Bezbednost videa žaštićenog vodenim žigom skremblovanim GMSAT algoritmom

Zoran Veličković
Visoka tehnička škola strukovnih studija
Niš, Srbija
zoran.velickovic@vtsnis.edu.rs

Marko Veličković
Visoka tehnička škola strukovnih studija
Niš, Srbija
marko.velickovic93@yahoo.com

Sadržaj — **Radi zaštite video sekvenci od kopiranja, u ovom radu je korišćena tehnika insertovanja skremblovanog vodenog žiga. Skremblovanje vodenog žiga je izvršeno GMSAT algoritmom, a ugradnja je realizovana u DWT-SVD domenu videa. Predloženi algoritam je evaluiran na tri različite video sekvence, gde je pokazana njegova otpornost na podmetanje lažnog vodenog žiga. U prikazanim eksperimentima je bilo nemoguće ekstrahovati vodeni žig bez poznavanja originalnog, kao i svih parametara inverznog GMSAT-a. U radu je pokazana da predloženi algoritam zadovoljava visok nivo bezbednosti i omogućavaju ekstrakciju vodenog žiga dobrog kvaliteta iz kodovanog videa. Povećanjem broja etapa GMSAT algoritma se može obezbediti proizvoljno visok nivo zaštite.**

Ključne riječi – Multistage Arnold transformation; Watermark; H.264/AVC; SVD; SSIM, DWT.

I. UVOD

Na osnovu podataka dobijenih analizom globalnog IP saobraćaja može se reći da se 2016. godine ušlo u tzv. Zettabyte eru [1]. Globalni godišnji IP saobraćaj je 2016. godine dostigao granicu od 1ZB ($1ZB=10^{21}B$). Predviđa se da će se globalni godišnji IP saobraćaj udvostručiti do 2019. godine. Pored PC računara, ulasku u Zettabyte eru najviše su doprineli savremeni mobilni multimedijalni uređaji kao što su smartfoni, tableti, smart TV uređaji i IoT (engl. *Internet of Things*) moduli. IP saobraćaj generisan sa bežičnih i mobilnih uređaja je takođe 2016. godine imao veći udeo od saobraćaja generisanog sa žičnih konekcija [2]. Na dostizanje Zettabyte granice znatno je uticala i struktura globalnog IP saobraćaja. Naime, 64% globalnog IP saobraćaja se odnosi na neku formu video saobraćaja koji po svojoj prirodi zahteva prenos ogromnih količina podataka. Multimedijalne aplikacije VoIP-a (engl. *Voice over Internet Protokol*), videa na zahtev VoD-a (engl. *Video on Demand*) i video telefona su doprinele enormnom povećanju IP saobraćaja jer po svojoj prirodi zahtevaju veliki mrežni protok. Istovremeno, u porastu je i broj uređaja koji podržavaju nove video standarde visoke rezolucije (HD, UHD i 4K), tako da se u bliskoj budućnosti očekuje neprestano povećanje udela video paketa u globalnom IP saobraćaju. Povećanje rezolucije video sadržaja nosi sa sobom niz novih problema, ali je bazičan onaj koji se odnosi na zahtevani bitski protok. Naime, bitska brzina neophodna za prenos 4K videa dvostruko je veća od one potrebne za HD, odnosno, devet puta veća od one potrebne za SD video rezoluciju. Pretpostavlja se da će se udeo video saobraćaja u ukupnom IP saobraćaju povećati na 80% do kraja 2019. godine. Iz prezentovanih činjenica se može nedvosmisleno zaključiti da je razmena digitalnih multimedijalnih sadržaja, a posebno videa, već postala dominantni oblik IP saobraćaja. Web portal Youtube je izuzetno doprineo ovoj činjenici jer je pružio mogućnost svakom korisniku Interneta da objavi sopstveni video i na taj način ga učini globalno dostupnim. Na *Youtube*-u se u jednoj minuti postavi 300 sati novog video sadržaja, dok istovremeno 2.78 miliona posetilaca gleda neki već postavljeni video sadržaj. Sa druge strane, *Netflix* globalni provajder filmova i TV serija, strimuje preko 77K sati video sadržaja u minuti. Globalna dostupnost, kao i karakteristika digitalnih multimedijalnih sadržaja da se za razliku od analognih, pri kopiranju ne gubi na kvalitetu, su pogodovale pojavi piraterije, odnosno, nelegalnom kopiranju i distribuciji multimedijalnih sadržaja na Internetu. U pomenutim uslovima zaštita autorskih prava nad vlasništvom video sadržaja je veoma kompleksna.

Zaštita video sadržaja od kopiranja i nelegalne distribucije postaje nezaobilazna aktivnost autora pre objavljivanja originalnih video sadržaja [3] – [8]. Za zaštitu od kopiranja digitalnih multimedijalnih sadržaja se mogu primeniti standardne kriptografske tehnike. Kriptografske tehnike zasnovane na infrastrukturi javnog ključa ne pružaju adekvatnu zaštitu multimedijalnom sadržaju jer se pre reprodukcije moraju dekriptovati i time izložiti riziku. Za praktičnu primenu mnogo su pogodnije metode bazirane na insertovanju vodenog žiga u sam multimedijalni sadržaj [3]. Kod ovih metoda, insertovani vodeni žig ostaje trajno u multimedijalnom sadržaju i ne odstranjuje se iz njega ni prilikom reprodukcije. Osobina digitalnog vodenog žiga da nikada ne napušta multimedijalni sadržaj, dodatno povećava nivo bezbednosti zaštićenog videa. Takođe, ova osobina značajno doprinosi preživljavanju vodenog žiga u video sadržaju pri pokušaju mnogih malicioznih i destruktivnih ataka na video.

U ovom radu je razmatrana ugradnja šifrovanog vodenog žiga u nekodovani video sadržaj u cilju zaštite autorskih prava nad multimedijalnim sadržajem [4]. Ovaj koncept zaštite autorskih prava zahteva pouzdanu ekstrakciju insertovanog vodenog žiga iz samog multimedijalnog sadržaja. Ekstrahovani vodeni žig treba svojim sadržajem i izgledom da odgovara insertovanom vodenom žigu i da nedvosmisleno identifikuje autora, odnosno, vlasnika multimedijalnog sadržaja. Binarni logo vlasnika multimedijalnog sadržaja se često koristi kao

vodeni žig. Poznavanje sadržaja vodenog žiga može sniziti nivo bezbednosti samog videa. Zbog toga je u ovom radu predložena primena generalizovane višeetapne Arnoldove transformacije GMSAT (engl. *Generalized MultiStage Arnold Transformation*) za šifrovanje (skremblovanje) sadržaja vodenog žiga [5]. Za dobijanje originalnog vodenog žiga iz skremblovanog razvijen je inverzni GMSAT. Samo poznavanjem svih parametra inverznog GMSAT-a moguće je skrermblovani vodeni žig transformisati u originalni. Obzirom da GMSAT algoritam pripada klasi invertibilnih haotičnih mapa (engl. *Chaotic Maps*) [6], neophodno je poznavati i početne transformacione uslove na koje su sve haotične mape izuzetno osetljive. Kroz nekoliko primera pokazana je robusnost predloženog algoritma na pokušaje dešifrovanja kada nisu poznati svi ili su samo delimično poznati parametri GMSAT-a. Važno je napomenuti da se primenom GMSAT-a može realizovati željeni nivo bezbednosti. U radu je takođe predložen pouzdani SVD algoritam ugradnje skremblovanog vodenog žiga u video zasnovan na kombinovanju DWT-a (engl. *Discrete Wavelet Transform*) i SVD-a (engl. *Singular Value Decomposition*) [7]. Skremblovani vodeni žig se ugrađuje u svaki frejm nekodovane video sekvence. Pouzdani SVD algoritam ugradnje je otporan na pojavu podmetanja lažnog vodenog žiga što je bio značajni nedostatak svih klasičnih SVD tehnika. Bezbednost predloženog algoritma je verifikovana na tri poznate video sekvence. Posle ugradnje skremblovanog vodenog žiga video je kodovan H.264/AVC koderom kako bi bio dostupan na Internetu. H.264/AVC koder je izabran jer realizuju dobar odnos između kvaliteta videa i nivoa kompresije. Kodovanje se u ovom kontekstu može smatrati atakom na sam video sadržaj jer je bazirano na zanemarivanju detalja u frejmovima. Posledice kodovanja i matematičkih zaokruživanja rezultuju promenljivim kvalitetom ekstrahovanih vodenih žigova. U svrhu popravke kvaliteta ekstrahovanog žiga razvijen je napredni algoritam popravke [8].

U drugom poglavlju su ukratko prezentovane matematičke osnove primenjenih transformacionih tehnika GMSAT, DWT i SVD. U trećem poglavlju prikazan je modifikovani pouzdani algoritam za ugradnju/ekstrakciju vodenog žiga zasnovanog na DWT-SVD transformaciji-dekompoziciji. U četvrtom poglavlju je prikazana primena predloženog algoritma na tri različite video sekvence. Verifikovana je robusnost algoritma na podmetanje lažnog žiga i nekorektnih parametara GMSAT-a. U petom poglavlju su prikazani dobijeni rezultati i izvedeni odgovarajući zaključci na bazi sprovedenih ispitivanja.

II. MATEMATIČKE OSNOVE TRANSFORMACIONIH TEHNIKA

A. Generalizovana višeetapna Arnoldova transformacija GMSAT

U prethodnim radovima autori su predložili višeetapnu Arnoldovu transformaciju [3] za skremblovanje (kriptovanje) sadržaja vodenog žiga. Skremblovanjem se prepoznatljiv sadržaj žiga preuređuje u naizgled besmislen. Osnovna ideja ove transformacije se zasniva na uzastopnoj primeni više različitih Arnoldovih transformacija - etapa (I) sa sopstvenim parametrima na vodeni žig. Transformacioni parametri i-te etape a_i, b_i, broj uzastopnih iteracija etape k_i predstavljaju ključeve za kriptovanje, dok se perioda Arnoldove transformacije etape T_i dodatno zahteva za dekriptovanje. Dimenzija kvadratnog vodenog žiga N je konstanta i jednaka je za sve etape. Ovo ima za posledicu da se višeetapna Arnoldova transformacija uvek primenjuje nad kompletnim vodenim žigom. U ovom radu se primenjuje generalizovana višeetapna Arnoldova transformacija GMSAT kod koje je dozvoljena varijacija dimenzije kvadratnog vodenog žiga N_i u svakoj etapi [5]. Tako, u svakoj etapi (i) ove transformacije moguće je birati proizvoljnu vrednost dimenzije kvadratnog žiga na koju se primenjuje uz uslov $N_i \leq N$. Svaka od etapa generalizovane višeetapne 2D Arnoldove transformacije (i) se može opisati izrazima (1) i (2):

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \left(\begin{bmatrix} 1 & b_i \\ a_i & a_i b_i + 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \right) mod N_i \quad (1)$$

$$N_i \leq N, i \in (1, 2, \dots I)$$

$$(x, y) \in (0,1, \dots, N_i - 1) \times (0,1, \dots, N_i - 1) \subset Z^2 \quad (2)$$

gde x_n, y_n i x_{n+1}, y_{n+1} predstavljaju lokacije piksela slike, a a_i, b_i i N_i predstavljaju parametre Arnoldove transformacije. Primena inverznog GMSAT-a [5], koji se svodi na produženu primenu GMSAT-a , zahteva poznavanje i dodatnih parametara k_i i T_i . Skup parametara Key_I koji određuju (inverznu) generalizovanu višeetapnu Arnoldovu transformaciju se može predstaviti izrazom (3):

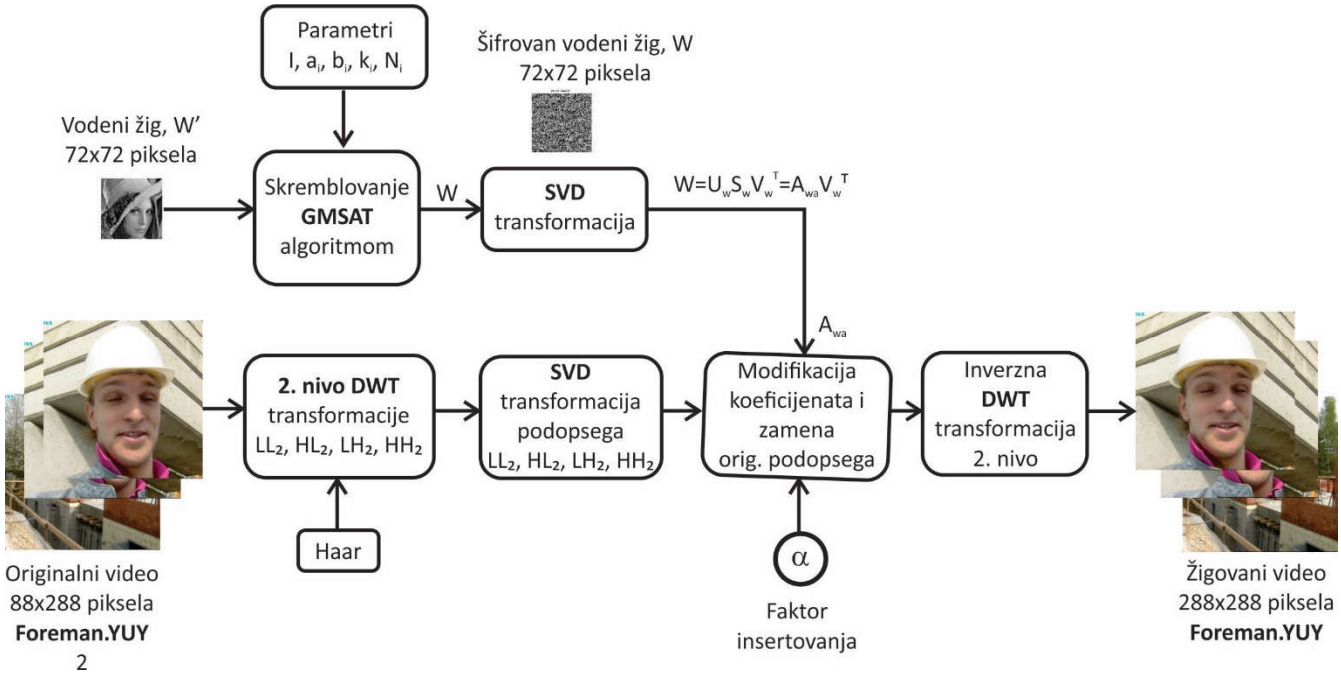
$$Key_{\mathrm{I}} = f\left(E_i\left(a_i, b_i, k_i, N_i, T_i\right)\right), i = 1,2, \dots I \quad (3)$$

gde E_i predstavlja i-tu etapu od I etapa GMSAT-a. Prilikom skremblovanja (preuređivanja) lokacije piksela na ulaz prve etape E_1 dovodi se originalni vodeni žig, dok se na izlazu iz I-te etape E_1 dobija transformisani vodeni žig.

B. Diskretna Wavelet transformacija DWT

Na osnovu svojih karakteristika, DWT [7] se može svrstati u klasu „*multi-resolution*“ „*multi-level*“ transformacija što algoritmima za ugradnju vodenog žiga znatno proširuje mogućnosti primene. U slučaju zaštite videa, vodeni žig se može ugraditi u željeni transformacioni podopseg svakog video frejma. Izborom odgovarajućeg podopsega, ugrađeni vodeni žig se može zaštiti od pojedinih vrsta smetnji i ataka. Na svakom nivou dekompozicije video frejma dobijaju se četiri frekvencijska podopsega koji se označavaju sa LL, LH, HL i HH. Podopseg LL je dobijen filtriranjem frejma niskopropusnim filtrom u horizontalnom i vertikalnom pravcu. Ovaj podopseg nosi najveću energiju frejma. Ugradnja vodenog žiga u LL podopsegu može izazvati značajnu degradaciju video frejma, ali istovremeno obezbediti robusnost vodenog žiga na pokušaje njegove ekstrakcije. Frekvencijski podopseg HH je dobijen filtriranjem visokopropusnim filtrom u horizontalnom i vertikalnom pravcu i sadrži visokofrekvencijske komponente frejma duž dijagonala. Ovaj podopseg uključuje ivice i teksturu frejma. Frekvencijski podopsezi HL i LH se dobijaju

niskofrekvenciskim filtriranjem u jednom pravcu i visokofrekvencijskim filtriranjem u drugom pravcu. LH podopseg sadrži informacije o vertikalnim detaljima koji



Slika 1. Blok dijagram DWT-SVD algoritma za insertovanje skremblovanog vodenog žiga u video sekvencu Foreman.

odgovaraju horizontalnim ivicama, dok HL podopseg sadrži informacije o horizontalnim detaljima koji odgovaraju vertikalnim ivicama. Ugradnja vodenog žiga u frekvencijske podopsege HL i LH predstavlja kompromis između robusnosti vodenog žiga i perceptualnog kvaliteta zaštićenog videa. Daljom dekompozicijom LL podopsega dobija se sledeći nivo dekompozicije. Nivo dekompozicije zavisi od potrebe aplikacije, a u ovom radu je korišćen drugi nivo dekompozicije sa poznatim *Harr* wavelet filtrom. Na ovaj način su izjednačene rezolucije LL_2 podopsega i žiga.

C. SVD dekompozicija

SVD dekompozicija se koristi kao alat za umetanje vodenog žiga i bazirana je na teoremi da se pravougaona matrica $\boldsymbol{A}$ dimenzija $m \times n$ može razložiti na tri matrice:

$$\boldsymbol{A} = \boldsymbol{U}\boldsymbol{S}\boldsymbol{V}^T \tag{4}$$

gde je $\boldsymbol{A} \in \Re^{n\times n}$, $\boldsymbol{U} \in \Re^{n\times m}$ i $\boldsymbol{V} \in \Re^{m\times m}$. Matrice $\boldsymbol{U}$ i $\boldsymbol{V}$ su ortogonalne matrice, a kolone ovih matrica se nazivaju levi, odnosno, desni singularni vektori. Matrica, $\boldsymbol{S}$ je dijagonalna matrica, poznata pod nazivom matrica singularnih vrednosti. Ako je r rang matrice $\boldsymbol{A}$, tada elementi matrice $\boldsymbol{S}$ zadovoljavaju sledeću relaciju:

$$\sigma_1 \geq \sigma_2 \geq \cdots \sigma_r \geq \sigma_{r+1} = \sigma_{r+2} = \cdots = \sigma_n = 0, \tag{5}$$

a matrica $\boldsymbol{A}$ se može predstaviti na sledeći način:

$$A = \sum_{p=1}^{r} \sigma_p \boldsymbol{u}_p \boldsymbol{v}_p^T, \tag{6}$$

gde $\boldsymbol{u}_p$ i $\boldsymbol{v}_p$ predstavljaju p-tu sopstvenu vrednost matrica $\boldsymbol{U}$ i $\boldsymbol{V}$, dok je σ_p p-ta singularna vrednost. Singularni vektori specificiraju geometriju matrice $\boldsymbol{A}$, dok singularne vrednosti specificiraju energiju (osvetljaj slike) matrice $\boldsymbol{A}$. Ako se matricom $\boldsymbol{A}$ predstavi jedan video frejm, onda se nizom sličnih matrica može predstaviti video. Najvažnije karakteristike SVD dekompozicije koje su važne za ovaj rad su invarijantnost na transponovanje, skaliranje, rotaciju i zamenu kolona i vrsta matrice. Ove karakteristike su značajne za očuvanje samog video sadržaja kao i za obezbeđenje otpornosti insertovanog vodenog žiga na geometrijske i druge atake.

III. ALGORITMI ZA INSERTOVANJE I EKSTRAKCIJU VODENOG ŽIGA

U ovom radu se ugradnja i ekstrakcija vodenog žiga u video frejm u SVD domenu obavlja pouzdanim algoritmom [8]. Pouzdani SVD algoritam rešava problem lažne detekcije žiga koji je svojstven standardnom SVD algoritmu. Detalji algoritma za ugradnju kriptovanog vodenog žiga su prikazani blok dijagramom na Sl. 1, dok su detalji algoritma za ekstrakciju kriptovanog vodenog žiga u DWT-SVD domenu predstavljeni blok dijagramom na Sl. 2. Matematičke osnove algoritma insertovanja su predstavljene nizom I koraka, dok su matematičke osnove algoritma ekstrahovanja predstavljene nizom E koraka u nastavku.

A. Algoritam ugradnje vodenog žiga

Korak I_1: Dekompozicija frejma $\boldsymbol{F}$ primenom drugog nivoa DWT transformacije:

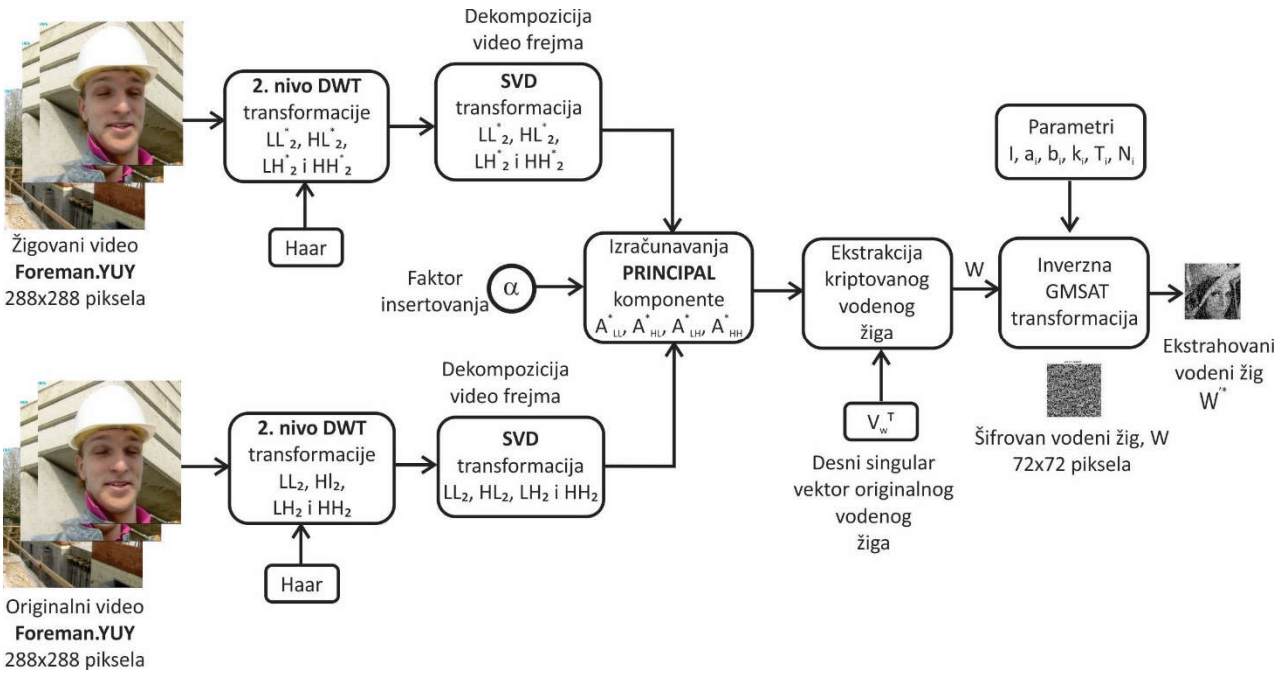
$$\{\boldsymbol{F}^k, \boldsymbol{F}^l\} = \underset{Haar}{DWT_2}(\boldsymbol{F}) \tag{7}$$

$$k \epsilon \{LL_2, HL_2, LH_2, HH_2\}$$

$$l\epsilon\{HL_1, LH_1, HH_1\}$$

$$\boldsymbol{F}^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_F^k \cdot (\boldsymbol{V}_F^k)^T \,. \quad (8)$$

Korak I_2: SVD dekompozicija podopsega $\boldsymbol{F}^k$:



Slika 2. Blok dijagram DWT-SVD algoritma za ekstrakciju skremblovanog vodenog žiga iz video sekvence Foreman.

Korak I_3: Kriptovanje originalnog vodenog žiga $\boldsymbol{W}'$ (niže rezolucije) primenom generalizovane višeetapne Arnoldove transformacije i dobijanje vodenog žiga $\boldsymbol{W}$ koji se insertuje u svaki frejm.

$$\boldsymbol{W} = \underset{E_i(a_i,b_i,k_i,N_i,T_i)}{Gen\_Arnold}(\boldsymbol{W}') \quad (9)$$

$$i = 1,2,\dots I$$

Korak I_4: SVD dekompozicija kriptovanog vodenog žiga $\boldsymbol{W}$ i računanje principal komponente $\boldsymbol{A}_{\text{wa}}$.

$$\boldsymbol{W} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w \cdot \boldsymbol{V}_w^T = \boldsymbol{A}_{wa} \cdot \boldsymbol{V}_w^T \,;\; \boldsymbol{A}_{wa} = \boldsymbol{U}_w \cdot \boldsymbol{S}_w \,. \quad (10)$$

Korak I_5: Ugradnja principal komponente $\boldsymbol{A}_{\text{wa}}$ u dijagonalnoj matrici podopsega $\boldsymbol{S}_F^k$ sa faktorom insertovanja α:

$$\boldsymbol{S}_{F\_1}^k = \boldsymbol{S}_F^k + \alpha \cdot \boldsymbol{A}_{wa}. \quad (11)$$

Korak I_6: Kreiranje modifikovanog podopsega sa ugrađenim vodenim žigom:

$$\boldsymbol{F}_w^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_{1\_F}^k \cdot (\boldsymbol{V}_F^k)^T \,. \quad (12)$$

Korak I_7: Zamena originalnih podopsega drugog nivoa frejma sa modifikovanim i primena inverzne diskretne wavelet transformacije IDWT_2 za dobijanje žigovanog frejma.

$$\boldsymbol{F}_w = \underset{Haar}{IDWT_2}(\boldsymbol{F}_w^k,\ \boldsymbol{F}^l) \,. \quad (13)$$

B. Algoritam ekstrakcije vodenog žiga

Proces ekstrakcije vodenog žiga $\boldsymbol{W}^*$ iz zaštićenog videa se može obaviti sledećim *E* koracima:

Korak E_1: Dekompozicija originalnog frejma $\boldsymbol{F}$ primenom drugog nivoa DWT transformacije:

$$\{\boldsymbol{F}^k, \boldsymbol{F}^l\} = \underset{haar}{DWT_2}(\boldsymbol{F}) \quad (14)$$

$$k\epsilon\{LL_2, HL_2, LH_2, HH_2\}$$

$$l\epsilon\{HL_1, LH_1, HH_1\}$$

Korak E_2: SVD dekompozicija podopsega $\boldsymbol{F}^k$:

$$\boldsymbol{F}^k = \boldsymbol{U}_F^k \cdot \boldsymbol{S}_F^k \cdot (\boldsymbol{V}_F^k)^T \quad (15)$$

Korak E_3: Dekompozicija potencijalno atakovanog frejma F_w^* primenom drugog nivoa DWT transformacije:

$$\{\boldsymbol{F}_w^{*k}, \boldsymbol{F}_w^{*l}\} = \underset{haar}{DWT_2}(\boldsymbol{F}_w^*) \quad (16)$$

Korak E_4: SVD dekompozicija podopsega $\boldsymbol{F}_w^{*k}$:

$$\boldsymbol{F}_w^{*k} = \boldsymbol{U}_{Fw}^{*k} \cdot \boldsymbol{S}_{Fw}^{*k} \cdot (\boldsymbol{V}_{Fw}^{*k})^T \quad (17)$$

Korak E_5: Kreiranje razlike originalnog ($\boldsymbol{F}^k$) i zaštićenog frejma (F_w^{*k}):

$$\boldsymbol{F}_1^k = \boldsymbol{F}_w^{*k} - \boldsymbol{F}^k \quad (18)$$

Korak E_6: Određivanje principal komponente:

$$\boldsymbol{A}_{wa}^{*k} = \frac{\left(\boldsymbol{U}_F^k\right)^{-1} \cdot \boldsymbol{F}_1^k \cdot \left(\boldsymbol{V}_F^T\right)^{-1} \cdot \left(\boldsymbol{V}_F^k\right)^T}{\alpha} \quad (19)$$

Korak E_7: Izračunavanje insertovanog kriptovanog vodenog žiga W'^* se obavlja na sledeći način:

$$\boldsymbol{W}^{*k} = \boldsymbol{A}_{wa}^{*k} . \boldsymbol{V}_w^T \quad (20)$$

Korak E_8: Dekriptovanje originala vodenog žiga $\boldsymbol{W}^{*k}$ primenom inverzne generalizovane višeetapne Arnoldove transformacije [5] i dobijanje originalnog žiga $\boldsymbol{W}^{*k}$:

$$\boldsymbol{W}'^{*k} = \underset{E_i(a_i,b_i,k_i,N_i,T_i)}{Inv\_Gen\_Arnold}(\boldsymbol{W}^{*k})$$
$$i = 1,2,\dots I\,. \tag{21}$$

IV. PRIKAZ EKSPERIMENTA I ANALIZA REZULTATA

A. Prethodne napomene

U ovom radu je pretpostavljeni *.yuv* format za čuvanje nekodovanog video sadržaja. Kod ovog video formata informacije o svakom frejmu se čuvaju u karakterističnim matricama označenim kao $\boldsymbol{Y}$, $\boldsymbol{C}_r$ i $\boldsymbol{C}_b$. U matrici $\boldsymbol{Y}$ se čuvaju vrednosti osvetljaja za svaki piksel frejma, dok se informacije o boji čuvaju u matricama $\boldsymbol{C}_r$ i $\boldsymbol{C}_b$. Insertovanje vodenog žiga u nekodovanom domenu se obavlja upravo u matrici $\boldsymbol{Y}$, dok se vrednosti elemenata matrica $\boldsymbol{C}_r$ i $\boldsymbol{C}_b$ zadržavaju.

B. Simulacioni rezultati

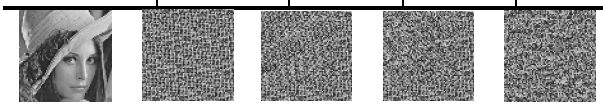
U eksperimentalnom delu ovog rada korišćen je centralni deo poznate slike „*Lena.bmp*“ u rezoluciji 72×72 piksela kao vodeni žig (Sl. 3a). Da bi se povećao nivo zaštite, sadržaj vodenog žiga se pre inserovanja u frejmove skrembluje GMSAT-om. U ovom radu je primenjena 4-etapna Arnoldova transformacija čiji su parametri dati u Tabeli 1, kolone *Ok*. Skup parametara (22) predstavlja ključ Key_4 za skremblovanje vodenog žiga 4-etapnim GMSAT-om primenjenom u ovom radu.

$$Key_4 = f(E_1, E_2, E_3, E_4\,). \tag{22}$$

Na Sl. 3b) - 3e) prikazani su izgledi vodenih žigova na kraju svake etape GMSAT-a respektivno. Vodeni žig dobijen posle četvrte etape predstavlja skremblovani vodeni žig koji se insertuje u svaki frejm videa. Izlaz iz prethodne etape predstavlja ulaz u narednu etapu čime se postavljaju početni uslovi na koje je predložena transformacija veoma osetljiva. U svim etapama skremblovanja se jasno može uočiti prostorna dekorelacija piksela originalnog vodenog žiga čime se ostvaruje vizuelna neprepoznatljivost žiga. Veća prostorna dekorelacija piksela originalnog vodenog žiga se može uočiti kod primene generalizovane višeetapne Arnoldove transformacije [5] u odnosu na primenu višeetapne Arnoldove transformacije [3] što se može smatrati njenom prednošću. Za vraćanje skremblovanog vodenog žiga u originalni, nužno je poznavati sve parametre svih etapa kao i početne uslove svake etape. Ako samo jedan parametar višeetapne Arnoldove transformacije nije poznat nije moguće dešifrovati skremblovani vodeni žig. Kroz nekoliko primera u nastavku je potvrđena ova činjenica. Kako se može videti iz predloženog algoritma insertovanja, za primenu pouzdanog SVD algoritma, prvo se određuju transformacioni koeficijenti drugog nivoa DWT-a. Na Sl. 4 je prikazana DWT transformacija drugog nivoa 22. frejma iz video sekvence „*Foreman*“. Dekompozicija je obavljena primenom Haar filtera. Prikazani su transformacioni koeficijenti sledećih podopsega: LL2, LH2, HL2, HH2, LH1, HL1 i HH1.

TABELA 1: PARAMETRI 4-ETAPNOG GMSAT-A KORIŠĆENI U RADU

Parametri	Etapa 1		2		3		4	
	Ok	Err	Ok	Err	Ok	Err	Ok	Err
a	2	5	1	3	4	2	3	1
b	2	1	1	2	2	5	1	3
N	72	72	60	60	50	50	72	72
k	9	5	5	9	7	5	7	5
T	12	12	60	60	18	18	18	18

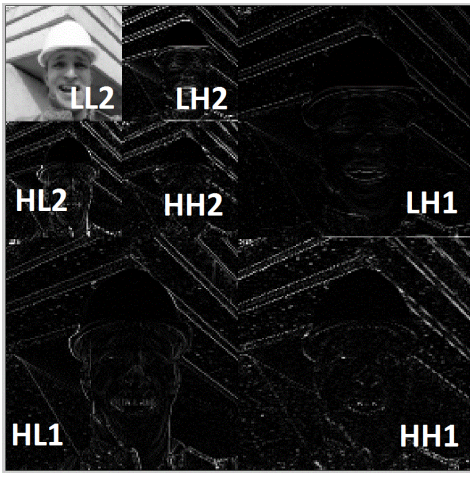


a) b) c) d) e)

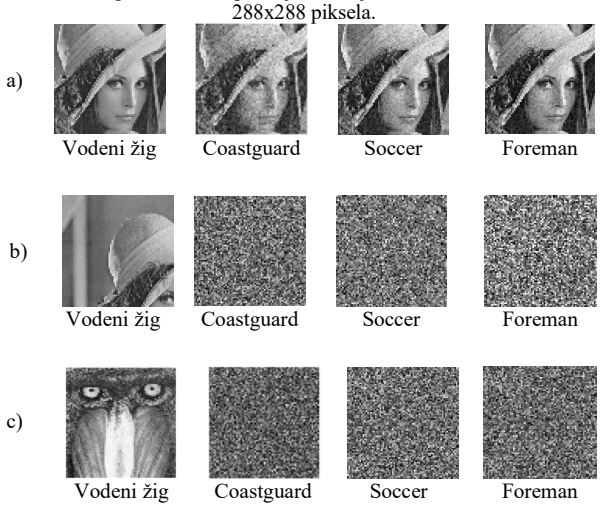
Slika. 3. Izgled vodenog žiga posle a) prve b) druge c) treće i d) četvrte etape višeetapne Arnoldove transformacije.

Iako se insertovanje vodenog žiga može obaviti u svim podopsezima, u ovom radu se insertovanje skremblovanog vodenog žiga sa Sl. 3e) obavlja samo u LL2 podopsegu. Prikazanim SVD-DWT algoritmom insertovanja je ugrađen kriptovan vodeni žig sa faktorom insertovanja α=0.05. Vodeni žig je ugrađen u sve frejmove videa. Posle insertovanja vodenih žigova u sve frejmove nekodovanog videa izvršeno je kodovanje H.264/AVC koderom. Kodovanje video sekvenci obavljeno je JM referentnim softverom ITU-a (engl. *International Telecommunication Union*) u verziji 18.4 FRExt. Kvalitet kodovanja je definisan skupom FRExt parametara. Ključni uticaj na izbor kvaliteta kodovanja imaju sledeći parametri: *IntraPeriod*=12, *NumberReferenceFrames*=5 *NumberBFrames*=1.

Iz svih zaštićenih frejmova se primenom prezentovanog algoritma za ekstrakciju može izdvojiti niz vodenih žigova. Zbog pomenutih razloga, ekstrahovani vodeni žigovi su promenljivog kvaliteta. Kvalitet ekstrahovanih vodenih žigova iz svakog frejma je procenjivan izračunavanjem SSIM indeksa. Veći SSIM indeks predstavlja bolji kvalitet ekstrahovanog vodenog žiga. Varijacija SSIM indeksa za razmatrane video sekvence se kreće u opsegu od 0.05 do 0.52. Da bi se popravio kvalitet ekstrahovanog vodenog žiga primenjen je napredni algoritam za popravku kvaliteta [8]. Na Sl. 5 su prikazani popravljeni ekstrahovani vodeni žigovi iz razmatranih video sekvenci. Razmatrane su poznate video sekvence *Coastguard*, *Soccer* i *Foreman* u koje je insertovan (umetnut) skremblovani vodeni žig sa Sl. 3e). Zaštićene video sekvence su kodovane, a zatim i dekodovane kako bi se iz njih ekstrahovali vodeni žigovi iz svakog frejma. Na slici 5a) prikazani su izgledi popravljenih ekstrahovanih vodenih žigova iz video sekvenci Coastguard, Soccer i Foreman kada je u procesu ekstrakcije korišćen korektan vodeni žig. Ispod svakog ekstrahovanog vodenog žiga označena je video sekvenca iz koje je ekstrahovan.



Slika 4. Drugi nivo dekompozicije 22. frejma videa Foreman u rezoluciji 288x288 piksela.

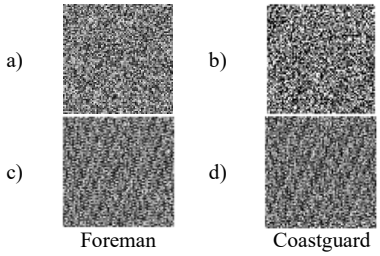


Slika 5. Ekstrahovani vodeni žigovi iz razmatranih sekvenci sa a) korektnim i b) i c) nekorektnim vodenim žigovima.

Sa Sl. 5a) se može primetiti različiti kvalitet ekstrahovanih vodenih žigova. U prikazanom primeru ekstrahovani su vodeni žigovi sa SSIM indeksima od 0.8956 za video sekvencu *Foreman*, 0.8624 za video sekvencu *Soccer* i 0.7537 za video sekvencu *Coastguard*. Na slikama 5b) i 5c) prikazan je izgled ekstrahovanih vodenih žigova kada u procesu ekstrakcije nije upotrebljen korektan vodeni žig. Na slici 5b) kao referentni vodeni žig korišćen je deo slike Lena - ali ne onaj koji je korišćen prilikom insertovanja. SSIM indeksi ovih ekstrahovanih vodenih žigova bili su veoma niski (oko 0.0045) što jasno ukazuje da nisu pronađeni insertovani vodeni žigovi. Na ovaj način je pokazano da je predloženi algoritam otporan na podmetanje lažnog žiga. Sličan se zaključak može izvesti i sa slike 5c) gde je u procesu ekstrakcije kao vodeni žig upotrebljen centralni deo slike „*Monkey*“. Iz zaštićenog videa nije bilo moguće ekstrahovati vodeni žig koji je insertovan. U svim slučajevima sa Sl. 5 korišćeni su korektni parametri GMSAT-a. Na Sl. 6a) i 6b) su prikazani ekstrahovani vodeni žigovi iz video sekvenci Foreman i Coastguard kada je u procesu ekstrakcije upotrebljen korektan vodeni žig ali su izmenjeni parametri GMSAT-a kako je to prikazano u kolonama *Err* Tabele 1. Na Sl. 6c) i 6d) prikazani su ekstrahovani vodeni žigovi kada su izmenjeni parametri samo prve etape GMSAT-a. Evidentno je da ni u jednom slučaju nije moguće ekstrahovati korektan vodeni žig čime su potvrđuju dobre bezbednosne karakteristike prikazanog algoritma.

V. ZAKLJUČAK

Potreba zaštite video sadržaja postaje sve zahtevnija u uslovima savremenog Interneta. Radi zaštite od kopiranja, u ovom radu je korišćena tehnika insertovanja skremblovanog vodenog žiga u nekodovane video sekvence. Skremblovanje sadržaja vodenog žiga je obavljeno GMSAT algoritmom, a insertovanje u video frejmove je obavljeno pouzdanim DWT-SVD algoritmom. U radu je pokazana otpornost predloženog algoritma kako na detekciju lažnog žiga tako i na nepoznavanja parametara inverznog GMSAT-a. U radu je pokazano da je ekstrakcija insetovanog vodenog žiga nije bila moguća u slučaju neposedovanja originalnog vodenog žiga, odnosno svih parametara GMSAT-a. Zbog toga što u procesu kodovanja dolazi do zanemarivanja detalja u frejmovima, ekstrahovani



Slika 6. Ekstrahovani vodeni žigovi sa izmenjenim a) i b) svim GMSAT parametrima i c) i d) izmenjenim parametrima prve etape.

vodeni žigovi su promenljivog kvaliteta što zahteva primenu naprednog algoritma za popravku. Ovim algoritmom je realizovan maksimalni SSIM indeks od 0.8956 iz video sekvence Foreman. Iz drugih video sekvenci su takođe ekstrahovani vodeni žigovi dobrog kvaliteta ali sa nešto nižim SSIM indeksom. U radu je pokazano da predloženi algoritam zadovoljava visok nivo bezbednosti i omogućava ekstrakciju vodenog žiga dobrog kvaliteta iz kodovanog videa. Povećanjem broja etapa GMSAT algoritma se može obezbediti proizvoljno visok nivo zaštite.

LITERATURA

[1] Cisco White Paper, “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2015–2020”, Feb. 2016.

[2] M. Jevtović, Z. Veličković, “Protokoli prepletenih slojeva”, Akademska misao, Beograd, 2012.

[3] Z. Veličković, Z. Milivojević, M. Jevtović, „Multi-stage Arnold transformation for 2D watermarking encription“, Vol. 2, pp. 130-135, UNITECH, 2015.

[4] E. Chrysochos, V. Fotopoulos, M. Xenos, A. N. Skodras, “Hybrid watermarking based on chaos and histogram modification”, *Sig. Im. Video Proc*, pp. 843-857, 2014.

[5] Z. Veličković, D. Blagojević, Z. Milivojević, M. Veličković “Poboljšanje bezbednosti skremblovanog vodenog žiga u haos domenu”, INFOFEST 2016, pp. 174-182, Budva 2016.

[6] C. Pradhan, V. Saxena, A. Bisoi, “Imperceptible Watermarking Technique using Arnold’s Transform and Cross Chaos Map in DCT Domain”, *Int. Jour. Comp. App.*, Vol. 55, No. 15, pp. 50 – 53, 2012.

[7] M. Ibrahim, N. Kader, M. Zorkany, “Video Multiple Watermarking Technique Based on Image Interlacing Using DWT,” *The Scientific World Journal*, Vol. 2014.

[8] Z. Veličković, Z. Milivojević, M. Veličković, M. Jevtović, “The impact of prediction structures H.264 encoder on the quality of the extracted watermark from the chaos domain”, ETF Jour. of Electrical Engineering, Vol. 22 , pp. 111-121, Podgorica, 2016.

ABSTRACT

To protect the video sequence of the copying, technique of inserting scrambled watermark is proposed. Scrambling watermark is made by GMSAT algorithm, and insertion was carried out in DWT-SVD video domain. The proposed algorithm is evaluated on three different video sequences, where it demonstrate resistivity on false positive watermark. The paper shows that the proposed algorithm satisfies the high security level.

SECURITY OF THE VIDEO PROTECTED BY SCRAMBLED WATERMARK WITH GMSAT ALGORITHM

Zoran Veličković, Marko Veličković