SAVREMENE TEHNOLOGIJE ZAŠTITE PODATAKA KOD DIGITALNOG PRAVA

Zoran Bojković, Andreja Samčović
Saobraćajni fakultet u Beogradu

Sadržaj: *U ovom radu govori se o savremenim tehnologijama zaštite podataka kod digitalnog prava. S tim u vezi, opisani su osnovni koncept i neki problemi sa kojima se sreće digitalno pravo. Zatim se ističu zahtevi vlasnika autorskih prava nad video materijalom, kao i kako se ti zahtevi odražavaju na očekivanja i zahteve korisnika. Opisana je i opasnost od potencijalne digitalne krađe. Predlaže se tehnika kriptovanja videa, da bi se ostvarila zaštita video podataka.*

Ključne reči: *multimedija, digitalno pravo, kriptografija, votermarking, video.*

1. Uvod

Savremena dostignuća u izgradnji komunikacione infrastrukture, obrade signala, kao i tehnologije digitalnog memorisanja podataka, omogućila su invazivan razvoj digitalnih medija. Distribucija digitalnih medija pruža fleksibilne i efikasne komercijalne multimedijalne transakcije. Digitalna priroda informacija takođe omogućava manipulisanje, umonažavanje, kao i jednostavan pristup medijima, zavisno od uslova same transakcije. Legalna distribucija digitalnih medija treba da obezbedi legitimne servise svim učesnicima u procesu, kako krajnjim korisnicima, tako i ostalim učesnicima u distribucionom lancu.

Ovim pitanjima se bavi nova oblast, koja se zove digitalno pravo. Ono u sebi obuhvata specifična prava korisnika u aktivnostima, kao što su pristup, pregledanje, i kopiranje digitalnih multimedijalnih sadržaja. Digitalno pravo treba da izbalansira funkcionalnost, zaštitu informacija, nove marketinške mogućnosti, kao i smanjenje troškova. Upravljanje digitalnim pravom uzima u obzir efikasne ekonomske modele, legalnu politiku, uticaj društva, kao i dostupnu tehnologiju [1].

Najveći problem današnjih multimedijalnih komunikacija je bezbednost podataka. Budući da je Internet organizovan kao skup velikog broja mreža koje koriste isti protokol za razmenu informacija, nemoguće je uspostaviti totalnu kontrolu. Šteta koju prave zlonamerni korisnici i piraterija procenjuje se godišnje na više milijardi dolara.

S tim u vezi, cilj ovog rada biće da ukaže na neke mogućnosti legalne zaštite multimedijalnih podataka, kako bi se ostvarila prava učesnika u lancu multimedijalne

distribucije. Prvi deo ovog rada odnosi se na koncept i na probleme sa kojima se susreće digitalno pravo, kao nova oblast multimedije. Zatim se govori o zaštiti autorskih prava, kao i zahtevima koje postavljaju vlasnici multimedijalnog materijala. Veoma važno pitanje digitalne krađe, predmet je narednog poglavlja. U nastavku ovog rada govori se o video kriptovanju, kao važnom segmentu zaštite video podataka. Na kraju su data zaključna razmatranja.

2. Digitalno pravo

Menadžment digitalnog prava (*Digital Rights Management, DRM*) treba da omogući kompromis između bezbednosti materijala, koju zahteva vlasnik prava; privatnosti krajnjeg korisnika, kao i cene sistema koji će biti korišćen između učesnika u tom lancu. U digitalnom svetu, bezbednost i privatnost se implementiraju korišćenjem raznih kriptografskih algoritama i protokola [2]. Na samom kraju lanca, digitalni sadržaj se prikazuje u analognoj formi: digitalna slika se transformiše u svetlo putem displeja, dok se digitalni zvuk transformiše u akustičke talase. Ponovna digitalizacija ovih analognih signala je uvek moguća. Deo savremenih DRM sistema predstavlja tehnika *votermarkinga* (vodenog žiga), koja podrazumeva utiskivanje digitalnih signala u vidu žigova, kako bi se ostvarilo praćenje i kontrola digitalnih kopija, čak i prilikom transformacije u analogne signale. Susretanje sa problemom specifičnih verzija talasnih signala, uključujući i njihovo analogno predstavljanje, dovodi do složenih kriterijuma. Proces votermarkinga može da se posmatra kroz analizu rizika (sa tačke gledišta provajdera), kao i analize dobitka korisnika. Postavlja se pitanje koji je rizik za provajdera, ako uvede votermarking, kao i koji bi bio dobitak za korisnika, u pokušaju da ukloni vodeni žig sa digitalnog medijuma [3].

Cilj DRM scenarija bio bi da analizira potencijalne slabosti u bezbednosti distribucionog lanca, kao i da identifikuje pri svakoj tački lanca koja sredstva treba da budu uključena, kako bi se problem prevazišao. Nekoliko sledećih scenarija se odnose na distribuciju slike:

- Distribucija kod digitalnog bioskopa: video materijal se prikazuje u bioskopskoj dvorani. Votermarking identifikuje prostor i vreme projekcije, što se skenira kamerom za vreme predstave. Parametri neautorizovane kopije mogu da se dobiju iz originalne verzije.
- Linkovi za distribuciju video sadržaja i arhiviranje između studija, pre pakovanja programa.
- Scenario radiodifuzije, kod koje se koriste tkz. set-top dekoderi za praćenje sadržaja i kontrola kopija na DVD (*Digital Versatile Disc*), ili personalnim računarima.
- Veb publikacija digitalnih slika.

Dve najvažnije stavke vezane za distribuciju videa jesu plaćanje za pristup videu, kao i zaštita autorskih prava (*copyright*). Prva stavka se odnosi na e-komercijalu, i mora da obezbedi sigurnost pri novčanim transakcijama kako za potrošača, tako i za distributora. Druga stavka se odnosi na zaštitu od krađe, prilikom distribucije videa.

Ukoliko neki provajder želi nacionalnu distribuciju VoD servisa, cena implementacije takvog poduhvata bila bi ekstremno visoka. Najpre, cena inicijalne hardverske implementacije bila bi veoma visoka, čak i u slučaju raspodele takvih troškova između više provajdera. Druga vrsta troškova odnosi se na održavanje i troškove

propusnog opsega, kako bi servis uvek bio dostupan potrošačima. Finalni troškovi odnose se na nadoknadu zaštite autorskih prava, kako bi njihovi vlasnici imali nadoknadu prilikom svakog emitovanja filma.

Svaki provajder u ovom poslu želi da vidi profit od svojih investicija, tako da korisnici moraju da plate korišćenje jednog takvog servisa. Zbog onlajn prirode te aplikacije, onlajn plaćanje bio bi najpogodniji metod plaćanja. Međutim, tu se krije nedostatak ovog načina, a to je da mnogi potrošači nemaju mogućnost, ili nisu familijarni sa ovim vidom novčanog transfera, koji bi išao preko Interneta. Sa druge strane, ako provajderi nisu u mogućnosti da obezbede punu sigurnost ovakve transakcije, pristup video materijalima bio bi slobodan, a time i redukovana mogućnost povraćaja uloženih sredstava. Ovaj vid e-komercijale je istovetan kako za onlajn video, tako i za ostale onlajn novčane transakcije, tako da rešenja koja budu važila za druge onlajn biznis transfere, važiće i za VoD industriju.

Vlasnici autorskih prava plaćaju veliki novac da bi obezbedili pravo nad kontrolom svakog emitovanja njihovog materijala. Problem sa konceptom VoD servisa je taj što se video distribuira putem Interneta, infrastrukturom javne mreže, dok se memoriše na potencijalno nesigurnim serverima, čineći sebe lakim objektom krađe. Ukoliko se to desi, vlasnici autorskih prava potencijalno gube povraćaj svog novca. Kod analognih sistema, ova mogućnost je manja, zbog degradacije kvaliteta prilikom svakog narednog kopiranja.

Prema tome, zaštita autorskih prava je krucijalna kod obezbeđenja VoD servisa. Ako vlasnici prava nisu ubeđeni da njihov materijal neće biti predmet digitalne krađe, onda ga neće učiniti dostupnim onlajn. U nedostatku većeg izbora video sadržaja, servis neće biti korišćen u dovoljnoj meri od strane potencijalnih korisnika, zbog smanjenog interesovanja. Vlasnici autorskih prava moraju da budu uvereni da će njihovo vlasništvo biti zaštićeno, pre nego što dođe do realizacije onlajn distribucije.

Vlasništvo autorskih prava podrazumeva ekskluzivno pravo nad izradom i distribucijom kopija, kao i njihovim javnim emitovanjem. Prilikom distribucije video materijala preko mreže, jedino vlasnici kopirajta mogu da vrše modifikacije sadržaja, i distribuiraju ga drugim korisnicima sa mreže. O tome da li će sadržaj biti distribuiran slobodno, ili uz plaćanje, odlučuje samo vlasnik autorskih prava.

Vlasništvo kopirajta je ekonomska investicija. Vlasnik očekuje pri tome da će povratiti uložena sredstva, i ostvariti određenu zaradu. Plaćanje vlasnicima muzičkog, ili audio materijala, se odvija izdvajanjem određenog procenta prilikom svakog emitovanja, ili plaćanjem određene takse pri emitovanju od strane neke radio ili televizijske stanice. Na sličaj način, plaćanje vlasnicima videa može da se ostvari bilo izdvajanjem određenog procenta, bilo taksom prilikom emitovanja videa.

Koncept isporuke audio ili video sadržaja preko javnih mreža stvara nove probleme u oblasti kopirajta. Naime, treba obezbediti sistem za prikupljanje taksi ili procentaulne zarade, zaštitu od digitalne krađe, kao i to koji učesnici u procesu su odgovorni za obezbeđenje svake karike u tom lancu. Svi ti izazovi se nameću pred tehničkim pitanjima kako primeniti postojeće pravne propise u digitalnom domenu. Najčešće, takse plaćaju televizijske kuće, ili vlasnici video klubova. Pri tome, master kopije analognog video sadržaja se najčešće nalaze kod video distributerskih kuća.

Kod distribucije digitalnog videa, do korisnika stižu digitalne kopije visokog kvaliteta, i svaka reprodukcija će biti ujednačeno dobrog kvaliteta. Međutim, prenosom takvog materijala javnim mrežama, dolazi do mogućnosti krađe od strane pirata. Pošto

problem sigurne onlajn novčane transakcije još nije rešen, vlasnici autorskih prava su zabrinuti oko povraćaja svojih ulaganja, kao i oko krađe digitalnog videa sa javne mreže. Uprkos tome što digitalna krađa nije toliko laka kako vlasnici kopirajta misle, ona se dešava, tako da ima mesta njihovoj brizi.

Generalno, vlasnici autorskih prava nisu eksperti u Internet tehnologijama. Oni Internet često doživljavaju kao medijum gde je njihov materijal svima dostupan onlajn. Sa druge strane, krađa materijala sa Interneta je moguća, iako nije baš jednostavna. Nesiguran prenos digitalnih podataka preko neke druge mreže je uvek otvoren za krađu administratora te mreže. Jedan od načina da vlasnici prava budu ubeđeni u siguran prenos je kriptovanje materijala pri tranzitu kroz mrežu, i direktno dekriptovanje pre emitovanja sadržaja.

Zaštita digitalnog materijala od krađe je od izuzetnog značaja. Vlasnici prava treba da budu uvereni da će njihovo vlasništvo biti obezbeđeno od krađe, kao i da će tok novca od strane potrošača ka njima biti dobro definisan i bezbedan. Sve dok ti uslovi ne budu zadovoljeni, ekonomski rast video servisa neće biti znatnije ostvaren.

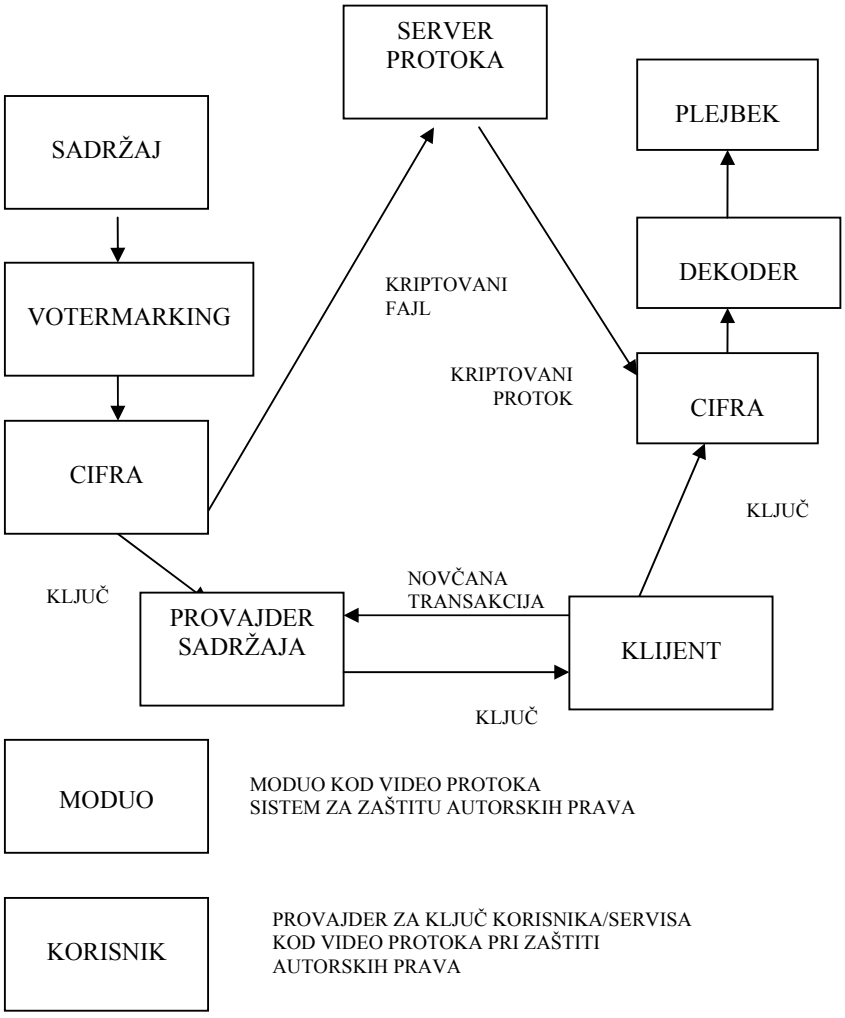
3. Zaštita autorskih prava

Pri razmatranju aplikacija digitalnog videa sa stanovišta vlasnika autorskih prava, postaje očigledno da je njihov značaj više ekonomski, nego tehnički. Postoji četiri dela funkcionisanja VoD sistema, koji se odnose na zaštitu autorskih prava, što je naznačeno na Slici 1.

- Pasivna zaštita sadržaja – korišćenjem votermarkinga, sadržaj može da bude utisnut u nevidljivi digitalni signal. Ovaj pristup ne štiti aktivno od ataka na digitalni materijal, ali može da se upotrebi da bi se odredio izvor napada
- Garantovano plaćanje za pristup – u današnjoj ekonomiji, velike sume novca se ulažu u zaštitu autorskog prava. Vlasništvo nad multimedijalnim materijalom omogućava pravo upravljanja i prezentacije tog materijala. U praksi, to znači da je neophodna taksa za emitovanje na televiziji, prikazivanje u bioskopu, ili iznajmljivanje video kaseta. Kao i za svako drugo ulaganje, očekuje se da sredstva koja se dobijaju tom distribucijom multimedijalnog materijala, budu tretirana kao i svaka druga sredstva koja nastaju nečijim ulaganjem. Pri tome se zahteva garantovana šema isplate, na osnovu emitovanja video sadržaja.
- Kriptovanje video striminga – ovaj koncept se sastoji u tome da sadržaj treba da bude kriptovan sve vreme, dok korisnik može da ga dekriptuje pre plejbeka. Koncept kriptovanja video materijala ne služi samo za prevenciju od gledanja osoba koje nemaju za to pravo, već i za prevenciju od nelegalne izrade digitalnih kopija.
- Menadžment ključa – srce svakog sistema za kriptovanje je ključ za cifre, sa odgovarajućim menadžmentom.

Glavni problem za vlasnike autorskih prava nad multimedijalnim materijalom, je eventualna mogućnost njihove krađe. Korisnici mogu da naprave kopije potpuno legitimno, naime snimanjem emitovanog televizijskog signala, i pri tome mnogi VHS video rikorderi imaju mogućnost emitovanja snimljenog materijala. Međutim, ova mogućnost nelegalnog emitovanja ne zabrinjava mnogo vlasnike, jer je svaka kopija

analogna, uz relativno loš kvalitet, koji se pri tom rapidno gubi svakim narednim kopiranjem. VHS emitovanje iz DVD (*Digital Versatile Disc*) izvora je takođe lošijeg kvaliteta nego original. Čak i digitalno snimanje sa DVD originala pati od degradacije kvaliteta, zato što imamo najpre konverziju digitalne slike u analognu, pre ponovne konverzije u digitalni oblik pogodan za emitovanje.



Slika 1. *Šema za zaštitu autorskih prava kod video protoka*

Pri razmatranju aplikacija digitalnog video protoka, originalni sadržaj je u digitalnoj formi, koji se zatim prenosi preko javnih mreža ponovo digitalno, sve do opreme korisnika, gde ponovo egzistira u digitalnoj formi. Kod vlasnika video materijala postoji opravdan strah da može doći do neovlašćenog digitalnog kopiranja, bilo pri prenosu po mreži, bilo od strane opreme krajnjeg korisnika. Bilo koja digitalna kopija filma teško može da se razlikuje od originala, bez ikakve degradacije kvaliteta slike kod te, ili naredne kopije [4]. To u praksi znači da može doći do izrade mnogo kopija jednako dobrog kvaliteta, koje zatim mogu biti prodate video piratima, ostvarajući time nelegalnu zaradu, i pri tome minimizirajući povraćaj sredstava za vlasnika autorskih prava.

Prilikom projektovanja sistema videa na zahtev (*Video on Demand VoD*) javlja se ograničenje sa zahtevom zaštite sadržaja koju sistem treba da ostvari. Potencijalni uspeh šeme za zaštitu autorskih prava se povećava, ukoliko je proces generički, što znači da nije vezan za specifičnu platformu.

Značajan faktor kod ovog sistema je potreba za kriptovanjem, na prvom mestu. Zahtevi vlasnika autorskih prava diktiraju kako treba obaviti kriptovanje. Ekonomski značaj umreženog VoD sistema zavisi od dostupnosti materijala potrošačima koji su u mogućnosti da plate gledanje tog materijala. Vlasnici autorkih prava treba da budu ubeđeni da njihov materijal neće biti predmet potencijalne krađe. Ukoliko ova garancija nije moguća, dostupnost željenog materijala biće teško ostvariva, a time i implementacija VoD sistema.

4. Digitalna krađa

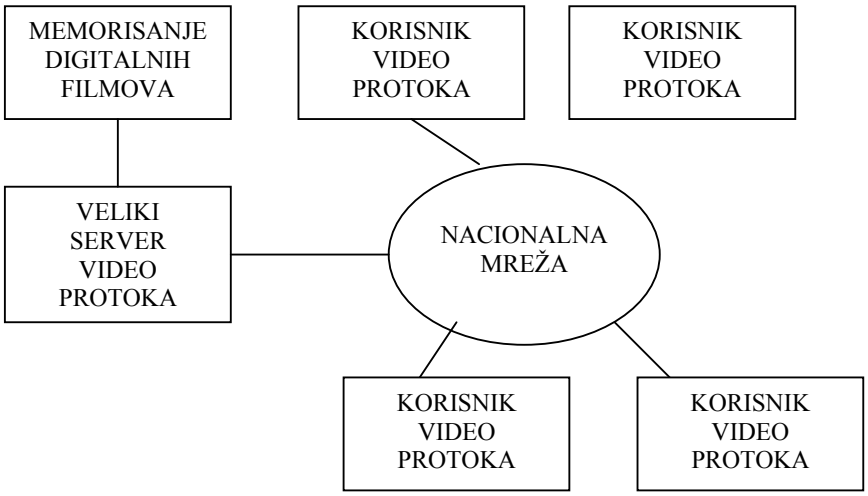
Imajući u vidu značaj zaštite digitalnog video materijala od krađe, potrebno je sagledati koje su to osetljive tačke VoD sistema, gde mogu da se dogode takve krađe. Jedino tada može da se definiše niz zahteva u pogledu bezbednosti pri projektovanju takvog sistema [5].

U slučaju da neki provajder odluči da obezbedi VoD servis preko Interneta, najpre bi morao da obezbedi snažnu radnu stanicu opremljenu sa moćnim diskom, i visokokvalitetnim softverom za video protok. Sledeći korak bi bilo povezivanje ovog servera sa Internetom, preko konekcija širokog propusnog opsega. Dokle god bude bio obezbeđen visok kvalitet servisa koji se nudi korisnicima, sistem će obezbeđivati adekvatan protok servisa. Primer jednog takvog sistema je pokazan na Slici 2, sa velikim video serverom, koji obezbeđuje kvalitetan video signal po mreži nacionalnog značaja. Problem sa ovim sistemom je u visokoj ceni propusnog opsega, visokoj ceni nadogradnje sistema, osetljivosti na otkaze, kao i skalabilnosti pri projektovanju sistema.

Jedna od potencijalno ranjivih tačaka jeste bezbednost prisutna kod centralnog servera. Server je vlasništvo distributora digitalnog sadržaja, a njegov zadatak je da prihvati zahteve za videom od strane potrošača, i zatim da ga transferiše do lokalnih servera koji opslužuju korisnike. Ovaj sistem je osetljiv na napade hakera koji nemaju autorizovan pristup serveru i digitalnim podacima koji su na njemu instalirani. Ako server nije siguran, neovlašćeni pristup može biti relativno jednostavan, tako da ova tačka može biti potencijalno opasna za nepvlašćeno preuzimanje video fajlova od servera.

Postoje dve tehnike koje mogu da se koriste kako bi se korigovao ovaj potencijalan problem; jedna od njih je poboljšanje bezbednosti samog servera. Rekonfiguracija samog servera protiv neautorizovanog pristupa može biti sprovedena bilo korišćenjem postojećih bezbednosnih mera, kao što je zaustavljanje servisa koji nisu

neophodni na serveru, i/ili korišćenjem boljih mera bezbednosti operativnog sistema. Drugo rešenje ovog problema bilo bi memorisanje videa na centralnom serveru u kriptovanoj formi. Ovaj postupak ne štiti od krađe kriptovanog materijala, ali obezbeđuje da kriptovani materijal bude siguran od pokušaja hakera da dospe do njega, pošto haker neće moći da učita materijal bez sistema za dekriptovanje. Primena bilo kojeg od ova dva rešenja, ili oba zajedno, smanjuje mogućnost krađe digitalnog video materijala na strani centralnog servera.



Slika 2. *Primer jednog VoD sistema*

U slučaju više učesnika u ovom procesu, zaštićeni sadržaj se smešta na distribuiranom serveru koji je kontrolisan od strane provajdera date mreže. Time se mogućnost krađe povećava, jer se može desiti da neki od tih servera ne bude siguran. Jedino rešenje pri tome je da video imovina bude instalirana na serveru u kriptovanoj formi. Budući da u ovom procesu može da bude uključeno više različite opreme za servere, tehnike kriptovanja moraju da zadovolje zahteve širokog opsega video servera.

Pošto Internet predstavlja javnu mrežu, podaci koji se prenose njime su dostupni svim učesnicima u prenosu. Digitalni podaci ne mogu fizički da budu zaštićeni od eventualnih krađa, budući da mreža nije privatna.

Krađa digitalnog videa može da se desi prilikom tranzita paketa podataka. Podaci u okviru paketa mogu da se reasembluju u originalni digitalni fajl. U slučaju VoD servisa, podaci mogu da budu ukradeni pri tranzitu na dva načina. Jedan je da se podaci preusmere pri tranzitu od centralnog do lokalnih servera, a drugi pri tranzitu od lokalnih servera ka korisnicima.

Ova vrsta krađe nije tako jednostavna kao što izgleda, posebno pri protoku video podataka od lokalnog servera ka potrošačima. To je zato što se video podaci šalju obično po odgovarajućem protokolu. Kada pirat pokuša da memoriše pakete iz mreže, mora da

dekoduje protokol da bi rekonstruisao originalni digitalni video signal. Rešenje ovog problema bilo bi u kriptovanju, i u proveri da li je signal svaki put kriptovan pri prenosu kroz mrežu. Na taj način, digitalno vlasništvo bilo bi sigurno, jer potencijalni pirat ne bi mogao da učita video podatke u kriptovanoj formi [6].

Digitalni video materijal može da bude ukraden i na strani krajnjeg korisnika. To može da se obavi tako što se plati za legalnu isporuku videa, i zatim se napravi njegova digitalna kopija, u cilju daljeg emitovanja. Pošto je video sadržaj poslat u digitalnoj formi, relativno je jednostavno za programera da sačuva materijal na disku, pre nego što ga dekoduje i prikaže. Kopija zatim može biti ilegalno korišćena. I za ovu eventualnost rešenje bi bilo u kriptovanju. Ako video dolazi do korisnika već u kriptovanoj formi, dekodovanje i dekriptovanje može da se obavi prilikom emitovanja video materijala. Korisnika tada može videti samo kriptovani video, ili kompletno dekriptovani i dekodovani video signal.

5. Video kriptovanje

Imajući u vidu komercijalne zahteve za video servisima, navedene zahteve servera, kao i zahteve korisnika autorskih prava, očigledno je da postupak kriptovanja mora da zadovolji sve te zahteve. Sistem treba da zaštiti video vlasništvo od krađe pri tranzitu kroz mrežu, memorisanju na serveru, kao i prilikom dekodovanja i prikazivanja na strani korisnika. Sa tačke gledišta korisnika, mora takođe da bude obezbeđeno da ništa od kvaliteta video signala pri tome ne bude izgubljeno.

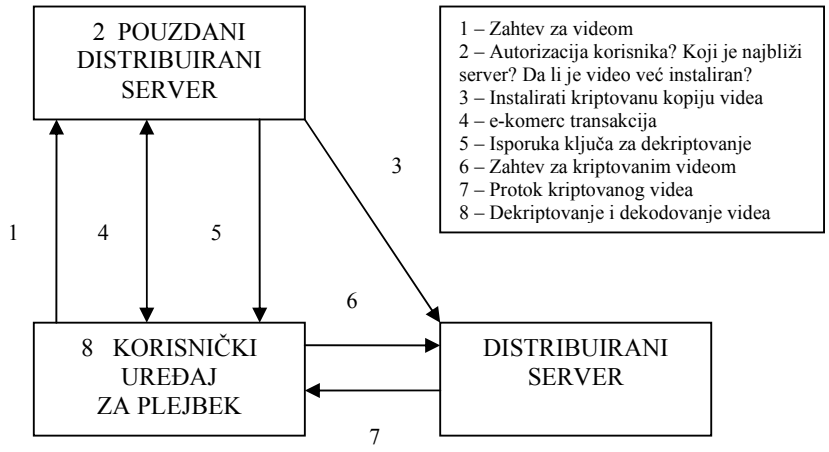
Vlasnik kopirajta ima pravo da postavi niz zahteva pred projektante sistema za video servise. Ukoliko ovi zahtevi budu zadovoljeni, vlasnici će biti uvereni da će njihova investicija biti propisno zaštićena. Prvi zahtev se odnosi na autorizaciju korisnika, i garanciju za siguran transfer novčanih sredstava ka vlasniku kopirajta. Ovaj problem može biti rešen odgovarajućim e-komerc modelom. Ovlašćeni korisnik u tom slučaju dobija "ključ" kojim će dešifrovati kriptovani video signal. Sistem kriptovanja javnog ključa je složen postupak sam po sebi. Takođe, i algoritmi za kriptovanje su relativno složeni. Osnovna procedura menadžmenta ključa je pokazana na Slici 3.

Drugi zahtev vlasnika autorskih prava bi se odnosio na aktivnu zaštitu njihovog vlasništva putem kriptovanja. Oni će tražiti da digitalni video bude kriptovan sve vreme tranzita kroz javnu mrežu. Takođe, imaće zahtev da video bude kriptovan i pri memorisanju na bilo kom uređaju mreže koji nije bezbedan i pouzdan. Ovaj zahtev uvodi ograničenje da svi serveri u lancu moraju da obezbede nesmetan protok kriptovanog video signala. Konačno, vlasnici kopirajta mogu zahtevati da se video dekriptuje samo na uređajima krajnjeg korisnika, i to tako da korisnik nema direktan pristup dekriptovanom video sadržaju, kako ga ne bi mogao dalje kopirati.

Ova ograničenja se ne odnose samo na sistem za protok videa, već i za projektovanje algoritma za video kriptovanje. Onlajn video servis mora da obezbedi autentifikaciju potrošača, kao i mogućnosti za nesmetano plaćanje, što bi štitilo ne samo vlasnika kopirajta, već i korisnika od monetarne krađe. Takođe, zahteva se da video bude kriptovan od kada napusti centralni server, pa sve dok ne bude dekriptovan i dekodovan na strani korisničkog uređaja za plejbek.

Široki opseg servera podrazumeva različit hardver, operativne sisteme, kao i softver, što znači da kriptovani digitalni video signal mora da bude kompatibilan sa svim postojećim i budućim video serverskim sistemima. Pošto je nemoguće tačno predvideti

kako će budući serveri da izgledaju, moguće je sagledati postojeće, i obaviti ekstrapolaciju. U slučaju da kriptovani digitalni video fajl ima isti format kao i nekriptovani, razumno je očekivati da kriptovani sadržaj može da se instalira na serveru koji nema unapred saznanje o algoritmu za kriptovanje. Međutim, ako kriptovani digitalni video zahteva da lokalni server bude upoznat sa šemom kriptovanja, nameću se ograničenja pred novim tehnologijama video servera. Da bi se izbegle eventualne teškoće, kriptovani video mora biti instaliran na svim video serverskim platformama.



Slika 3. *Procedura za autentifikaciju korisnika*

Serveri za protok videa često podržavaju pri emitovanju mogućnosti kao što su pretraživanje, brzo premotavanje unapred, ili unazad. Kompatibilnost sa ovim funkcijama traži posebne zahteve. Pri pretraživanju, video server mora da poseduje vremenski indeks da zaustavi tada protok videa, i usmeri protok prema vremenskom indeksu. U slučaju da se radi sa nekriptovanim videom, ovo nije problem, pošto bitska brzina može da aproksimativno locira poziciju fajla, i prođe kroz fajl radi finog indeksiranja. Ako se radi o kriptovanom video signalu, tada binarni protok mora da omogući serveru da locira tačno određene vremenske indekse. Brzo premotavanje unapred, ili unazad, takođe zahtevaju posebnu pažnju. Da bi se minimiziralo korišćenje propusnog opsega mreže, postojeći serveri video protoka radije preskaču pojedine kadrove, nego što ih sve obrađuju pri većoj brzini. Pri tome se prenosi samo deo komprimovanih video podataka, dok se audio podaci kompletno izostavljaju. To se obično radi tako što se obavi protok samo I-kadrova komprimovanog video fajla, pošto oni ne zahtevaju susedne kadrove da budu prisutni pre dekodovanja. U slučaju da je ova funkcionalnost podržana i sa kriptovanim videom, video server mora da locira pojedinačne kadrove u okviru kriptovanog fajla, i da odredi tip kadra koji su preneti. Na ovaj način, server može da locira pojedinačne kriptovane kadrove, i da ih prosledi ka korisnicima.

6. Zaključak

Danas još uvek nije moguća isporuka kvalitetnog video signala preko Interneta, u cilju zabave. Pri projektovanju tehničih rešenja, moraju se uzeti u obzir zahtevi vlasnika autorskih prava nad video sadržajima, kao i zaštita njihovog video vlasništva od mogućih digitalnih krađa. Dok se ne obezbedi puna zaštita, vlasnici kopirajta neće omogućiti sadržaj dostupan onlajn video servisima.

Zaštita autorskih prava može biti garantovana samo nekim vidom kriptovanja. Zahtevi koji se odnose na jedan takav sistem su sledeći:

- Video signal mora biti kriptovan, pre nego što bude onlajn dostupan. Video mora biti distribuiran serverima protoka, i instaliran na njima u kriptovanom obliku
- Video mora doći do korisnika u kriptovanoj formi
- Funkcionalnosti servera protoka moraju da budu zadržane pri protoku kriptovanog videa. Format kriptovanog fajla mora da zadovolji široki opseg postojećih i budućih servera protoka

Literatura

[1] R.Owens, R.Akalu: "Legal policy and digital rights management", *Proceedings of the IEEE,* Vol.92, No.6, pp 997-1003, June 2004.

[2] J.E.Cohen: "DRM and privacy", *Commun. ACM,* Vol.46, No.4, pp 47-49, April 2003.

[3] J.Dittmann, P.Wohlmacher, K.Nahrstedt: "Using cryptographic and watermarking algorithms", *IEEE Multimedia,* Vol.8, No. Oct-Dec, pp 54-65, 2001.

[4] S.Western, K.Lagendijk, J.Biemond: "Perceptual image quality based on a multiple channel VHS model", in *Proc. ICASSP,* pp 2351-2354, 1995.

[5] D.Augot at al: "Secure delivery of images over open networks", *Proceedings of the IEEE,* Vol.87, No.6, pp 1251-1266, July 1999.

[6] A.Eskicioglu, E.Delp: "An overview of multimedia content protection in consumer electronics devices", *Signal Processing: Image Communication,* Vol.16, pp 681-699, 2000.

Abstract: *This paper discusses some advanced technologies for copyright protection, concerning digital rights. We start by describing the concept and some problems of digital rights. Then we outline the requirements of copyright protection as concerns copyright owners, as well as how these concerns relate to end user expectations and requirements. We describe also the danger of potential digital theft. Finally, we propose the video encryption technique.*

Keywords: *multimedia, digital right, criptography, watermarking, video.*

ADVANCED TECHNOLOGIES FOR COPYRIGHT PROTECTION IN DIGITAL RIGHTS

Zoran Bojković, Andreja Samčović