# ALGORITMI SELEKTIVNOG ŠIFROVANJA – PREGLED SA OCENOM PERFORMANSI

Jovanović Ž. *Boriša*, Generalštab Vojske Srbije, Uprava za telekomunikacije i informatiku (J-6), Centar za primenjenu matematiku i elektroniku, Beograd

UDC: 621.391.037.37 ; 681.188

*Sažetak:*

*Digitalni multimedijalni sadržaj postaje zastupljeniji i sve više se razmenjuje putem računarskih mreža i javnih kanala (satelitske komunikacije, bežične mreže, internet, itd.) koji predstavljaju nebezbedne medijume za prenos informacija osetljive sadržine. Sve više na značaju dobijaju mehanizmi kriptološke zaštite slika i video sadržaja. Tradicionalni sistemi kriptografske obrade u sitemima za prenos ovih vrsta informacija garantuju visok stepen sigurnosti, ali i imaju svoje nedostatke – visoku cenu implementacije i znatno kašnjenje u prenosu podataka. Pomenuti nedostaci se prevazilaze primenom algoritama selektivnog šifrovanja.*

Ključne reči: *selektivno šifrovanje, algoritam kompresije, multimedijalni sadržaj, računarske mreže.*

## Uvod

U tradicionalnim sistemima za prenos slike i video sadržaja celokupni sadržaj koji se prenosi najpre se kompresuje primenom nekog od algoritama kompresije. Zatim se tako dobijeni niz podataka u celosti kriptološki zaštiti primenom nekog od standardnih kriptografskih algoritama (DES – *Data Encryption Algorithm,* IDEA – *International Data Encryption Algorithm,* AES – *Advanced Encryption Algorithm*). Specifične karakteristike podataka ovog tipa, velika bitska brzina prenosa podatka i ograničena dozvoljena širina propusnog opsega, čine standardne kriptografske algortime neadekvatnim za primenu u ove svrhe. Drugo ograničenje tradicionalnih sistema za prenos podataka ovog tipa jeste što se primenom tradicionalnih tehnika zaštite menja struktura i sintaksa samog toka podataka, čime se onemogućavaju određene funkcionalnosti kodera koji generišu taj tok podataka kao i dekodera koji, na prijemnoj strani, interpretiraju primljene podatke. Novi trend u oblasti kriptografske zaštite slika i video sadržaja jeste primena mehanizama selektivnog šifrovanja. Kako samo ime kaže, ovi mehanizmi se sastoje od kriptološke obrade samo određenog podskupa podataka. Cilj primene mehanizama selektivnog šifrovanja jeste da se smanji količina podataka koju treba kriptološki obraditi a da istovremeno



borisa.jovanovic@vs.rs

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 to da se sadržaj koji se prenosi putem komunikacionog sistema deli 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 kriptološke tehnike. Na taj način se postiže da samo autorizovani korisnici imaju pristup zaštićenom delu podataka. Na osnovu ove podele otkriva se jedna veoma bitna karakteristika ovakvih sitema – nastojanje da se zaštićeni deo, deo koji treba kriptološki obraditi, učini što je moguće manjim.

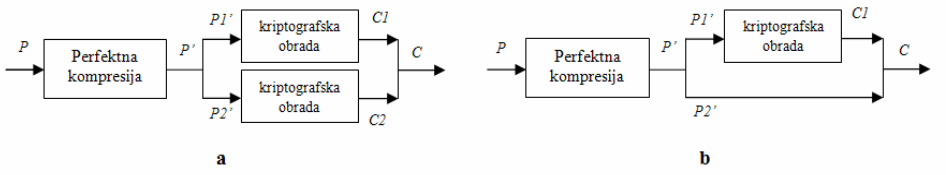
Način na koji se vrši definisanje javnog i zaštićenog dela isključivo zavisi od oblasti u kojoj se ovakvi mehanizmi primenjuju. U komercijalnim primenama (televizijski sistemi i prenos video sadržaja) uloga sistema selektivnog šifrovanja je da potencijalnom korisniku daju samo onoliko informacija koliko je potrebno da donese odluku da kupi pravo na prijem celokupnog sadržaja. U ovakvim sistemima postiže se samo nizak nivo vizuelne degradacije video sadržaja, tako da potencijalni napadač još uvek ima mogućnosti da delimično protumači sadržaj, ali ipak donosi odluku da plati i dobije pristup nešifrovanom video sadržaju u njegovom punom kvalitetu. U složenijim sistemima koji prenose video sadržaje od velikog značaja primenjuju se tehnike koje pružaju veoma visok nivo vizuelne degradacije kojima se postiže da se video sadržaj u potpunosti učini nedostupnim neautorizovanim korisnicima.

U ovom radu predočen je kratak pregled algoritama selektivnog šifrovanja sa mogućim oblastima primene. Na samom početku date su teorijske osnove selektivnog šifrovanja, izvršena je klasifikacija algoritama selektivnog šifrovanja i definisani su osnovni kriterijumi na osnovu kojih se vrši ocenjivanje kvaliteta nekog algoritma iz ove grupe algoritama. U glavnom delu rada dat je opis i ocena najpoznatijih algoritama selektivnog šifrovanja i ukazano na njihove dobre i loše osobine, kao i na moguće oblasti njihove primene. Na samom kraju, u zaključku, prikazan je osvrt na glavne izazove i probleme u primeni različitih algoritama iz ove familije, kao i na perspektivu primene sistema selektivog šifrovanja u komunikacionim sistemima.

## Teorijske osnove selektivnog šifrovanja

Prve indirektne teorijske osnove selektivnog šifrovanja dao je Klod Šenon još 1949. godine, u svom radu 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 koje su sa bezbedonosne tačke gledišta na nešto nižem nivou. Šenon u svom radu [1] 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. Na osnovu ovoga se može izvući zaključak da bi kriptološki zaštićeni sadržaj bio što sigurniji neophodno je da izvor sadržaja ima što manje ponavljanja. 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 1a) gde su ***C1*** i ***C2*** kriptološki obrađeni sadržaj poruka ***P1'*** i ***P2'*** respektivno.




*Slika 1* – (a) Tradicionalni sistem i (b) sistem selektivnog šifrovanja

Savršena kompresija podrazumeva da ako nam je poznat sadržaj poruke ***P1'*** onda se sadržaj poruke ***P2'*** ne može predvideti. Ovakva konstatacija može se 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[2]. 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 1b), dok je sigurnost cele poruke obezbeđena prethodno diskutovanim i dokazanim postupcima, uz pretpostavku da su sva ponavljanja iz izvora poruka uklonjena. Poruka ***P1'*** je zaštićena i njen sadržaj se ne može predvideti na osnovu ***P2'*** jer se koristi perfektan algoritam kompresije.

Na osnovu ovoga se može zaključiti da je dobra kompresija neophodan preduslov efikasnog algoritma selektovnog šifrovanja. Jedino pitanje koje preostaje je kako izabrati i koji deo toka podataka selektivno šifrovati kako bi time postigli željeni nivo vizuelene 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 (JPEG – *Joint Photographic Experts Group*) algoritma komresije biti kojima se kodiraju DC koeficijenti imaju veći uticaj na kvalitet rekonstrukcije od bita kojima se kodiraju AC koeficijenti (DC and AC coefficient – *normalizovani koeficijenti diskretne kosinusne transformacije*). Jedna prednost ovakvih algoritama kompresije koji koncentrišu informacije neravnomerno je to što oni na taj način istovremeno i pomažu pri izboru koji deo toka podataka treba kriptološki obraditi. Mnogi algoritmi selektivnog šifrovanja se upravo zasnivaju na ovim karakteristikama algoritama kompresije.

Ova praznina između teorijski opisanog selektivnog šivrovanja koje se bazira na postupcima perfektne kompresije i postojećih algoritama selektivnog šifrovanja predstavlja glavni problem pri ocenjivanju bezbedonosnih aspekata i kvaliteta određenog algoritma selektivnog šifrovanja. U mnogim slučajevima se pri ocenjivanju bezbednosti kao jedini parametar koristi nivo vizuelne degradacijie sa pretpostavkom da ukoliko je snažnije vizuelno izobličenje to je i veća sigurnost primenjene tehnike.

## *Kriterijumi za ocenu performansi algoritama selektivnog šifrovanja*

Za potrebe vrednovanja kvaliteta pojedinih algoritama selektivnog šifrovanja, kao i za njihovo međusobno poređenje, definisan je čitav skup kriterijuma:

– Podesivost

Mnogi od predloženih algoritama selektivnog šifrovanja koriste statičko definisanje dela koji se kriptološki obrađuje kao i statičke definicije kriptoloških parametara. Ovakvo svojstvo ograničava upotrebljivost takve vrste algoritama na ograničeni skup aplikacija. Veoma je poželjno 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 šifrovane video poruke (ili slike) u odnosu na originalnu video poruku (ili sliku). On

podrazumeva da se kriptografski obrađena video poruka (ili slika) može dekodovati i pregledati bez potreba da se dešifruje. Ova pretpostavka nije zadovoljena za sve postojeće algoritme selektivnog šifrovanja. U nekim primenama, može biti poželjno da nivo vizuelene 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 često se javlja zahtev da nivo vizuelne degradacije bude na zadovoljavajuće visokom stepenu tako da se sadržaj poruke u potpunosti sakriva i nije dostupan neovlašćenim korisnicima. Shodno ovome 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 gore navedeno, vizuelna degradacija je subjektivni kriterijum tako da nije moguće samo njega koristiti pri oceni kriptološke snage određenog algoritma selektivnog šifrovanja. Kriptografska bezbednost algoritama selektivnog šifrovanja zasniva se na dva elementa: na izvoru ključa i na nepredvidivosti izbora dela podataka koji se kritpološki obrađuje.

– Kriptografski koeficijent

Ovaj kriterijum prikazuje odnos između veličina kriptološki obrađenog dela poruke i ukupne veličine originalne poruke. Cilj algoritama selektivnog šifrovanja jeste da se postigne što je moguće manji kriptografski koeficijent.

– 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.

– Usklađenost formata

Kriptografski obrađeni tok podataka trebalo bi da bude usaglašen sa formatom koji je kompatibilan sa primenjenim algoritmom kompresije. Bilo koji standardni dekoder trebalo bi da može da dekodira kriptološki obrađeni tok podataka bez prethodnog dešifrovanja. Ovaj kriterijum je veoma važan, jer omogućava očuvanje određenih osobina primenjenog algoritma kompresije (omogućava očuvanje skalabilnosti).

– Otpornost na greške

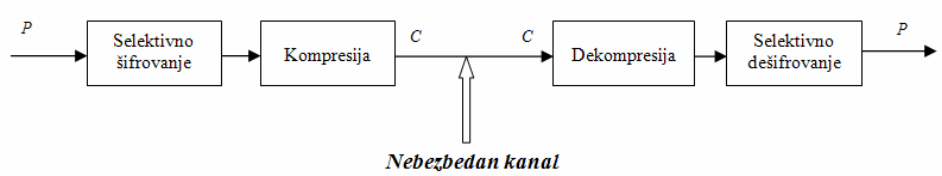
Ovaj kriterijum je veoma značajan, posebno u mrežama koje nisu otporne na greške. Standardni kritpografski algoritmi u svom radu postižu veoma izražen efekat lavine, tako da ukoliko dođe do greške u samo jednom bitu podataka, ta greška će se propagirati na veći broj uzastopnih bita. Ovakva pojava prouzrokuje grešku u procesu dekodiranja ili značajna izobličenja podataka na prijemnoj strani. Cilj postojećih istraživačkih radova jeste da se dizajnira siguran algoritam selektivnog šifrovanja koji istovremeno održava dovoljno dobar efekat lavine, ali ima zadovoljavajuću otpornost na greške.

## *Podela algoritama selektivnog šifrovanja*

Jedna moguća podela algoritama selektivnog šifrovanja izvršena je na osnovu trenutka izvršavanja kriptografske obrade toka 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 značaj na ponašanje kompletnog algoritma selektivnog šifrovanja. Analizom određenog kriterijuma podele utvrđena su tri tipa algoritama selektivnog šifrovanja:

– Prekompresioni

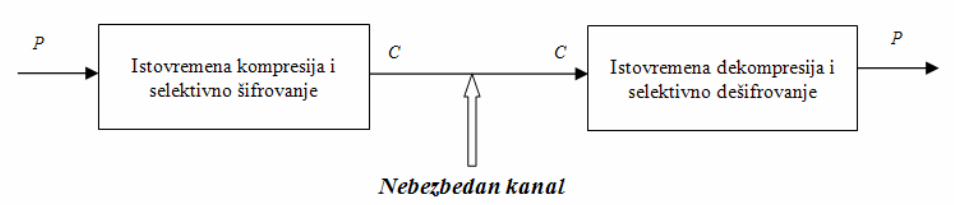
Algoritmi selektivnog šifrovanja iz ove grupe algoritama na predajnoj strani najpre primenjuju kriptološku obradu podatka pa onda primene algoritam kompresije, dok je na prijemnoj strani taj redosled obrnut (slika 2). Na osnovu samog opisa ponašanja može se zaključiti da algoritmi iz ove grupe sigurno zadovoljavaju kriterijum održivosti 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 2* – Šematski prikaz prekompresionih algoritama selektivnog šifrovanja

– Algoritmi istovremene kompresije i kriptografske obrade

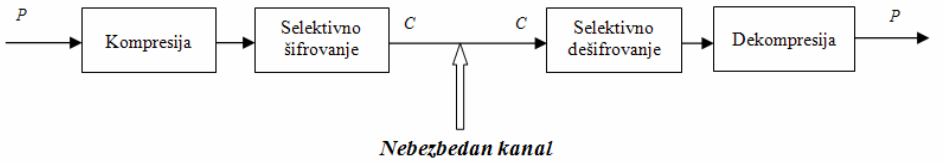
Kod ove klase algoritama selektivnog šifrovanja kriptografska obrada podataka je objedinjena, integrisana, zajedno sa algoritmom kompresije (slika 3). Algoritmi iz ove klase podrazumevaju određene modifikacije i na koderu i na dekoderu tako da se ne može reći da se njima postiže održivost formata i mali uticaj na kompresiju podataka




*Slika 3* – Šematski prikaz algoritama istovremene kompresije i kriptografske obrade

– Postkompresioni

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 4). 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.




*Slika 4* – Šematski prikaz postkompresionih algoritama selektivnog šifrovanja

# Pregled algoritama selektivnog šifrovanja

Prema prethodno definisanoj podeli algoritama selektivnog šifrovanja izvršeno je i njihovo međusobno poređenje sa kratkim opisom, isticanjem dobrih i loših osobina i ocenom kvaliteta. Pregled ponuđenih algoritama realizovan je obrađivanjem prethodno definisanih kriterijuma.

## *Prekompresioni algoritmi*

1. Osnovna ideja prekompresionog algoritma, definisanog u [3], zasniva se na kriptološkoj obradi I frejmova (I frame – deo slike koji je kodiran bez referenciranja drugih delova iste slike) u okviru samog MPEG

(MPEG – *Motion Picture Experts Group*) toka podataka kada je u pitanju selektivno šifrovanje video sadržaja. U slučaju kriptološke obrade slika I frejma algoritam se svodi na primenu DES blokovskog kriptografskog algoritma u CBC (engl. CBC – *Cipher Block Chaining*) modu na DC koeficijentima dok se na AC koeficijente primeni slučajna permutacija koja se razlikuje od standardno primenjene cik-cak permutacije. Ocena kvaliteta pomenutog algoritma selektivnog šifrovanja prema prethodno definisanim kriterijumima bi izgledala ovako:

a. Podesivost – algoritam ne spada u grupu podesivih algoritama jer su parametri kriptografskog algoritma ali i parametri selektivno odabranih podataka statički.
b. Vizuelna degradacija – kako se P i B frejmovi (P and B frame – delovi slike koji se kodiraju zavisno od sadražaja I frejmova) MPEG toka podataka izračunavaju na osnovu sadržaja I frejmova onda se može reći da se kriptološkom obradom samo I frejmova postiže visok stepen vizuelne degradacije.
c. Kriptografska bezbednost – cik-cak, tj. unakrsno, raspoređivanje AC koeficijenata u okviru I frejmova zamenjuje se nekom pseudoslučajnom permutacijom. Na taj način statističke karakteristike AC koeficijenata su sačvane. Bez obzira na očuvanje statističkih karakteristika postoji mogućnost da se klasičnim tehnikama kriptoanalize (raspoloživi šifrovni sadržaj ili napad putem poznatog otvorenog teksta) rekonstruiše stvarni, ispravni raspored AC koeficijenata. Zaključak koji se izvlači jeste da visok stepen vizuelnog izobličenja ne mora da podrazumeva i visok nivo kriptografske bezbednosti.
d. Kriptografski koeficijent – u pomenutom radu nije razmatran odnos kriptološki obrađenog dela poruke i veličine cele poruke tako da ovaj parametar ocene nije razmatran.
e. Uticaj na kompresiju podataka – neoptimalno skeniranje DCT (DCT – *Discrete Cosine Transform*) koeficijenata značajno utiče na efikasnost algoritma kompresije. Ovakvi oblici skeniranja DCT koeficijenata su direktno suprotni Huffmanovom kodovanju koje je sastavni deo algoritma kompresije.
f. Usklađenost formata – ponuđena šema selektivnog šifrovanja je u potpunosti kompatibilna sa JPEG i MPEG standardima.
g. Otpornost na greške – ponuđeni algoritam selektivnog šifrovanja nije otporan na greške koje se dešavaju na DC koeficijentima. Efekat lavine koji izazivaju simetrični kriptografski algoritmi u ovom slučaju može da izazove značajnu propagaciju greške.

2. U [4] opisan je jedan novi pristup u realizaciji algoritma selektivnog šifrovanja. Autori definišu svoj algoritam (VEA – *Video Encryption Algorithm*) kod koga se uz pomoć tajnog ključa na slučajan način vrši pro-

mena znaka svakog DCT koeficijenta u MPEG toku podataka. U [5] je dat nešto unapređeni osnovni algoritam koji smanjuje složenost izračunavanja i na taj način poboljšava performanse. On se sastoji od kriptološke obrade bita koji određuje znak različitih DC koeficijenata u okviru I frejmova kao i bita koji određuje znak različitih vrednosti vektora pokreta u okviru P i B frejmova. Isti autori u [6] opisuju algoritam čije su performanse unapređene tako da se može koristiti u sistemima za rad u realnom vremenu (RVEA – *RealTime Video Encryption Algorithm*). U ovom algoritmu se kriptološki obrađuju samo odabrani biti znaka DC koeficijenata i/ili biti znaka vektora pokreta u preostalim frejmovima. 64 bita znaka po frejmu podataka se kriptološki obradi.

a. Podesivost – algoritam spada u grupu nepodesivih algoritama selektivnog šifrovanja jer su svi parametri algoritma statički definisani.
b. Vizuelna degradacija – uzevši u obzir da se kriptološki obrađuju i DCT koeficijenti, ali i biti znaka vektora pokreta, ovakvim algoritmom se postiže veoma visok nivo vizuelne degradacije.
c. Kriptografska bezbednost – algoritmi ponuđeni u [4] i [5] imaju dobru kriptografsku bezbednost, ali samo u slučaju kada se ključ koristi samo jednom. U svakom drugom slučaju kriptografska bezbednost je nedovoljna, jer je lako moguće primenom napada putem odabranog teksta izvršiti kriptoanalizu kriptološki obrađenih podataka. Kada je u pitanju [6], kod njega se kriptološki obrađuje samo prvih 64 bita znaka, može se reći da to nije dovoljno sa bezbedonosne tačke gledišta. Ako posmatramo video sadržaje sa velikim rezolucijama i visokom bitskim brzinama, prvih 64 bita stvarno predstavlja veoma mali deo podataka.
d. Kriptografski koeficijent – dok kod [4] i [5] kriptografski koeficijent nije određen u [6], gde se kriptografski obrađuju samo 64 bita po frejmu video podataka, ovaj koeficijent isključivo zavisi od bitske brzine samog toka video podataka.
e. Uticaj na kompresiju podataka – u samim radovima nije jasno preciziran uticaj na algoritam kompresije.
f. Usklađenost formata – ovako kriptološki obrađen MPEG tok podataka je usklađen po formatu sa MPEG standardom.
g. Otpornost na greške – uzevši u obzir da ponuđeni algoritmi selektivnog šifrovanja imaju uticaja i na vektore pokreta u frejmovima MPEG podataka može se reći da imaju malu otpornost na greške i da samo jedna mala greška može imati izrazito nepovoljan uticaj.

3. U algoritmu selektivnog šifrovanja o kome se govori u [7] predložen je postupak selektivnog šifrovanja odabranog polja bita i prikazani su eksperimentalni rezultati na slikama kod kojih se nivo osvetljenosti, odnosno skaliranje sive boje, predstavlja osmobitnim podacima. Ideja koja je primenjena u ovom algoritmu je da se kriptološki obradi samo podskup uređenih polja bita

i to tako da se počne najpre sa poljima bita koja sadrže samo bite najveće težine, tj. MSB bite (MSB – *Most Significant Bit*). Kriptološka obrada podskupa podataka u kome su samo polja bita koja sadrže samo MSB bite ne daje valjane kriptografske rezultate i nije otporna na poznate napade. Dobri bezbedonosni rezultati se postižu kada se pored MSB bita kriptografske tehnike primene i na bar još jedno polje bita, dok se kriptološka obrada tri polja bita pokazala kao veoma dobra i dala značajnu vizuelnu degradaciju. Pomenuti algoritam je namenjen za kriptografsku obradu slika i može se, shodno unapred definisanim kriterijumima, oceniti na sledeći način:

a. Podesivost – ovaj algoritam nije iz grupe podesivih algoritama jer je potrebno kriptografski obraditi tačno definisan broj bita kako bi se postigli željeni efekti.
b. Vizuelna degradacija – za nekompresovanu sliku kod koje se elementi slike (pikseli) predstavljaju osmobitnim podacima, visok nivo vizuelne degradacija se postiže kriptološkom obradom prva tri bita najveće težine.
c. Kriptografska bezbednost – iako se koriste pouzdane kriptografske tehnike pomenuti algoritam nije otporan na napad zamenom sadržaja ukoliko se kriptološki obrađuje samo MSB bit. Sa povećanjem broja bita koji se kriptografski obradi povećava se i sama kriptografska bezbednost. Dobra kriptografska bezbednost se postiže tek u slučajevima kada se kriptografski obrade četiri polja bita, odnosno 50% cele slike.
d. Kriptografski koeficijent – kako je potrebno najmanje tri polja bita, od mogućih osam, kriptografski obraditi da bi se postigla željena vizuelna degradacija i zadovoljavajuća kriptografska bezbednost, to nam govori da je kriptografski koeficijent veći od 0,375.
e. Uticaj na kompresiju podataka – kako je algoritam namenjen za nekompresovane slike a sastoji se u kriptografskoj obradi *n* MSB bita onda značajno utiče na proširenje širine propusnog opsega i ima uticaj na kompresiju podataka.
f. Usklađenost formata – kao potpuno prekompresioni algoritam u potpunosti je usklađen sa različitim formatima.
g. Otpornost na greške – efekat lavine koji je izražen kod blokovskih kriptografskih algoritama (kao što je AES koji se koristi u ovom radu) ima negativan uticaj na otpornost na greške ovako definisanih algoritama.

## Algoritmi istovremene kompresije i kriptografske obrade

1. U [8] opisan je algoritam selektivnog šifrovanja nazvan SEC-MPEG koji je namenjen selektivnom šifrovanju MPEG toka podataka. U svom radu algoritam može da koristi asimetrični RSA (RSA – *Rivest,*

*Shamir, and Adleman*) ili simetrični DES algoritam u CBC modu. Autori su kroz opis algoritma definisali četiri nivoa bezbednosti:

i. Kriptografska obrada svih zaglavlja toka podataka
ii. Kriptografska obrada svih zaglavlja toka podataka i svih DC i nižih AC koeficijenata uzajamno kodiranih blokova
iii. Kriptografska obrada svih I-frejmova i svih I-blokova u P i B frejmovima
iv. Kriptografska obrada celokupnog toka podataka

Ovako opisani algoritam može se, prema definisanim kriterijumima, oceniti na sledeći način:

a. Podesivost – ovaj algoritam se na određeni način može smatrati podesivim algoritmom. Naime, radi se o algoritmu kod koga je definisan veći broj nivoa bezbednosti, koji proizilaze od podskupa podataka koji se bira za kriptografsku obradu, te se može smatrati podesivim.
b. Vizuelna degradacija – kriptografski sadržaj nije kompatibilan sa MPEG formatom pa odatle sledi da se i sadržaj ne može pregledati bez dešifrovanja i ne može se ništa govoriti o stepenu vizuelne degradacije koji je ostvaren.
c. Kriptografska bezbednost – pomenutim algoritmom se postiže veći broj različitih bezbedonosnih nivoa. Ukoliko se vrši kriptografska obrada celog toka podataka postiže se najviša kritpografska bezbednost ali se sa druge strane gube sve prednosti selektivnog šifrovanja. Algoritam koji postiže kriptografsku obradu samo zaglavlja toka podataka imaju veoma nisku kriptografsku bezbednost uzevši u obzir da se vrši kritpografska obrada zaglavlja toka podataka čiji se sadržaj može lako predvideti.
d. Kriptografski koeficijent – broj I blokova u P i B frejmovima može biti jednak broju I blokova u I frejmu što govori da kriptografski koeficijent ovog algoritma može biti veoma blizak vrednosti 1 što značajno umanjuje efikasnost ponuđenog algoritma selektivnog šifrovanja.
e. Uticaj na kompresiju podataka – nema značajnijih uticaja na algoritam kompresije podataka.
f. Usklađenost formata – ponuđeni algoritam nije kompatibilan sa MPEG tokom podataka jer zahteva značajne dodatke i izmene u samom standardu. Da bi pročitali ovako obrađeni tok podataka potreban nam je poseban dekoder.
g. Otpornost na greške – algoritam ima malu otpornost na greške a to je posledica značajnog efekta lavine koji se sreće kod kriptografskih algoritama koji su upotrebljeni.

2. U [9] opisan je generalizovani algoritam selektivnog šifrovanja koji se oslanja na kodove promenljive i fiksne dužine kodne reči. Suština je u

tome da se tok podataka deli na dva dela, prvi deo koji nosi značajne informacije i drugi deo koji nosi informacije koje su od manjeg značaja i koje bez poznavanja prvog dela nemaju nikakvog smisla. Za svako polje iz prve grupe (grupa značajnih informacija) izabiraju se odgovarajuće kodne reči fiksne ili promenljive dužine. Onda se svakoj kodnoj reči, bilo da se radi o rečima fiksne ili promenljive dužine, dodeljuje indeks fiksne dužine. Ukoliko se želi kriptografski obraditi sekvenca određenih kodnih reči dovoljno je samo kriptografski obraditi niz indeksa. Nakon kriptografske obrade indeksi se inverznom funkcijom mapiraju nazad u kodne reči promenljive dužine. Na ovaj način se postiže potpuna kompatibilnost i usaglašenost sa formatom sa malim nedostatkom koji se ogleda u dodatnim informacijama.

a. Podesivost – ovaj algoritam nije podesiv, jer se unapred definiše skup informacija koji ima određeni značaj i nije ga moguće menjati.
b. Vizuelna degradacija – ovim algoritmom se postiže veoma visok stepen vizuelne degradacije, što se može i videti u samom radu koji opisuje ovaj algoritam.
c. Kriptografska bezbednost – postiže se veoma dobar nivo kriptografske bezbednosti koja se zasniva na tajnosti Huffmanovih tabela (tabela koja se koristi pri kodovanju).
d. Kriptografski koeficijent – ovim algoritmom se postiže značajno smanjenje količine podataka koju je potrebno kriptografski obraditi. Procenjeno je da se ovim algoritmom obrađuje manje od 15% celokupnog toka podataka, pa je sam koeficijent manji od 0,15.
e. Uticaj na kompresiju podataka – mana ovog algoritma je ispoljeni uticaj na kompresiju podataka. Naime, reč je o tome da se kodne reči promenljive dužine menjaju indeksima koji mogu da budu i veće dužine od same reči koju zamenjuju, što može značajno da utiče na algoritam kompresije i u suprotnosti je sa samom idejom kompresije podataka.
f. Usklađenost formata – pomenuti algoritam koristi jedan uopšteni pristup selektivnoj kriptografskoj obradi podataka čime se postiže potpuna kompatibilnost sa različitim vrstama kompresionih algoritama.
g. Otpornost na greške – algoritam ima malu otpornost na greške, jer se jedna greška koja se desi na kodnoj reči promenljive dužine može preneti i na ostale kodne reči iz skupa.

3. U [10] dat je opis algoritma koji je namenjen za selektivnu kriptografsku obradu toka video podataka prema H.264/AVC standardu. Kriptografska obrada podskupa podataka uvrštena je u sam enkoder. Da bi se postigla sintaksna kompatibilnost izabrane kodne reči se na slučajan način permutuju sa ostalim kodnim rečima. Pravilo prema kome se vrši permutacija, tj. pomeraj kojim se definiše premeštanje kodnih reči odre-

đuje se na osnovu podataka koje daje kriptografski algoritam AES u brojačkom modu rada.

a. Podesivost – ovaj algoritam nije podesiv, unapred je definisan skup kodnih reči koje su obuhvaćene procesom permutacije.
b. Vizuelna degradacija – ovim algoritmom se postiže odnos signal šum čija se vrednost kreće od 25 do 30 dB. Ovakva vrednost vizuelne degradacije je zadovoljavajuća za primenu u nekim aplikacijama.
c. Kriptografska bezbednost – glavni nedostatak ovako definisanog algoritma je nedostatak kriptografske bezbednosti. Naime, kriptografska bezbednost ovog algoritma ne zavisi od kriptografske snage samog kriptografskog algoritma AES. Njegova kriptografska bezbednost zavisi od veličine izabranih kodnih reči. Veličina izabranih kodnih reči direktno utiče na veličinu prostora podataka iz koga se uzimaju nešifrovani sadržaji što značajno umanjuje snagu primenjenog kriptografskog algoritma.
d. Kriptografski koeficijent – u samom radu nije direktno definisana vrednost kriptografskog koeficijenta ali se, na osnovu analize, može reći da se vrednost kriptografskog koeficijenta kreće od 0,3–0,6 što predstavlja veliku vrednost.
e. Uticaj na kompresiju podataka – primenjena šema ima mali uticaj na kompresiju podataka jer se dodaje mala količina dodatnih informacija koje čine oko 0.1%.
f. Usklađenost formata – tok podataka se može dekodovati primenom bilo kog standardnog dekodera i to bez dešifrovanja podataka. Da bi se dobio kompletan uvid u sadržaj video podataka neophodan je dekoder koji u sebi ima ugrađen mehanizam potreban za dešifrovanje.
g. Otpornost na greške – algoritam ima malu otpornost na greške a ona je posledica slučajnih permutacija i određenom skupu kodnih reči.

## *Postkompresioni algoritmi*

1. Algoritam opisan u [11] predstavlja postkompresioni algoritam selektivnog šifrovanja i sastoji se od kriptografske obrade prefiksa svih I frejmova, svih zaglavlja toka video podataka (informacije koje su vezane za dekodiranje podataka – veličina frejma, bitska brzina, itd.) kao i 32 bita koji predstavljaju kod završetka MPEG toka podataka prema ISO (ISO – *International Standards Organization*) standardu. Eksperimentalni rezultati u ovom radu potvrđuju značaj primene mehanizama selektivnog šifrovanja u sistemima prenosa koji zahtevaju velike bitske brzine prenosa i postižu prihvatljivo kašnjenje „sa kraja na kraj“ u prenosu video podataka. Pomenuti postkompresioni algoritam se može oceniti na sledeći način:

a. Podesivost – nije dozvoljeno podešavanje nikakvih parametara.
b. Vizuelna degradacija – kriptografski obrađeni sadržaj nije usklađen sa MPEG formatom tako da sadržaj nije moguće pregledati bez dešifrovanja. Na osnovu ovoga nije moguće govoriti o vizuelnoj degradaciji.
c. Kriptografska bezbednost – kriptografska bezbednost ovako definisanog algoritma je veoma mala jer kriptografska obrada samo I frejmova nije nedovoljna ako se uzme u obzir da su P i B blokovi u međusobnoj vezi sa I frejmovima. Slaboj kriptografskoj bezbednosti ponuđenog algoritma doprinosi i kriptografska obrada zaglavlja toka podataka koje se karakteriše šablonskim podacima koji su lako predvidivi čime ovaj algoritam čine veoma neotpornim na poznate napade.
d. Kriptografski koeficijent – kako I frejmovi čine od 30 do 60% toka video podataka može se reći da se ovim mehanizmom ne postiže značajno dobar kriptografski koeficijent. U samom radu je ponuđen mehanizam da se smanji učestalost I frejmova i na taj način poveća efikasnost ponuđenog algoritma. Međutim, smanjenje frekvencije I frejmova značajno utiče na kompresiju podataka što dalje utiče na kvalitet video sadržaja.
e. Uticaj na kompresiju podataka – kako se kriptografska obrada vrši nakon kompresije nema značajnog uticaja na sam algoritam kompresije.
f. Usklađenost formata – tok podataka koji se dobija nakon kriptografske obrade nije usklađen sa MPEG formatom jer kriptografska obrada koda koji označava kraj MPEG toka podataka prikriva tip samog sadržaja.
g. Otpornost na greške – ima malu otpornost na greške jer je veoma izražen efekat lavine primenjenog kriptografskog algoritma.

2. JPSEC (JPSEC – *JPEG2000 Security*) deo je JPEG2000 standarda koji je namenjen da obezbedi standardizovano okruženje za implementaciju bezbedonosnih mehanizama i servisa kao što su selektivno šifrovanje, autentikacija, integritet, itd. U [12] definisan je predlog koji ima za cilj da pruži podršku mehanizmima selektivnog šifrovanja u JPSEC-u. Koriste se dva pokazivačka segmenta, *opis bezbedonosnih komponenata* čija je svrha da signaliziraju prisustvo delova u toku podataka koji su kriptografski obrađeni i *objedinjeni kriptografski parametri i bezbedonosne informacije toka podataka* čija je namena da označe bezbedonosne parametre svakog pojedinačnog kriptografski obrađenog dela (metoda koja je primenjena, podatke koji su vezani za očuvanje integriteta, digitalno potpisivanje itd). Prema definisanim kriterijumima analiza ponuđenog mehanizma izgleda ovako:

a. Podesivost – algoritam spada u grupu veoma fleksibilnih i podesivih algoritama. Informacije koje su smeštene u pokazivačkim segmentima određuju na koji način kriptografski zaštititi određene delove toka podataka. Ovakav koncept daje veliku prednost ovom algoritmu, jer sama fleksibilnost (podesivost) omogućava dinamičko određivanje vrednosti ostalih kriterijuma.
b. Vizuelna degradacija – podesivost ponuđenog algoritma utiče na to da i nivo vizuelne degradacije bude u potpunosti podesiv i da zavisi od izabranih parametara.
c. Kriptografska bezbednost – uzevši u obzir da je ovo uopšteni pristup selektivnog šifrovanja kriptografska bezbednost je u potpunosti određena primenjenim kriptografskim elementima.
d. Kriptografski koeficijent – zavisi od primenjenih kriptografskih parametara a kako su oni promenljivi sledi da je i kriptografski koeficijent promenljiv.
e. Uticaj na kompresiju podataka – kako pokazivački parametri sadrže dodatne informacije ponuđeni algoritam unosi dodatne podatke čija je veličina 104 bajta te se može reći da ima blago nepovoljan uticaj na kompresiju podataka. U samom radu dat je veći broj različitih testova sa rezultatima. Pri merenju veličine dodatnih informacija treba imati u vidu i veličinu slike, ali i kriptogtafske parametre i to da oni mogu biti promenljivi.
f. Usklađenost formata – u potpunosti je u skladu sa JPEG2000 i JPSEC formatima.
g. Otpornost na greške – zavisi od primenjenih kriptografskih parametara, a svakako je mala ako se uzme u obzir primena blokovskih kriptografskih algoritama u nekom od modova rada (npr. CBC mod).

3. JPEG2000 standard uređen je kao kompaktan niz bita. I pored toga, najznačajniji podaci se šalju na samom početku toka podataka. Na osnovu ovakve analize i zaključaka autori su u [13] opisali algoritam selektivne kriptografske obrade JPEG2000 toka podataka koji primenom AES algoritma šifruje odabrane podatke. Ovaj algoritam koristi dva opciona markera, i to: 0xFF91 kojim se označava početak paketa (SOP – *Start Of Packet*) i 0xFF92 kojim se označava završetak paketa (EOP – *End Of Packet*). Kada su markeri postavljeni tako dobijeni paket se kriptografski obradi primenom AES algoritma u CFB (CFB – *Cipher Feedback*) modu rada. Ovaj mod je izabran jer se radi o kriptološkoj obradi paketa različite dužine. U samom radu se navodi da je kriterijum za ocenu kvaliteta primenjenog algoritma stepen vizuelne degradacije koji se postiže napravljenim izborom podatka koje treba obraditi. Detaljnija ocena kvaliteta ovog algoritma prema navedenim kriterijumima izgleda ovako:

a. Podesivost – zahvaljujući fiksnim parametrima ovaj algoritam spada u grupu nepodesivih algoritama.

b. Vizuelna degradacija – napravljenim izborom podatka koje treba kriptografski obraditi dolazi se do veličine oko 20%. Na osnovu ovoga može se reći da se zavisno od količine podatka koji se kriptografski obrađuju postiže izuzetno visok stepen vizuelne degradacije.
c. Kriptografska bezbednost – visok stepen vizuelne degradacije ne mora nužno da znači i visoku kriptografsku bezbednost. U ponuđenom algoritmu kriptografska bezbednost zavisi isključivo od kriptografskog algoritma i njegovih parametara.
d. Kriptografski koeficijent – zadovoljavajući novo vizuelne degradacije postignut je kriptografskom obradom jedne petine informacija pa se može reći da je kriptografski koeficijent veoma dobar i iznosi 0,2.
e. Uticaj na kompresiju podataka – nema dodavanja nikakvih podataka tako da ovaj algoritam ne ispoljava uticaj na kompresiju podataka.
f. Usklađenost formata – ponuđeni algoritam nije u skladu sa JPEG 2000 formatom jer sama primena AES algoritma u CFB modu zahteva dodavanje zabranjenih kodnih reči [0xFF91 i 0xFF92].
g. Otpornost na greške – primena AES algoritma u CFB modu ima izraženo negativan uticaj na otpornost na greške ponuđenog algoritma.

## Oblasti primene

Mehanizmi selektivnog šifrovanja sve više dobijaju na značaju i primenjuju se u različitim oblastima. Neke od mogućih oblasti primene ovih mahanizama su sledeće:

– nadgledanje kriptografski obrađenog sadržaja – pretpostavimo situaciju u kojoj možemo sam kriptografski obrađeni sadržaj da koristimo za nadgledanje. Na primer, u sistemima video nadzora u kojima se primenjuju mehanizmi selektivne kriptografske obrade, moguće je analizirati pojedine delove video sadržaja bez prethodnog dešifrovanja;

– PDA (PDA – *Personal Digital Assistent*) uređaji, mobilni telefoni i drugi prenosivi uređaji, koji se sve češće koriste za prenos i razmenu multimedijalnih sadržaja. Mnogi od tih multimedijalnih sadržaja zahtevaju zaštitu autorskih prava i kontrolu pristupa. Njihova ograničena rezolucija, ograničena procesorska snaga i ograničeni životni vek baterije nameću upotrebu mehanizama koji omogućavaju smanjenje složenosti kriptografske obrade podatka. Na taj način produžavaju životni vek baterije i doprinose većem kvalitetu i nižim cenama ovakvih uređaja;

– višestruka kritpografska obrada sa ciljem da se sačuva propusni opseg – primena u sistemima prenosa putem kablovskih i digitalnih TV kanala, gde provajder usluga želi da razdvoji korisnike i druge provajdere, a da istovremeno uštedi na propusnom opsegu. Za svakog novog provajdera primenjuje se novi mehanizam selektivne kriptografske obrade parcijalno odabra-

nih informacija, dok se zajedničke nešifrovane informacije prenose javnim kanalom koji je dostupan svim korisnicima. Na ovaj način se postiže ušteda propusnog opsega koja je direktno srazmerna broju korisnika a obrnuto srazmerna kriptografskom koeficijentu primenjenog selektivnog šifrovanja;

– transkodabilnost[1] i skalabilnost kriptografski obrađenog sadržaja – za neke kompresione algoritme koji nemaju ugrađene ove mehanizme potrebno je u ruterima na prenosnom putu, na malim bitskim brzinama, izvršiti dekompresiju i rekompresiju. U sistemima sa kriptogrsfskom obradom celokupnog toka podataka da bi se ostvario proces kriptografske obrade, kompresije i dekompresije podataka potrebno je da sam ruter (mrežni čvor) na prenosnom putu ima ovakve sposobnosti. Ovo može prouzrokovati dodatno kašnjenje u prenosu toka podataka i da sa sobom nosi još jedan bezbedonosni nedostatak, a to je da se kriptografski parametri nalaze na mrežnom čvoru. Ovaj problem se može na elegantan način rešiti primenom algoritama selektivnog šifrovanja. Kriptografski se obrađuje mali deo informacija dok se ostali podaci šalju u originalnom obliku što omogućava zadovoljavanje uslova za transkodabilnost i sklabilnost bez pristupa bezbedonosnim parametrima. Osnovni deo, koji je potreban svima šalje se u originalnom obliku dok se manji, kriptografski obrađeni deo šalje samo autorizovanim korisnicima.

## Zaključak

Na osnovu prethodnih analiza može se reći da su podesivost, kriptografska bezbednost i otpornost na greške kriterijumi koji, kod opisanih algoritama, uglavnom nisu zadovoljeni.

Algoritmi selektivnog šifrovanja koji su zasnovani na statičkim parametrima ne mogu da budu podesivi. Podesivost je veoma značajna karakteristika posebno u sistemima koji su namenjeni za kriptografsku zaštitu podataka koji se distribuiraju na različite načine, skladište na različite medijume i prenose različitim prenosnim kanalima. Prema tome veoma je značajno definisati algoritam selektivnog šifrovanja sa dinamičkim određivanjem kriptografskih parametara.

Kriptografska bezbednost se kod mnogih algoritama selektivnog šifrovanja ne posmatra na dovoljno značajnom nivou. Za mnoge autore bitnija je vizuelna degradacija (vizuelno izobličenje) koja predstavlja karakteristiku koja je subjektivnog karaktera. Kriptografska bezbednost ovih algoritama zavisi od izvora ključa ali i od nepredvidivosti izabranog dela koji će se kriptografski obrađivati [14]. Na osnovu iznetih činjenica i analiza postkompresionih algoritama može se zaključiti da su postkompresioni algoritmi najbolji sa aspekta kriptografske bezbednosti.

[1] Transkodabilnost je osobina podataka da se lako mogu transformisati iz jednog formata u drugi.

Najveći problem koji se javlja pri konstruisanju algoritma selektivnog šifrovanja je konstruisati algoritam koji će biti otporan na greške. Standardni kriptografski algoritmi imaju veoma izražen efekat lavine, koji direktno utiče na malu otpornost na greške algoritama selektivnog šifrovanja. Odista, u mrežama koje nisu otporne na greške, greška na jednom bitu kriptografski obrađene poruke može usloviti grešku na većem broju bajta poruke dobijene dešifrovanjem. Odatle se može zaključiti da se otpornost na greške i visok stepen kriptografske bezbednosti nalaze u direktnoj suprotnosti. Ovaj problem se može rešiti primenom blokovskih kriptografskih algoritama u brojačkom modu (CTR – *Counter mode*).

Iako je do sada predložen i definisan veliki broj različitih algoritama selektivnog šifrovanja ova oblast predstavlja tek otvoreno istraživačko polje sa velikim brojem pitanja koja čekaju svoje odgovore. Neka od tih pitanja su sledeća:

– Da li je moguće definisati opšti skup načela prema kojima bi trebalo dizajnirati algoritme selektivnog šifrovanja? Prethodnom analizom pokazalo se da nedostatak ovakvih načela prouzrokuje veliki broj različitih algoritama sa manjim ili većim nedostacima. Na primer, neki od algoritama imaju zadovoljavajući stepen vizuelne degradacije ali je kriptografska bezbednost minimalna.

– Da li je moguće definisati algoritam selektivnog šifrovanja za svaki algoritam kompresije koji postoji? Svakako, neki algoritmi kompresije su pogodniji za definisanje algoritama selektivnog šifrovanja a neki pak ne. Na osnovu prethodne analize, može se zaključiti da je JPEG2000 algoritam kompresije jedan od najpogodnijih kandidata za dizajniranje algoritama selektivnog šifrovanja. Ovo je posledica njegove fleksibilnosti i dizajna algoritma kompresije.

– Da li je moguće dizajnirati algoritam selektivnog šifrovanja koji neće zavisiti od oblasti primene? Da li je moguće osmisliti takav algoritam, koji će se podjednako lako primenjivati u mobilnim uređajima, u zaštiti toka video podatka pri prenosu kroz računarsku mrežu, u zaštiti digitalnih multimedijalnih podataka na Internetu i dr.

## *Literatura*

[1] Shannon, C. E., *Communication theory of secrecy systems*, Bell System Technical Journal vol.28(4), page 656–715, 1949.

[2] Lookabaugh, T., *Selective encryption, information theory, and compression*, in Proceedings of the 38th Asilomar Conference on Signals, Systems and Computers, vol.1, page 373–376, Calif, USA, 2004.

[3] Tang, L., *Methods for encrypting and decrypting MPEG video data efficiently*, in Proceedings of the 4th ACM International Multimedia Conference and Exhibition, page 219–229, Boston, Mass, USA, 1996.

[4] Shi, C., Bhargava, B., *A fast MPEG video encryption algorithm*, in Proceedings of the 6th ACM International Conference on Multimedia, page 81–88, Bristol, UK, 1998.

[5] Shi, C., Bhargava, B., *An efficient MPEG video encryption algorithm*, in Proceedings of the 17th IEEE Symposium on Reliable Distributed Systems (*SRDS '98*), page. 381–386, West Lafayette, USA, 1998.

[6] Shi, C., Wang, S. Y., Bhargava B., *MPEG video encryption in real-time using secret key cryptography*, in Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications (*PDPTA '99*), page. 191– 201, Las Vegas, USA,1999.

[7] Podesser, M., Schmidt, H. P., Uh, I A., *Selective bitplane encryption for secure transmission of image data in mobile environments*, in Proceedings of the 5th Nordic Signal Processing Symposium (*NORSIG '02*),Tromsø, Norway, 2002.

[8] Meyer, J., Gadegast, F., *Security mechanisms for multimedia data with the example MPEG-1 video*, Project Description of SECMPEG, Technical University of Berlin, Germany, 1995.

[9] Wen, J., Severa, M., Zeng, W., Luttrell, M. H., Jin, W., *A format-compliant configurable encryption framework for access control of video*, IEEE Transactions on Circuits and Systems for Video Technology, vol. 12, No. 6, page 545–557, 2002.

[10] Bergeronand, C., Lamy-Bergot, C., *Compliantselective encryption for H.264/AVC video streams*, in Proceedings of the 7th IEEE Workshop on Multimedia Signal Processing (*MMSP '05*), page 1–4, Shanghai, China, 2005.

[11] Spanos, G. A., Maples, T. B., *Performance study of a selective encryption scheme for the security of networked, realtime video*, in Proceedings of the 4th International Conference on Computer Communications and Networks (*ICCCN '95*),page 2–10, Las Vegas, USA, 1995.

[12] Sadourny, Y., Conan, V., *A proposal for supporting selective encryption in JPSEC*, IEEE Transactions on Consumer Electronics, vol. 49, No. 4, page 846–849, 2003.

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

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

SELECTIVE ENCRYPTION ALGORITHMS – OVERVIEW WITH PERFORMANCE EVALUATION

*Summary:*

*Digital multimedia content is becoming widely used and increasingly exchanged over computer network and public chanels (satelite, wireless networks, Internet, etc.) which is unsecured transmission media for ex-*

*changing that kind of information. Mechanisms made to encrypt image and video data are becoming more and more significant. Traditional cryptographic techniques can guarantee a high level of security but at the cost of expensive implementation and important transmission delays. These shortcomings can be exceeded using selective encryption algorithms.*

## Introduction

*In traditional image and video content protection schemes, called fully layered, the whole content is first compressed. Then, the compressed bitstream is entirely encrypted using a standard cipher (DES – Data Encryption Algorithm, IDEA – International Data Encryption Algorithm, AES – Advanced Encryption Algorithm etc.). The specific characteristics of this kind of data, high-transmission rate with limited bandwidth, make standard encryption algorithms inadequate. Another limitation of traditional systems consists of altering the whole bitstream syntax which may disable some codec functionalities on the delivery site coder and decoder on the receiving site. Selective encryption is a new trend in image and video content protection. As its name says, it consists of encrypting only a subset of the data. The aim of selective encryption is to reduce the amount of data to encrypt while preserving a sufficient level of security.*

## Theoretical fundation of selective encryption

*The first theoretical fundation of selective encryption was given indirectly by Claude Elwood Shannon in his work about communication theory of secrecy systems. It is well known that statistics for image and video data differ much from classical text data. Indeed, image and video data are strongly correlated and have strong spatial/temporal redundancy.*

## Evaluation criteria for selective encryption algorithm performance evaluation

*We need to define a set of evaluation criteria that will help evaluating and comparing selective encryption algorithms.*

- *Tunability*
- *Visual degradation*
- *Cryptographic security*
- *Encryption ratio*
- *Compression friendliness*
- *Format compliance*
- *Error tolerance*

## Classification of selective encryption algorithms

*One possible classification of selective encryption algorithms is relative to when encryption is performed with respect to compression. This classification is adequate since it has intrinsic consequences on selective encryption algorithms behavior. We consider three classes of algorithms as follows:*

- *Precompression*

*– Incompression*
*– Postcompression*

Overview of selective encryption algorithms

*In accordance with their precedently defined classification, selective encryption algorithms were compared, briefly described with advantages and disadvantages and their quality was assessed.*

Applications

*Selective encryption mechanisms became more and more important and can be applied in many different areas. Some potential applicatiion areas of this mechanism are:*
*– Monitoring encrypted content*
*– PDAs (PDA – Personal Digital Assistant), mobile phones, and other mobile terminals*
*– Multiple encryptions*
*– Transcodability/scalability of encrypted content*

Conclusion

*As we can see through foregoing analysis, we can notice that tunability, cryptographic security and error tolerance are the main unsatisfied criteria.*

*Selective encryption algorithms based on static encryption parameters do not allow tunability. Tunability is a desirable property especially for content protection systems targeting different applications with differen requirements in terms of security or visual degradation and different devices with different capabilities in terms of memory, computational power, or display capabilities. It is therefore appreciated to design a tunable selective encryption algorithm with dynamic encryption parameters.*

Key words: *selective encryption, compression algorithm, multimedia data, computer network*

Datum prijema članka: 30. 07. 2009.
Datum dostavljanja ispravki rukopisa: 28. 12. 2009.
Datum konačnog prihvatanja članka za objavljivanje: 29. 12. 2009.