost - podesiv je, moguće je izabrati podskup definisanog skupa od šest različitih sintaksnih elemenata i njega šifrovati izabranim simetričnim blokovskim kriptografskim algoritmom. Izbor podskupa sintaksnih elemenata za šifrovanje zavisi od oblasti primene ponuđenog algoritma i potrebe za omogućavanjem ili onemogućavanjem navedenih naprednih modifikacija video toka podatka.
- Vizuelna degradacija - kao posledica podesivosti stepen vizuelne degradacije varira i različit je. Najveći stepen vizuelne degradacije je u situaciji kada su, između ostalih, šifrovani indikatori predikcije vektora pokreta, razlike vektorskih pokreta i informacije o razlici između prediktovane slike i stvarne slike. Generalno gledano, nivo vizuelne degradacije je veoma mali za neku ozbiljnu primenu navedenog algoritma za očuvanje tajnosti HEVC video toka podataka.
- Kriptografska bezbednost - sami autori u radu kažu da je kriptografska bezbednost navedenog algoritma mala jer se AES kriptografski algoritam koristi u ECB modu rada. U samom radu nije data detaljna analiza otpornosti navedenog algoritma na poznate napade kriptoanalize.
- Kriptografski koeficijent - kriptograski koeficijent se kreće u granicama od 0,33% do 4,56% što prouzrokuje i slabiju vizuelnu degradaciju i manju kriptografsku bezbednost.
- Uticaj na kompresiju podataka - nema uticaja na kompresiju podataka. Šifrovanje sintaksnih elemenata se izvršava u vreme kodiranja video toka podataka.
- Usaglašenost formata - po formatu je potpuno usaglašen sa standardnim HEVC video tokom podataka.
- Otpornost na greške - otporan je na greške jer nema ulančavanja blokova prilikom šifrovanja podataka.

3.5.3. Algoritam autora V. A. Memos i K.E. Psannis

Autori u svom radu predstavljaju novi algoritam za selektivno šifrovanje i slanje, koji obezbeđuje efikasan mehanizam isporuke HEVC video toka podataka. Njihov algoritam se zasniva na poznatim algoritmima predloženim za prethodne standarde kompresije video podataka, koji su prilagođeni tako da budu primenljivi na novodefinisanom HEVC standardu. Tačnije, autori spajaju dva poznata algoritma koji se namenjeni za

selektivno šifrovanje video toka po prethodnom standardu (H.264) modufikujući ih na taj način da mogu lako biti integrisani sa novim H.265/HEVC standardom. Algoritam definisan u [33] je modifikovan tako da se umesto tajnog ključa AES simetričnog blokovskog kriptografskog algoritma dužine 128 bita koristi ključ dužine 256 bita. Druga modifikacija se odnosi na algoritam selektivnog šifrovanja koji je definisan u [34] a ogleda se u definisanju nove i naprednije šeme za deljenje tajnog ključa između većeg broja korisnika. Ovakva podela tajnog ključa omogućava definisanje tačno određenog broja potrebnih učesnika koji treba da dostave svoj deo kako bi bilo moguće kreirati tajni ključ.

Kombinacijom navedena dva algoritma, ponuđeni algoritam selektivnog šifrovanja vrši šifrovanje samo intra kodovanih slika (frejmova), jer su P i B inter kodovane slike beskorisne bez poznavanja odgovarajućih intra kodovanih slika. U okviru intra kodovane slike šifrovani su samo biti koji predstavljaju bit znaka. Štaviše, istraživanja su pokazala da se šifrovanjem samo intra kodovanih slika može uštedeti od 30 do 50% vremena za šifrovanje/dešifrovanje dok se veličina kriptografski obrađenog dela video toka podataka ne menja[35]. Eksperimentalni rezultati pokazuju da je predloženi algoritam sigurniji i efikasniji u odnosu na prethodne algoritme koji se koriste za prethodni H.264 standard kompresije video podataka.

Ocena performansi navedenog algoritma selektivnog šifrovanja, prema prethodno definisanim kriterijumima:

- Podesivost - nije podesiv, šifruju se unapred definisani sintaksni elementi u svakoj intra kodovanoj slici tako da nema podesivosti.
- Vizuelna degradacija - vizuelna degradacija je na visokom nivou jer se šifrovanjem određenih elemenata intra kodovane slike šifruju podaci potrebni za dekodiranje P i B inter kodovanih slika. Tako dekoder na prijemnoj strani, koji ne poznaje primenjeni algoritam selektivnog šifrovanja, nema mogućnost da ispravno dekoduje i prikaže ništa u primljenom video toku.
- Kriptografska bezbednost - autori u radu navode da je kriptografska bezbednost na zadovoljavajućem nivou jer se koristi AES kriptografski algoritam sa ključem veličine 256 bita. Za ključ dužine 256 bita potrebno vreme za *brutte-force* attack je $3{,}31 \times 10^{56}$ godina. Kako u radu nije navedeno u kom kriptografskom modu se

koristi AES kriptografski algoritam nije moguće dati detaljni kritički osvrt na ocenu kriptografske bezbednosti.

- Kriptografski koeficijent - kriptografski koeficijent varira i zavisi od sekvence do sekvence jer je direktno uslovljen tipom video i sadržajem intra kodovane slike. Generalno, kriptografski koeficijent za sekvence iz klase A (4K UHD sekvence) se kreće od 22,34% do 29,45%.
- Uticaj na kompresiju podataka - nema uticaja na kompresiju podatka jer se šifrovanje dešava nakon kompresije.
- Usaglašenost formata - usaglašen je po formatu sa standardnim HEVC video tokom podataka.
- Otpornost na greške - kako nije navedeno u kom modu rada radi simetričan blokovski kriptografski algoritam nije moguće ni detaljno diskutovati otpornost na greške. Generalno gledano, nije otporan na greške jer ako se greška dogodi na šifrovani sintaksni element unutar intra kodovane slike, automatski će ta greška biti propagirana na sve sledujuće P i B inter kodovane slike.

3.5.4. Algoritam autora Mohammed A. Saleh, Nooritawati Md. Tahir i Habibah Hashim

U ovom radu autori razmatraju novu tehniku šifrovanja pokretnih objekata u HEVC video toku podataka. Kako bi se uštedelo procesorsko vreme šifrovanja/dešifrovanja, u ponuđenom algoritmu selektivnog šifrovanja za šifrovanje su izabrani vertikalni podaci razlike vektorskih pokreta (engl. *MVD - Motion Vector Difference*). Tačnije, reč je o osetljivim sintaksnim elementima HEVC video toka koji se direktno tiču pokretnih objekata. Izabran je jedan od četiri sintaksnih elemenata kojima se predstavlja jedinica predviđanja pokretnog objekta. Ovako izabrani podaci se kriptografski obrađuju AES kriptografskim algoritmom u CFB modu rada.

Ponuđeni algoritam selektivnog šifrovanja se označava i kao prvi uopšte definisani mehanizam za selektivno šifrovanje informacija o pokretnim objektima u HEVC video toku. Eksperimentalni rezultati dati u [36] pokazuju da ponuđeni algoritam selektivnog šifrovanja obezbeđuje adekvatan nivo kriptografske sigurnosti za informacije o pokretnim objektima uz istovremeno razmatranje kompromisa između računarske

složenosti, pouzdanosti ponuđenog postupka selektivnog šifrovanja i efikasnosti kodiranja video podataka za primenu u sistemima za rad u realnom vremenu.

Ocena performansi navedenog algoritma selektivnog šifrovanja, prema prethodno definisanim kriterijumima:

- Podesivost - nije podesiv, fiksno definisani skup sintaksnih elemenata se kriptografski obrađuje.
- Vizuelna degradacija - nivo vizuelne degradacije je direktno proporcionalan procentu pokretnih objekata u video sekvenci. Tačnije, što je veći procenat pokretnih objekata to je veća vizuelna degradacija selektivno šifrovanog video toka i obrnuto.
- Kriptografska bezbednost - iz eksperimentalnih rezultata se jasno može zaključiti da je kriptografska bezbednost predloženog algoritma na zadovoljavajućem nivou iako on kriptografski obrađuje samo pokretne objekte u video sekvencama a preskače nepokretne objekte. Ako je potrebno kriptografski zaštiti samo pokretne objekte onda predloženi kriptografski algoritam ima visoko zadovoljavajuću kriptografsku bezbednost. U radu je pokazana i dokazana otpornost navedenog algoritma selektivnog šifrovanja na poznate napade kriptoanalize.
- Kriptografski koeficijent - kriptografski koeficijent se kreće u granicama od 8,30 do 21,52%. Srednja vrednost kriptografskog koeficijenta je 11.71% što daje prednost navedenom algoritmu selektivnog šifrovanja za primenu i sistemima za rad u realnom vremenu.
- Uticaj na kompresiju podataka - nema uticaja na kompresiju podataka. Šifrovanje sintaksnih elemenata se izvršava u vreme kodiranja video toka podataka.
- Usaglašenost formata - po formatu je potpuno usaglašen sa standardnim HEVC video tokom podataka.
- Otpornost na greške - nije otporan na greške, jer primenjeni CFB mod rada blokovskog kriptografskog algoritma nije otporan na greške. Tačnije, greška nastala prilikom dešifrovanja jednog bloka podataka propagira se na ostale blokove.

3.5.5. Algoritam autora Heinz Hofbauer, Andreas Uhl, Andreas Unterweger

U radu navedenih autora ponuđen je algoritam selektivnog šifrovanja HEVC video toka koji omogućava transparentno (perceptualno) šifrovanje širokog opsega parametara kvantizacije. Transparentno ili perceptualno šifrovanje podrazumeva da korisnici mogu da pregledaju ponuđenu verziju video zapisa ali u lošijem kvalitetu. Na taj način neovlašćenim korisnicima je onemogućeno da pristupe punoj verziji video toka, dok je ona istovremeno dostupna ovlašćenim korisnicima. Suprotno od transparentnog šifrovanja, autori definišu pojam adekvatno selektivno šifrovanje čiji je cilj sprečavanje prijatnog iskustva prilikom gledanja video toka. U praksi to znači smanjenje kvaliteta video toka do tačke gde je video izuzetno izobličen, ali i dalje može biti prepoznatljiv. Pošto je sadržaj video zapisa još uvek prepoznatljiv, adekvatno šifrovanje je srednji stadijum gradacije algoritama selektivnog šifrovanja između transparentnog i kriptografski sigurnog selektivnog šifrovanja kod koga video sadržaj ne sme da bude prepoznatljiv[37].

Navedeni algoritam selektivnog šifrovanja fokusira se na šifrovanje znaka AC koeficijenata, zato što se oni mogu šifrovati i direktno promeniti u binarnom toku podataka bez ponovnog kodovanja entropije. Ovakav pristup omogućava brzu realizaciju procesa šifrovanja i dešifrovanja uz očuvanje usaglašenosti po formatu. U prethodnom periodu predložen je veliki broj različitih pristupa selektivnog šifrovanja DCT koeficijenata u multimedijalnom sadržaju u različitim standardima (MPEG-2 video, MPEG-4 i H.264). Navedeni algoritmi selektivno šifruju sve postojeće znakove AC koeficijenata sa ciljem postizanja kriptografski sigurnog selektivnog šifrovanja. Nasuprot tome, Hofbauer i saradnici selektivno šifruju samo znakove AC koeficijenata kanala osvetljenja omogućavajući na taj način transparentno selektivno šifrovanje sa malim ali primetnim smanjenjem kvaliteta video toka[37]. Osim toga ponuđeni algoritam svoj rad realizuje na nivou bitova, tj. može se primeniti na nivou bitskog toka video podataka bez potrebe da se video dekodira u potpunosti. Promena (šifrovanje) znakova AC koeficijenata se realizuje na pseudoslučajan način.

Ocena performansi navedenog algoritma selektivnog šifrovanja, prema prethodno definisanim kriterijumima:

- Podesivost - nije podesiv, jer se navedenim algoritmom šifruje fiksno definisan skup znakova AC koeficijenata.

- Vizuelna degradacija - vizuelna degradacija je na niskom nivou jer se radi o transparentnom selektivnom šifrovanju čiji cilj nije visoka vizuelna degradacija.
- Kriptografska bezbednost - kriptografsku bezbednost nije lako odrediti iz dva razloga. Prvo nije precizno naveden način, tj. pseudoslučajni algoritam po kome se radi promena znakova AC koeficijenata. Drugo, u [38] je praktično dokazano da šifrovanje samo znakova AC koeficijenata ne može da obezbedi zadovoljavajući nivo kriptografske bezbednosti.
- Kriptografski koeficijent - kritpografski koeficijent nije fiksno definisan i zavisi od veličine parametra kvantizacije i od strukture i rasporeda intra i inter kodovanih slika. Za izabrane test sekvence i vrednosti parametara sa kojima je navedeni algoritam testiran, oko 25% znakova AC koeficijenata menja svoju vrednost šifrovanjem.
- Uticaj na kompresiju podataka - nema uticaja na kompresiju podataka. Promena znaka AC koeficijenata na pseudoslučajan način može da se odvija i istovremeno sa kompresijom video podataka i nakon što je kodovanje video toka završena. Tako se ovaj algoritam može istovremeno svrstati u obe grupe algoritama selektivnog šifrovanja.
- Usaglašenost formata - po formatu je potpuno usaglašen sa standardnim HEVC video tokom podataka.
- Otpornost na greške - otporan je na greške jer se zamena vrednosti jednog znaka AC koeficijenata odvija nezavisno od vrednosti ostalih znakova AC koeficijenata na pseudoslučajan način.

3.5.6. Algoritam autora Mokhtar Ouamri i Kamel Mohamed Faraoun

U ovom radu je predstavljen nov i originalan postupak selektivnog šifrovanja HEVC video toka podataka. Ponuđeni algoritam šifruje izabrane sufikse eksponencijalnih Golomb kodova primenom AES kriptografskog algoritma u CBC modu rada. Za šifrovanje se biraju samo sufiksi podblokova koji pripadaju intra kodovanim odsečcima, a šifrovanje izabranih sufiksa vrši se pre binarnog aritmetičkog kodovanja.

Na osnovu dobijenih rezultata u[39], može se zaključiti da predloženi algoritam postiže dobar nivo vizuelne degradacije. Autori takođe upoređuju vreme kodovanja

video podataka sa i bez selektivnog šifrovanja i pokazuju su da je dodatno vreme koje unosi selektivno šifrovanje zanemarljivo u odnosu na vreme potrebno za kodovanje video podataka. Na osnovu toga se može zaključiti da je predloženi algoritam selektivnog šifrovanja pogodan za primenu u aplikacijama za rad u realnom vremenu.

Ocena performansi navedenog algoritma selektivnog šifrovanja, prema prethodno definisanim kriterijumima:

- Podesivost - nije podesiv, elementi koji se šifruju su fiksno definisani i ne mogu se menjati niti prilagođavati različitim potrebama.
- Vizuelna degradacija - vizuelna degradacija je na visokom nivou što je u radu potvrđeno prikazom slika izvučenih iz selektivno šifrovanog video toka testiranih sekvenci ali i vrednostima odnosa signal-šum koji se koristi kao merilo vizuelne degradacije.
- Kriptografska bezbednost - Kriptografska bezbednost je na zadovoljavajućem nivou. Ovakvu činjenicu dodatno potkrepljuje to što je korišćen AES kriptografski algoritam u CBC modu rada pa se kriptografska bezbednost svodi na sam standardni kriptografski simetrični algoritam.
- Kriptografski koeficijent - kriptografski koeficijent se, za testirane sekvence i vrednosti parametra kvantizacije manjeg od 24, kreće oko 10%. Ako se veličina parametra kvantizacije povećava povećavaće se i broj izabranih sintaksnih elemenata koje treba šifrovati pa se samim tim povećava i kriptografski koeficijent.
- Uticaj na kompresiju podataka - nema uticaja na kompresiju podataka. Šifrovanje sintaksnih elemenata se izvršava u vreme kodiranja video toka podataka.
- Usaglašenost formata - po formatu je potpuno usaglašen sa standardnim HEVC video tokom podataka.
- Otpornost na greške - nije otporan na greške, jer primenjeni CFB mod rada blokovskog kritpografskog algoritma nije otporan na greške. Tačnije, greška nastala prilikom dešifrovanja jednog bloka podataka propagira se na ostale blokove.

3.6. Opšte karakteristike algoritama selektivnog šifrovanja HEVC video toka

Analizirajući prethodne opise postojećih algoritama selektivnog šifrovanja HEVC video toka može se zaključiti sledeće:

- svi ponuđeni algoritmi selektivnog šifrovanja HEVC video toka generišu selektivno šifrovani video tok koji je u potpunosti usaglašen po formatu sa standardim HEVC video tokom.
- stepen vizuelne degradacije je usko povezan za predviđenom primenom konkretnog algoritma selektivnog šifrovanja tako da se na jednoj strani nalaze algoritmi koji imaju izuzetno veliku vizuelnu degradaciju, dok se na drugoj strani nalaze algoritmi koji pružaju transparentno (perceptualno) šifrovanje i nizak nivo vizuelne degradacije.
- uglavnom svi opisani algoritmi (pet algoritama od šest opisanih) za šifrovanje izabranih sintaksnih elemenata koriste AES blokovski simetrični kriptografski algoritam u nekom od modova rada. Ovo je i očekivana činjenica jer je AES trenutno aktuelni javno publikovani standardni simetrični algoritam za šifrovanje podataka.
- kod dizajniranja svakog od navedenih algoritama autori teže da kriptografski koeficijent bude što manji a da kriptografska bezbednost bude na zadovoljavajućem nivou. Manji kriptografski koeficijent sa sobom donosi mogućnost primene ponuđenog algoritma selektivnog šifrovanja za aplikacije koje rade u realnom vremenu.
- nijedan od dostupnih algoritama selektivnog šifrovanja ne razmatra problem kriptografske sinhronizacije procesa šifrovanja i dešifrovanja prilikom operacije slučajnog pristupa selektivno šifrovanom HEVC video toku. Kriptografska sinhronizacija procesa dešifrovanja selektivno šifrovanog video toka podataka sa procesom njegovog šifrovanja je neophodna ako je potrebno obezbediti slučajni pristup selektivno šifrovanom HEVC video toku. Slučajni pristup se definiše kao akt započinjana procesa dekodovanja video toka u tački koja ne predstavlja tačku početka video toka. Ako je video tok selektivno šifrovan šifrovanjem nekog od sintaksnih elemenata na način koji je usaglašen po formatu, onda slučajni pristup može biti značajno drugačiji. U odnosu na tačku slučajnog pristupa, proces

dekodiranja i proces dešifrovanja u algoritmu selektivnog šifrovanja moraju imati potrebne podatke kao bi bili u saglasnosti sa procesom šifrovanja koji se izvršava (ili se izvršavao) na strani odakle potiče selektivno šifrovani video tok. Drugim rečima, proces dešifrovanja mora biti u mogućnosti da se kriptografski sinhronizuje sa procesom šifrovanja. Ukoliko proces dešifrovanja nije kriptografski sinhronizovan, dešifrovani podaci neće biti validni a samim tim i rezultat dešifrovanja i dekodiranja video toka podataka neće biti validan.

Posmatrajući navedene zaključke može se videti da je jedan od glavnih nedostataka predloženih algoritama selektivnog šifrovanja nepostojanje efikasnog mehanizma kriptografske sinhronizacije prilikom slučajnog pristupa selektivno šifrovanom HEVC video toku. Kako bi ovaj problem bio rešen u okviru ove disertacije je dizajniran i implementiran efikasan mehanizam kriptografske sinhronizacije koji je nezavistan od primenjenog algoritma selektivnog šifrovanja HEVC video toka.

4. KRIPTOGRAFSKA OSNOVA PONUĐENOG REŠENJA

Kriptografija je nauka koja se bavi proučavanjem, definisanjem i konstruisanjem metoda za zaštitu poruka bez obzira na vrstu informacionog sadržaja (nezavisno od toga da li je u pitanju tekst, govor, slika, video sadržaj ili nešto drugo). Naziv potiče od grčkih reči "*crypto*" što znači tajan-tajno i "*graphien*" što znači pisati. Ukratko rečeno kriptografija predstavlja skup tehnika "tajnog pisanja". Jedan od osnovnih elementa koji istražuje i proučava kriptografija kao nauka je kriptografski algoritam. Kriptografski algoritam je transformacija, zakon, koji razumljivi informacioni sadržaj transformiše u nerazumljiv niz znakova na takav način da je inverzna transformacija jednoznačna[40]. Kriptografski algoritam se može definisati i kao skup matematičkih postupaka koji se koriste u procesu kriptografske transformacije informacionog sadržaja.

U savremenoj kriptografiji postoje dve velike grupe kriptografskih algoritama: simetrični kriptografski algoritmi i asimetrični kriptografski algoritmi. Podela je realizovana na osnovu raspoloživosti parametara potrebnih za šifrovanje i dešifrovanje. Tačnije rečeno, podela je zasnovana na načinu korišćenja kriptografskog ključa.

U grupu simetričnih kriptografskih algoritma spadaju oni algoritmi kod kojih je ključ koji se koristi za šifrovanje informacionog sadržaja identičan ključu koji se koristi za njegovo dešifrovanje. Algoritmi koji se nalaze u ovoj grupi su takođe poznati i po nazivu „algoritmi sa tajnim ključem" jer je očuvanje tajnosti ključa, koji se koristi za šifrovanje i za dešifrovanje, od suštinske važnosti za bezbednost informacionog sadržaja koji se razmenjuje. Ovi algoritmi predstavljaju fundamentalnu osnovu tradicionalne kriptografske teorije i razvijaju se dugi niz godina. Kako se zaštita informacija uglavnom primenjuje u komunikacionim sistemima vezanim za državne strukture (vojska, policija i diplomatska predstavništva), ovi algoritmi su bili isključivo tajni, namenski definisani algoritmi koje realizuje nadležna državna institucija[41].

Ubrzani razvoj Interneta i primena različitih oblika elektronskih komunikacija uslovljava potrebu za razvojem i postojanjem javnih simetričnih kriptografskih algoritama. Zbog toga je u poslednjih tridesetak godina definisan veći broj javnih

simetričnih kriptografskih algoritama koji se mogu primenjivati u različitim oblicima komunikacije na Internetu. Ovako kreirani javni kriptografski algoritmi uglavnom su našli primenu u poslovnim aplikacijama i komunikacionim sistemima finansijskih institucija. Ubrzani razvoj različitih informacionih sistema i sve veći broj finansijskih transakcija doprinose činjenici da javni simetrični kriptografski algoritmi počinju da dominiraju na polju simetrične kriptografije. Nijedan od tadašnjih javnih simetričnih kriptografskih algoritama nije usvojen kao opšte primenljivi standard za zaštitu tajnosti informacionog sadržaja, već gore navedeni komunikacioni sistemi uglavnom koriste liste identifikatora raspoloživih javnih simetričnih kriptografskih algoritama. Tako se, kao jedan od parametara komunikacije, razmenjuje i identifikator simetričnog kriptografskog algoritma koji će se koristiti za zaštitu tajnosti informacionog sadržaja koji se razmenjuje.

Druga grupa savremenih kriptografskih algoritama, asimetrični kriptografski algoritmi, predstavljaju fundamentalno dostignuće savremene kriptografije sa kraja dvadesetog veka. Nastali su kao rezultat istraživačkog rada usmerenog ka rešavanju dva ozbiljna problema koji su uočeni u toku primene simetričnih kriptografskih algoritama. Prvi problem je bio vezan za zaštitu tajnosti ključeva i njihovu distribuciju u sistemima zaštite podataka primenom simetričnih kriptografskih algoritama. Drugi problem se očigledno razlikuje od prvog. Praktično, problem se svodi na to, kako upotrebom simetričnih kriptografskih algoritama, postići potpisivanje digitalnog informacionog sadržaja. Kako obezbediti mehanizam koji će predstavljati ekvivalent svojeručnom potpisu poruke na papiru. Taj mehanizam bi trebao da garantuje da u toku prenosa nije promenjen integritet informacionog sadržaja ali i da omogući postupak provere autentičnosti njegovog pošiljaoca[42].

Godine 1976. Whitfield Diffie i Martin Hellman sa Stendford univerziteta ostvarili su zapanjujući prodor na polju savremene kriptografije[43]. Oni su uveli pojam sistema sa javnim ključevima, tehnologiju koja se drastično razlikovala od svih postupaka korišćenih u poslednjih 400 godina. Njihovo otkriće je rešilo oba, prethodno navedena, problema vezana za primenu simetričnih kriptografskih algoritama. Ubrzo nakon otkrića, ovi algoritmi dobijaju naziv asimetrični kriptografski algoritmi.

Kod asimetričnih kriptografskih algoritama koriste se različiti ključevi za šifrovanje i dešifrovanje. Kod navedene grupe kriptografskih algoritama postoje, i koriste se, javni i

tajni ključ. Navedeni ključevi se koriste na takav način da ključ za šifrovanje (javni ključ) može posedovati svako od učesnika u komunikaciji, a samo onaj ko poseduje ključ za dešifrovanje (tajni ključ) može dešifrovati informacioni sadržaj. Velika računarska zahtevnost, kao jedna od karakteristika algoritama iz grupe asimetričnih kriptografskih algoritama, ima veliki uticaj na performanse komunikacionih sistema u kojima su primenjeni. Ta činjenica prouzrokuje da se u praksi ne preporučuje njihova upotreba za zaštitu tajnosti informacionog sadržaja u sistemima u kojima se razmenjuje velika količina informacija. Ova činjenica ne nipodaštava značaj asimetričnih kriptografskih algoritama jer način na koji je, uz korišćenje algoritama iz ove grupe, moguće implementirati mehanizme očuvanja integriteta, autentičnosti i neporecivosti ima ogromnu prednost nad tehnikama korišćenim u tradicionalnim kriptografskim algoritmima.

Simetrični kriptografski algoritmi se dalje mogu podeliti na sekvencijalne i blokovske kriptografske algoritme. Sekvencijalni kriptografski algoritmi transformišu pojedinačne karaktere, bite ili bajtove otvorenog teksta, koristeći matematičku transformaciju koja zavisi od dva elementa: od primenjenog tajnog ključa i od precizno definisanog trenutka u vremenu u kome se matematička transformacija primenjuje. Za razliku od sekvencijalnih, blokovski kriptografski algoritmi transformišu blokove otvorenog teksta matematičkom transformacijom koja se ne menja tokom šifrovanja celokupnog informacionog sadržaja. U praksi, najčešće, ova podela nije tako kruta. Postoje matematičke transformacije koje se mogu po svojim karakteristikama svrstati i u jednu i u drugu grupu. Tako na primer, izlazni povratni mod i mod povratnog šifrovanja, kao modovi rada blokovskih kriptografskih algoritama, imaju neke osobine sekvencijalnih kriptografskih algoritama. Sa druge strane, sekvencijalni kriptografski algoritmi predstavljaju blokovske kriptografske algoritme čija je dužina bloka jedan karakter (jedan bit, jedan bajt ili jedna mašinska reč dužine 16, 32 ili 64 bita).

Blokovski kriptografski algoritmi nastali u toku dvadesetog veka transformišu blokove otvorenog teksta u blokove šifrata i obrnuto, u blokovima čija je veličina 64 bita. Kod blokovskih algoritama novijeg datuma veličina bloka je najčešće 128 bita. Sekvencijalni kriptografski algoritmi transformišu otvoreni tekst i šifrat u nizovima bita, bajtova ili mašinskih reči (veličine 16, 32 ili 64 bita). Ako se, u toku matematičke transformacije informacionog sadržaja nekim blokovskim kriptografskim algoritmom,

veći broj puta pojavljuje isti blok otvorenog teksta rezultat će uvek biti isti blok šifrata. Ovakvo ponašanje se ne pojavljuje kada se koristi neki sekvencijalni kriptografski algoritam. Kod sekvencijalnih kriptografskih algoritama verovatnoća da ista povorka bita, bajtova ili reči otvorenog teksta, prilikom svakog pojavljivanja u informacionom sadržaju, proizvodi istu povorku šifrovanog teksta teži nuli ukoliko su pseudoslučajna sekvenca koja se koristi za šifrovanje i otvoreni tekst koji se šifruje međusobno nezavisni. Blokovski kriptografskih algoritmi se danas koriste u različitim oblicima finansijskih i poslovnih transakcija ali i u različitim komunikacionim sistemima (za zaštitu računarskih mreža, zaštitu govorne komunikacije, zaštitu platnih transakcija i slično). Postoji veliki broj javnih (javno dostupnih) blokovskih kriptografskih algoritama (kao što su na primer RC2, DES, 3-DES, IDEA, Serpent, Twofish i drugi) koji se svakodnevno upotrebljavaju u savremenim komunikacionim sistemima. U 2001. godini, Nacionalni institut za standarde i tehnologiju (engl. *NIST – National Institute of Standards and Technology*), agencija Američkog ministarstva trgovine koja odobrava standarde u ime vlade SAD, usvojila je novi standardni blokovski kriptografski algoritam i nazvala ga AES (engl. *AES - Advanced Encryption Standard*).

4.1. AES kriptografski algoritam

Kako se prethodno korišćeni standard, DES (engl. *DES - Data Encryption Standard*) približavao kraju svog korisničkog veka, čak i uz trostruku upotrebu za šifrovanje i dešifrovanje podataka (3-DES), NIST donosi odluku da je vladi neophodan novi kriptografski standard za upotrebu u javnim oblicima komunikacije.

NIST se opredeljuje za pristup koji je neobičan i nesvojstven za vladine institucije: NIST organizuje javno kriptografsko nadmetanje. Januara 1997. godine NIST raspisuje konkurs i upućuje poziv istraživačima širom sveta da podnesu svoje predloge za novi standard. Prema uslovima konkursa, novi standard bi trebao da se zove napredni standard za šifrovanje (engl. *Advanced Encryption Standard*). Raspisan je konkurs koji je imao sledeća pravila:

- Algoritam mora raditi kao simetrični blokovski algoritam,
- Projekat u celosti mora biti javan, bez ikakvih tajnih elemenata,
- Moraju biti podržane različite dužine kriptografskog ključa i to 128, 192 i 256 bita,

- Algoritam treba biti takav da ga je podjednako lako implementirati i u softveru i u hardveru,
- Algoritam mora biti javan ili se može licencirati bez ikakvog uslovljavanja.

Na samom početku nadmetanja prijavljeno je petnaest interesantnih predloga koji su prikazivani na javnim skupovima, a istovremeno je istraživačka zajednica podsticana da im traži slabosti, propuste i potencijalne slabe tačke. Avgusta meseca 1998. godine NIST izabira pet finalista uglavnom se rukovodeći sledećim razlozima: bezbednost, jednostavnost, fleksibilnost, efikasnost i memorijski zahtevi. Nakon toga je usledilo održavanje određenog broja novih stručnih konferencija na kojima su prikupljena različita kritička mišljenja. Na poslednjoj održanoj stručnoj konferenciji organizovano je neformalno i neobavezujuće glasanje koje je kao rezultat dalo sledeću listu finalista:

1. Rijndael - autora Joana Daemona i Vincenta Rijnmena - dobio 86 glasova [44]
2. Serpent - autora Ross Andersona, Eli Biham i Larsa Knudsena - dobio 59 glasova[45]
3. Twofish - autorski tim Brucea Schneiera - dobio 31 glas [47]
4. RC6 - autorski tim iz RSA laboratorije - dobio 23 glasa [48]
5. MARS - autorski tim iz IBM-a - dobio 13 glasova [49]

U oktobru 2000. NIST saopštava da je njegov glas dobio Rijndael[4] algoritam, a novembra 2001. Rijndael algoritam biva imenovan za novi standard Američke vlade pod imenom *Federal Information Processing Standard - FIPS 197*. Zbog načina sprovođenja javnog nadmetanja stručnih timova iz celog sveta i specifičnih tehničkih karakteristika samog Rijndael algoritma, očekivalo se da će Rijndael algoritam dominirati u oblasti javnih kriptografskih standarda sledećih petnaestak godina. Tako je i bilo, Rijandael algoritam, tj. AES kriptografski algoritam je i danas najdominantniji javni standardni blokovski kriptografski algoritam.

Rijndael je blokovski kriptografski algoritam koji podržava promenljivu dužinu kriptografskog ključa (128, 192 i 256 bita) kao i promenljivu dužinu bloka otvorenog teksta (128, 192 i 256 bita). Rijndael algoritam je u odnosu na direktne konkurente u finalnom nadmetanju (Serpent, Twofish, RC6 i MARS algoritme) bio brži i zahtevao je manje radne memorije za potrebe realizovanja procesa šifrovanja i dešifrovanja informacionog sadržaja. Sa druge strane, Rijndael algoritam sa 128-bitnom dužinom

[4] Ime Rijndael algoritma izvedeno je od delova imena autora: Rijmen + Daemen.

ključa je 2,5 puta brži u odnosu na 3-DES algoritam. AES algoritam realizuje operacije šifrovanja i dešifrovanja bloka podataka u promenljivom broju rundi. Broj rundi zavisi od veličine ključa i iznosi 10/12/14 za veličinu ključa 128/192/256 bita, respektivno, dok je veličina bloka podatka, koji se šifruje AES kriptografskim algoritmom jednaka 128 bita[49].

4.1.1. Osnovne karakteristike AES kriptografskog algoritma

Pre nego što bude dato kratko objašnjenje procesa šifrovanja i dešifrovanja u okviru AES algoritma, evo još nekoliko njegovih osnovnih karakteristika:

- AES kriptografski algoritam spada u blokovske kriptografske algoritme koji po svojoj strukturi spadaju u supstituciono-permutacione mreže.
- Za svaku rundu algoritma izvodi se podključ runde po algoritmu ekspanzije ključeva koji će kasnije biti objašnjen.
- Algoritam koristi četiri različite transformacije, od kojih su tri transformacije zamenjivanja a jedna je transformacija premeštanja (*ShiwtRows* – predstavlja transformaciju premeštanja).
- Osnovna struktura algoritma je veoma jednostavna. I kod operacije šifrovanja i kod operacije dešifrovanja, algoritam počinje jednom *AddRoundKey* transformacijom, a zatim sledi devet, jedanaest ili trinaest rundi (u zavisnosti od veličine ključa) i svaka od njih obuhvata sve četiri transformacije. Na samom kraju je deseta, dvanaesta ili četrnaesta runda, u kojoj nedostaje operacija *MixColumns*.
- Samo se o okviru *AddRoundKey* transformacije koristi ključ. Tačnije koristi se deo ključa. To uslovljava činjenicu da šifrovanje počinje i završava se *AddRoundKey* transformacijom.
- *AddRoundKey* transformacija je jednostavno sabiranje po modulu 2, pri čemu se sabira deo otvorenog teksta sa delom ključa. Ovako definisana transformacija ne unosi složenost i težinu u algoritam. Preostale tri transformacije su zadužene za unošenje pometnje, difuzije i nelinearnosti, dok, sa druge strane, one same po sebi ne zadovoljavaju bezbednosne aspekte jer u realizaciji njihovih operacija ne učestvuje tajni ključ.

- Svaku od korišćenih transformacija je lako invertovati, tj. lako je odrediti transformaciju koja joj je inverzna. *ByteSub*, *ShiftRows* i *MixColumns* imaju ekvivalentne inverzne transformacije koje se po logici stvari primenjuju u postupku dešifrovanja.
- Sve četiri transformacije se odvijaju nad elementima jednodimenzinog niza *B*,

$$B_{00}B_{10}B_{20}B_{30}B_{10}B_{11}B_{12}B_{13}B_{20}B_{21}B_{22}B_{23}B_{30}B_{31}B_{32}B_{33}$$

koji se predstavlja u obliku matrice B_{ji} na sledeći način[5] (prikazan je primer za 128-bitnu vrednost, tj. za 16 bajta):

$$\begin{pmatrix} B_{00} & B_{10} & B_{20} & B_{30} \\ B_{01} & B_{11} & B_{21} & B_{31} \\ B_{02} & B_{12} & B_{22} & B_{32} \\ B_{03} & B_{13} & B_{23} & B_{33} \end{pmatrix} \quad (11)$$

- Sve transformacije, osim transformacije *AddRoundKey*, svoje operacije realizuju samo nad vrednostima matrice međurezultata B_{ji}. Transformacija *AddRoundKey* pored vrednosti matrice B_{ji} kao ulazni parametar koristi i podključ date runde K_r.
- U AES kriptografskom algoritmu operacije množenja i sabiranja vrše se nad elementima konačnog polja od 256 elemenata (ovo konačno polje se označava sa $GF(2^8)$[6]). Bajtovi se sabiraju primenom bitske operacije sabiranja po modulu dva, dok je rezultat množenja bilo koje dve vrednosti jednak proizvodu po modulu nerazloživog polinoma (za polinom *y(x)* n-tog stepena kaže se da je nerazloživ ako nije deljiv ni sa jednim polinomom stepena *m*, gde *je* $0 < m < n$)[50]:

$$c(x)=a(x)*b(x) \bmod m(x) \quad (12)$$

pri čemu je nerazloživi polinom dat formulom:

$$m(x)=x^8+x^4+x^3+x+1 \quad (13)$$

Svaki element u konačnom polju, *a(x)*, ima jednoznačnu inverznu vrednost, $a_{inv}(x)$, takvu da zadovoljava uslov:

---

[5] U matrici B_{ji}, *j* predstavlja red dok *i* predstavlja kolonu.

[6] Pored konačnih polja od *r*-elemenata (*r*-prost broj) postoje i konačna polja od $q=r^m$ elemenata, gde je *m* prirodan broj. Navedena konačna polja se nazivaju i polja Galoa (engl. *Galois Fields*) u oznaci $GF(r^m)$. Naziv su dobila u čast francuskog matematičara Galoa (E. Galois).

$$a(x) * a_{inv}(x) \bmod m(x)=1 \quad (14)$$

- Za potrebe ubrzavanja procesa množenja u skupu u kome je 256 elemenata konačnog polja formirane su logaritamska i njoj odgovarajuća antilogaritamska tabela. Vrednost svakog od elemenata u konačnom polju *p* može se predstaviti u obliku stepena prostog broja. U AES kriptografskom algoritmu za kreiranje logaritamske i antilogaritamske tabele korišćen je prost broj *{03}*. U logaritamskoj tabeli za svaki od elemenata u konačnom polju *x* postoji vrednost *L* takva da važi uslov *{x} = {03}L*. U antilogaritamskoj tabeli za svaki od elemenata u konačnom polju *x* postoji vrednost *E* takva da je zadovoljen uslov *{E} = {03}x*. U operaciji množenja dva elementa, *a* i *b*, u okviru konačnog polja, koristeći logaritamsku tabelu odrede se koeficijenti α i β takvi da je $a = \{03\}\alpha$ i $b = \{03\}\beta$. Množenjem elemenata *a* i *b* dobija se vrednost jednaka $a * b = \{03\}\alpha+\beta$. Traženi proizvod se može dobiti kada se iz antilogaritamske tabele na osnovu ulazne vrednosti $x = \alpha + \beta$ odredi vrednost za koju važi relacija $E = a * b$. Ovako kreirane logaritamska i antilogaritamska tabela se koriste za izračunavanje inverznog elementa. Na primer, iz logaritamske tabele se za dati element konačnog polja *a*, odredi vrednost α, takva da je zadovoljen uslov $a = \{03\}\alpha$. Inverzna vrednost $E = a - 1$, date veličine, dobija se kada se iz antilogaritamske tabele na osnovu ulazne vrednosti $x = 255 - \alpha$, pročita izlazna vrednost *E*.

Jedna od najznačajnijih operacija u AES kriptografskom algoritmu je operacija ekspanzije kriptografskog ključa. Postupkom ekspanzije kriptografskog ključa vrši se generisanje podključeva K_r i njihovo učitavanje u jednodimenzioni niz *W*. Dužina jednodimenzionog niza *W* zavisi od veličine primenjenog kriptografskog ključa, i u nizu *W* se nakon ekspanzije ključeva nalaze podključevi K_r za svaku rundu *r*. Sledi ukratko objašnjenje kako AES kriptografski algoritam vrši šifrovanje i dešifrovanje bloka otvorenog teksta *B*, veliče 128 bita, upotrebom kriptografskog ključa *K*, veličine 128 bita. Objašnjenje je podeljeno na dva dela: ekspanzija ključa - postupak kojim se obezbeđuju podključevi rundi K_r i sam postupak šifrovanja i dešifrovanja (kroz 10 ciklusa za blok dužine 128 bita).

4.1.2. Algoritam ekspanzije ključeva

Algoritam ekspanzije ključeva kao ulaznu vrednost dobija ključ *K*, proširuje ga i kao povratnu vrednost vraća jednodimenzioni niz *W*. *W* je jednodimenzioni niz dužine $N = N_b * (N_r + 1)$, pri čemu je N_b broj kolona matrice B_{ji} a N_r broj rundi. Za naš konkretni primer, broj kolona matrice je jednako $N_b = 4$ i i broj rundi u procesu šifrovanja je jednako $N_r = 10$. Na osnovu ovoga se dobija da jednodimenzioni niz *W* sadrži 4 * (10 + 1) = 44 reči od po 32 bita. Svaki blok od četiri sukcesivnih reči sadrži tačno 128 bita i oni predstavljaju podključ K_r. Prvi podključ je podključ $K_0 = (W_0, W_1, W_2, W_3)$ i on predstavlja kopiju vrednosti ulaznog ključa *K*. Ostali podključevi rundi izvode se na osnovu sadržaja ključa K_0, tačnije na osnovu sadržaja tajnog simetričnog ključa, na osnovu sledećeg pravila:

$$
\begin{aligned}
W_4 &= W_0 \text{ xor } temp_1 \\
W_5 &= W_1 \text{ xor } W_1 \\
W_6 &= W_2 \text{ xor } W_2 \\
W_7 &= W_3 \text{ xor } W_3 \\
W_8 &= W_4 \text{ xor } temp_2 \\
&\vdots \\
W_{43} &= W_{39} \text{ xor } W_{42} \\
W_{44} &= W_{40} \text{ xor } temp_{11}
\end{aligned}
\qquad (15)
$$

Gde za izračunavanje W_i postoje dva različita slučaja i to po sledećim pravilima:

$$W_i = W_{i-Nk} \text{ xor } W_{i-1}, \quad \text{za } (i \bmod N_k \neq 0) \qquad (16)$$

$$W_i = W_{i-Nk} \text{ xor } temp_k, \text{ za } (i \bmod N_k = 0) \qquad (17)$$

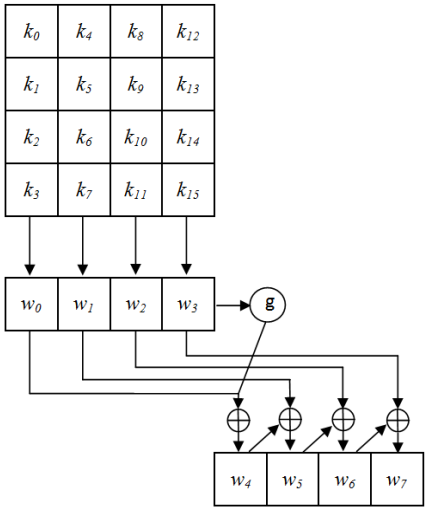
pri čemu je

$$temp_k = ByteSub(S_1, W_{i-1}) \text{ xor } rcon_k \qquad (18)$$

ByteSub se primenjuje na W_{i-1} sa šiftovanim bajtima, i $rcon_k$ je definisano kao:

$$rcon_k = (RC_k, 00, 00, 00) \qquad (19)$$

gde važi da je $RC_1 = 1$, $RC_k = X * RC_{k-1} = X^{k-1}$ i $RC_k \in GF(2^8)$ za svaku vrednost $k = i/4$ i $i = 4, 8, 12, ...,44$. Algoritam ekspanzije ključeva je grafički prikazan na slici 15.



Slika 15. Ekspanzija ključeva u AES kriptografskom algoritmu

4.1.3. Postupak šifrovanja i dešifrovanja u AES kriptografskom algoritmu

Postupak šifrovanja u AES kriptografskom algoritmu sadrži jednu inicijalnu rundu (transformacija *AddRoundKey*), i *r* standardnih rundi čiji broj zavisi od dužine bloka, tj. dužine primenjenog ključa. Prvih *r - 1* rundi su identične i one sadrže četiri transformacije. To su:

- *ByteSub* transformacija predstavlja operaciju nelinearne zamene bajtova pomoću supstitucione tabele. U opisu AES algoritma je definisana matrica 16 x 16, u kojoj su elementi veličine jednog bajta, i koja je poznata pod imenom *S-box*. U njoj je smeštena permutacija svih mogućih osmobitnih vrednosti od 0 do 255. Svaki pojedinačni bajt matrice stanja mapira se u izlazni bajt na osnovu sledećeg pravila: najlevija 4 bita predstavljaju redni broj reda dok najdesnija 4 bita predstavljaju redni broj kolone. Tačnije, ove dve vrednosti definišu indekse kojima se iz *S-box* tabele selektuje osmobitna izlazna vrednost,
- *ShiftRows* transformacija predstavlja promenu mesta bajtova unutar istog reda. Prvi red u matrici stanja ostaje nepromenjen. Bajtovi drugog reda se cirkularno pomeraju za jedno mesto u levo. Nad bajtovima trećeg reda izvrši se cirkularno pomeranje bajtova za dva mesta ulevo, dok se nad bajtovima u četvrtom reda matrice stanja izvrši cirkularno pomeranje bajtova za tri mesta ulevo,
- *MixColumns* transformacija je operacija transformacije bajtova unutar iste kolone i izvršava se individualno nad svakom kolonom. Svaki bajt u datoj koloni mapira se u

novu vrednost koja se dobija kao rezultat funkcije koja kao argumente dobija sva četiri bajta date kolone. Bajtovi date kolone matrice predstavljaju koeficijente polinoma, pri čemu svaki koeficijent predstavlja jedan element u konačnom polju $GF(2^8)$. Tako dobijeni polinomi množe se sa konstantnim polinomom $\boldsymbol{n(x)='03'x^3 + '01'x^2 + '01'x + '02'}$ po modulu $\boldsymbol{x^4 + 1}$,

- *AddRoundKey* transformacija predstavlja operaciju sabiranja po modulu dva odgovarajućih bajtova matrice stanja sa odgovarajućim bajtovima podključa date runde. Operacija sabiranja po modulu dva realizuje se na bitskom nivou.

Poslednja runda šifrovanja ne sadrži transformaciju bajtova unutar iste kolone (transformacija *MixColumns*).

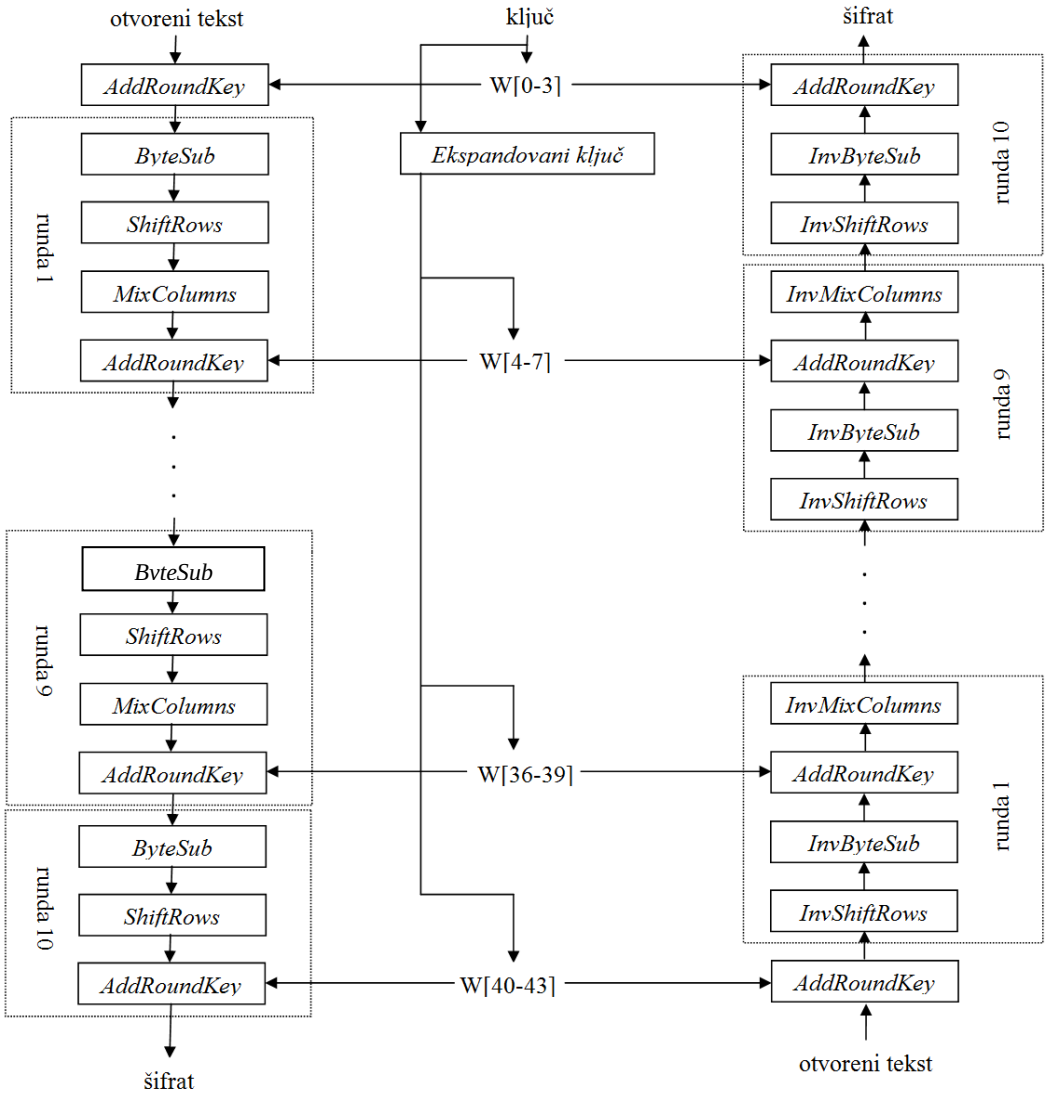
Postupak dešifrovanja poruke u AES kriptografskom algoritmu sličan je procesu šifrovanja. Proces dešifrovanja takođe sadrži jednu inicijalnu rundu (transformacija *AddRoundKey*), i r standardnih rundi čiji broj zavisi od veličine primenjenog kriptografskog ključa. Prvih $r - 1$ rundi su identične i one sadrže četiri transformacije. U procesu dešifrovanja se takođe primenjuju četiri transformacije nad elementima matrice međurezultata, i to:

- *InvByteSub* transformacija je nelinearna transformacija ulazne matrice međurezultata koja se vrši pomoću inverzne supstitucione *S-box* tabele. Postupak supstitucije bajtova identičan je sa postupkom korišćenom u procesu šifrovanja, a jedina razlika je što se sada koristi inverzna supstituciona *S-box* tabela,
- *InvShiftRows* transformacija obavlja operacije nad elementima u redovima matrice međurezultata, dobijenom nakon transformacije *InvByteSub*. Promena mestu bajtova unutar istog reda matrice se realizuje prema sledećim pravilima. Prvi red u matrici stanja ostaje nepromenjen. Bajtovi drugog reda se cirkularno pomeraju za jedno mesto u desno. Nad bajtovima trećeg reda primenjuje se cirkularno pomeranje bajtova za dva mesta udesno, dok se nad bajtovima četvrtog reda matrice stanja primenjuje cirkularno pomeranje bajtova za tri mesta udesno,
- *InvMixColumns* transformacija vrši transformaciju elemenata kolone matrice međurezultata koja je rezultat izvršenja transformacije *InvShiftRows*. Elementi kolone matrice predstavljaju koeficijenti polinoma, pri čemu je svaki koeficijent

element u konačnom polju $GF(2^8)$. Tako dobijeni polinomi, množe se konstantnim polinomom $\boldsymbol{p(x)='0B'x^3 + '0D'x^2 + '09'x + '0E'}$ po modulu $\boldsymbol{x^4 + 1}$,

- *AddRoundKey* transformacija predstavlja sabiranja po modulu dva odgovarajućih bajtova matrice stanja sa ogovarajućim bajtovima podključa date runde. Operacija sabiranja po modulu dva realizuje se na bitskom nivou. Ova transformacije nema inverznu transformaciju jer je operacija sabiranja po modulu dva sama sebi inverzna.

Poslednja runda dešifrovanja ne sadrži transformaciju bajtova unutar iste kolone (transformacija *InvMixColumns*). Celokupan postupka šifrovanja i dešifrovanja prikazan je dijagramom na slici 16.



Slika 16. Proces šifrovanja i dešifrovanja AES kriptografskim algortimom

4.2. Modovi rada blokovskih kriptografskih algoritama

I pored sveukupne složenosti, AES kriptografski algoritam (tačnije rečeno bilo koji blokovski kriptografski algoritam) u osnovi predstavlja zamenu slova slovom (zamenu znaka znakom), pri čemu su, kada je u pitanju AES algoritam, znakovi 128-bitni. Svaki put kada, u informacionom sadržaju koji treba šifrovati, naiđe isti blok otvorenog teksta, blokovski kriptografski algoritam kao rezultat šifrovanja daje isti blok šifrata. Na primer, ako se otvoreni tekst *abcdefghijklmnop* šifruje 200 puta AES kriptografskim algoritmom i istim ključem, dobiće se 200 puta isti šifrovani tekst. Potencijalni napadači mogu da zloupotrebljavaju ovakvo svojstvo blokovskih kriptografskih algoritama. Zbog toga se, da bi se smanjila mogućnost zloupotrebe, blokovski kriptografski algoritmi koriste u nekom od kriptografskih modova rada.

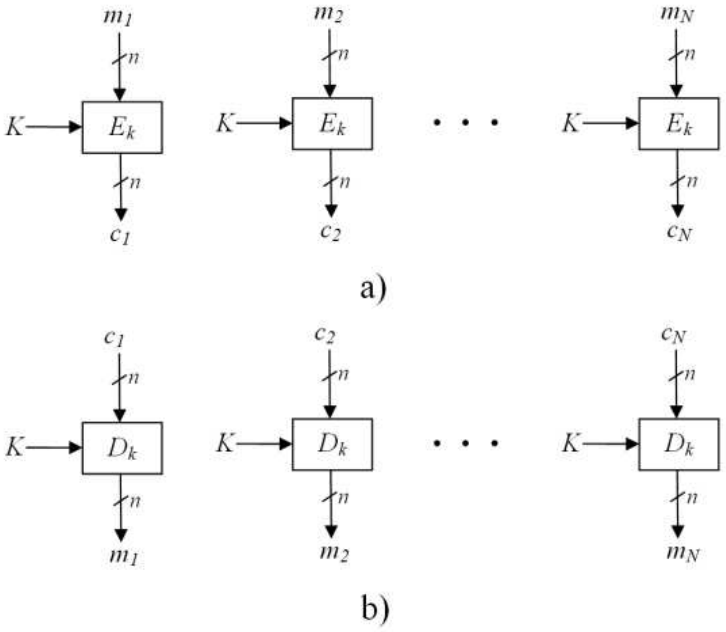
Kriptografski mod predstavlja način rada elementarnog blokovskog kriptografskog algoritma i, suštinski gledano, predstavlja ili tehniku za poboljšanje efekata primenjenog blokovskog kriptografskog algoritma ili tehniku za prilagođenje samog elementarnog blokovskog algoritma za šifrovanje povorke blokova ili povorke bitova i bajtova otvorenog teksta[7]. Kriptografski mod rada najčešće predstavlja kombinaciju nekih jednostavne operacije i neke vrste specifične povratne petlje. Operacije koje se primenjuju u različitim načinima rada elementarnih blokovskih kriptografskih algoritama su uglavnom jednostavne operacije jer je bezbednost celokupnog sistema određena kvalitetom elementarnog blokovskog kriptografskog algoritma a ne njegovim načinom rada. Blokovski kriptografski algoritmi mogu se primenjivati u različitim kriptografskim modovima rada. U praktičnoj primeni se danas najčešće koriste sledeći modovi: mod elektronske kodne knjige - ECB mod (engl. *ECB - Electronic CodeBook*), mod ulančavanja blokova - CBC mod (engl. *CBC - Cipher Block Chaining*), mod povratnog šifrovanja - CFB mod (engl. *CFB - Cipher FeedBack*), izlazni povratni mod - OFB mod (engl. *OFB - Output FeedBack*) i brojački mod - CTR mod (engl. *CTR - Counter mode*)[51].

[7] Šifrovanjem povorke bitova i bajtova otvorenog teksta, modovi rada pružaju mogućnost da se elementarni blokovski kriptografski algoritam koristi kao sekvencijalni.

4.2.1. Mod elektronske kodne knjige

Mod elektronske kodne knjige predstavlja najjednostavniji i najprirodniji način rada blokovskog kriptografskog algoritma. U ovom modu rada, otvoreni tekst se obrađuje tako da se u jednom trenutku vremena šifruje, nezavisno, samo jedan blok otvorenog teksta a svaki blok otvorenog teksta je šifrovan primenom istog kriptografskog ključa (slika 17a). Jednostavnije rečeno, svaki blok otvorenog teksta šifruje se nezavisno od svih ostalih blokova. Takođe, pri dešifrovanju, svaki blok šifrata dešifruje se nezavisno od svih ostalih blokova šifrata(slika 17b). Gledano sa aspekta bezbednosti dobijenog šifrata, mod elektronske kodne knjige je poprilično problematičan. Naime, za određeni kriptografski ključ postoji jedinstveni blok šifrata za svaki *n*-bitni blok otvorenog teksta. Koristeći navedenu osobinu, potencijalni napadač (kriptoanalitičar) može da bez poznavanja ključa, ukoliko poseduje parove otvorenog teksta i šifrata određenog broja poruka, formira elektronsku kodnu knjigu (engl. *codebook*) koja predstavlja skup svih odgovarajućih parova otvorenih tekstova i šifrata. Sa druge strane, informacioni sadržaj u realnim komunikacionim sistemima ima sledeće karakteristike: fragmenti informacionog sadržaja teže ponavljanju, različiti informacioni sadržaji imaju zajedničke delove, informacioni sadržaj generisan na računaru (kao na primer poruke elektronske pošte ili različiti tipovi tekstualnih fajlova) imaju regularnu strukturu, neki informacioni sadržaji mogu da sadrže duge povorke nula ili neki sličan sadržaj fiksne vrednosti. Prethodno navedene karakteristike najistaknutije su na početku i na kraju informacionog sadržaja, gde se najčešće u zaglavljima, naslovnim elementima i fusnotama nalaze ustaljene i stalno ponavljane informacije o onome ko šalje dati sadržaj, o onome ko takav sadržaj prima, informacije o kratkom sadržaju i slično. Formiranjem reprezentativne elektronske kodne knjige potencijalni napadač može da nesmetano pristupa informacionom sadržaju koji se razmenjuje između strana u komunikaciji. Takođe, reprezentativna elektronska kodna knjiga pruža mogućnost napadaču da modifikuje i ponavlja šifrovane segmente informacionog sadržaja bez poznavanja ključa i primenjenog kriptografskog algoritma. Navedene slabosti elementarnog načina rada blokovskih kriptografskih algoritama uticale su na stvaranje novih kriptografskih modova rada

kod kojih se uspostavlja zavisnost između određenog broja susednih blokova šifrata.



Slika 17. Grafički prikaz operacija u ECB modu

4.2.2. Mod ulančavanja blokova

Da bi se prevazišli navedeni bezbednosni nedostaci ECB moda, potrebno je implementirati mehanizam kojim se postiže da se blok otvorenog teksta, uvek kad se ponovi u informacionom sadržaju, uvek šifruje u različiti blok šifrata. Kod moda ulančavanja blokova primenjen je mehanizam ulančavanja koji povezuje blokove šifrata na taj način da se rezultat šifrovanja svih prethodnih blokova koristi prilikom šifrovanja tekućeg bloka otvorenog teksta. Preciznije rečeno, tekući blok šifrata zavisi od primenjenog kriptografskog ključa, od tekućeg bloka otvorenog teksta i svih prethodnih blokova šifrata. I u ovom modu rada, za šifrovanje svakog bloka otvorenog teksta nekog informacionog sadržaja koristi se isti kriptografski ključ.

Implementacija navedenog mehanizma ulančavanja blokova, kako u procesu šifrovanja tako i u procesu dešifrovanja, grafički je prikazana na slici 18. Tekući blok šifrata se dobija tako što se primenjenim blokovskim kriptografskim algoritmom šifruje blok koji je rezultat sabiranja po modulu 2 (ekskluzivna ili funkcija bit za bit) tekućeg bloka otvorenog teksta i prethodnog bloka šifrata. Za dobijanje prvog bloka šifrata koriste se sadržaj prvog bloka otvorenog teksta i

sadržaj inicijalnog vektora. Ukoliko je sadržaj inicijalnog vektora uvek isti, dve identične poruke informacionog sadržaja će uvek dati identične šifrate pod uslovom da su šifrovane istim kriptografskim ključem i istim algoritmom. Da bi se postiglo da se dve iste poruke informacionog sadržaja šifruju u dva potpuno različita šifrata sa istim ključem i algoritmom, potrebno je da se sadržaj inicijalnog vektora bira na slučajan način. Za potrebe kriptografske sinhronizacije, sadržaj inicijalnog vektora mora biti dostupan i pošiljaocu i primaocu poruke a nedostupan ostalima[42].

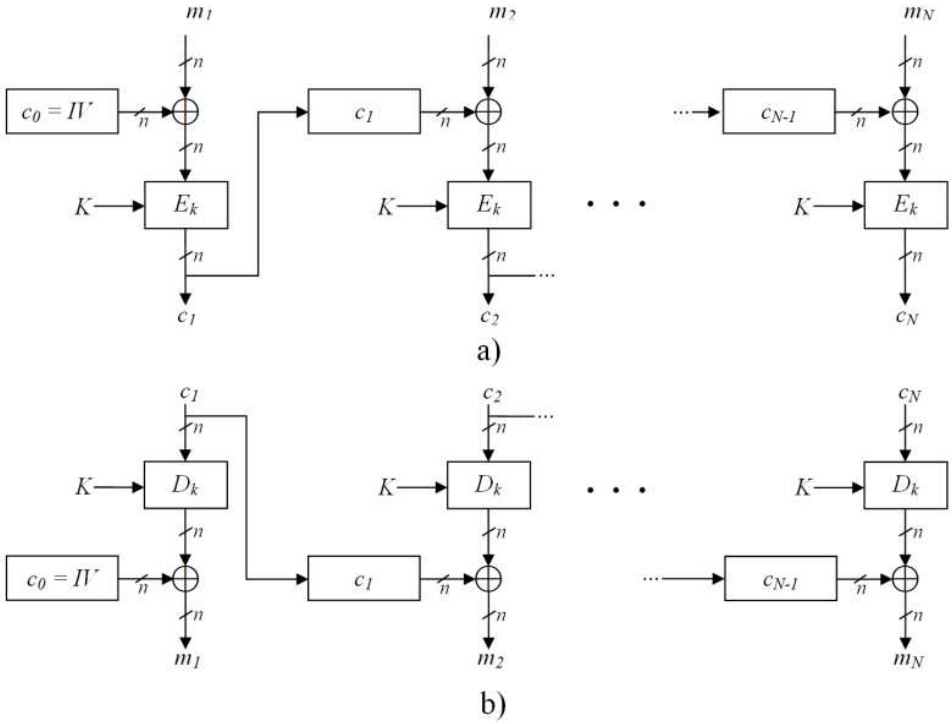
Princip rada mehanizma ulančavanja blokova, prilikom šifrovanja informacionog sadržaja, može se opisati na sledeći način (slika 18a):

1. Poruka informacionog sadržaja se, ukoliko je potrebno, dopuni tako da sadrži celobrojni umnožak blokova otvorenog teksta.
2. U povratni registar se smesti sadržaj inicijalnog vektora.
3. Tekući blok otvorenog teksta, $m_{j,}$ sabere se po modulu 2 sa tekućim sadržajem povratnog registra pa se tako dobijeni blok šifruje primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem K čime se dobija tekući blok šifrata c_j.
4. Sadržaj tekućeg bloka šifrata, c_j, smešta se u povratni registar i postupak šifrovanja se ponavlja od koraka 3 sve dok ima blokova otvorenog teksta u informacionom sadržaju.

Na ovaj način postiže se traženi efekat, rezultat šifrovanja tekućeg bloka šifrata zavisi od svih prethodnih blokova šifrata.

Na prijemnoj strani, mehanizam ulančavanja blokova prilikom dešifrovanja informacionog sadržaja, može se opisati na sledeći način (slika 18b):

1. U povratni registar se smesti sadržaj inicijalnog vektora.
2. Tekući blok šifrata, c_j, dešifruje se primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem K. Tako dobijeni blok podataka sabere se po modulu 2 sa tekućim sadržaj povratnog registra što kao rezultat daje tekući blok otvorenog teksta, m_j.
3. Sadržaj tekućeg bloka šifrata, c_j, smešta se u povratni registar i postupak se ponavlja od koraka 2 sve dok ima raspoloživih blokova šifrata.



Slika 18. Grafički prikaz operacija u CBC modu

Postupak šifrovanja u modu ulančavanja blokova matematički je prikazan relacijom 20 dok je postupak dešifrovanja prikazan relacijom 21, pri čemu E_k predstavlja postupak šifrovanja bloka podataka primenjenim kriptografskim algoritmom i kriptografskim ključem K, dok D_k predstavlja postupak dešifrovanja. Takođe, za $j = 1$, c_0 je jednako sadržaju inicijalnog vektora - IV.

$$c_j = E_k(m_j \oplus c_{j-1}) \tag{20}$$

$$m_j = c_{j-1} \oplus D_k(c_j) \tag{21}$$

Dok su kod ECB moda rada bezbednosni problemi očigledni, u modu ulančavanja blokova takođe postoje potencijalni bezbednosni problemi koji nisu tako očigledni. Naime, navedeni problemi se mogu predstaviti kao potencijalna mogućnost da napadač (kriptoanalitičar) dodaje precizno odabrane blokove na krajeve poruka koje se razmenjuju ili činjenicom da veoma duge poruke nisu imune na mogućnost pojavljivanja identičnih povorki blokova šifrata iako se vrši proces ulančavanja.

4.2.3. Mod povratnog šifrovanja

U definiciji moda rada kriptografskog algoritma rečeno je da on predstavlja i tehniku za prilagođenje elementarnog blokovskog algoritma za šifrovanje povorke bitova ili bajtova otvorenog teksta. U mnogim aplikacijama[8] javlja se potreba da se blokovski kriptografski algoritam ponaša nalik ponašanju nekog sekvencijalnog algoritma, tj. da je moguće delove otvorenog teksta šifrovati i poslati prijemnoj strani u jedinicama veličine *r* bita, pri čemu je *r* manje od veličine bloka primenjenog blokovskog algoritma. Ovakav način rada nije moguće realizovati primenom ECB i CBC modova rada. Još jedna prednost načina rada koji blokovski kriptografski algoritam pretvara u nešto nalik sekvencijalnom je činjenica da u tom slučaju nije potrebno dopunjavanje informacionog sadržaja do celobrojnog umnoška veličine bloka otvorenog teksta. Na ovaj način se eliminiše mogući napad dodavanjem poznatog sadržaja na kraj poruke koja se šifruje. Primenom ovog moda rada šifrat je uvek identične dužine kao i otvoreni tekst.

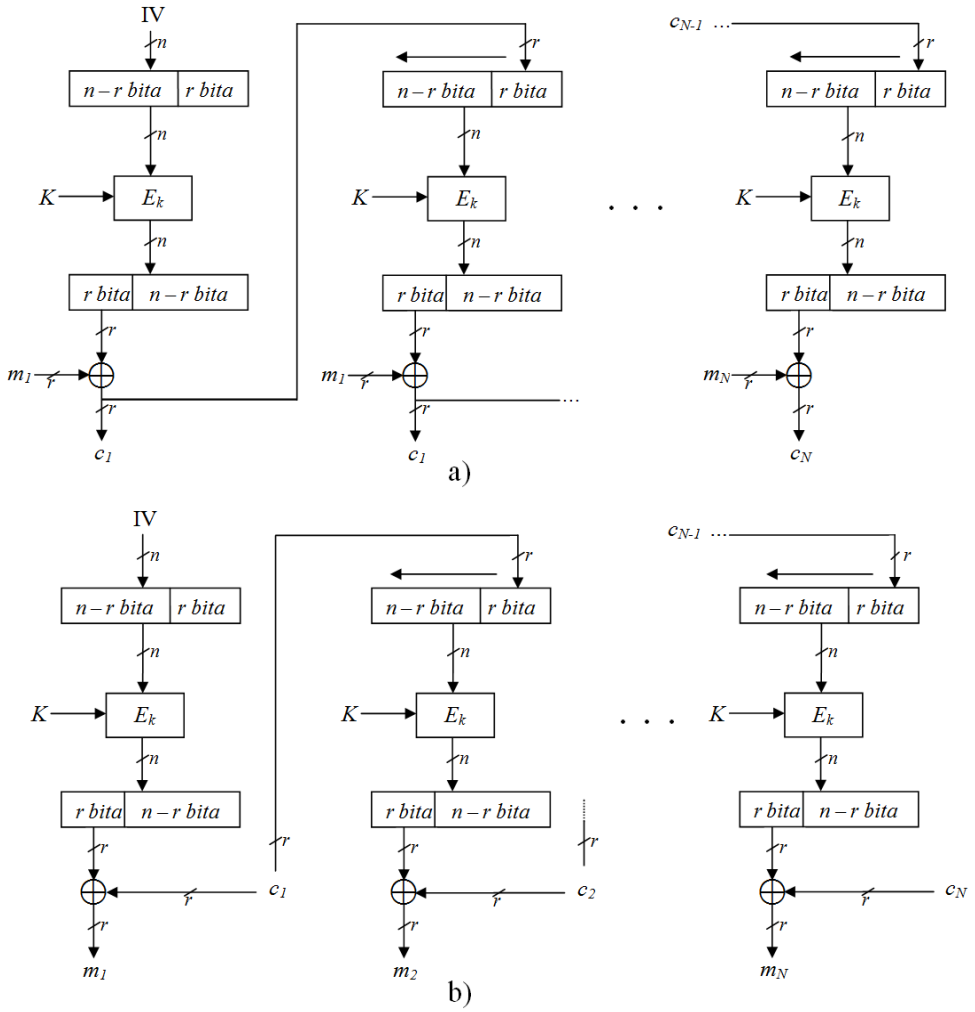
U modu povratnog šifrovanja, informacioni sadržaj se šifruje u jedinicama manjim od veličine bloka primenjenog blokovskog kriptografskog algoritma i ovaj mod rada se najčešće označava kao *r*-bitni CFB mod, pri čemu je *r* manje ili jednako od veličine bloka primenjenog blokovskog kriptografskog algoritma.

Princip rada povratnog šifrovanja, prilikom šifrovanja informacionog sadržaja, može se opisati na sledeći način (slika 19a):

1. Poruka informacionog sadržaja se podeli u blokove veličine *r* bita.
2. Generiše se inicijalni vektor veličine bloka primenjenog blokovskog algoritma i smesti u povratni registar.
3. Tekući sadržaj povratnog registra se šifruje primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem *K* i kao rezultat se dobija izlazni blok, O_j.
4. Tekući blok šifrata, veličine *r* bita, izračunava se tako što se saberu po modulu 2 sadržaj tekućeg bloka otvorenog teksta i *r* bita najmanje težine izlaznog bloka O_j.
5. Tekući sadržaj povratnog registra se pomera u levo za *r* bita i na poziciji *r* bita najmanje težine smešta se tekući blok šifrata.

[8] Najčešće su to aplikacije za rad u realnom vremenu, tj. kriptozaštićeni prenos multimedijalnih sadržaja

Koraci 3-5 se ponavljaju sve dok ima *r*-bitnih blokova otvorenog teksta u informacionom sadržaju.



Slika 19. Grafički prikaz operacija u CFB modu

Na prijemnoj strani, princip rada CFB moda prilikom dešifrovanja šifrovanog informacionog sadržaja, može se opisati na sledeći način (slika 19b):

1. Generiše se inicijalni vektor veličine bloka primenjenog blokovskog algoritma i smesti u povratni registar.
2. Tekući sadržaj povratnog registra se šifruje primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem *K* i kao rezultat se dobija izlazni blok, O_j.
3. Tekući blok otvorenog teksta se dobija kao rezultat sabiranja po modulu 2 sadržaja tekućeg bloka šifrata i *r* bita najmanje težine tekućeg sadržaja izlaznog bloka O_j.
4. Tekući sadržaj povratnog registra se pomera u levo za *r* bita i na mesto *r* bita najmanje težine se smešta tekući blok šifrata.

Koraci 2-4 se ponavljaju se sve dok ima *r*-bitnih blokova šifrata.

Uloga inicijalnog vektora u ovom modu rada je identična kao i kod CBC moda, da spreči dobijanje istih šifrata u slučaju šifrovanja istih poruka informacionog sadržaja istim blokovskim algoritmom i ključem.

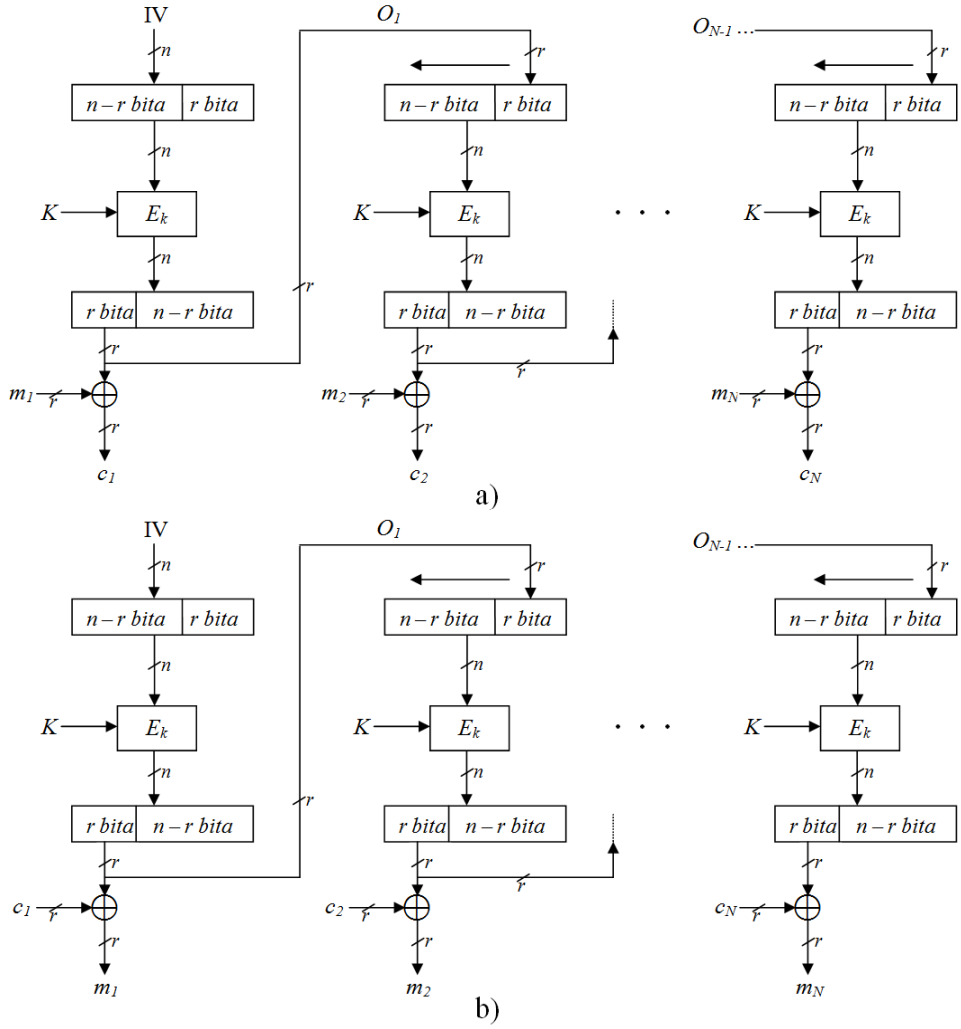
4.2.4. Izlazni povratni mod

Izlazni povratni mod je sličan po strukturi modu povratnog šifrovanja, i predstavlja udruživanje dobrih karakteristika ECB i CFB modova rada. Njegova najveća prednost je što prilikom njegove primene nema propagacije greške. Druga dobra karakteristika ovog moda rada je što se veliki deo izračunavanja može realizovati *off-line*, nakon čega se samo obavlja operacija sabiranja po modulu 2 nad *r*-bitnim blokovima tako dobijene sekvence i *r*-bitnim blokovima otvorenog teksta. Primena OFB moda rada takođe pruža mogućnost slanja šifrovanog informacionog sadržaja prijemnoj strani u jedinicama manjim od veličine bloka.

Princip rada izlaznog povratnog moda, prilikom šifrovanja informacionog sadržaja, može se opisati na sledeći način (slika 20a):

1. Poruka informacionog sadržaja se podeli u blokove veličine *r* bita.
2. Generiše se inicijalni vektor veličine bloka primenjenog blokovskog algoritma i smesti u povratni registar.
3. Tekući sadržaj povratnog registra se šifruje primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem *K* i kao rezultat se dobija izlazni blok, O_j.
4. Tekući blok šifrata, veličine *r* bita, izračunava se tako što se saberu po modulu 2 sadržaj tekućeg bloka otvorenog teksta i *r* bita najmanje težine izlaznog bloka O_j.
5. Tekuća vrednost izlaznog bloka O_j kopira se u sadržaj povratnog registra.

Koraci 3-5 se ponavljaju sve dok ima *r*-bitnih blokova otvorenog teksta u informacionom sadržaju.



Slika 20. Grafički prikaz operacija u OFB modu

Na prijemnoj strani, princip rada OFB moda prilikom dešifrovanja šifrovanog informacionog sadržaja, može se opisati na sledeći način (slika 20b):

1. Generiše se inicijalni vektor veličine bloka primenjenog blokovskog algoritma i smesti u povratni registar.
2. Tekući sadržaj povratnog registra šifruje se primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem *K* i kao rezultat se dobija izlazni blok, O_j.
3. Tekući blok otvorenog teksta se dobija kao rezultat sabiranja po modulu 2 sadržaja tekućeg bloka šifrata i *r* bita najmanje težine tekućeg sadržaja izlaznog bloka O_j.
4. Tekuća vrednost izlaznog bloka O_j kopira se u sadržaj povratnog registra.

   Koraci 2-4 se ponavljaju sve dok ima *r*-bitnih blokova šifrata.

Prethnodno analizirani opis OFB moda rada je definisan standardom ISO 10116[52]. U dosadašnjoj praksi mogu se naći i druge varijacije na temu definicije

OFB moda rada (kao što je na primer standard FIPS-81[51]) ali se, za sada, najbezbednijom varijacijom smatra verzija OFB moda data standardom ISO 10116. Detaljnom analizom OFB moda rada potvrđeno je da se ovaj mod rada treba koristiti samo u slučajevima kada je *r* jednako polovini dužine bloka primenjenog blokovskog kriptografskog algoritma[53]. Preciznije rečeno, blokovske kriptografske algoritme, kao što je AES algoritam sa blokom veličine 128 bita, poželjno je koristiti u 64-bitnom OFB modu.

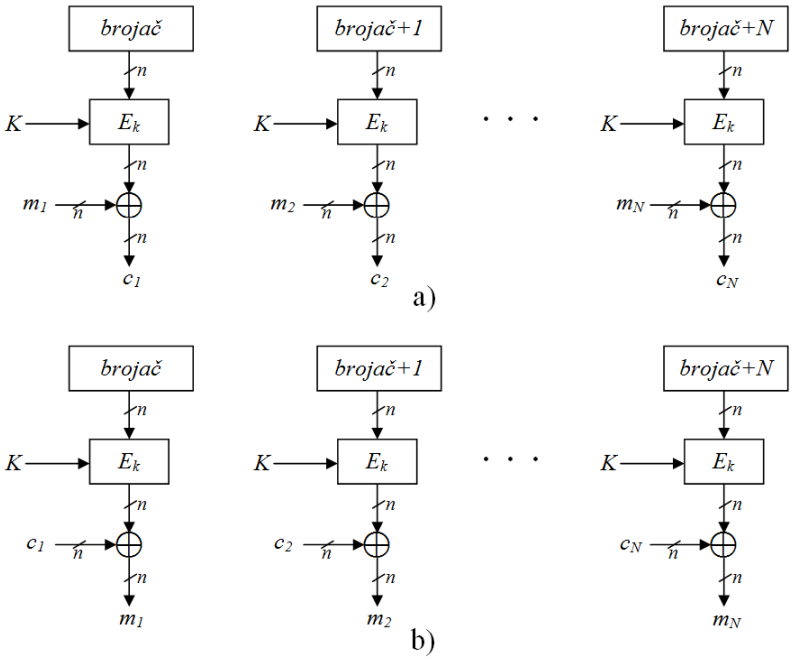
4.2.5. Brojački mod

Kao i OFB moda, brojački mod pretvara blokovski kriptografski algoritam i neku vrstu sekvencijalnog algoritma. U njemu se sledeći blok pseudoslučajne sekvence generiše operacijom šifrovanja sukcesivne vrednosti "*brojača*", primenom elementarnog blokovskog kriptografskog algoritma. U ovom modu rada koristi se brojač čija je veličina, u bitima, jednaka veličini bloka bazičnog blokovskog algoritma. Brojač može biti bilo koja funkcija koja kao rezultat daje niz za koji se može garantovati da se u dužem periodu vremena neće ponoviti. U realnim primenama najjednostavnija i najpopularnija je funkcija inkrementiranja vrednosti brojača za jedan u svakom sledećem koraku. Mada, primena jednostavne funkcije inkrementiranja vrednosti brojača za jedan ima svoje protivnike koji tvrde da je nepotreban rizik izlagati elementarni blokovski kriptografski algoritam načinu korišćenja sa deterministički poznatim ulaznim vrednostima[42].

Princip rada brojačkog moda, prilikom šifrovanja informacionog sadržaja, može se opisati na sledeći način (slika 21a):

1. Vrednost brojača se inicijalizuje na neku početnu vrednost.
2. Vrednost brojača se inkrementira za jedan.
3. Tekuća vrednost brojača se šifruje primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem *K* i rezultat se dobija izlazni blok, O_j.
4. Tekući blok šifrata izračunava se tako što se po modulu 2 saberu sadržaj tekućeg bloka otvorenog teksta i tekući sadržaj izlaznog bloka O_j.

   Koraci 2-4 se ponavljaju sve dok ima blokova otvorenog teksta u informacionom sadržaju koji treba šifrovati.



Slika 21. Grafički prikaz operacija u CTR modu

Princip rada brojačkog moda, prilikom dešifrovanja šifrata, može se opisati na sledeći način (slika 21b):

1. Vrednost brojača se inicijalizuje na neku početnu vrednost.
2. Vrednost brojača se inkrementira za jedan.
3. Tekuća vrednost brojača se šifruje primenjenim blokovskim kriptografskim algoritmom i kriptografskim ključem K i rezultat se dobija izlazni blok, O_j.
4. Tekući blok otvorenog teksta izračunava se tako što se po modulu 2 saberu sadržaj tekućeg bloka šifrata i tekući sadržaj izlaznog bloka O_j.

   Koraci 2-4 se ponavljaju sve dok ima blokova šifrata koji treba dešifrovati.

   Upotreba brojačkog moda rada donosi sa sobom sledeće prednosti:

- **Hardverska i softverska efikasnost**: Za razliku od prethodno navedenih modova kod kojih postoji ulančavanje blokova, ovaj mod je pogodan za paralelizaciju pri čemu se različiti blokovi otvorenog teksta mogu kriptografski obrađivati na različitim procesorskim jezgrima u isto vreme. Ovo ima za posledicu da je vreme šifrovanja celog skupa podataka približno proporcionalno vremenu šifrovanja jednog bloka otvorenog teksta.

- **Mogućnost pretprocesiranja**: Izvršavanje elementarnog algoritma ne zavisi od blokova otvorenog teksta ili blokova šifrata, tako da je unapred moguće izgenerisati sekvencu blokova koji se memorišu a potom, po potrebi, sabiraju po modulu 2 sa blokovima otvorenog teksta ili blokovima šifrata.
- **Slučajni pristup**: mogućnost da se *i*-tom bloku otvorenog teksta ili šifrata pristupi i da bude procesiran na slučajan način, nema zavisnosti od prethodnih blokova otvorenog teksta ili blokova šifrata.
- **Dokaziva sigurnost**: moguće je dokazati da je podjednako siguran kao i ostali modovi rada pod uslovom ako vrednost polovine brojača bude nepredvidiva[54]. Na primer, ako je veličina brojača 128 bita onda bi trebalo da 64-bita vrednosti brojača bude nepredvidivo.
- **Jednostavnost**: Za razliku od prethodno navedenih modova rada, dovoljno je implementirati samo proces šifrovanja. Ovakva funkcionalnost je posebno interesantna kod kriptografskih algoritama kod kojih se operacija dešifrovanja značajno razlikuje od operacije šifrovanja.

4.3. Modovi rada i kriptografska sinhronizacija

Postoji veliki broj definicija pojma kriptografska sinhronizacija. Jedna od njih je da je to postupak kojim se postiže da kriptografska logika u procesu dešifrovanja na prijemnoj strani ima isto unutrašnje stanje kao kriptografska logika u procesu šifrovanja na predajnoj strani. Uopštenija definicija kaže da je to proces koordinacije procesa šifrovanja i dešifrovanja. Nezavisno od načina kako je definisana, kratko se može reći da je svrha kriptografske sinhronizacije da obezbedi potrebno i dovoljno okruženje za nesmetano dešifrovanje podataka na prijemnoj strani.

Na osnovu prethodnog opisa postojećih algoritama selektivnog šifrovanja HEVC video toka, može se zaključiti sledeće: dominantno se koriste blokovski kriptografski algoritmi, tačnije AES algoritam kao trenutno aktuelni standard; navedeni kriptografski algoritam se koristi u različitim modovima rada (nekom od prethodno definisanih) sa ciljem da se postigne željena kriptografska sigurnost ali i da se postignu željeni efekti implementacije dizajniranog algoritma selektivnog šifrovanja. Sa druge strane, svaki od navedenih modova rada prikazuje neznatno drugačije ponašanje kada se suočava sa greškama na bitu/bitovima podataka u šifratu ili sa greškama sinhronizacije granica

blokova koje mogu biti posledica brisanja ili umetanja dodatnog bita u selektivno šifrovani video tok.

Za navedene modove rada važi da, ukoliko postoji bilo kakva greška na jednom bitu u bloku šifrata tada će dešifrovanje tog bloka šifrata biti pogrešno, tj. tako dešifrovani blok će se razlikovati od originalnog bloka otvorenog teksta. U CFB, OFB i CTR modu rada, greška u jednom bitu u dešifrovanom bloku šifrata javlja se na istoj poziciji na kojoj je ta greška bila u bloku šifrata. U ECB i CBC modovima rada, greška na jednom bitu se može pojaviti nezavisno, u bilo kojoj tački dešifrovanog bloka šifrata, sa očekivanom stopom greške od 50%, što zavisi od primenjenog blokovskog kriptografskog algoritma i efekta lavine koji se njime postiže.

Brisanje ili ubacivanje bitova u blok šifrata može da onemogući kriptografsku sinhronizaciju (sinhronizacija granica blokova), tačnije, greške u bitima mogu da se javljaju na mestima obrisanog ili ubačenog bita ali i u svakoj sledećoj poziciji bita. Zbog toga, dešifrovanje narednih blokova šifrata će gotovo sigurno biti netačno sve dok se ne izvrši kriptografska resinhronizacija. Kada se koristi 1-bitni CFB mod rada, kriptografska sinhronizacija se automatski uspostavlja nakon $n + 1$ pozicija (gde je sa n označena veličina bloka u bitima) od pozicije na kojoj je ubačen ili obrisan bit. Za ostale vrednosti parametra r u CFB modu rada, i za sve preostale prethodno navedene modove rada kriptografska sinhronizacija se mora obaviti eksternom akcijom[51].

Eksterna akcija podrazumeva raspolaganje tačnim i ispravnim vrednostima inicijalnog vektora ili vrednosti brojača koji su potrebni za otpočinjanje procesa dešifrovanja. Inicijalni vektor za proces dešifrovanja tekućeg bloka šifrata, kada su u pitanju CBC mod rada i CFB i OFB modovi rada kod kojih je $r = n$, je prethodni blok šifrata. Ako se radi o r bitnim ($r \neq n$) CFB i OFB modovima rada, inicijalni vektor su prethodnih j bita bloka šifrata (gde je $j = n - r$, a n veličina bloka u bitima), na koje se dodaje u preostali sadržaj inicijalnog vektora prilikom šifrovanja datog bloka. Tačnije rečeno, u tom slučaju inicijlani vektor su prethodnih n bita šifrata. Kada je u pitanju CTR mod, sinhronizacioni podatak je celokupna vrednost brojača, tj. vrednost promenljivog dela brojača na koju se dodaje 64-bitni nepredvidivi statički deo brojača.

Ako se problem kriptografske sinhronizacije posmatra kroz objektiv algoritama selektivnog šifrovanja HEVC video toka, može se zaključiti da, kada su u pitanju CBC, CFB i OFB modovi rada, vrednosti inicijalnih vektora (sinhronizacioni podaci) nalaze

se negde u šifrovanim sintaksnim elementima u prethodnom video toku. Sadržaj prethodnog bloka šifrata može ili da bude smešten kontinuirano - ceo blok u jednom segmentu video toka ili pak može biti raspršen i umetnut između delova video toka koji nisu kriptografski obrađeni. Da li će on biti u komadu ili će biti raslojen na različite delove i u različitim tačkama video toka zavisi od primenjenog algoritma selektivnog šifrovanja i sintaksnih elemenata koje on kriptografski obrađuje. Kada je u pitanju CTR mod, sinhronizacioni podatak je ekzaktna vrednost brojača koja nema nikakve veze sa prethodnim blokovima šifrata pa je samim tim i nema u prethodnom video toku.

Ako se, sa druge strane, posmatra slučajni pristup selektivno šifrovanom HEVC video toku, ovakav raspored sinhronizacionih podataka ima značajan uticaj. Ukoliko dekoder kreće operaciju dekodovanja u tački slučajnog pristupa onda je njemu neophodno da raspolaže sinhronizacionim podacima. Dekoder može da otpočne operaciju parsiranja prethodne slike u video toku podataka, kako bi u njoj našao sinhronizacione podatke. Ova operacija zahteva dodatno procesorsko vreme. Štaviše, u slučaju greške (ili gubitka) čak i jednog bita u prethodnom bloku šifrata, algoritam selektivnog šifrovanja na strani dekodera ne bi bio sinhronizovan i samim tim slučajan pristup ne bi bio moguć. Dodatan problem, kada je reč o raspolaganju sinhronizacionim podacima, unose i operacije spajanja video tokova i promene kanala. Kod navedenih operacija prethodni deo video toka, a samim tim i sinhronizacioni podaci, nisu dostupni.

Prethodno navedene činjenice navode na zaključak da je neophodno postojanje mehanizma koji će omogućiti kriptografsku sinhronizaciju u okviru selektivno šifrovanog HEVC video toka, nezavisnu od primenjenog moda rada blokovskog kriptografskog algoritma. Ukoliko je takav mehanizam nezavistan od primenjenog moda rada blokovskog kriptografskog algoritma, automatski je nezavistan i od primenjenog elementarnog blokovskog kriptografskog algoritma.

5. IMPLEMENTACIJA PREDLOŽENOG MEHANIZMA KRIPTOGRAFSKE SINHORNIZACIJE

5.1. Sintaksa i semantika predloženog rešenja

Da bi HEVC dekoder imao mogućnost slučajnog pristupa selektivno šifrovanom HEVC video toku, algoritam selektivnog šifrovanja koji se izvršava unutar dekodera mora biti kriptografski sinhronizovan sa algoritmom selektivnog šifrovanja u enkoderu koji je generisao dati HEVC video tok. Da bi se postigla takva mogućnost, dizajniran je i implementiran originalan i efikasan mehanizam kriptografske sinhronizacije.

Za potrebe definisanja efikasnog mehanizma kriptografske sinhronizacije u algoritmima selektivnog šifrovanja HEVC video toka i realizacije HEVC enkodera i dekodera koji imaju mogućnost slučajnog pristupa selektivno šifrovanom video toku, u ovom radu je definisan novi sintaksni element HEVC standarda. Tačnije, definisana je sintaksa i semantika nove ne-VCL NAL jedinice sa ciljem da se omogući prethodno navedena kriptografska sinhronizacija.

Prema HEVC standardu [5], HEVC video tok bita (engl. *bitstream*) može biti u jednom od dva moguća formata: u formatu niza NAL jedinica ili u formatu niza bajtova. Konceptualno gledano format niza NAL jedinica je više "bazni", elementarni tip formata. Ovaj format se sastoji od sekvence sintaksnih struktura[9] poznatih pod imenom NAL jedinice. Postoji precizno definisano ograničenje koje se primenjuje na redosled dekodiranja (i na sadržaj) NAL jedinica u okviru niza NAL jedinica. Format niza bajtova se pravi od niza NAL jedinica, tako što se NAL jedinice spakuju u sekvencu po redosledu dekodiranja i pre svake NAL jedinice se doda prefiks sa početnim unificiranim kodom prefiksa i nijednom, jednom ili više pratećih vrednosti nula. Format niza NAL jedinica se lako može ekstrahovati iz formata niza bajtova operacijom

[9] Sintaksna struktura je struktura koja sadrži nijedan, jedan ili više sintaksnih elemenata predstavljenih zajedno u video toku u tačno određenom rasporedu.

pretraživanja lokacije unikatnog startnog prefiksa. Standard H.265/HEVC specificira samo ovaj način frejmovanja NAL jedinica u format niza bajtova i bilo koji drugi način frejmovanja je izvan navedenog standarda[9].

Pored toga što specificira format toka bita, HEVC standard takođe specificira i formate slika, tehnike deljenja slika, procese skeniranja i odabiranja odbiraka sirove slike (navedeni elementi standarda definisani su i objašnjeni u poglavlju II ovog rada). HEVC standard[5] ne specificira sam proces kodovanja slike već specificira sintaksu kodirane reprezentacije koja je dizajnirana da omogući visoku sposobnost kompresije za željeni kvalitet video toka. Kodirana reprezentacija video toka sastoji se od sekvence ne-VCL i VCL NAL jedinica koje imaju precizno definisanu sintaksu svojih sintaksnih elemenata[10] i njihovu semantiku.

Za definisanje sintakse elemenata HEVC video toka, HEVC standard koristi sintaksne tabele. Sintaksna tabela predstavlja nadskup sintaksi svih dozvoljenih nizova bita validnog HEVC video toka[5]. U sintaksnoj tabeli pored sintaksnih elemenata mogu se naći i deklaracije koje mogu biti ili sintaksni element sa pridruženim deskriptorom ili izraz koji se koristi kako za specifikaciju uslova za postojanje sintaksnog elementa, tako i sa specifikaciju vrste i količine sintaksnih elemenata. Deklaracije mogu da se grupišu vitičastim zagradama čime se dobija složena deklaracija koja se funkcionalno tretira kao jedna prosta deklaracija. Takođe, u sintaksnoj tabeli se mogu naći i deklaracije kontrole toka (nalik sličnim deklaracijama u programskom jeziku “C”) kojima se određuje tok i uslovi evaluacije određenih deklaracija u zavisnosti od toga da li je uslov tačan ili nije. Moguće kontrole toka su one nalik kontrolama *while, do, if ... else ..., for* koje se sreću u programskom jeziku “C”.

Pored sintaksnih elemenata, deklaracija i kontrola toka, u sintaksnoj tabeli se još mogu naći i sintaksne funkcije i deskriptori sintaksnih elemenata. Povratne vrednosti sintaksnih funkcija se izražavaju u odnosu na vrednost pokazivača na niz bita koji

[10] Sintaksni element je neki element podataka predstavljen u nizu bajta. Svaki sintaksni element se definiše imenom sintaksnog elementa i pridruženim deskriptorom koji definiše metodu njegove kodirane reprezentacije (način njegovog kodovanja u nizu bita).

ukazuje na položaj sledećeg bita koji će biti pročitan procesom dekodiranja iz video toka. U sintaksnim tabelama se mogu pojaviti sledeće sintaksne funkcije:

- *byte_aligned()* - vrednost ove funkcije je jednaka vrednosti TRUE ako je trenutna pozicija pokazivača na niz bita video toka na granici bajtova, tj. sledeći bit u nizu bita je prvi bit u sledećem bajtu. U svakom drugom slučaju vrednost ove funkcije je FALSE.
- *more_data_in_byte_stream()* - ako video tok sadrži još podataka iza tekuće pozicije pokazivača vrednost ove funkcije je TRUE, inače vrednost je FALSE.
- *more_rbsp_data()* - ako nema više podataka u sirovoj sekvenci bajta[11] (engl. *RBSP - Raw Byte Sequence Payload*) vrednost ove funkcije je FALSE. U suprotnom u sirovoj sekvenci bajtova se traži (bit najmanje težine) bit koji je jednak 1. Ako se uzme u obzir pozicija ovog bita koji predstavlja prvi bit sintaksne strukture *rbsp_trailing_bits( )*, primenjuje se sledeće pravilo: ako postoji još podataka pre *rbsp_trailing_bits()* sintaksne strukture, vrednost ove funkcije je TRUE, u suprotnom vrednost je FALSE.
- *more_rbsp_trailing_data()* - ukoliko postoji još podataka u sirovoj sekvenci bajta onda ova funkcija vraća vrednost TRUE, inače vraća vrednost FALSE.
- *next_bits(n)* - obezbeđuje operaciju čitanja sledećih *n* bita za potrebe operacije poređenja vrednosti, bez inkrementiranja vrednosti pokazivača na tekuću poziciju u nizu bita video toka. Pruža uvid u vrednost sledećih *n* bita u nizu bita, gde se vrednost *n* prosleđuje kao argument funkcije. Ako nije u mogućnosti da pročita n bita, ova funkcija vraća vrednost 0.
- *read_bits(n)* - čita sledećih *n* bita iz niza bitova video toka i inkrementira vrednost pokazivača za *n*.

---

[11] RBSP - (*Raw Byte Sequence Payload*) predstavlja sintaksnu strukturu koja predstavlja celobrojni broj bajtova enkapsuliranih u jednu NAL jedinicu. Može biti ili prazna ili da sadrži niz bita podataka koji sadrže sintaksne elemente praćenje RBSP stop bitom (koji ima vredsnost 1) i nijednim ili više bita čija je vrednost 0 (broj nula je dopuna do punog bajta na kraju sirove sekvence).

Kada su u pitanju deskriptori sintaksnih elemenata oni predstavljaju definiciju načina kodovanja datog sintaksnog elementa u nizu bita video toka. Standardom su definisani sledeći deskriptori sintaksnih elemenata:

- ***ae(v)*** - sintaksni element se kodira konteksno adaptivnim koderom entropije;
- ***b(8)*** - bajt koji ima bilo koji raspored niza bitova;
- ***f(n)*** - niz bita sa fiksnim šablonom rasporeda bita koji je predstavljen sa *n* bita napisanih sa leva na desno;
- ***i(n)*** - označena celobrojna vrednost predstavljena sa *n* bita. Kada se u sintaksnoj tabeli umesto *n* nađe vrednost "*v*" broj bitova varira u zavisnosti od veličine drugih sintaksnih elemenata;
- ***se(v)*** - označena celobrojna vrednost sintaksnog elementa kodovana eksponencijalnim Golomb kodom;
- ***st(v)*** - niz karaktera kodiran kao univerzalni skup karaktera u formatu UTF-8;
- ***u(n)*** - neoznačena celobrojna vrednost predstavljena sa *n* bita. Kada se u sintaksnoj tabeli umesto *n* nađe vrednost "*v*" broj bita varira u zavisnosti od veličine drugih sintaksnih elemenata;
- ***ue(v)*** - neoznačena celobrojna vrednost sintaksnog elementa kodovana eksponencijalnim Golomb kodom.

5.1.1. Sintaksa elemenata predloženog rešenja

Specifično proširenje HEVC standarda u ovom radu realizovano je definisanjem nove ne-VCL NAL jedinice. Nova ne-VCL NAL jedinica nazvana je CSPS NAL jedinica (engl. *CSPS - Crypto Synchronization Parameter Set*), tj. skup parametara kriptografske sinhronizacije. Kako bi navedena NAL jedinica mogla biti nedvosmisleno identifikovana u nizu bajtova HEVC sekvence, dodeljen joj je jedinstveni identifikator. Dodeljena joj je vrednost 48 koja je prva slobodna vrednost iz opsega nespecificiranih non-VCL identifikatora, kao što je pokazani u tabeli 1. U tabeli 2 prikazano je proširenje tabele 1 dodavanjem novog reda koji definiše novi tip NAL jedinice.

Za vrednost identifikatora uzeta je prva vrednost iz opsega nespecificiranih jer za njih standard garantuje da neće biti korišćeni u budućim unapređenjima standarda, pa samim tim mogu biti korišćenje za specifične oblasti primene i aplikacije. Takođe,

standard ne specificira proces dekodiranja za nijednu NAL jedinicu iz ovog opsega. Pošto različite aplikacije mogu da koriste navedene vrednosti tipova NAL jedinica za različite namene, posebno se mora obratiti pažnja prilikom dizajna enkodera i dekodera koji, na jednoj strani generišu a na drugoj strani tumače sadržaj navedenih NAL jedinica. Sa druge strane, standard kaže da nemodifikovani dekoderi treba da ignorišu NAL jedinice sa identifikatorima iz ovog opsega, osim prilikom određivanja količine podataka u mernim jedinicama za dekodiranje[5].

Tabela 2. Proširenje tabele 1, ID i značenje novodefinisane CSPS NAL jedinice

ID tipa NAL jedinice	Značenje	Klasa NAL jedinice
.....	.....	.....
48	Skup parametara kriptografske sinhronizacije (CSPS)	ne-VCL
49-63	Nespecifikovani (dostupni za upotrebu)	ne-VCL

Da bi razumeli definiciju sintakse nove, CSPS NAL jedinice, najpre treba prikazati i objasniti opštu sintaksu NAL jedinice. Opšta sintaksa NAL jedinice prikazana je u sintaksnoj tabeli, prikazanoj tabelom 3, koja je izvorno preuzeta iz standarda[5]. Sintaksa zaglavlja NAL jedinice data je u tabeli 4. Takođe, sintaksa zaglavlja NAL jedinice je izvorno preuzeta iz standarda. Opšta sintaksa NAL jedinice i sintaksa zaglavlja NAL jedinice, kod definisanja nove ne-VCL CSPS NAL jedinice, ostaju nepromenjene. Ono što je novo definisano to je sirova sekvenca bajtova (RBSP) za novu NAL jedinicu - CSPS RBSP. *Crypto Synchronization Parameter Set* je sintaksna struktura koja obuhvata sintaksne elemente kojima se definiše skup parametara i vrednosti neophodnih i dovoljnih u procesu kriptografske (re)sinhronizacije. Sintaksa CSPS RBSP strukture data je u tabeli 5. HEVC standard striktno ističe da nijedan sintaksni element koji nije naveden u nekoj sintaksnoj tabeli ne može kasnije da bude prisutan i nizu bita video toka.

Sintaksno gledano, NAL jedinica je specificirana da formatira podatke i obezbeđuje informacije u svom zaglavlju na način koji je prikladan za prenos video podataka putem raznih komunikacionih kanala ali i za njegovo skladištenje na različitim vrstama memorijskih medijuma. Podaci i metapodaci o kompresovanom videu se isključivo nalaze u NAL jedinicama od kojih svaka NAL jedinica ima celobrojni broj bajtova.

NAL jedinica specificira generički format za upotrebu bilo da se video upotrebljava u paketski orijentisanim ili u strimovski orijentisanim sistemima prenosa.

Tabela 3. Opšta sintaksa NAL jedinice

nal_unit(NumBytesInNalUnit) {	**Deskriptor**
nal_unit_header( )	
NumBytesInRbsp = 0	
for(i = 2; i < NumBytesInNalUnit; i++)	
if(**i + 2 < NumBytesInNalUnit && next_bits(24) = = 0x000003) {**	
rbsp_byte[NumBytesInRbsp++]	b(8)
rbsp_byte[NumBytesInRbsp++]	b(8)
i += 2	
emulation_prevention_three_byte /* vrednost 0x03 */	f(8)
} else	
rbsp_byte[NumBytesInRbsp++]	b(8)
}	

Tabela 4. Sintaksa zaglavlja NAL jedinice

nal_unit_header( ) {	**Deskriptor**
forbidden_zero_bit	f(1)
nal_unit_type	u(6)
nuh_layer_id	u(6)
nuh_temporal_id_plus1	u(3)
}	

Tabela 5. Sintaksa CSPS RBSP sintaksne strukture

crypto_synchronization_parameter_set_rbsp( ) {	**Deskriptor**
csps_parameter_set_id	ue(v)
csps_crypto_parameter_ctx_id	ue(v)
csps_len_of_crypto_synh_data	ue(v)
for(i = 1; i < =csps_len_of_crypto_synh_data; i++)	
csps_crypto_synh_data[i]	b(8)
csps_extension_flag	u(1)
if(csps_extension_flag)	
while(more_rbsp_data( ))	
csps_extension_data_flag	u(1)
rbsp_trailing_bits( )	
}	

5.1.2. Semantika elemenata ponuđenog rešenja

Sintaksa u HEVC standardu predstavlja skup pravila po kojima se sintaksni elementi sklapaju u sintaksne strukture i skup pravila po kojima se sintaksne strukture spajaju tako da čine NAL jedinice. Semantika u HEVC standardu, sa druge strane, definiše opsege mogućih vrednosti, ograničenja i uslove koji se nameću sintaksnim elementima. Tačnije, semantika određuje značenje i namenu sintaksnog elementa, određuje opseg vrednosti koje on može da dobije kao i uslove i ograničenja koje mora da zadovolji.

Sintaksni elementi opšte NAL jedinice imaju sledeću semantiku:

- ***NumBytesInNalUnit*** - određuje veličinu NAL jedinice u bajtima. Ova vrednost je potrebna prilikom dekodiranja NAL jedinice. Da bi se odredila veličina NAL jedinice neophodno je postojanje nekog oblika demarkacije (definisanja granice između) dve NAL jedinice.
- ***rbsp_byte[i]*** - predstavlja *i-ti* bajt neke sirove sekvence bajtova (nekog RBSP). Sirova sekvenca bajtova predstavlja uređeni niz bitova podataka koji je uređen prema sledećim pravilima:
  - ako je uređeni niz bitova prazan onda je i sirova sekvenca bajtova prazna;
  - u suprotnom, prvi bajt sirove sekvence bajtova sadrži osam bita najviše težine niza bita podataka;
  - sledeći bajt RBSP sadrži sledećih osam bita niza bita podataka, i tako dalje sve dok ostaje manje od osam bita niza bita podataka;
  - nakon kraja niza bita podataka, nalazi se sintaksna struktura *rbsp_trailing_bits()*. Ova struktura sadrži preostalih ne više od sedam bitova niza podataka koje prati *rbsp_stop_one_bit* čija je vrednsot jednaka 1 a sledi ga potreban broj 0.
  - u nekin slučajevima, nakon *rbsp_trailing_bits( )* mogu se naći jedan ili više ***cabac_zero_word*** 16-bitnih sintaksnih elemenata koji imaju vrednost 0x0000.

  Sintaksne strukture koje imaju prethodno navedene osobine sirove sekvence bajtova (RBSP) u sintaksnim tabelama se označavaju korišćenjem sufiksa "***_rbsp***". Navedene strukture se prenose u okviru sadržaja NAL jedinica kao sadržaj niza bajtova označenog sintaksnim elementom ***rbsp_byte[i]***.

- ***emulation*_prevention_three_byte** je bajtovska veličina sa fiksnom vrednošću ***0x03***. Kada se ova vrednost nađe unutar NAL jedinice proces dekodovanja treba jednostavno da je odbaci.

NAL jedinica treba da bude kreirana prema sledećim ograničenjima:

- poslednji bajt NAL jedinice ne sme da bude jednak ***0x00***;
- sekvence bajtova ***0x000000***, ***0x000001*** i ***0x000002*** ne smeju se pojaviti na bilo kojoj bajtovski poravnatoj poziciji;
- bilo koja od sledećih sekvenci bajtova koje počinju sekvencom ***0x000003***, osim sekvenci: ***0x00000300***, ***0x00000301***, ***0x00000302***, ***0x00000303***, ne smeju se pojaviti na bilo kojoj bajtovski poravnatoj poziciji.

Sintaksni elementi zaglavlja NAL jedinice imaju sledeću semantiku:

- ***forbiden_zero_bit*** - je jednak bitskoj vrednosti 0.
- ***nal_unit_type*** - specificira tip sintaksne strukture predstavljen sirovom strukturom bajtova (RBSP) koja je sadržana unutar NAL jedinice (tabele 1 i 2).
- ***nuh_layer_id*** - specificira identifikator sloja kome pripada data VCL NAL jedinica ili identifikator sloja na koji se primenjuje data ne-VCL NAL jedinice. Vrednost ovog parametra mora biti u opsegu 0 do 62, uključujući i ove vrednosti. Vrednost 63 je ostavljena da bude specificirana u budućim nadogradnjama standarda.
- ***nuh_temporal_id_plus1*** **-** specificira vremenski identifikator NAL jedinice. Njegova vrednost ne sme biti jednaka 0.

Novodefinisana sintaksna struktura koja sadrži sintaksne elemente za kriptografsku sinhronizaciju ima sledeći semantiku[55]:

- ***csps_parameter_set_id*** - identifikuje CSPS skup parametara za potrebe referenciranja od strane drugog sintaksnog elementa ili od strane algoritma selektivnog šifrovanja na prijemnoj strani (strana dekodera). Pomenuta identifikacija ima za cilj identifikovanje tačke, tj. pozicije, u video toku podataka i identifikovanje skupa parametara koji su učestvovali u poslednjoj kriptografskoj (re)sinhronizaciji. Vrednost ovog parametra predstavljen je celobrojnim brojačem koji se, prilikom kreiranja selektivno šifrovanog HEVC video toka, inkrementira za jedan pri svakom sledećem kreiranju CSPS parametara. Kada vrednost dođe do gornje granice onda se ona vraća na 0 i postupak brojanja se nastavlja.

- ***csps_crypto_parameter_ctx_id*** - identifikuje kontekst kriptografske sinhronizacije na strani dekodera kome su sinhronizacioni podaci namenjeni. Navedeni kontekst predstavlja skup dva identifikatora kojima se primenjeni elementi identifikuju na sledeći način: prvi identifikator ukazuje na izvor selektivno šifrovanog video toka dok drugi identifikator ukazuje na primenjeni algoritam selektivnog šifrovanja. Identifikator izvora, pored što nedvosmisleno identifikuje izvor video toka koristi se i za identifikaciju tajnog ključa simetričnog kriptografskog algoritma[12]. Identifikatorom primenjenog algoritma selektivnog šifrovanja indirektno su definisani sintaksni elementi koji su kriptografski obrađeni, primenjeni simetrični blokovski kriptografski algoritam i kriptografski mod rada u kome blokovski kriptografski algoritam radi. Ovaj parametar se koristi za odvajanje i razlikovanje izvora kodiranih i selektivno šifrovanih video zapisana na strani dekodera. Ovako definisan identifikator konteksta kriptografske sinhronizacije omogućava da jedan izvor video toka koristi dva ili više algoritama selektivnog šifrovanja.

  Mogućnost nedvosmislenog razlikovanja izvora selektivno šifrovanog video toka podatka je posebno važna prilikom operacije spajanja video tokova (tj. operacije promene kanala, promene izvora selektivno šifrovanog video toka). Ova vrednost mora biti jedinstvena iz razloga jer mora postojati jedinstven i nedvosmislen mehanizam razlikovanja izvora selektivno šifrovanog video toka.

- ***csps_len_of_crypto_synh_data*** - je celobrojna vrednost broja bajtova u nizu kriptografskih sinhronizacionih podataka koje slede unutar sirove sekvence bajtova. Ova vrednost ne sme biti jednaka 0 jer ukoliko nema sinhronizacionih podataka onda nema ni smisla da cela CSPS NAL jedinica postoji u video toku. Veličina sinhronizacionih podataka (jednaka veličini inicijalizacionog vektora) je najčešće jednaka 16 bajta, jer se najčešće koristi AES kriptografski algoritam u CBC i CFB modu rada. Ova vrednost može biti i upola manja ako bi neki algoritam selektivnog šifrovanja koristio blokovski kriptografski algoritam u CTR modu rada. Tada je, za potrebe kriptografske sinhronizacije, potrebno i dovoljno preneti 64-bitni promenljivi

[12] Uvedena je pretpostavka da je tajni simetrični ključ prethodno rezmenjen između prijemne i predajne strane na naki od dobro poznatih načina razmene kriptografskih ključeva.

deo brojača. Preostalih 64-bita nepromenljivog dela brojača se može unapred razmeniti između prijemne i predajne strane.

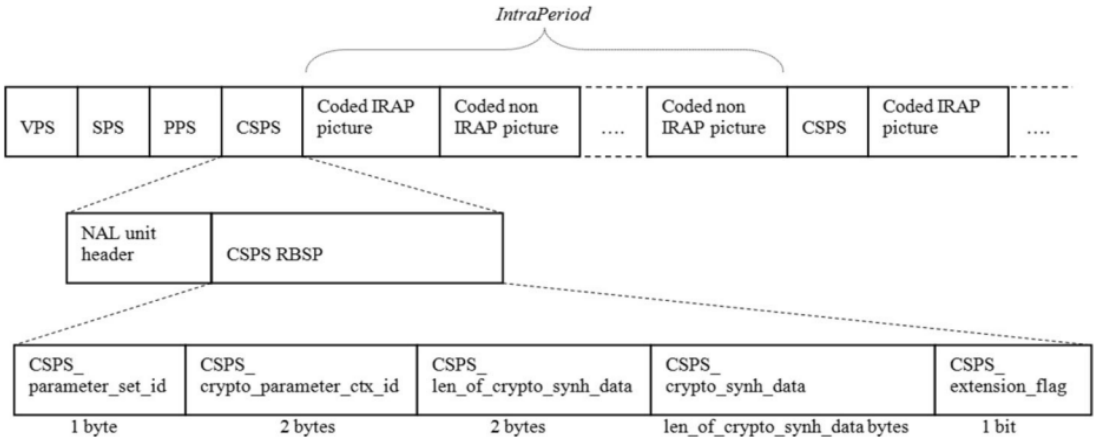
- ***csps_crypto_synh_data[i]*** - predstavlja i-ti bajt u sirovoj sekvenci bajtova podataka za kriptografsku sinhronizaciju. Sirova sekvenca bajtova je definisana na sledeći način: prvi bajt *csps_crypto_synh_data* parametra sadrži osam bita kriptografskih sinhronizacionih podataka najviše težine. Sledeći bajt *csps_crypto_synh_data* parametra sadrži sledećih osam bita kriptografskih sinhronizacionih podataka. Svaki sledeći bajt sadrži sledećih osam bita sinhronizacionih podataka, sve do poslednjeg bajta koji sadrži osam bita kriptografskih sinhronizacionih podataka najniže težine. Ovde je kao pretpostavka uzeta činjenica da je veličina kriptografskih sinhronizacionih podataka celobrojna veličina iskazana u broju bajtova.
- ***csps_extension_flag*** - ako je ova vrednost jednaka bitu 0, to znači da vrednost sintaksnog elementa csps_extension_data_flag nije prisutna u sirovom nizu bajtova RBSP CSPS. Ova vrednost mora biti jednaka 0 u video toku podataka koji je u skladu sa standardnim HEVC dekoderom, dok je vrednost 1 rezervisana za buduću upotrebu. Ovaj princip definisanja sintakse i semantike sintaksnih elemenata se koristi u ovom radu kako bi bio kompatibilan sa definicijama drugih sintaksnih elemenata. Prema najnovijoj definiciji HEVC standarda, standardni dekoderi mogu ignorisati sve vrednosti koje prate vrednost 1 ovog parametra u CSPS sirovoj sekvenci bajtova.
- ***csps_extension_data_flag*** - može imati bilo koju vrednost. Njegovo prisustvo i vrednosti ne utiču na uskalđenost našeg dekodera sa HEVC standardnim dekoderom koji će svakako da ignoriše sve vrednosti ovog parametra.

5.2. Pozicija CSPS NAL jedinice u video toku

Nakon što je definisana sintaksa i semantika nove ne-VCL NAL jedinice, sledeći korak je definisanje njihovog položaja u selektivno šifrovanom HEVC video toku. Izbor mesta za pozicioniranje nove NAL jedinice u HEVC video toku predstavlja kompromis između različitih zahteva koji moraju biti u skladu sa ograničenjima vezanim za raspored i položaj NAL jedinica, onako kako je to definisano u standardu[5]. Glavni zahtev koji se postavlja pri definisanju njenog položaja u HEVC video toku je to da on treba da omogući lako korišćenje za potrebe kriptografske (re)sinhronizacije algoritma

selektivnog šifrovanja pri implementaciji mehanizma slučajnog pristupa selektivno šifrovanom HEVC video toku.

Ako se u obzir uzme namena nove ne-VCL CSPS NAL jedinice, najlogičnije je da ona bude pozicionirana unutar IRAP jedinice pristupa neposredno pre VCL jedinice koja sadrži intra kodovanu sliku. Redosled NAL jedinica u okviru IRAP jedinice pristupa, bilo da se ona nalazi na početku ili nakon poslednje VCL NAL jedinice prethodno kodovane slike, može biti onakav kako je prikazano na slici 22. Ovako raspoređena ne-VCL CSPS NAL jedinica koja prethodi prvoj VCL NAL jedinici i koja nije praćena poslednjom VCL NAL jedinicom kodirane slike unutar IRAP jedinice pristupa, zadovoljava sva ograničenja vezana za raspored i položaj NAL jedinica unutar video toka koji je kompatibilan sa HEVC standardom.



Slika 22. Opšta struktura HEVC video toka, sa umetnutom CSPS NAL jedinicom

5.3. Formalna specifikacija efikasnosti ponuđenog rešenja

Dodavanje nove ne-VCL NAL jedinice, sa prethodno definisanom sintaksom i semantikom, u selektivno šifrovani HEVC video tok povećava broj bajtova upisanih u datoteku koja sadrži selektivno šifrovani HEVC video, tj. povećava broj bajtova u selektivno šifrovanom HEVC video toku. Ako sa $\boldsymbol{N_{SE}}$ označimo broj bajtova upisanih u datoteku koja sadrži selektivno šifrovani HEVC video sa umetnutom CSPS NAL jedinicom a sa $\boldsymbol{N_P}$ označimo broj bajtova iste video sekvence upisanih u datoteku koja sadrži otvoreni video (bez selektivnog šifrovanja i bez umetanja dodatnih podataka), onda se razlika između navedene vrednosti broja bajtova, označena sa $\boldsymbol{\Delta_B}$, može izračunati prema formuli (22):

$$\Delta_{B} = N_{SE} - N_{P} \quad (22)$$

Sa druge strane, prema karakteristikama ponuđenog rešenja efikasnog HEVC kripto enkodera i dekodera sa mogućnošću slučajnog pristupa selektivno šifrovanom video toku, vrednost parametra $\mathbf{\Delta_B}$ ne zavisi od broja bajtova u video toku. To je rezultat činjenice da predloženi i dostupni algoritmi selektivnog šifrovanja HEVC video toka ne unose dodatne bajtove niti bitove u selektivno šifrovani HEVC video tok. Vrednost parametra $\mathbf{\Delta_B}$, broj dodatnih bajtova koje predloženo rešenje efikasnog mehanizma kriptografske sinhronizacije unosi u selektivno šifrovani HEVC video tok, zavisi od sledećih vrednosti: od ukupnog broja slika (frejmova) u video sekvenci ($\boldsymbol{N_f}$), od vrednosti *IntraPeriod*[13] parametra ($\boldsymbol{T_{IP}}$) i od veličine CSPS NAL jedinice iskazane u bajtima ($\boldsymbol{N_{CSPS}}$). Broj dodatih bajtova direktno je proporcionalan veličini jedinice skupa sinhronizacionih parametara i ukupnom broju slika u video sekvenci, a obrnuto proporcionalan vrednosti *IntraPeriod* parametra. Vrednost parmetra $\mathbf{\Delta_B}$ može se izračunati prema formuli (23):

$$\Delta_{B} = \left\lceil \frac{N_f}{T_{IP}} \right\rceil * N_{CSPS} \quad (23)$$

Kako bi analizirali uticaj dodavanja ne-VCL CSPS NAL jedinica na povećanje broja bajtova u selektivno šifrovanom video toku možemo da izračunamo dodatni broj bajtova u selektivno šifrovanom HEVC video toku sa umetnutim CSPS parametrima. Uvodi se parametar $\mathbf{\Delta_P}$ koji se koristi da procentualno izrazi broj dodatih bajtova u selektivno šifrovanom HEVC video toku u odnosu na nešifrovan HEVC video tok. Vrednost parametra $\mathbf{\Delta_P}$ zavisi od ukupnog broja bajtova CSPS NAL jedinica dodatih u selektivno šifrovani HEVC video tok i od ukupnog broja bajtova u selektivno šifrovanom HEVC video toku i može se izračunati po formuli (24):

$$\Delta_{P} = \frac{100 * \Delta_B}{N_{SE}} \quad (24)$$

Ukupan broj bajtova koji se upisuju u fajl selektivno šifrovanog HEVC video toka sa dodatim ne-VCL CSPS NAL jedinicama ($\boldsymbol{N_{SE}}$) može se izračunati množenjem ukupnog broja slika (frejmova) i video toku ($\boldsymbol{N_f}$) srednjom vrednošću veličine jedne slike (frejma) ($\boldsymbol{S_f}$) uzimajući u obzir i veličine VCL i ne-VCL jedinica (formula 25):

[13] IntraPeriod parametar definiše broj slika između dve susedne IRAP slike

$$N_{SE} = N_f * S_f \quad (25)$$

Na osnovu formula 23, 24 i 25 može se zaključiti da se vrednost parametra $\boldsymbol{\Delta_P}$ može izračunati po formuli (formula 26):

$$\Delta_P = \frac{100 * N_{CSPS}}{S_f * T_{IP}} \quad (26)$$

Ako se dalje razmotre sledeće činjenice:

- ponuđeno rešenje može (ili treba) da pruža mogućnost realizacije i implementacije kriptografske (re)sinhronizacije svake sekunde, tako vrednost parametra *IntraPeriod* ($\boldsymbol{T_{IP}}$) može da se kreće (i najčešće se kreće) u opsegu od 30 do 60 frejmova;
- sa trenutno dostupnim i najčešće primenjivanih simetričnim blokovskim kriptografskim algoritmima veličina kriptografskih sinhronizacionih parametara zajedno sa potrebnim metapodacima i identifikatorima iznosi maksimalno 30 bajta (+/- jedan bajt),

može se zaključiti da je vrednost parametra $\boldsymbol{\Delta_P}$ približno jednako:

$$\Delta_P \approx \frac{100}{S_f} \quad (27)$$

Iz formule 27 može se zaključiti da se vrednost parametra $\boldsymbol{\Delta_P}$ smanjuje kada se srednja vrednost veličine slike (frejma) povećava. Povećanje rezolucije videa za sobom donosi i povećanje srednje vrednosti veličine slike. Prema tome se može zaključiti da je u slučaju video sadržaja sa većom rezolucijom procentualno izražen broj dodatih bajtova, potrebnih za kriptografsku (re)sinhronizaciju, manji.

5.4. Implementacija ponuđenog rešenja kriptografske sinhronizacije

Za potrebe implementacije predajne strane (enkodera) predloženog efikasnog mehanizma kriptografske sinhronizacije u algoritmima selektivnog šifrovanja, korišćena je referentna implementacija HEVC enkodera, HEVC referentni model (HM) verzija 15.0[56]. Sa ciljem određivanja efikasnosti ponuđenog rešenja prebrojavanjem bajtova dodatih u selektivno šifrovani HEVC video tok, najpre je skup test video sekvenci enkodovan bez primene algoritma selektivnog šifrovanja i bez ubacivanja dodatnih podataka za kriptografsku sinhronizaciju. Ovaj skup video sekvenci se u daljem delu rada naziva otvoreni (ili nešifrovani) video tokovi i generisani su korišćenjem nemodifikovane verzije enkodera iz HEVC referentnog modela verzije v15.0. Nakon

toga, zadržavajući iste uslove izvršavanja, enkodovan je isti skup test sekvenci primenom modifikovane referentne implementacije HEVC enkodera, HEVC referentnog modela v15.0. Referentni HM enkoder se koristi uglavnom da obezbedi opštu referentnu implementaciju HEVC enkodera i nije namenjen da bude primer realnog enkodera koji može da radi i realnom vremenu. Za enkodovanje test sekvence od nekih desetak sekundi potrebno je u proseku negde oko 20 časova [57]. Referentna implementacija HEVC enkodera realizovana je u C++ programskom jeziku.

U ovom radu, modifikacija referentne implementacije HEVC enkodera sadrži implementaciju dva različita algoritma selektivnog šifrovanja. Dva različita algoritma selektivnog šifrovanja implementirana su sa ciljem pokazivanja činjenice i dokazivanje polazne hipoteze da je ponuđeno rešenje nezavisno od primenjenog algoritma selektivnog šifrovananja. Za potrebe navedene modifikacije implementirani su sledeći algoritmi: algoritam autora Z. Shahid-a i W. Puecha[31] i algoritam autora M. Ouamri i K. M. Faraoun[39]. Pored implementacije algoritama selektivnog šifrovanja implementiran je i ponuđeni efikasni mehanizam kriptografske sinhronizacije tako što su podaci neophodni za kriptografsku (re)sinhronizaciju ubacivani u novo definisane sintaksne jedinice, CSPS NAL jedinice, i dodati u HEVC video tok na lokacije koje su prethodno definisane i opisane. Ovako dobijeni HEVC video tokovi se u daljem radu nazivaju selektivno šifrovani HEVC video tokovi sa mogućnošću slučajnog pristupa. Upoređivanjem veličina otvorenih i selektivno šifrovanih HEVC video tokova, iskazanih u broju bajtova, moguće je odrediti uticaj dodavanja kriptografskih sinhronizacionih podataka u selektivno šifrovani HEVC video tok na povećanje broja bajtova u video toku.

Za potrebe dekodiranja selektivno šifrovanog HEVC video toka nije korišćen referentni dekoder jer on nije u mogućnosti da radi u realnom vremenu i da istovremeno prikazuje dekodovani video. Celokupna kompleksnost HEVC dekodera nije nimalo veća od dekodera u prethodnim standardima kompresije videa (npr. kod H.264/AVC), što dekodovanje HEVC video toka čini veoma efikasnim u softverskim dekoderima na postojećem hardveru[57].

Na prijemnoj strani, strani dekodera, implementiran je modifikovani softverski HEVC dekoder baziran na softverskoj biblioteci ***libde265*** (verzija 1.0.2), koja predstavlja implementaciju H.265/HEVC video kodeka otvorenog koda. Navedena

biblioteka je napisana u programskom jeziku “C“, i ima čist i intuitivan API tako da se lako može koristiti i jednostavno integrisati u druga softverska rešenja. Ova biblioteka je sastavni deo sledećih aplikacija, video kodeka i video plejera dostupnih na Internetu: *VLC player*, *Windows DirectShow filters*, *ffmpeg decoder* i *libde265.js JavaScript decoder*[58].

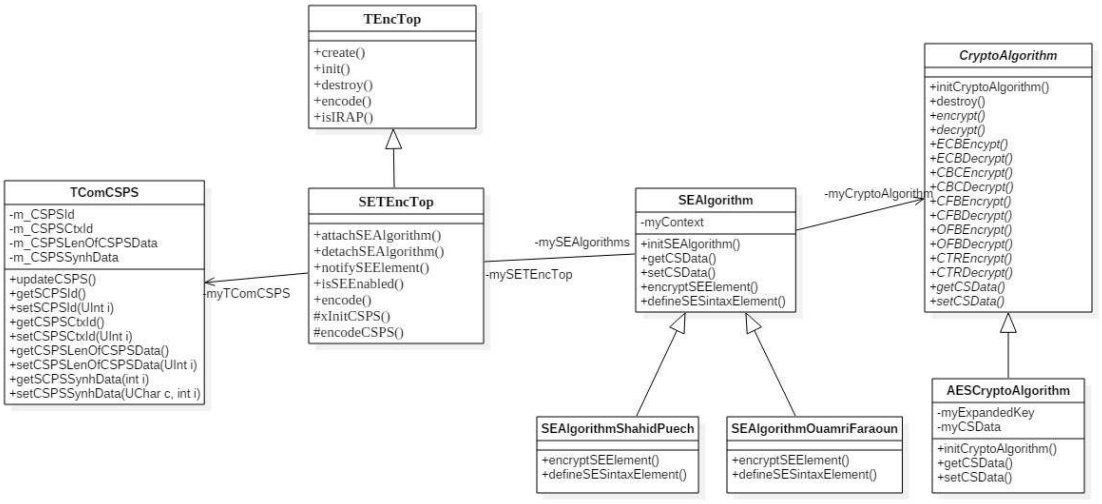
Dekodovani video se prikazuje uživo, u realnom vremenu, paralelno sa dešifrovanjem i dekodovanjem upotrebom demo plejera (***dec265***). Demo plejer je sastavni deo implementacije H.265/HEVC dekodera i predstavlja jednostavan plejer koji koristi modifikovani H.265/HEVC dekoder kao izvor video toka koji se prikazuje. Modifikacija dekodera se svodi na njegovo programsko “upoznavanje” sa novododatom CSPS NAL jedinicom i njenom sintaksom i semantikom. Tačnije, modifikovani dekoder ne odbacuje i ne zanemaruje novododatu NAL jedinicu, već podatke koja ona nosi u sebi, ako je potrebno, koristi da izvrši izbor algoritma selektivnog šifrovanja i/ili njegovu kriptografsku (re)sinhronizaciju. Detalji implementacije modifikovanog dekodera dati su u posebnom podpoglavlju koji sledi.

5.4.1. Modifikacija na strani enkodera

Kako je prethodno rečeno, referentni HEVC enkoder je implementiran u “C++” programskom jeziku, pa je, prema tome, za njegovu modifikaciju korišćen isti programski jezik. Modifikacija referentnog enkodera, proširena dodatim funkcionalnostima strukturno je prikazana dijagramom klasa na slici 23. Na navedenom dijagramu prikazane su klase, atributi i operacije kao i relacije između klasa. Tačnije prikazana je arhitektura proširenja referentnog enkodera kroz prikaz njegovih sastavnih elemenata i njihovih međusobnih veza i odnosa. Ovim je predstavljen statički pogled na dizajn proširenja referentnog HEVC enkodera.

Klasa ***TEncTop*** je deo originalnog referentnog HEVC enkodera i ona predstavlja njegovu centralnu klasu ali i tačku u kojoj se ponuđeno proširenje strukturno nadovezuje na referentni enkoder. Ostale klase na dijagramu sa slike 23 predstavljaju proširenje standardnog referentnog enkodera čija je namena implementacija ponuđenog mehanizma kriptografske sinhronizacije. Iz klase ***TEncTop*** izvedena je klasa ***SETEncTop*** koja predstavlja centralnu klasu referentnog HEVC enkodera sa funkcionalnostima algoritama selektivnog šifrovanja i upravljanja parametrima

kriptografske sinhronizacije. Proširenje je dizajnirano u formi *Observer* projektnog obrasca, u kome jedan objekat (subjekat), održava listu zavisnih objekata (posmatrača) i automatski ih obaveštava o nekoj promeni svog stanja i to najčešće pozivanjem neke od njihovih metoda[59]. U ponuđenom dizajnu klasa ***SETEncTop*** dobija ulogu subjekta za čije su promene i sadržaj zainteresovani posmatrači - algoritmi selektivnog šifrovanja. Tačnije, u ponuđenom dizajnu promenu stanja u klasi enkodera predstavlja pojavljivanje i proces enkodovanja sintaksnog elementa koji je od interesa nekom od algoritama selektivnog šifrovanja. Klasom ***SEAlgorithm*** predstavljeni su posmatrači - algoritmi selektivnog šifrovanja koji definišu specifične sintaksne elemente koji se kriptografski obrađuju kao i konkretan kriptografski algoritam kojim se ta operacija realizuje. Specifičnosti svakog ponaosob algoritma selektivnog šifrovanja su dalje generalizovane izvedenim klasama ***SEAlgorithmShahidPuech*** i ***SEAlgorithmOuamriFaraoun***. Svaka od izvedenih klasa algoritma selektivnog šifrovanja zasebno definiše sintaksni element koji će biti šifrovan i implementira specifičan način šifrovanja definisanog sintaksnog elementa. Sa definisanim sintaksnim elementom koji treba šifrovati klasa ***SETEncTop*** se upoznaje prilikom prijavljivanja posmatrača subjektu pozivom metode *attachSEAlgorithm()*.

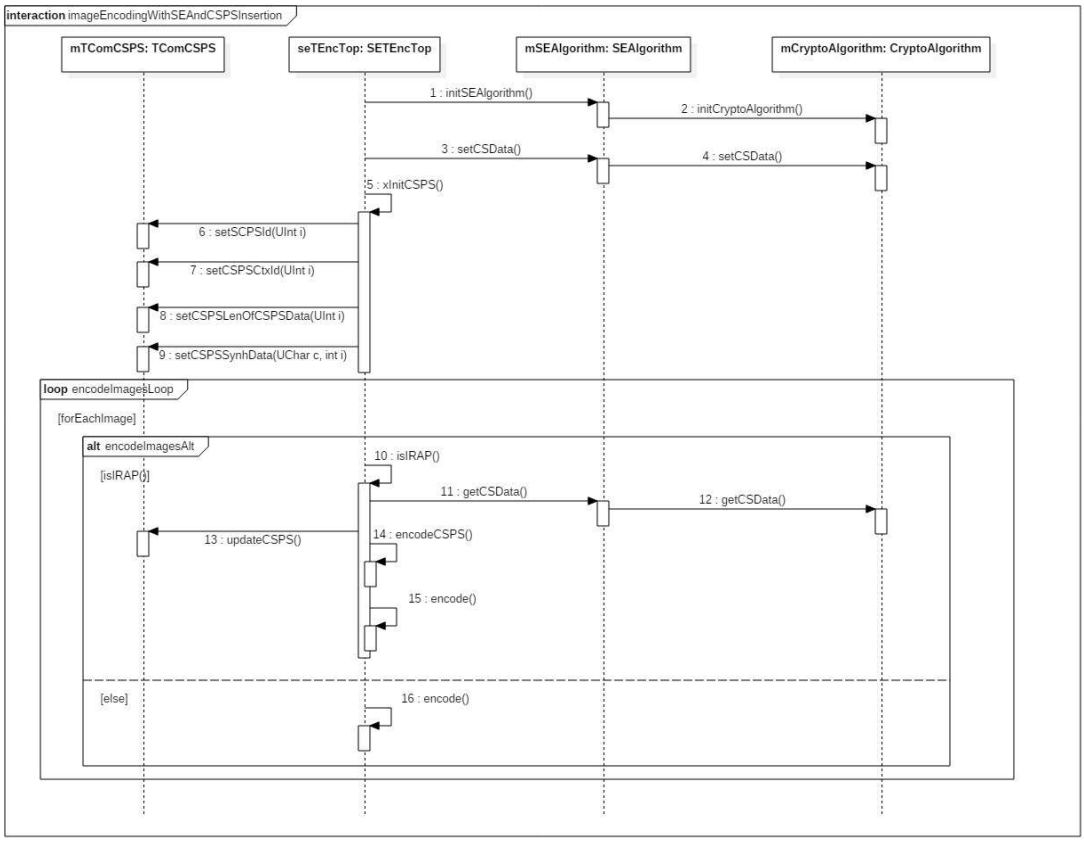


Slika 23. Arhitektura modifikacije referentnog HEVC enkodera - dijagram klasa

Apstraktna klasa ***CryptoAlgorithm*** definiše apstrakciju konkretnog kriptografskog algoritma (i njegov moda rada) kojim se vrši šifrovanje izabranog sintaksnog elementa. Konkretna implementacija apstrakcije kriptografskog algoritma, u ovom slučaju, je

implementacija AES kriptografskog algoritma predstavljenog klasom ***AESCryptoAlgorithm***.

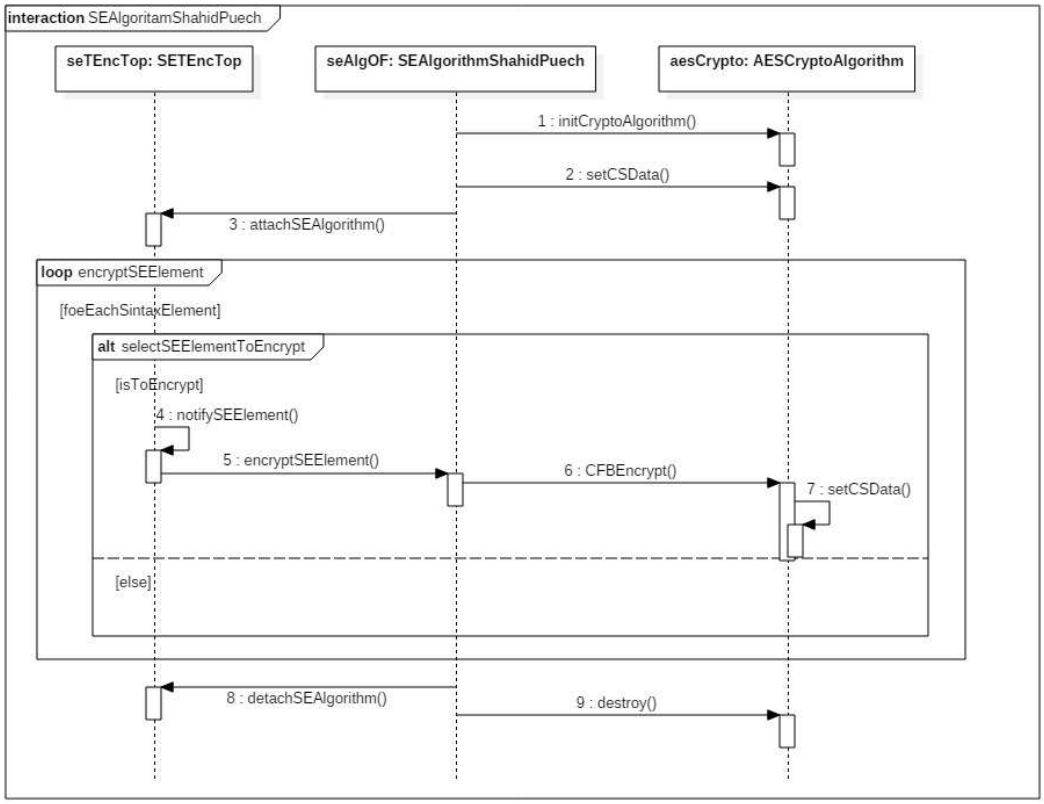
Struktura i sastavni elementi novodefinisane CSPS NAL jedinice predstavljeni su klasom ***TComCSPS***. Objekat navedene klase instancira, inicijalizuje i održava konzistentnim sinhronizacione podatke i obezbeđuje potrebne podatke enkoderu koji, između ostalog, upravlja i algoritmom selektivnog šifrovanja. Trenutni sadržaj elemenata ove klase se, u predviđenom trenutku, direktno enkodira i mapira u sadržaj CSPS NAL jedinice.



Slika 24. Dijagram sekvenci procesa enkodovanja video sekvence

Na slici 24 prikazan je dijagram sekvenci procesa enkodovanja video sekvence. Na početku procesa vrši se inicijalizacija algoritma selektivnog šifrovanja i inicijalizacija početnih vrednosti parametara kriptografske sinhronizacije. U toku procesa enkodovanja video sekvence vrši se enkodovanje slika prema definisanoj šemi i prema određenoj vrednosti *IntraPeriod* parametra. Kompresija svake od slika obuhvata i selektivno šifrovanje definisanih sintaksnih elemenata. Ako sledeća u nizu slika treba biti intra kodovana, vrši se enkodovanje trenutnih vrednosti parametara kriptografske

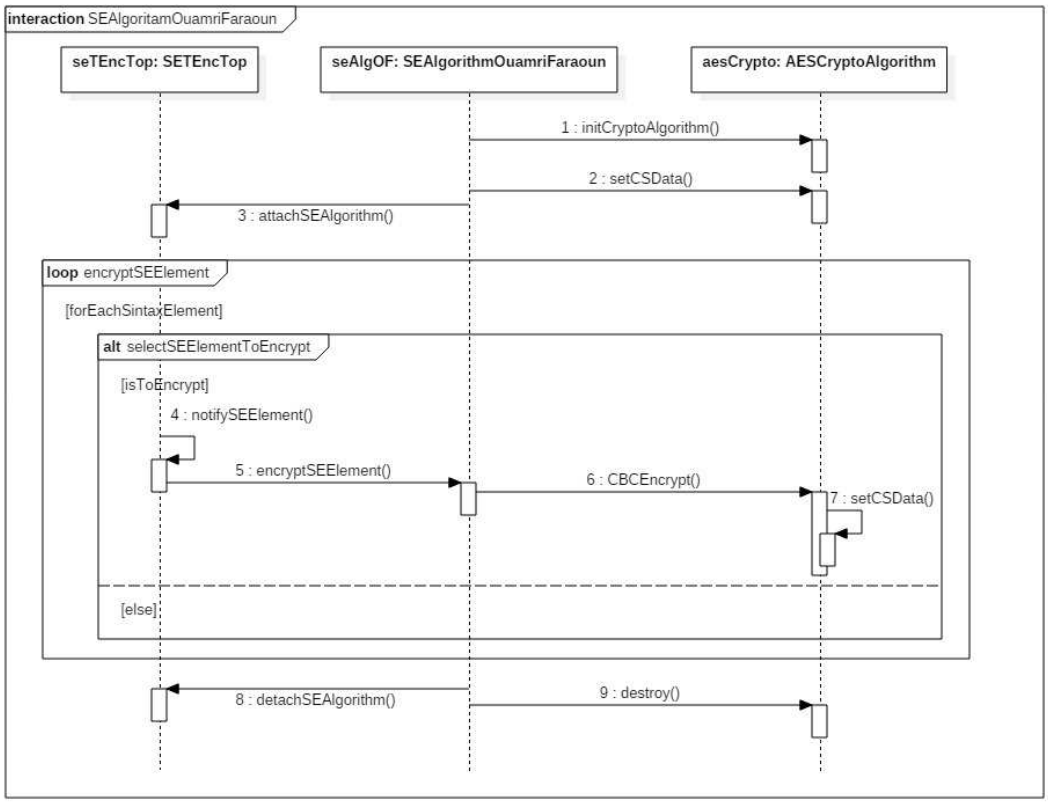
sinhronizacije u CSPS NAL jedinicu i tako enkodovana CSPS NAL jedinica se smešta u HEVC binarni niz neposredno pre intra kodovane IRAP slike. Ukoliko sledeća u nizu slika spada u inter kodovane slike vrši se njeno enkodovanje (kompresija) zajedno sa selektivnim šifrovanjem sintaksnih elemenata koji su definisani algoritmom selektivnog šifrovanja.



Slika 25. Dijagram sekvenci procesa enkodovanja (kompresije) slike, zajedno sa selektivnim šifrovanjem definisanih sintaksnih elemenata, primenom algoritma selektivnog šifrovanja autora Z. Shahid-a i W. Puecha

Proces enkodovanja (kompresije) slike, zajedno sa selektivnim šifrovanjem definisanih sintaksnih elemenata, primenom algoritma selektivnom šifrovanja autora Z. Shahid-a i W. Puecha prikazan je dijagramom sekvenci na slici 25. Na slici 26 prikazan je dijagram sekvenci ekvivalentnog procesa u kome se kao algoritam selektivnog šifrovanja koristi algoritam autora M. Ouamri i K. M. Faraoun. U oba slučaja, nakon što je izvršena inicijalizacija kriptografskog algoritma i sinhronizacionih parametara vrši se prijavljivanje posmatrača (algoritam selektivnog šifrovanja) subjektu (enkoder sa mogućnošću selektivnog šifrovanja) pri čemu se definišu i prijavljuju sintaksni elementi za koje se zahteva i očekuje da budu šifrovani. Prilikom obrade sintaksnih elemenata,

enkoder kada naiđe na očekivani (traženi) sintaksni element, obaveštava registrovani algoritam selektivnog šifrovanja i vrši se šifrovanje sintaksnog elementa izabranim kriptografskim algoritmom u definisanom modu rada. Posle šifrovanja sintaksnih elemenata, vrši se ažuriranje sadržaja sinhronizacionih podataka (poziv metode *setCSData()*) kako bi bili ispravni i konzistentni. Ostali sintaksni elementi ostaju nešifrovani i tako se upisuju u HEVC binarni tok.



Slika 26. Dijagram sekvenci procesa enkodovanja (kompresije) slike, zajedno sa selektivnim šifrovanjem definisanih sintaksnih elemenata, primenom algoritma selektivnom šifrovanja autora M. Ouamri i K. M. Faraoun

Nakon što su svi sintaksni elementi kompresovani, algoritam selektivnog šifrovanja se odjavljuje od subjekta i uništava kontekst trenutnog izvršavanja simetričnog kriptografskog algoritma. Ovakav pristup implementaciji pruža mogućnost naizmeničnog korišćenja više različitih algoritama selektivnog šifrovanja nad istim HEVC video tokom.

5.4.2. Modifikacija na strani dekodera

Na strani dekodera izvršena je modifikacija softverske biblioteke otvorenog koda ***libde265***. Modifikacija je realizovana u programskom jeziku "C" i, ukratko rečeno, sastoji se od upoznavanja softverskog HEVC dekodera sa postojanjem još jednog tipa ne-VCL NAL jedinice čija je namena da nosi kriptografske sinhronizacione podatke i omogući operaciju slučajnog pristupa selektivno šifrovanom HEVC video toku.

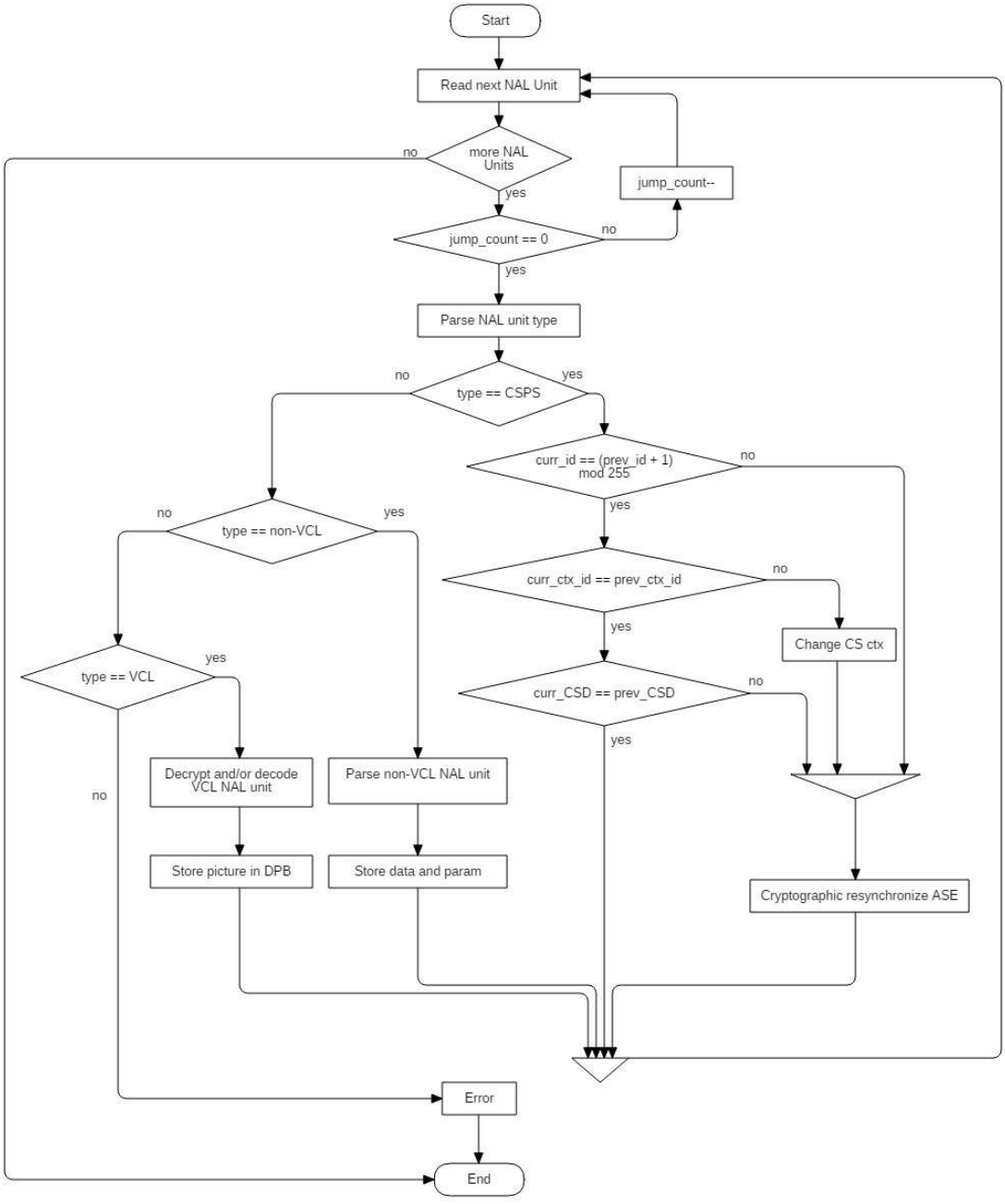
Nakon modifikacije, pomenuti softverski dekoder može i dalje da dekodira i prikazuje HEVC video koji nije selektivno šifrovan. Ukoliko HEVC video tok sadrži CSPS NAL jedinicu, onda se radi o selektivno šifrovanom HEVC video toku. Sa selektivno šifrovanim HEVC video tokom koji je usaglašen po formatu, postoje dve moguća postupka pri dekodiranju:

- Prva mogućnost je da, ukoliko HEVC dekoder ne prepoznaje implementaciju primenjenog algoritma selektivnog šifrovanja, prikaže video tok u vizuelno degradiranom obliku;
- Druga mogućnost podrazumeva da HEVC dekoder prepoznaje implementaciju primenjenog algoritma selektivnog šifrovanja. U tom slučaju, modifikovani HEVC dekoder omogućava operaciju slučajnog pristupa selektivno šifrovanom HEVC video toku i operaciju promene izvora selektivno šifrovanog HEVC video toka.

Ukoliko se radi sa selektivno šifrovanim HEVC video tokom koji nije usaglašen po formatu, navedena modifikacija prijavljuje grešku u radu i obustavlja dalji proces dekodovanja video podataka.

Procedura dekodovanja selektivno šifrovanog HEVC video toka, modifikovanim HEVC dekoderom, prikazana je dijagramom toka na slici 27. Sam proces dekodiranja HEVC sekvence bita realizuje se čitanjem i dekodiranjem NAL jedinica od kojih je sastavljen. Pri čitanju pojedinačne NAL jedinice, najpre se celokupna NAL jedinica izdvaja iz toka binarnih podataka. Zatim se određuje tip NAL jedinice na osnovu podataka iz zaglavlja i na kraju se obavlja operacija dekodiranja date NAL jedinice. Pri dekodiranju ne-VCL NAL jedinice najpre se proverava sintaksna ispravnost a zatim se podaci i parametri koje one nose u sebi čuvaju u privremene promenljive koje se potom koriste u postupku dekodiranja VCL NAL jedinica. Kod VCL NAL jedinica, nakon provere sintaksne ispravnosti, postoje dve opcije. Prva, ako je HEVC video selektivno šifrovan vrši se dešifrovanje i dekodiranje video podataka. Druga, ako HEVC video nije

sleketivno šifrovan vrši se samo dekodiranje. Rezultat dekodiranja (ili dešifrovanja i dekodiranja) VCL NAL jedinice su pojedinačne slike koje, kada se grupišu zajedno, čine povorku slika u redosledu prikazivanja koje daju finalni video. Tačnije, nakon dekodiranja svaka pojedinačna slika se smešta u skladište dekodiranih slika (engl. *DPB - Decoded Picture Buffer*) i sortiraju se u redosledu prikazivanja. U drugoj programskoj niti, navedeni demo plejer jednostavno čita slike iz skladišta dekodiranih slika i prikazuje ih.



Slika 27. Dijagram toka modifikovanog HEVC dekodera

Specifičnost modifikacije HEVC dekodera ogleda se u dekodiranju CSPS NAL jedinice. Naime, kada se u procesu dekodovanja HEVC sekvence naiđe na navedenu NAL jedinicu najpre se uporede vrednosti identifikatora skupa CSPS parametara tekuće i prethodne CSPS NAL jedinice. Ako vrednost tekućeg identifikatora skupa parametara nije veći za jedan po modulu $\boldsymbol{N}^{14}$ od prethodnog izvršava se kriptografska resinhronizacija. Ukoliko jeste veći za jedan po modulu $\boldsymbol{N}$, vrši se upoređivanje vrednosti identifikatora konteksta kriptografske sinhronizacije. Ukoliko se ovi identifikatori razlikuju došlo je do promene izvora[15] selektivno šifrovanog HEVC video toka pa je potrebno najpre izvršiti promenu konteksta kriptografske sinhronizacije a zatim uraditi kriptografsku resinhronizaciju. Ukoliko su identifikatori konteksta kriptografske sinhronizacije identični proces se dalje nastavlja upoređivanjem veličina i konkretnih vrednosti sinhronizacionih podataka. Ukoliko se konkretne vrednosti sinhronizacionih podataka razlikuju[16] izvršava se kriptografska resinhronizacija. Ukoliko se navedene vrednosti sinhronizacionih podataka ne razlikuju, nije potrebno izvršiti kriptografsku resinhronizaciju već se nastavlja postupak učitavanja i dekodovanja sledeće NAL jedinice.

Takođe, modifikacija navedene biblioteke otvorenog koda (***libde265***) i demo plejera (***dec265***) obuhvata i implementaciju mehanizama slučajnog pristupa selektivno šifrovanom HEVC video toku. Sa dijagrama toka na slici 27 može se videti da ukoliko je pokrenuta operacija slučajnog pristupa nekom delu video toka, promenljiva *jump_count* dobija pozitivnu vrednost različitu od 0 (nula). Konkretna vrednost ove promenljive se posebno proračunava za svaki skok (svaki slučajni pristup) posebno jer je potrebno preračunati sekunde konkrentog HEVC video toka u broj slika (frejmova) koje treba preskočiti. Preskakanje slika se realizuje sve dok je vrednost promenljive *jump_count* veće od nule ili se ne naiđe na prvu sledeću CSPS NAL jedinicu koja je

---

[14] Sa $\boldsymbol{N}$ je definisana gornja granica vrednosti identifikatora i on iznosi 2^{16}, izeto je u obzir da se koriste dva bajta za predstavljanje identifikatora.

[15] Promena izvora selektivno šifrovanog HEVC video toka ekvivalentna je promeni kanala.

[16] Ova razlika se može javiti kao posledica greške pri dešifrovanju prethodnog bloka šifrata ili kao posledica greške na prenosnom putu

neophodna za kriptografsku resinhronizaciju. Na osnovu dizajna ponuđenog rešenja, iza CSPS NAL jedinice u HEVC nizu bita sigurno se nalazi IRAP slika pa je moguće, nakon realizovane kriptografske resinhronizacije, nesmetano nastaviti proces ispravnog dešifrovanja i dekodovanja HEVC sekvence.

5.5. Eksperimentalni rezultati

Eksperimentalni rezultati se mogu podeliti na dve celine. U prvom delu je analizirana efikasnost ponuđenog rešenja sa aspekta broja dodatih bajtova u HEVC video tok. Drugi aspekt realizovan je implementacijom HEVC dekodera i pokazivanjem mogućnosti korišćenja predloženog mehanizma kriptografske sinhronizacije za implementaciju slučajnog pristupa selektivno šifrovanom HEVC video toku. Za potrebe evaluacije, testiranja i generisanja eksperimentalnih rezultata korišćene su test sekvence koje predstavjaju podskup test sekvenci korišćenih u procesu HEVC standardizacije.

5.5.1. Test sekvence

Test sekvence su definisane prema veličini slike i potencijalnim aplikacijama i one su klasifikovane u šest klasa označenih velikim slovima abecede od A do F[9]. U klasu A spadaju test sekvence sa rezolucijom većom od 1080p koja predstavlja HDTV. Ove sekvence se koriste za procenu i testiranje performansi kodiranja 4K i 8K videa (Ultra HDTV). Da bi se smanjilo vreme izračunavanja, veličine slike su odsecane na 2560x1600 piksela. Klasa B sadrži test sekvence za testiranje performansi 1080p HDTV videa i ova klasa sadrži HDTV sekvence sa veličinom slike 1920x1080 piksela. Klase C i D obuhvataju skup test sekvenci sa veličinom slika od 830x480 piksela i veličinom slika od 416x240 piksela repsektivno. Test sekvence koje spadaju u ove dve klase koriste se za kodiranje, testiranje i evaluaciju performansi mobilnih aplikacija. U klasu E spadaju test sekvence sa veličinom slike od 1280x720 piksela. Koriste se za evaluaciju performansi kodiranja aplikacija koje zahtevaju minimalno kašnjenje video signala kao što su, na primer, sistemi vizuelne komunikacije. Kao dodatak, pri uspostavljanju zajedničkih uslova testiranja i definisanju platforme na kojoj se izvode eksperimenti za procenu efikasnosti algoritama i alata kodiranja, definisana je i klasa test sekvenci F[60]. U ovu klasu spadaju sekvence koje se koriste za evaluaciju i

testiranje performansi kodiranja sadržaja koji nije snimljen kamerom, kao na primer sadržaj prikaza računarskog monitora koji može sadržati tekst ili računarsku grafiku.

Skup test sekvenci korišćenih u ovom radu sadrži 11 8-bitnih test sekvenci svrstanih u klase A do E. Ovaj skup je prikazan u tabeli 6 i predstavlja podskup sekvenci koje su korišćene u procesu standardizacije HEVC standarda[61].

Tabela 6. Skup test sekvenci korišćenih za evaluaciju predloženog rešenja

Sekvenca	Rezolucija	Ukupna broj frejmova	Broj slika (fps)	Klasa
Traffic	2560x1600	150	30	A
PeopleOnStreet	2560x1600	150	30	A
Kimono1	1920x1080	240	24	B
ParkScene	1920x1080	240	24	B
MobileCalendar	1280x720	504	50	E
City	1280x720	900	60	E
PartyScene	832x480	500	50	C
BQMall	832x480	600	60	C
BasketballPass	416x240	500	50	D
BlowingBubbles	416x240	500	50	D
RaceHorses	416x240	300	30	D

5.5.2. Efikasnost ponuđenog rešenja

Kako bi evaluirali efikasnost ponuđenog rešenja najpre su, korišćenjem nemodifikovanog referentnog HEVC enkodera, enkodovani otvoreni (nešifrovani) HEVC video tokovi. Zatim su, zadržavajući iste uslove izvršavanja upotrebom modifikovanog referentnog HEVC enkodera, enkodovani selektivno šifrovani HEVC video tokovi sa mogućnošću slučajnog pristupa. Kreirani su selektivno šifrovani video tokovi za svaki od dva implementirana algoritma selektivnog šifrovanja i za svaku od test sekvenci. Svi gore navedeni video tokovi, i otvoreni i selektivno šifrovani, enkodovani su korišćenjem Intel(R) Xeon(R) X5570 (2,93 GHz) procesora sa 6 GB RAM memorije.

Upoređivanjem veličina, iskazanih u broju bajtova upisanih u fajl, između otvorenih (nešifrovanih) i selektivno šifrovanih HEVC video tokova sa mogućnošću slučajnog prisutpa, moguće je odrediti efikasnost ponuđenog mehanizma kriptografske sinhronizacije. U tabeli 7 prikazan je broj bajtova upisan u fajl i odgovarajuća bitska brzina za otvorene (nešifrovane) i za selektivno šifrovane HEVC video tokove sa mogućnošću slučajnog pristupa. U navedenoj tabeli prikazani su rezultati za selektivno

šifrovane HEVC video tokove za oba implementirana algoritma selektivnog šifrovanja. Naime, reč je o algoritmima selektivnog šifrovanja koji ne dodaju nijedan jedini bit u HEVC video tok već samo šifruju izabrane sintakse elemente. Sa druge strane, algoritam autora Z. Shahid-a i W. Puecha izabrane sintaksne elemente šifruje AES kriptografskim algoritmom u CFB modu rada dok algoritam autora M. Ouamri i K. M. Faraoun izabrane sintaksne elemente šifruje AES kriptografskim algoritmom u CBC modu rada. Kada su u pitanju CBC i CFB modovi rada, za potrebe kriptografske sinhronizacije algoritama selektivnog šifrovanja potrebne su i dovoljne vrednosti inicijalnih vektora. Veličina inicijalnog vektora kada se koristi AES kriptografski algoritam, u CBC i CFB modu rada, jednaka je veličina bloka AES kriptografskog algoritma i iznosi 16 bajta.

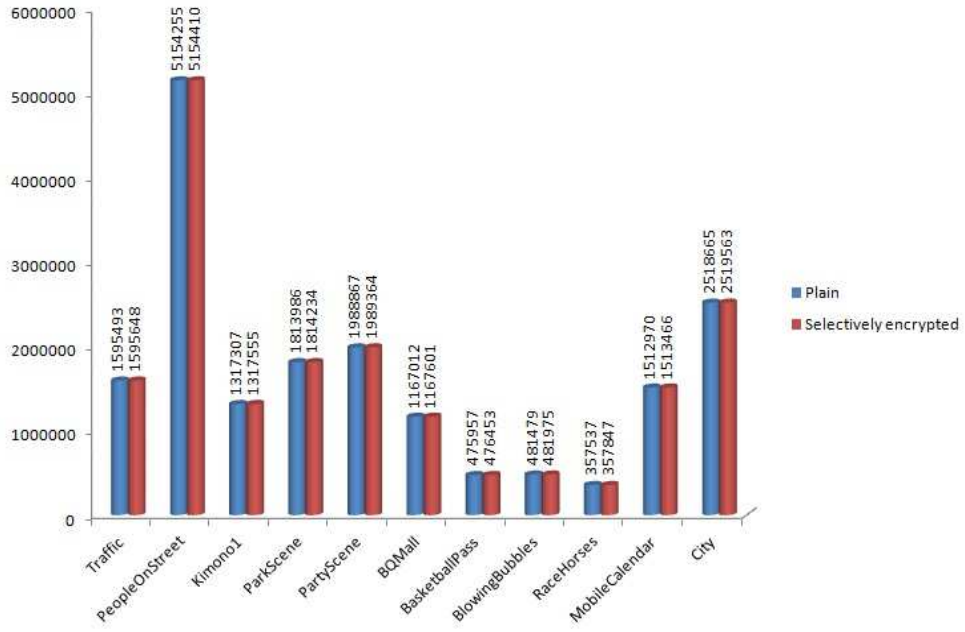
Tabela 7. Analiza efikasnosti predloženog rešenja na test sekvencama (*IntraPeriod* = 32)

Sekvenca	Otvorene (nešifrovane)		Selektivno šifrovane		Δ_B (b)	Δ_P (%)
	Bajtova upisanih u fajl	Bitrate (kbps)	Bajtova upisanih u fajl	Bitrate (kbps)		
Traffic	1595493	2552,79	1595648	2553,03	155	0,0097
PeopleOnStreet	5154255	8246,88	5154410	8247,05	155	0,0030
Kimono1	1317307	1053,86	1317555	1054,04	248	0,0188
ParkScene	1813986	1451,19	1814234	1451,38	248	0,0136
MobileCalendar	1512970	1203,17	1513466	1203,55	496	0,0327
City	2518665	1343,28	2519564	1343,76	899	0,0356
PartyScene	1988867	1591,04	1989363	1591,49	496	0,0249
BQMall	1167012	933,60	1167601	934,08	589	0,0504
BasketballPass	475957	380,76	476453	381,16	496	0,1041
BlowingBubbles	481479	385,13	481975	385,58	496	0,1029
RaceHorses	357537	286,00	357847	286,27	310	0,0866

Ako se pogledaju rezultati u tabeli 7 oni ukazuju na to da je broj bajtova upisanih u fajl selektivno šifrovanog HEVC video toka, sa dodatom ne-VCL CSPS NAL jedinicom, veći. Ako se kao primer uzme test sekvenca ***Traffic***, razlika između broja bajtova upisanih u fajlove, tj. vrednost parametra Δ_B iznosi tačno 155 bajtova. S obzirom da navedena sekvenca ima 150 frejmova (vidi tabelu 6), a pošto je vrednost *IntraPeriod* parametra jednaka 32, može se zaključiti da rezultujući video tok ima 5 intra kodovanih slika (5 IRAP slika) pa prema tome ima i 5 ne-VCL CSPS NAL jedinica od kojih je svaka velika po 31 bajt. Ovakav rezultat, između ostalog, potvrđuje bitnu činjenicu vezanu za algoritme selektivnog šifrovanja HEVC video toka. Naime,

ovim rezultatima je potvrđena bitna karakteristika algoritama selektivnog šifrovanja HEVC video toka da oni ne unose nijedan dodatan bit u HEVC video tok. Bajtovi dodati u selektivno šifrovani HEVC video tok pripadaju isključivo novodefinisanoj ne-VCL CSPS NAL jedinici i namenjeni su za kriptografsku sinhronizaciju. Navedeni bajtovi (njih 155), statistički gledano, čine svega 0,0097% ukupne količine bajtova u fajlu selektivno šifrovanog HEVC video toka za sekvencu ***Traffic***. Ako se nastavi dalja analiza dobijenih rezultata, za sekvencu ***PeopleOnStreet*** koja takođe pripada klasi A i ima 150 frejmova, razlika između broja bajtova upisanih u fajlove, tj. vrednost parametra Δ_B, takođe iznosi tačno 155 bajtova. U slučaju ***PeopleOnStreet*** sekvence, dodatni bajtovi čine svega 0,0030% ukupne količine bajtova u selektivno šifrovanom HEVC video toku. Može se oučiti da je broj dodatih bajtova identičan kod obe sekvence iz klase A ali se razlikuje statistički pogled iskazan procentualnim iznosom od ukupne količine bajtova. Ovakva razlika u procentualnom iznosu dodatih bajtova uslovljena je različitim veličinom enkodovanih slika (bilo da su intra kodovane ili inter kodovane). Različite veličine kodovanih slika uslovljene su različitom dinamikom pokretnih scena u dve različite sekvence pa je i prema tome broj bajtova u VCL NAL jedinicama veći kod sekvence u kojoj je dinamika pokreta veća. Ovo je u potpunoj saglasnosti sa formalnom specifikacijom efikasnosti ponuđenog rešenja.

Ako analiziramo sekvence sa manjim rezolucijama očekivano je da, na osnovu formalne specifikacije efikasnosti ponuđenog rešenja, procentualno iskazan udeo dodatog broja bajtova bude malo veći. Ako posmatramo sekvencu ***BlowingBubbles*** koja ima 500 frejmova i ako je vrednost *IntraPeriod* parametra 32, onda u okviru rezultujućeg video toka ima 16 intra kodovanih slika (16 IRAP slika). Iz tabele 7 može se videti da je razlika između broja bajtova upisanih u fajlove za sekvencu ***BlowingBubbles*** tačno 496 što u potpunosti odgovara činjenici da ima 16 intra kodovanih slika a samim tim i 16 dodatih ne-VCL CSPS NAL jedinica. Procentualno iskazan odeo dodatog broja bajtova u ukupnoj količine bajtova u selektivno šifrovanom HEVC video toku sekvence ***BlowingBubbles*** ima vrednost 0,1029%. Razlike u broju bajtova upisanih i fajlove sa otvorenim (nešifrovanim) i selektivno šifrovanim HEVC video tokom sa mogućnošću slučajnog pristupa, za sve test sekvence dati su u tabeli 7 i grafički ilustrovani na slici 28.



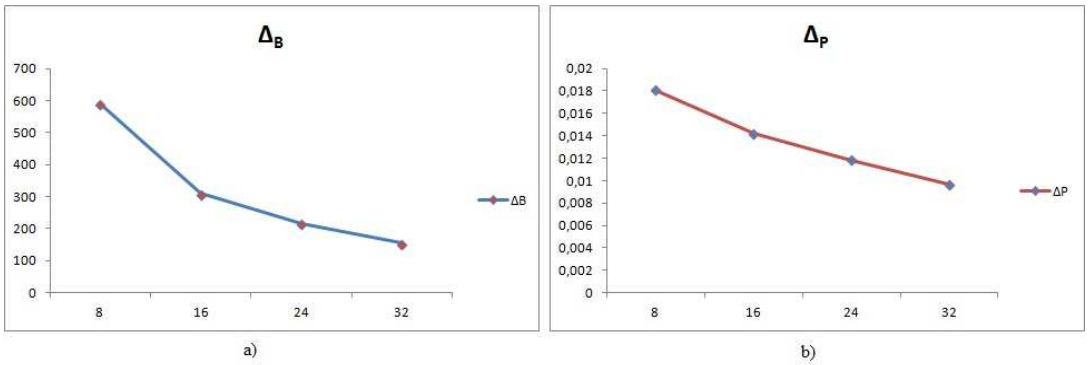
Slika 28. Grafički ilustrovana razlika u broju bajtova upisanih u fajlove sa otvorenim (nešifrovanim) i selektivno šifrovanim HEVC video tokom sa mogućnošću slučjanog pristupa

Selektivno šifrovani HEVC video tokovi sa mogućnošću slučajnog pristupa imaju onoliko CSPS NAL jedinica koliko je intra kodovanih IRAP slika. Na broj intra kodovanih IRAP slika direktno utiče vrednost *IntraPeriod* parametra. U tabeli 8 prikazan je broj bajtova upisan u fajl i odgovarajuća bitska brzina za otvorene (nešifrovane) i za selektivno šifrovane HEVC video tokove sa mogućnošću slučajnog pristupa za različite vrednosti *IntraPeriod* parametra. Konkretno, u navedenoj tabeli su prikazani rezultati broja bajtova upisanih u fajl za sekvencu ***Traffic,*** pri čemu *IntraPeriod* parametar ima vrednosti 8, 16, 24 i 32.

Tabela 8. Efikasnosti predloženog rešenja na *Traffic* test sekvenci (*IntraPeriod* = {8, 16, 24, 32}

IntraPeriod **vrednost**	**Otvorene (nešifrovane)**		**Selektivno šifrovane**		**Δ_B (b)**	**Δ_P (%)**
	Bajtova upisanih u fajl	**Bitrate (kbps)**	**Bajtova upisanih u fajl**	**Bitrate (kbps)**		
8	3257174	5211,47	3257763	5212,42	589	0,0181
16	2186523	3498,43	2186833	3498,93	310	0,0142
24	1833577	2933,72	1833794	2934,07	217	0,0118
32	1595493	2552,78	1595648	2553,03	155	0,0097

Na slici 29 prikazana je grafička ilustracija uticaja različitih vrednosti *IntraPeriod* parametra na: a) broj dodatih bajtova i b) procentualno iskazano učešće u ukupnom broju bajtova u selektivno šifrovanom HEVC video toka sekvence ***Traffic***.



Slika 29. Grafička ilustracija uticaja različitih vrednosti IntraPeriod parametra: a) broj dodatih bajtova, b) procentualno iskazano učešće u ukupnom broju bajtova

Na osnovu vrednosti iz tabele 8 i grafičke ilustracije prikazane na slici 29 može se zaključiti da je broj dodatih bajtova u selektivno šifrovanom HEVC video toku (a samim tim i broj CSPS NAL jedinica) inverzno proporcionalan vrednosti *IntraPeriod* parametra. U okviru iste video sekvence, ukupan broj dodatih bajtova namenjenih kriptografskoj sinhronizaciji prilikom operacije slučajnog pristupa selektivno šifrovanom video toku, smanjuje se sa povećanjem vrednosti *IntraPeriod* parametra.

Selektivno šifrovani HEVC video tokovi sa mogućnošću slučajnog pristupa, sa dodatim CSPS NAL jedinicama, potpuno su kompatibilni sa HEVC standardom. Naime, kada se ovi video tokovi dekoduju u komercijalnom HEVC plejeru, HEVC dekoder ih može dekodirati. Međutim, komercijalni dekoder ih ne može dešifrovati, što dovodi do slučajeva prikazanih na slici 30(d, e i f). Dekoder koji ne može da prepozna primenjeni algoritam selektivnog šifrovanja jednostavno ignoriše i odbacuje ne-VCL CSPS NAL jedinicu. Na slici 30 mogu se videti odabrani frejmovi ***BlowingBubbles*** sekvence sa i bez implementiranog algoritma selektivnog šifrovanja i dodatih sinhronizacionih podataka prikazani u komercijalnom HEVC plejeru. Na navedenoj slici prikazani su rezultati dobijeni primenom algoritma selektivnog šifrovanja autora Z. Shahid-a i W. Puecha.

Slika 30. Frejmovi #0 #8 i #32 (I, B i B frejm respektivno) *BlowingBubbles* sekvence sa i bez primenjenog algoritma selektivnog šifrovanja: a) Originalni frejm #0, b) Originalni frejm #8, c) Originalni frejm #32, d) Selektivno šifrovani sa CSPS frejm #0, e) Selektivno šifrovani sa CSPS frejm #8, f) Selektivno šifrovani sa CSPS frejm #32

5.5.3. Slučajni pristup selektivno šifrovanom HEVC video toku

Na strani dekodera, implementiran je modifikovani HEVC dekoder koji ima mogućnost slučajnog pristupa selektivno šifrovanom HEVC video toku. Tačnije, biblioteka ***libde265*** i demo plejer ***dec265*** modifikovani su sa ciljem da se to omogući. Operacija slučajnog pristupa simulirana je skokom na određeni vremenski interval i okviru selektivno šifrovanog HEVC video toka. Parametri operacije skoka na slučajno izabranu lokaciju u selektivno šifrovani HEVC video tok mogu se zadati na dva načina.

Prvi način je zadavanje parametara apsolutnog skoka od početka video sekvence i realizovan je kao parametar pokretanja programa iz komandne linije, kao što je prikazano listingom 1.

./dec265 -i file.bin -j n

Listing 1. Pokretanje dekodera i demo plejera sa pratećim parametrima

Parametrom -i sa pridruženom vrednošću definisan je ulazni fajl u kome je smešten HEVC video tok. U fajlu može biti smešten ili otvoreni (nešifrovani) ili selektivno šifrovani HEVC video tok. Parametrom *-j*, zajedno sa pridruženom vrednošću *n*, definisana je operacija skoka za *n* sekundi od početka videa. Implementacija modifikovanog HEVC dekodera, na osnovu parametara HEVC video toka smeštenih u VPS, SPS i PPS skupovima parametara, pronalazi karakteristike predmetnog video toka (broj frejmova u sekundi, vrednost *IntraPeriod* parametra) i vreme definisano u

sekundama preračunava u broj frejmova koje treba da preskoči i tako određenom vrednošću inicijalizuje promenljivu *jump_count*. Dalje se modifikovani dekoder ponaša onako kako je opisano u poglavlju 5.4.2. (modifikacija na strani dekodera) i prikazano dijagramom toka na slici 27. Dekoder svaki put uspešno odredi lokaciju, pronađe prvu sledeću ne-VCL CSPS NAL jedinicu, izvrši kriptografsku resinhronizaciju algoritma selektivnog šifrovanja i otpočne proces dešifrovanja, dekodovanja i prikazivanja selektivno šifrovanog HEVC video toka.

Drugi način je zadavanje parametara relativnog skoka u odnosu na trenutnu lokaciju reprodukcije selektivno šifrovanog HEVC video toka. Operater može da, u toku prikazivanja HEVC video toka klikne jednom na taster ↑ (strelica nagore u skupu upravljačkih tastera na tastaturi) parametar skoka *n* dobija vrednost 2 (skok za dve sekunde od trenutne lokacije). Ako operater dva puta u kratkom vremenskom intervalu klikne taster ↑, parametar *n* dobija vrednost 5 (skok za pet sekundi od trenutne lokacije). Nakon toga se ponavlja prethodno opisani algoritam preračunavanja vrednosti promenljive *jump_count* i postupak pronalaženja tražene ne-VCL CSPS NAL jedinice čiji se podaci koriste za resinhronizaciju algoritma selektivnog šifrovanja i otpočinjanje procesa dešifrovanja, dekodiranja i prikazivanja HEVC video toka od lokacije koja je zadata operacijom skoka.

6. PRIMENA U VOJNIM KOMUNIKACIONIM SISTEMIMA

Dve ključne činjenice utiču na razmatranje mogućnosti korišćenja H.265/HEVC standarda u različitim vojnim multimedijalnim aplikacijama i sistemima. Prva, H.265/HEVC standard donosi poboljšanje od 30-50% po pitanju efikasnosti kompresije video signala (u odnosu na prethodni standard) što omogućava prenos visoko kvalitetnog video sadržaja kroz postojeću širinu propusnog opsega ili uzročno posledično omogućava prenos istog kvaliteta video sadržaja kroz znatno manju širinu istog propusnog opsega. Druga, navedeni standard su osvojile organizacije NATO (engl. *NATO - North Athlantic Treaty Organization*) i MIBS of USA DoD (engl. *MISB - Motion Imagery Standard Board of United State Department of Defense*) kao njihov primarni standard kompresije video podataka koji se koristi u različitim vojnim sistemima i aplikacijama[62].

Navedene karakteristike pružaju mogućnost korišćenja novog standarda u već postojećim vojnim telekomunikacionim sistemima u kojima su već implementirani prethodni standardi kompresije video podataka (MPEG-2, H.264/AVC i drugi). Takođe, veoma je značajno korišćenje novog standarda kompresije video podataka u aplikacijama i sistemima čiji su razvoj i implementacija u toku ili se planiraju u bliskoj budućnosti.

U ovom poglavlju je dat kratak teorijski osvrt na mogućnost primene novog H.265/HEVC standarda kompresije video podataka u različitim sistemima za izviđanje i nadzor iz vazduha kao što su bespilotne letelice, u sistemima za video nadzor specifičnih infrastrukturnih objekata, kod sistema videokonferencijske komunikacije, u satelitskim komunikacionim sistemima, u vojnim bežičnim mrežama baziranim na standardu IEEE 802 (WiMAX i WiFi). Gde god je moguće primeniti H.265/HEVC standard, a potrebno je implementirati očuvanje tajnosti video toka, moguće je i primeniti neki (postojeći ili novodefinisani) algoritam selektivnog šifrovanja sa ponuđenim efikasnim mehanizmom kriptografske sinhronizacije.

6.1. Primena H.265/HEVC standarda u sistemima za izviđanje i nadzor iz vazduha

Video tok koji se šalje i prima u realnom vremenu postao je veoma važan izvor bitnih informacija u procesima izviđanja i nadzora iz vazduha, kolekcije obaveštajnih informacija, praćenja situacije na bojnom polju i u postupku donošenja odluka. Prilikom izviđanja i nadzora iz vazduha (engl. *AVS - Air Video Surveillance*) sposobnost povezivanja geoprostornih informacija sa slikovito prikazanim obaveštajnim informacijama, omogućava donosiocima odluka da sagledaju i analiziraju geografski sadržaj borbene ili neborbene situacije, prate i vizuelizuju događaje onako kao što se oni odvijaju u realnoj situaciji, kao i da predvide moguće ishode situacija koja se upravo razvijaju[63].

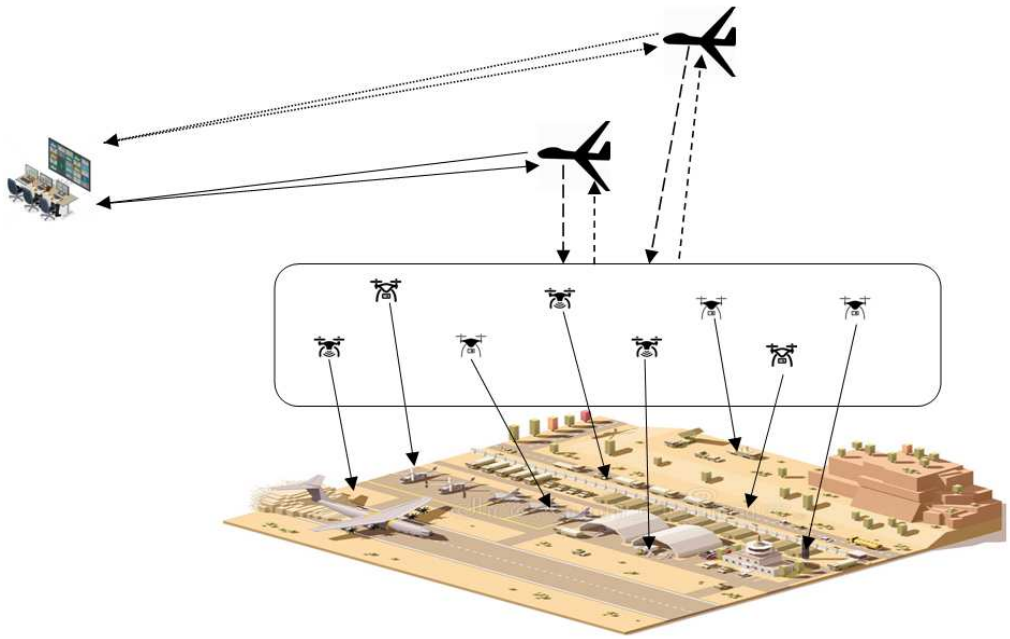
Današnji sofisticirani sistemi na bespilotnim letelicama ne obezbeđuju sposobnost izviđanja, nadzora, praćenja i prepoznavanja ciljeva sa visokim rezolucijama. Navedene bespilotne letelice su pre svega velikih dimenzija i moraju da lete na srednjim i velikim visinama što prouzrokuje degradiranje prostorne rezolucije snimljenog videa[64]. Upotreba standardnih sistema bespilotnih letelica prikazana je na slici 31.

Slika 31. Upotreba standardnih sistema bespilotnih letelica (preuzeto iz [64])

Ultrabrzi napredak informacionih tehnologija i elektronike posebne namene, pored ostalog i na polju bespilotnih letelica, omogućio je: minijaturizaciju različitih vrsta senzora sa aspekta primenjenog hardvera (digitalne kamere i fotoaparati, termovizijske kamere), napredne vizuelne tehnologije za automotizovano upravljanje, napredne

tehnike fizičkog dizajna, unapređenu upravljivost kroz napredne elektro-mehaničke kontrole, unapređenu bežičnu komunikaciju između različitih učesnika, bilo da se oni nalaze na zemlji, vodi ili u vazduhu. Navedena činjenica kao posledicu ima realizaciju i upotrebu, po svim dimnezijama manjih i lakših bespilotnih letelica, mikro bespilotnih letelica (engl. *M-UAV – Micro-Unmmanned Aerial Vehicle*). Prednost mikro bespilotnih letelica u odnosu na konvencionalne sisteme bespilotnih letelica ogleda se u nižoj ceni i kraćem vremenu potrebnom za razvoj i proizvodnju.

Fleksibilnost i sposobnost mikro bespilotnih letelica da lete na manjim visinama omogućavaju i olakšavaju procese prikupljanja detaljnih video informacija, što omogućava uspešnije praćenje, prepoznavanje i identifikovanje potencijalnog cilja[64]. Na polju primene bespilotnih letelica, veliki izazov predstavlja dizajn i razvoj sistema za kontrolu i upravljanje velikom grupom mikro bespilotnih letelica kojom bi se omogućilo izviđanje i nadzor iz vazduha sa velike udaljenosti. Na slici 32 je prikazana jedna moguća implementacija i konfiguracija predloženog sistema sa velikom grupom mikro bespilotnih letelica, jednom glavnom i jednom rezervnom standardnom bespilotnom letelicom.



Slika 32. Potencijalna arhitektura sistema za izviđanje i nadzor iz vazduha sa velike udaljenosti sa standardnim i mikro bespilotnim letelicama[17]

[17] Delovi slike preuzeti sa web stranica *www.dreamstime.com* i *www.shutterstock.com*

Kod ovakvih konfiguracija glavna i rezervna bespilotna letelica su standardne letelice velikih dimenzija, lete na većim visinama i automatski upravljaju grupom mikro bespilotnih letelica koje lete na dosta manjim visinama. Samo ime kaže, rezervna bespilotna letelica ima potpuno iste funkcije kao i glavna i služi kao redudansa za slučaj otkazivanja ili gubitka glavne letelice. Glavna bespilotna letelica poseduje istaknutije hardverske resurse i elektronske sklopove za geoprostorno lociranje u realnom vremenu i ima uređaje za komunikaciju sa komandno-kontrolnim centrom putem bežičnog komunikacionog kanala. Nakon preciznog geoprostornog lociranja i globalne kompenzacije pokreta pomoću kamere, glavna bespilotna letelica identifikuje i selektuje statičke i dinamičke ciljeve koji će detaljnije biti praćeni. Glavna bespilotna letelica distribuira podatke o geoprostornim lokacijama, kao i vizuelni sadržaj o cilju do pomoćnih mikro bespilotnih letelica, usmeravajući i navodeći ih da prate svaki od dodeljenih ciljeva[64].

Mikro bespilotne letelice lete na manjim visinama, prate i usmeravaju se na dodeljene ciljeve unutar vidnog polja svojih kamera sa ciljem da zabeleže video informacije većih rezolucija i sa što je moguće više detalja. Nakon primene efikasne kompresije video podataka, pomoćne mikro bespilotne letelice prosleđuju kompresovani video tok o dodeljenom cilju glavnoj i redudantnoj bespilotnoj letelici. Nakon toga, glavne (velike) bespilotna letelice multipleksiraju video tokove o svim ciljevima dobijene od pomoćnih mikro bespilotnih letelica, kao i metapodatke o geoprostornim lokacijama svakog cilja i prosleđuje ih sve zajedno do kontrolno-komandnog centra za potrebe automatskog ili poluautomatskog prepoznavanje ciljeva, analizu dobijenih informacija i na samom kraju donošenje odluke. Povratnim mehanizmom od kontrolno-komandnog centra do glavne bespilotne letelice definišu se ciljevi od interesa za koje je potrebno video praćenje visokog kvaliteta od strane pomoćnih mikro bespilotnih letelica, kao i zahtevi komunikacionoj i senzorskoj opremi da obezbedi potrebne mehanizme kriptografske zaštite za video tok visokog prioriteta.

Kod tipičnog video toka koji je namenjen zabavi, video scenom dominiraju slučajni pokreti pokretnih objekata. Međutim, video nastao praćenjem iz vazduha od strane mikro bespilotnih letelica prikazuje veoma statičan i čvrst globalni pokret. Ova karakteristika jedinstvena kod izviđanja i nadzora iz vazduha može se iskoristiti za značajno unapređenje efikasnosti video kodovanja.

Primena H.265/HEVC standarda kod standardnih bespilotnih, ali i kod mikro bespilotinih letelica ogleda se pre svega u činjenici da u poređenju sa prethodnim standardima, H.265/HEVC srandard, obezbeđuje veći stepen kompresije, efikasnije kodovanje video sadržaja, kao i niže bitske protoke (do 50%) uz mnogo prihvatljiviji perceptualni kvalitet. Takođe, novi standard podržava fleksibilnost u kodovanju, kao i organizaciju kodovanih video podataka na način koji povećava otpornost na greške i smanjuje gubitke u video sadržaju koji se prenosi kroz sistem za izviđanje i nadzor iz vazduha u realnom vremenu.

6.2. Primena H.265/HEVC standarda u sistemima za video nadzor specifičnih infrastrukturnih objekata

Video nadzor predstavlja industrijski koncept koji je star već 30-ak godina ali koji se iz godine u godinu menja i usavršava. Generator svakodnevnih promena su krajnji korisnici čiji su zahtevi pokretač mnogih novih rešenja u ovoj oblasti. Među najčešćim zahtevima su: bolji kvalitet videa (veća rezolucija), brža i pouzdanija tehnologija, mogućnost skladištenja i čuvanja veće količine snimljenog video materijala, laka upotreba i mogućnost integracije sa drugim sistemima[65]. U cilju ispunjavanja ovih zahteva, video nadzor je doživeo mnoge promene. Najnovija promena je uvođenje novog H.265/HEVC standarda sa svim prednostima koje on donosi.

H.265/HEVC standard zahvaljujući svojim performansama može naći primenu u sistemima za lokalni i udaljeni video nadzor različitih vojnih instalacija na teritoriji cele države među kojima se nalaze vojni kompleksi, kasarne, različita skladišta, komandni objekti i punktovi, poligoni i tereni za izvođenje različitih vrsta obuke, čvorišta i centri veze, radarski centri i položaji, različite izviđačke stanice dr.

6.3. Primena H.265/HEVC standarda u sistemima videokonferencijske komunikacije

Video konferencijska komunikacija je vid komunikacije između dva korisnika ili grupe korisnika, bez obzira na njihove trenutne lokacije, koji omogućava učesnicima da vide i da saslušaju jedni druge na način određen vrstom video konferencije. Ona predstavlja savremeni visokotehnološki komunikacioni alat za povećanje poslovne efikasnosti, optimizaciju poslovnih procesa, ubrzavanje procesa donošenja odluka i

uštedu resursa (bilo da se tiče vremena ili novca). H.265/HEVC standard kompresije video podataka i prednosti koje on donosi koriste se u okviru navedenih sistema kako bi komunikacija bila efikasnija i efektivnija. Ovakvi napredni sistemi komunikacije su potrebni različitim poslovnim sistemima i organizacijama, a mogu se koristiti i za vojne potrebe.

Impresivno povećanje performansi koje donosi novi standard kompresije videa omogućava vladinim i nevladinim organizacijama, a samim tim u vojsci, da za prihvatljivu cenu koštanja usvoje i koriste video konferenciju u većoj meri preko tačaka konekcije u okviru mreža koje podržavaju H.265/HEVC standard na svojim krajnjim uređajima. Krajnji uređaji mogu biti hardverski ili softverski definisani za primenu u specijalnim prostorijama, na računarima opšte namene, mobilnim uređajima ili u okviru Internet pretraživača.

Prednosti upotrebe video konferencijskih sistema, koji se baziraju na H.265/HEVC standardu, u vojsci su:

- **Unapređeno upravljanje članovima radnih timova koji su raštrkani širom teritorije nadležnosti vojske**: vojska, kao i velike kompanije, ima stručnjake i specijaliste za različite oblasti koji se nalaze širom teritorije jedne zemlje. Videokonferencije omogućava vojnom komandovanju i rukovođenju da lakše raspoređuje i upravlja ljudskim resursima i da skoro pa stalno (skoro u realnom vremenu) ima mogućnost sastanaka, izdavanja zadataka i izveštavanja na liniji nadređeni i njegovi podređeni kao i na nivou različitih radnih grupa i radnih tela koje izvršavaju različite misije i zadatke.
- **Smanjenje troškova**: korišćenje video konferencijskih sistema koji se baziraju na H.265/HEVC standardu utiče značajno na smanjenje troškova. Navedeno smanjenje troškova ogleda se u smanjenju troškova službenih putovanja na različite sastanke, implementacije i održavanja komunikacione mreže i mogućnost komunikacije sa najnižim nivoima komandovanja.
- **Povećanje obima realizacije svih zadataka**: ogleda se kroz povećanje korišćenja video konferencijske komunikacije iz dana u dan, i korišćenja ovog vida komunikacije u realizaciji kritičnih misija. Korisnici na svim nivoima komandovanja mogu da realizuju različite zadatke i misije daleko brže i efikasnije.

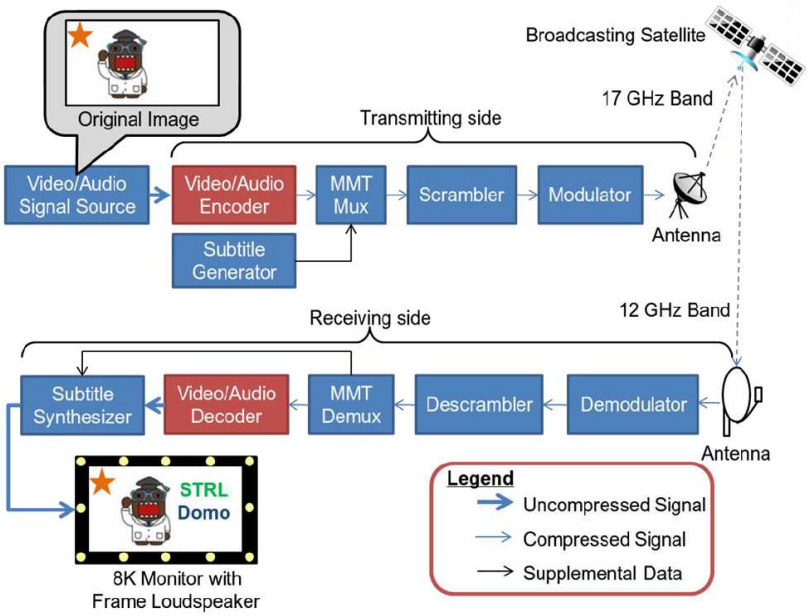
- **Efikasniju komunikaciju**: video se pokazao daleko efikasnijim alatom za komunikaciju nego glas ili Web kod većine aplikacija[66]. Kada korisnici preko video konferencijskih sistema imaju značajnu i korisnu razmenu informacija, kao i saradnju sa različitim nivoima komandovanja, sam proces komandovanja postaje daleko efikasniji.
- **Efikasnije iskorišćenje mrežne infrastrukture**: video konferencijski sistemi bazirani na H.265/HEVC standardu, zahvaljujući prethodno navedenim performansama, efikasnije koriste dodeljeni propusni opseg u okviru mrežne infrastrukture za prenos video sadržaja i mogu se povezivati na postojeću komponente u okviru mrežne infrastrukture.
- **Mogućnost povezivanje sa prethodnim generacijama video konferencijskih sistema**: video konferencijski sistemi bazirani na H.265/HEVC standardu mogu se povezati preko bridževa i mrežnih gejtveja sa krajevima mreže gde se za komunikaciju koriste drugi video kodni standardi (H.261, H.264/AVC itd.).

6.4. Primena H.265/HEVC standarda u satelitskim komunikacionim sistemima

H.265/HEVC standard se uveliko primenjuje u oblasti satelitskih komunikacija, kako komercijalnih tako i vojnih. Kada je u pitanju komercijalna primena ističe se rezultat istraživanja publikovan u [67] u kome je predstavljen prvi (u svetu uopšte) dostupan sistem video i audio kodeka koji je kompatibilan sa standardima za emitovanje 8K video podataka. U navedenom radu su detaljno opisani eksperimenti prenosa putem satelita upotrebom ponuđenog sistema. Na slici 33 prikazan je logička šema eksperimentalnog sistema emitovanja 8K video podataka.

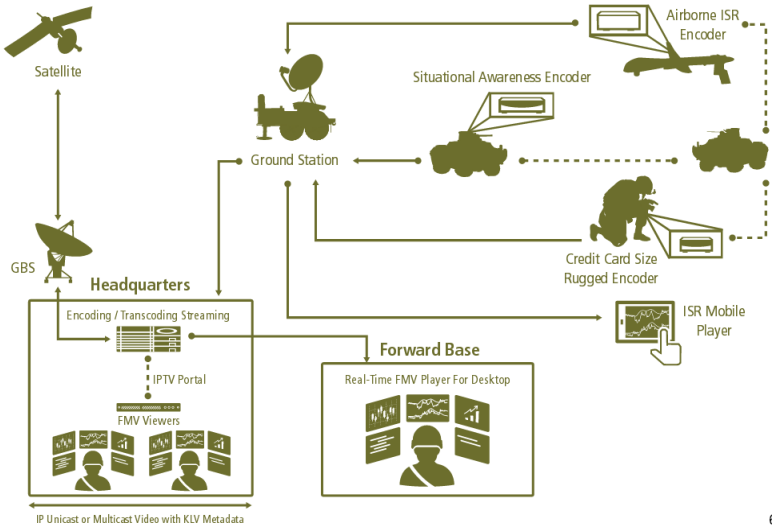
Kao primer primene H.265/HEVC standarda u vojnim komunikacijama mogu se navesti neki od prenosivih enkodera multinacionalne kompanije VITEC[68]. Na slici 34 prikazana je kompletna logička arhitektura sistema u kome su integrisani prenosni i prevozni enkoderi pomenute firme a koji pružaju mogućnost prenosa video podataka sa bojnog polja u realnom vremenu. Video kamera, kao krajnji senzorski uređaj (na bespilotnoj letelici, na vojnom motornom vozilu ili u rukama vojnika), generiše video i prosleđuje ga nekom od prenosnih ili prevoznih hardverskih HEVC enkodera. HEVC enkoder je povezan sa satelitskim sistemom pa se na taj način HEVC video tok

podataka prenosi do satelitskog prijemnog centra na zemlji i dalje primenom različitih mrežnih tehnologija do komandnog mesta.



Slika 33. Logička šema eksperimentalnog sistema emitovanja 8K video podataka (preuzeto iz [67])

Navedena VITEC arhitektura obezbeđuje vojne servise putem sveobuhvatnog prenosa video podataka sa kraja na kraj video konekcije i optimizovan je za upotrebu u mobilnim i IP uslovima korišćenja. Bazirajući se na novom H.265/HEVC standardu, navedena arhitektura obezbeđuje prenos video podataka visokog kvaliteta i malog kašnjenja sa bilo koje tačke sa bojnog polja.



Slika 34. Arhitektura sistema za potrebe satelitskog prenosa HEVC video toka u vojnim komunikacionim sistemima (preuzeto iz [68])

6.5. Primena H.265/HEVC standarda u vojnim bežičnim mrežama baziranim na standardu IEEE 802 (WiMAX i WiFi)

H.265/HEVC standard kompresije video podataka poseduje metode, tehinke i alate koje svojim karakteristikama omogućavaju njegovu primenu u različitim mrežnim okruženjima. Samim tim, navedeni standard je moguće primeniti u vojnim bežičnim telekomunikacionim sistemima koji se baziraju na primeni WiFi[18] i WiMAX[19] tehnologija prenosa[69].

WiFi, odnosno bežične lokalne mreže, (engl. *WLAN - Wireless Local Area Nettwork*) predstavljaju komunikacionu tehnologija koja definiše standarde za komunikacionu opremu koja u skladu sa različitim verzijama IEEE 802.11 standarda, implementiranog u frekventnom opsegu 2,4 GHz. Navedena tehnologija bežične komunokacije obezbeđuje prenos podataka sa brzinama 1, 2, 5.5 i 11 Mb/s [70][71]. IEEE 802.11 kao standard za bežično mrežno povezivanje definiše i fizički sloj (engl. *Physical Layer*) i sloj kontrole pristupa medijumu (engl. *MAC - Medium Access Control*)[64]. MAC nivo kod 802.11 standarda je baziran na CSMA/CA (engl. *CSMA/CA - Carrier Sense Multiple Access/Collision Avoidance*) mehanizmu. Mehanizam izbegavanja kolizije je obezbeđen pomoću DCF funkcije (engl. *DCF - Distributed Coordination Function*) koja određuje vremenski raspored pristupa bežičnim medijumu. Iako dizajniran za mreže upravljane pomoću baznih stanica, DCF funkcija kod IEEE 802.11 dozvoljava mobilnim korisnicima da pristupe radio prenosnom putu bez potrebe za radio baznom stanicom. Većina protokola dizajniranih za *ad-hoc* mreže baziraju se na pretpostavci da se IEEE 802.11 koristi na najnižim slojevima komunikacije[72].

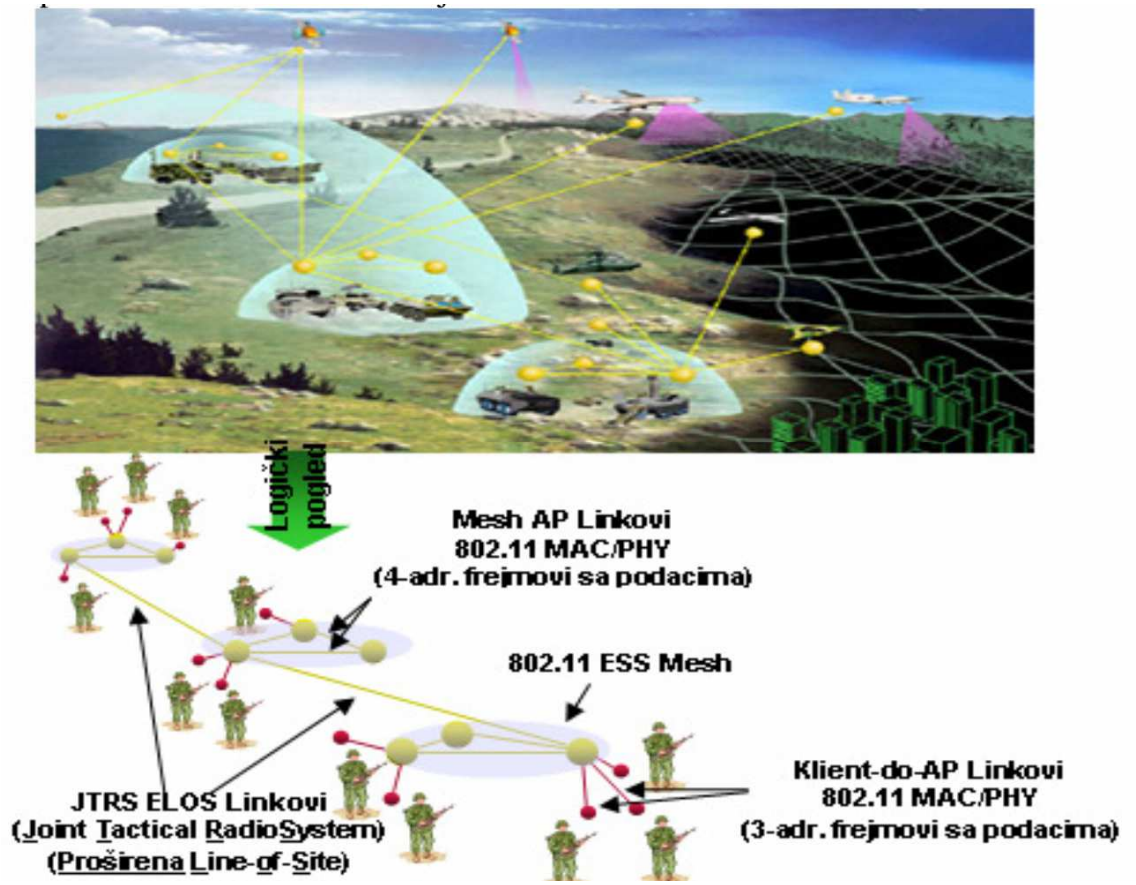
Koristeći opremu na bazi WiFi tehnologija može se uspostaviti *ad-hoc* mreža učesnika grupisanih na malom prostoru, ili pak korisnici mogu biti opsluženi od strane "hot-spot" servisne tačke koja je locirana na centralnoj lokaciji o okviru neke oblasti[73]. Korišćenjem takvih tačaka pristupa postiže se domet od oko 50ak metara unutar nekog prostora ili do 100 metara izvan navedenog prostora. Da bi se postigle veće brzine prenosa i veći domet, posebno na teško pristupačnom terenu, koriste se

[18] WiFi - IEEE 802.11 WLAN (engl. WLAN - Wireless Local Area Networks)

[19] WiMAX - IEEE 802.16 standard

dualne antene, radio pojačavači ili usmerene antene tako da se može postići pokrivanje u prostoru od nekoliko kilometara pod uslovom da postoji optičko dogledanje[64].

WLAN tehnologija je široko primenjena u vojnim komunikacionim sistemima, pre svega u sistemima koji se koriste u borbenim vozilima, na komandnim mestima, kod ad-hoc mreža jedinica specijalne namene i kod malih timova koji koriste taktički personalni radio. Nove i savremene aplikacije, a koje su u procesu evaluacije, obuhvataju korišćenje WiFi komunikacija za međusobnu komunikaciju članova tima raspoređenih u integrisanih i borbena odela pešadije. Takođe značajna je primena i kod drugih aplikacija koje obuhvataju mrežu nepovezanih zemaljskih senzora za praćenje, zaštitu snaga i prikupljanje obaveštajnih informacija[64]. Slika 35 prikazuje mogući scenario korišćenja Wi-Fi u operativnom borbenom scenariju.



Slika 35. Mogući scenario korišćenja Wi-Fi u operativnom borbenom scenariju (preuteto iz [64])

WiMAX bežična tehnologija pruža mogućnost komunikacije sa velikim propusnim opsegom i na realtivno većim rastojanjima. WiMAX je bežična širokopojasna

tehnologija, definisana IEEE 802.16 standardom. Navedeni standard je izveden iz IEEE 802.11 WiFi standarda koji trenutno opslužuje "*hot-spots*" i bežične lokalne mreže širom sveta i široko je prihvaćen od strane vojske. Za razliku od WiFi tehnologije, koji pokriva manja rastojanja i ima ograničenja pri primeni u urbanom području zbog prostiranja, WiMAX može da radi u višim frekventnim opsezima i da obezbedi pokrivenost na distanci i do 50 km, kada se koriste stacionarne konekcije sa optičkim dogledanjem[64]. Mreža podržava brzinu prenosa podataka do 50 Mb/s, sa stabilnom brzinom prenosa korisničkih podataka od 0.5 do 2 Mb/s obezbeđujući pri tome simultani prenos podataka (uključujući i sliku visoke rezolucije), glas (engl. *VoIP - Voice over IP*) i video. Takođe, WiMAX tehnologija efikasno obezbeđuje servise na rastojanju od 5 do 8 km za mobilne korisnike (bez direktnog optičkog dogledanja)[74].

Kako WiMAX koristi više frekventne opsege nego sadašnje vojne i komercijalne komunikacije, postojeći antenski stubovi mogu da dele WiMAX ćelijski sistem bez kompromitovanja komunikacionih servisa. Takav način implementacije može da se koristi za raspoređivanje WiMAX stanica radi povećanja propusnog opseg za specifične i u pogledu raspoloživih kapaciteta zahtevne aplikacije unutar postojeće mreže. Takođe, integracija WiMAX talasnih formi je već razvijena za budući softverski definisani radio (engl. *SDR -Software Deffined Radio*) i može biti odmah uveden u buduću taktički radio sistem (engl. *JTRS - Joint Tactical Radio System*). WiMAX može da se koristi za pokrivanje područja gde se izvodi obuka, obezbeđujući pri tome infrastrukturu za potpunu integraciju obuke u realnim uslovima i simulacije ratnih igara. WiMAX standard obezbeđuje osnovu za izgradnju mobilnih prostornih multikorisničkih mreža (engl. MANET - Mobile Area Networks)[75].

Bežični komunikacioni kanali, sa svojim specifičnim karakteristikama kao što su senke, feding i interferencija, prostiranje po više kanala, ograničavaju dodeljeni propusni opseg za različite aplikacije. U skladu sa navedenim činjeničnim stanjem, tehnike kompresije multimedijalnih podataka postaju neophodni i suštinski deo razmene multimedijalnih podataka preko WLAN mreža.

H.265/HEVC standard kodovanja video podataka postiže efikasnu kompresiju video podataka u propusnom opsegu od nekoliko kilobita do nekoliko megabita u sekundi. Prema tome, važna komponenta mnogih bežičnih multimedijalnih servisa jeste prenos H.265/HEVC video podataka. Kao što je prethodno rečeno, HEVC standard definiše

sloj apstrakcije mreže koji realizuje adaptaciju izlaznih podataka iz enkodera i njihovo prilagođavanje zahtevima različitih tehnologija prenosa. Na taj način, HEVC video tok može biti prilagođen zahtevima WiFi i WiMAX tehnologija. Takođe, HEVC standard je uveo niz tehnika kao što su podela na isečke, adaptivna “quadtree” struktura stabla kao osnovna jedinica kodiranja, napredne tehnike raspoređivanja osnovnih jedinica kodiranja, koje čine navedeni standard otpornim na greške.

7. ZAKLJUČAK

U ovom radu definisan je novi, originalan i efikasan mehanizam kriptografske sinhronizacije u algoritmima selektivno šifrovanog video toka najnovijeg HEVC/H.265 standarda kompresije video podataka. Ponuđeni mehanizam kriptografske sinhronizacije realizovan je definisanjem sintakse i semantike nove HEVC ne-VCL NAL jedinice koja sadrži sintaksne elemente koji svi zajedno predstavljaju skup parametara kriptografske sinhronizacije (*CSPS - Crypto Synchronization Parameter Set*). Samim tim što je definisan kao ne-VCL NAL jedinica, sa svim pratećim elementima, ponuđeno rešenje predstavlja proširenje HEVC standarda.

Ovako definisan skup parametara kriptografske sinhronizacije omogućava slučajni pristup selektivno šifrovanom HEVC video toku. Pri čemu, slučajni pristup selektivno šifrovanom video toku podrazumeva sposobnost prijemne strane (dekodera) da otpočne dešifrovanje i dekodiranje video podataka u proizvoljnoj tački slučajnog pristupa, u okviru selektivno šifrovanog HEVC video toka, lako i efikasno kao i u bilo kojoj drugoj tački slučajnog pristupa, bez obzira na to koliko tačaka slučajnog pristupa postoji u selektivno šifrovanom video toku. Navedeni mehanizam je izrazito efikasan jer je, kako je u radu pokazano, broj bajtova koje unosi u HEVC video tok minimalan u odnosu na celokupni broj bajtova u selektivno šifrovanom video toku. Veću efikasnost pokazuje kod video sekvenci sa većom rezolucijom, što je pozitivno jer je novi HEVC/H.265 standard kompresije video podataka pre svega kreiran da omogući enkodovanje video sekvenci većih rezolucija. Takođe, u radu je pokazano da je, ponuđeni mehanizam kriptografske sinhronizacije, nezavistan od primenjenog algoritma selektivnog šifrovanja, što na neki način predloženi mehanizam kriptografske sinhronizacije čini univerzalnim u odnosu na postojeće i nove algoritme selektivnog šifrovanja HEVC video toka.

Ovako definisani mehanizam kriptografske sinhronizacije nema primenu samo pri implementaciji operacije slučajnog pristupa selektivno šifrovanom HEVC video toku. On se može primenjivati, i primenjuje se, za brzo ispravljanje posledica brisanja ili

umetanja bita u blok šifrata selektivno šifrovanog dela video toka, koji za posledicu ima neispravno dešifrovanje svih sukcesivnih blokova šifrata a samim tim i neuspešno dekodiranje video toka. U tom slučaju, maksimalan broj frejmova (slika) koji treba da prođe (da se propusti), pre kriptografske resinhronizacije i ponovnog uspešnog dešifrovanja i dekodovanja video toka, je veći ili jednak nuli a manji od vrednosti *IntraPeriod* parametra. Na osnovu ovoga se može zaključiti da je predloženi mehanizam podjednako efikasno primenljiv i u *random acces* i u *real-time* modu rada HEVC dekodera.

Zahvaljujući svojim performansama koje se prvenstveno odnose na povećanje efikasnosti kodovanja, laku integraciju u različite sisteme prenosa, otpornost na gubitak podataka i olakšanu implemetaciju na različitim paralelnim arhitekturama, H.265/HEVC standard nalazi sve veću primenu, pored ostalih, i u vojnim komunikacionim sistemima i aplikacijama. Ovu tvrdnju dodatno podstiče činjenica da su pojedine vojne organizacije i savezi usvojili navedeni standard kao njihov prioritetni standard kompresije video podataka koji se koristi i planira da se koristi u širokom spektru vojnih aplikacija i sistema. U radu je dat teorijski osvrt na mogućnost primene ponuđenog rešenja u vojnim komunikacionim sistemima.

Ovaj rad otvara nekoliko novih pravaca istraživanja koji bi u budućem istraživačkom radu mogli biti sprovedeni. Jedan pravac bi mogao da bude istraživanje elementarnih struktura za dizajniranje algoritama selektivnog šifrovanja koji eksploatišu prednosti olakšane implementacije na paralelnim arhitekturama. Moguće paralelne arhitekture na kojima bi se razmatrale implementacije navedenih algoritama selektivnog šifrovanja su FPGA (engl. *FPGA - Field-programmable Gate Array*) platforma ili grafičke kartice sa CUDA (engl. *CUDA - Compute Unified Device Architecture*) tehnologijom. Istovremeno sa dizajniranjem navedenih algoritama selektivnog šifrovanja na paralelnim arhitekturama, automatski će se pojaviti potreba da se nastavi istraživački proces redizajniranja ponuđenog efikasnog mehanizma kriptografske sinhronizacije i njegovo prilagođavanje potrebama kriptografske sinhronizacije novih algoritama selektivnog šifrovanja koji eksploatišu mogućnosti implementacije HEVC enkodera i dekodera na paralelnim arhitekturama. Drugi pravac istraživanja mogao bi da obuhvata sagledavanje mogućnosti za implementaciju postojećih ali i potpuno novih algoritama

selektivnog šifrovanja HEVC video toka u postojećim i u novim sistemima i aplikacijama u okviru vojnih komunikacionih sistema.

LITERATURA

[1] G. J. Sullivan, J.-R. Ohm, W.-J. Han, and T. Wiegand, "Overview of the High Efficiency Video Coding (HEVC) Standard", *IEEE Circuits and Systems for Video Technology*, volume 22, no. 12, pp. 1649 –1668. doi: 10.1109/TCSVT.2012.2221191

[2] ITU-T Rec. H.262 and ISO/IEC 13818-2 (2000) *Generic coding of moving pictures and associated audio information: Video*. (MPEG-2 Video), 2nd editon.

[3] ITU-T Rec. H.264 and ISO/IEC 14496-10 (2012) *Advanced video coding. 7th edition*.

[4] ITU-R Rec. BT.2020 (2012) Parameter values for ultra-high definition television systems for production and international programme exchange.

[5] ITU-T Rec. H.265 and ISO/IEC 23008-10 (2013) *High efficiency video coding.*

[6] P. Chen, Y. Ye, M. Karczewicz, "*Video coding using extended block sizes*". ITU-T SG16 Q6 Video Coding Experts Group (VCEG), Document VCEG- AJ23, San Diego, Octobar 2008.

[7] K. Ugur, K.R. Andersson, A. Fuldseth, Video coding technology proposal by Tandberg, Nokia, and Ericsson, Joint Collaborative Team on Video Coding (JCT-VC), Document JCTVCA119, Dresden, April 2010.

[8] S. Kanumuri, T.K. Tan, F. Bossen, Enhancements to intra coding, Joint Collaborative Team on Video Coding (JCT-VC), Document JCTVC-D235, Daegu, Januar 2011.

[9] V. Sze, M. Budagavi, G. J. Sulliven, *Hight Efficinecy Video Coding (HEVC), Algorithms and Architectures*, Springer International Publishing, Switzerland 2014.

[10] A.M. Tourapis, F. Wu, S. Li, "Direct mode coding for bipredictive slices in the H.264 standard", *IEEE Transaction of Circuits Systems for Video Technologies*, volume 15, no. 1, pp. 119–126.

[11] A. Norkin, G. Bjøntegaard, A. Fuldseth, M. Narroschke, M. Ikeda, K. Andersson K, M. Zhou, G.V. der Auwera, "HEVC deblocking filter", *IEEE Transaction of Circuits Systems for Video Technologies*, volume 22, no. 11, pp. 1746–1754.

[12] D. Marpe, H. Schwarz, T. Wiegand, "Context-adaptive binary arithmetic coding in the H.264/AVC video compression standard", *IEEE Transaction of Circuits Systems for Video Technologies*, volume 13, no. 7, pp. 620–636, Jul. 2003.

[13] V. Sze, M. Budagavi, "High Throughput CABAC Entropy Coding in HEVC", *IEEE Transaction of Circuits Systems for Video Technologies*, volume 22, no. 12, pp. 1778 - 1791.

[14] C.E. Shannon, "A mathematical theory of communications", *Bell Systems Techical Journal*, volume 27, pp. 379–423, 1948.

[15] R. Sjöberg, Y. Chen, A. Fujibayashi, M.M. Hannuksela, J. Samuelsson, T.K. Tan, Y.-K. Wang, S. Wenger, "Overview of HEVC high-level syntax and reference picture management", *IEEE Transaction of Circuits Systems for Video Technologies*, volume 22, no. 12, pp. 1858–1870.

[16] A. Fujibayashi, T.K. Tan, *Random access support for HEVC, Joint Collaborative Team on Video Coding (JCT-VC)*, Document JCTVC-D234, Daegu, Januar 2011.

[17] Y.-K. Wang, Y. Sanchez, T. Schierl, S. Wenger, M.M. Hannuksela, RTP payload format for high efficiency video coding. RFC 7789, mart 2016.

[18] T. Schierl, M.M. Hannuksela, Y.-K. Wang, S. Wenger S, "System layer integration of high efficiency video coding", *IEEE Transaction of Circuits Systems for Video Technologies*, volume 22, no. 12, pp. 1871–1884

[19] C.E. Shannon, "Communication theory of secrecy systems", *Bell System Technical Journal*, volume 28, pp. 656–715, 1949.

[20] B. Jovanović, "Algoritmi selektivnog šifrovanja – pregled sa ocenom performansi", *Vojnotehnički glasnik 4/2010*, Ministarstvo odbrane Republike Srbije, Beograd, 2010.

[21] T. Lookabaugh, "Selective encryption, information theory, and compression", *in Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers*, volume1., pp 373–376, Calif, USA, 2004.

[22] J. Baumgartner, "Deciphering the CA conundrum," *Communications Engineering and Design*, March 2003.

[23] T. Lookabaugh, D.C. Sicker, “Selective encryption for consumer applications”, *IEEE Communications Magazine*, volume 42, no. 5, pp. 124–129, 2004.

[24] A. Massoudi, F. Lefebvre, C. De Vleeschouwer, B. Macq, J.-J. Quisquater, “Overview on Selective Encryption of Image and Video: Challenges and Perspectives”, *EURASIP Journal on Information Security*, Volume 2008, Article ID 179290, doi:10.1155/2008/179290

[25] D. Van de Ville, W. Philips, R. Van de Walle, I. Lemahieu, “Image scrambling without bandwidth expansion,” *IEEE Transactions on Circuits and Systems for Video Technology*, volume 14, no. 6, pp. 892–897, 2004.

[26] S. Li, C. Li, K.-T. Lo, G. Chen, “Cryptanalysis of an image scrambling scheme without bandwidth expansion”, *IEEE Transactions on Circuits and Systems for Video Technology*, volume 18, no. 3, pp. 338–349, 2008.

[27] R. Lundin, S. Lindskog, A. Brunstrom, S. Fischer-Hubner, “Measuring confidentiality of selectively encrypted messages using guesswork”, *in Proceedings of the 3rd Swedish National Computer Networking Workshop (SNCNW’05)*, pp. 99–102, Halmstad, Sweden, November 2005.

[28] J.O. Pliam, “Guesswork and Variation Distance as Measures of Cipher Security”, *Selected Areas in Cryptography. SAC 1999. Lecture Notes in Computer Science*, volume 1758. Springer, Berlin, Heidelberg.

[29] D. Malone, W. G. Sullivan, “Guesswork and entropy”, *IEEE Transactions on Information Theory*, volume 50, no. 3, pp. 525– 526, 2004.

[30] R. Norcen, A. Uhl, “Selective encryption of the JPEG2000 bitstream,” *in Communications and Multimedia Security, volume 2828 of Lecture Notes in Computer Science*, pp. 194–204, Springer, Berlin, Germany, 2003.

[31] Z. Shahid, W. Puech, “Visual protection of HEVC video by selective encryption of CABAC binstrings”, *IEEE Transactions on Multimedia*, volume 16, pp. 24-36. doi:10.1109/TMM.2013.2281029

[32] G. Van Wallendael, A. Boho, J. De Cock, A. Munteanu, R. Van de Walle, “Encryption for high efficiency video coding with video adaptation capabilities”, *IEEE Transaction on Consumer Electronics*, volume 59, no. 3, pp 634–642. doi:10.1109/TCE.2013.6626250

[33] K. J. Nehete, M.B. Bhagyalakshmi, B. Manjunath, S. Chaudhari, T.R Ramamohan, "A real-time MPEG video encryption algorithm using AES", *The national conference on communications (NCC)*, pp. 164–168, 2003.

[34] V. Vijayalakshmi, L. M. Varalakshmi, G. F. Sudha, "Efficient encryption of intra and inter frames in MPEG video", *Recent trends in network security and applications communications incomputer and information science*, volume 89, pp. 93–104. New York, Springer, 2010.

[35] V. A. Memos, K. E. Psannis, "Encryption algorithm for efficient transmission of HEVC media", *Journal of Real-Time Image Processing*, Volume 12, Issue 2, pp 473–482. August 2016. doi: 10.1007/s11554-015-0509-3

[36] A. S. Mohammed, Md. T. Nooritawati, H. Habibah, "Moving Objects Encryption of High Efficiency Video Coding (HEVC) using AES Algorithm", *Journal of telecommunication electronic and computer enginiering*, Volume 8, no. 3, pp 31-36. 2017.

[37] H. Hofbauer, A. Uhl, A. Unterweger, "Transparent encryption for HEVC using bit-stream-based selective coefficient sign encryption", *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 4.-9. maj 2014. doi: 10.1109/ICASSP.2014.6853946

[38] Y. Wang, S. Member, "A Tunable Encryption Scheme and Analysis of Fast Selective Encryption for CAVLC and CABAC in H.264/AVC", *IEEE Transactions on Circuits and Systems for Video Technology*, volume 23, no.9, pp. 1476–1490, Septembar 2013.

[39] M. Ouamri, K. M. Faraoun, "Robust and fast selective encryption for HEVC videos", *Journal of communication software and systems*, volume 10, no. 4, decembar 2014.

[40] B. Jovanović, "Kriptografska sfera zaštite računarskih sistema", *Skripta za studente Vojne akademije*, Ministarstvo odbrane i Vojska Srbije, 2007.

[41] G. Đorđević, M. Marković, T. Unkašević, "Neki aspekti implementacije IDEA algoritma na signal procesorima TI TMS320C45x familije", *9. Telekomunikacioni forum TELFOR 2001.*, 20.-22. Novembar 2001., Beograd

[42] W. Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition", Prentice Hall, 16. Novembar 2005.

[43] W. Diffie, M.E. Hellman, “New directions in cryptography”, *IEEE Transactions on Information Theory*, Volume 22, no. 6, pp. 644-654, 1976.

[44] J. Daemen, V. Rijmen, “AES Proposal: Rijndael“, *NIST AES Proposal*, 1998.

[45] R. Anderson, E. Biham, L. Knudsen, “Serpent: A Proposal for the Advanced Encryption Standard“, *NIST AES Proposal*, 1998.

[46] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, “Twofish: A 128-bit Block Cipher“, *NIST AES Proposal*, 1998.

[47] R. Rivest, M. Robshaw, R. Sidney: “The RC6 Block Cipher“, *NIST AES Proposal*, 1998.

[48] C. Burwick, D. Coppersmith, E. D’Avignon, R. Gennaro, S. Halevi, C. Jutla, S. Matyas, L. O’Connor, M. Peyravian, N. Safford, N Zunic: “MARS-a candidate cipher for AES“, *NIST AES Proposal*, 1998.

[49] FIPS 197, “Advanced Encryption Standard“, *Federal Information Processing Standard Publication 197*, 26. Novembar 2001.

[50] A. Menezes, P. van Orschot, S. Vanstone, “Handbook of Applied Cryptography“, CRC Press, New York, 1997.

[51] M. Dworkin, “Recommendation for block cipher modes of operation, Methods and techniques“, *NIST special publication 800-38a*, 2001.

[52] “Information technology - Security techniques - Modes of operation for an n-bit block cipher“, *International standard ISO/IEC 10116:2006*.

[53] P. Rogaway, “Evaluation of some blockcipher modes of operation“, *University of California*, 10. Februar 2011.

[54] D. A. McGrew, “Counter Mode Security: Analysis and Recommendations”, *Cisco Systems*, Novembar 2002.

[55] B. Jovanović, S. Gajin, “An efficient mechanism of cryptographic synchronization within selectively encrypted H.265/HEVC video stream”, *Multimedia tools and applications*, volume 77, no 2, pp 1537-1553, 15. januar 2018.

[56] K. McCann, B. Bross, W.J. Han, I.K. Kim, K. Sugimoto, G.J. Sullivan, “High Efficiency Video Coding (HEVC) Test Model 15 (HM 15) Encoder Description”, *JCTVC-Q1002*, Valencia, Spain, 2014.

[57] F. Bossen, B. Bross, K. Suhrnig, D. Flynn, "HEVC complexity and Implementation analysis", *IEEE Circuits and Systems for Video Technology*, Volume 22, no. 12, pp. 1685-1696, decembar 2012.

[58] *http://www.libde265.org*, poslednji put pregledano januara 2018. godine.

[59] E. Gama, R. Helm, R. Johnson, J. Vlissides, "Design patterns: elements of reusable object-oriented software", Addison-Wesley, 1995.

[60] F. Bossen, "Common test conditions and software reference configurations, Joint Collaborative Team on Video Coding (JCT-VC)", *Document JCTVC-L1110*, Geneva, Januar 2014.

[61] V. Baroncini, J.R. Ohm, G. Sullivan, "Report of subjective test results of responses to the joint call for proposals (CfP) on Video Coding Technology for High Efficiency Video Coding (HEVC)", *ITU-T/ISO/IEC Joint Collaborative Team on Video Coding (JCT-VC), Document JCTVCA204*, Geneva, CH, fabruar 2010.

[62] MIBS US DoD, "Motion Imageri Standard Profile – MISP-2017.2", Februar 2017. godine.

[63] T. Siglin, "Video in the war zone: The current state of military streaming", *Streaming media magazine – Streaming in War Zone*, januar/feburar 2015. godine.

[64] Z. Miličević, "Multimedijalni H.264/AVC standard u vojnim komunikacionim sistemima", *XXVI Simpozijum o novim tehnologijama u poštanskom i telekomunikacionom saobracaju – PosTel 2008*, Beograd, 16. i 17. decembar 2008.

[65] F. Nilson, "Inteligent network video: understanding modern video surveillance systems", CRC Press, 2009. godine

[66] A.M. Davis, I.M. Weinstein, "The business case for videoconferencing – Achieving a competitive edge", *Wainhouse research*, 2005. godine

[67] Y. Sugito, K. Iguchi, A. Ichigaya, K. Chida, S. Sakaida, H. Sakate, Y. Matsuda, Y. Kawahata and N. Motoyama, "HEVC/H.265 codec system and transmission experiments aimed at 8K broadcasting", *IBC 365 Business Knowledge for the Global Media, Entertainment & Technology Community*, januar. 2018. godine.

[68] *https://www.vitec.com/fileadmin/downloads/Company_Downloads/Brochures/Military_Solutions_Brochure_Web_Rev2.3.pdf*, pregledano 24. decembra 2018. godine.

[69] K. E. Psannis, “HEVC in wireless environments”, *Journal of Real-Time Image Processing*, volume 12, no. 2. pp. 509–516, Jul 2015. godine, DOI 10.1007/s11554-015-0514-6

[70] K.R. Rao, Z.S. Bojković, D.A. Milovanović, “Introduction to Multimedia Communications: Applications, Middleware, Networking”, *John Wiley & Sons, Inc.*, USA, 2006.

[71] K.R. Rao, Z.S. Bojković, D.A. Milovanović, “Wireless Multimedia Communications: Convergence, DSP, QoS and Security”, *CRC Press, Boca Raton, Florida*, USA, 2008.

[72] C. Chaudet, D. Dhoutaut, I.G. Lassous, “Performance issues with IEEE 802.11 in ad hoc networking”, *IEEE Communications Magazine*, pp. 110-116, Jul 2005.

[73] J. Jormakka, H. Jormakka, J. Väre, “A Lightweight Management System for a Military Ad Hoc Network“, *Information Networking, Towards Ubiquitous Networking and Services, ICOIN 2007, Lecture Notes in Computer Science, vol 5200*,. Springer, Berlin, Heidelberg

[74] F.A. Adebari, O. Bello, “Mobile WiMAX as a next generation broadband wireless network”, *International Journal of Science and Technology*, Volume 2, no. 1, Januar 2013.

[75] M. Seyedzadegan, M. Othman, “IEEE 802.16: WiMAX Overview, WiMAX Architecture”, *International Journal of Computer Theory and Engineering*, Volume 5, no. 5, Octobar 2013.

BIOGRAFIJA AUTORA

Rođen je u Surdulici 17.02.1982. godine. Osnovnu školu završio je u Crnoj Travi, a gimnaziju, prirodno matematički smer, u Vlasotincu. Diplomirao je na Vojnoj akademiji – Odsek Logistike, smer Služba Informatike po programu Računarska tehnika i informatika. Odbranio je diplomski rad u oblasti Veštačke inteligencije i ekspertskih sistema, sa osvrtom na njihovu primenu u nastavno obrazovnom procesu. Od 2006. godine zaposlen je u Centru za primenjenu matematiku i elektroniku, Uprave za telekomunikacije i informatiku, Generalštaba Vojske Srbije. Kao Viši kriptolog i Načelnik odseka za kriptozaštitu u računarskim mrežama, radi na rukovođenju i realizaciji većeg broja projekta u oblasti višeslojne arhitekture zaštite računarskih mreža i kriptozaštite u mobilnim komunikacijama. Navedeni projekti i postignuti rezultati su od velikog značaja za bezbednost računarskih mreža Ministarstva odbrane i Vojske Srbije. Takođe, radi kao saradnik u nastavi i asistent na predmetima „Zaštita računarskih sistema“ i „Operativni sistemi“ na Vojnoj akademiji u Beogradu.

Tokom doktorskih studija bavio se istraživanjem u oblasti bezbednosti računarskih sistema, višeslojne arhitekture kriptozaštite računarskih mreža i primenjene kriptografije. Poseban akcenat u istraživačkom radu dat je u oblasti primenjene kriptografije i na istraživanju mehanizama šifrovanja i selektivnog šifrovanja u multimedijalnim informacijama – posebno u oblasti video kompresije.

Autor je jednog rada u međunarodnom časopisu sa *impact* faktorom, jednog rada na međunarodnoj konferenciji i većeg broja radova na domaćim konferencijama i u domaćim časopisima.

Na doktorskim studijama je stipendista Ministarstva odbrane Republike Srbije.

IZJAVA O AUTORSTVU

Ime i prezime autora Boriša Jovanović

Broj indeksa 5040/2016

Izjavljujem

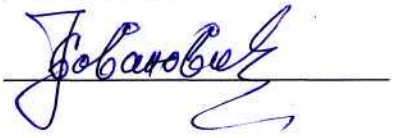
da je doktorska disertacija pod naslovom

Efikasan mehanizam kriptografske sinhronizacije u algoritmima selektivnog šifrovanja multimedijalnih sistema nove generacije

- rezultat sopstvenog istraživačkog rada;
- da disertacija u celini ni u delovima nije bila predložena za sticanje druge diplome prema studijskim programima drugih visokoškolskih ustanova;
- da su rezultati korektno navedeni i
- da nisam kršio/la autorska prava i koristio/la intelektualnu svojinu drugih lica.

Potpis autora

U Beogradu, 31.05.2018.



IZJAVA O ISTOVETNOSTI ŠTAMPANE I ELEKTRONSKE VERZIJE DOKTORSKOG RADA

Ime i prezime autora:	Boriša Jovanović
Broj indeksa	4050/2016
Studijski program	Softversko inženjerstvo
Naslov rada	*Efikasan mehanizam kriptografske sinhronizacije u algoritmima selektivnog šifrovanja multimedijalnih sistema nove generacije*
Mentor	docent dr. Slavko Gajin dipl. inž.

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao/la radi pohranjena u **Digitalnom repozitorijumu Univerziteta u Beogradu.**

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog naziva doktora nauka, kao što su ime i prezime, godina i mesto rođenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu.

Potpis autora

U Beogradu, 31.05.2018.

IZJAVA O KORIŠĆENJU

Ovlašćujem Univerzitetsku biblioteku „Svetozar Marković“ da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom:

Efikasan mehanizam kriptografske sinhronizacije u algoritmima selektivnog šifrovanja multimedijalnih sistema nove generacije

koja je moje autorsko delo.

Disertaciju sa svim prilozima predao/la sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalnom repozitorijumu Univerziteta u Beogradu i dostupnu u otvorenom pristupu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio/la.

1. Autorstvo (CC BY)
2. Autorstvo – nekomercijalno (CC BY-NC)
3. Autorstvo – nekomercijalno – bez prerada (CC BY-NC-ND)
4. Autorstvo – nekomercijalno – deliti pod istim uslovima (CC BY-NC-SA)
5. Autorstvo – bez prerada (CC BY-ND)
6. Autorstvo – deliti pod istim uslovima (CC BY-SA)

(Molimo da zaokružite samo jednu od šest ponuđenih licenci.
Kratak opis licenci je sastavni deo ove izjave).

Potpis autora

U Beogradu, 31.05.2018.

1. **Autorstvo**. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.
2. **Autorstvo – nekomercijalno**. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.
3. **Autorstvo – nekomercijalno – bez prerada**. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.
4. **Autorstvo – nekomercijalno – deliti pod istim uslovima**. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.
5. **Autorstvo – bez prerada**. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način određen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.
6. **Autorstvo – deliti pod istim uslovima**. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način određen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.