Model primene sopstvenih kriptografskih i steganografskih algoritama na primeru Web galerije slika

Mladen Veinović, Aleksandar Jevremović, Goran Šimić

***Sadržaj* — U ovom radu je predstavljen model rešenja za tajni prenos šifrovanih podataka. Rešenje se bazira na korišćenju sopstvenih kriptografskih i steganografskih algoritama. Kao podrazumevani nosilac podataka kod steganografskih funkcija uzima se Web galerija slika. Rešenje podrazumeva korišćenje PNG i JPEG formata bez gubitka kvaliteta.**

***Ključne reči* — kriptografija, steganografija, sopstveni algoritam, zaštićena komunikacija.**

I. UVOD

U savremenim računarskim mrežama kod pitanja bezbednosti podataka tokom prenosa podrazumeva se upotreba kriptografskih rešenja. U profesionalnim sistemima zaštite korišćenje sopstvenog algoritma u simetričnim šifarskim sistemima i tajnost simetričnih šifarskih ključeva jesu osnova garancije bezbednosti. Primenom ovog principa – razvojem sopstvenog kriptografskog rešenja – i korišćenjem pouzdanih gotovih komponenti može se ostvariti komunikacija u čiji sadržaj posrednici nemaju uvid te se takva komunikacija može smatrati bezbednom.

Prvi problem koji izlazi van prostora u kome rešenje nudi kriptografija jeste taj da se zaštićena komunikacija može ometati (onemogućiti) ukoliko treća strana ima mogućnosti uticaja na infrastrukturu korišćenu za komunikaciju (komunikacioni kanal). Lokalne mreže (odnosno mreže sa čijom infrastrukturom treća strana nema dodira) najčešće se smatraju bezbednim te u njima često i nema potrebe za jakim bezbednosnim mehanizmima. Sa druge strane, kanali Internet mreže najčešće nisu pod kontrolom korisnika tako da se rešenje pomenutog problema često nalazi u korišćenju redundantnih kanala.

Sledeći problem vezan za upotrebu kriptografskih rešenja jeste mogućnost snimanja komunikacije od strane posrednika u komunikaciji. S obzirom na to da većina kriptografskih rešenja u upotrebi ne nudi apsolutnu već praktičnu (računski sigurnu) bezbednost, problem snimanja komunikacije (stavljen u odnos sa sve većom procesorskom snagom savremenih računara) može se smatrati izuzetno značajanim. Ovaj problem je moguće rešavati na više načina. Jedan od načina predstavlja upotreba bezbednosnih rešenja koja nude apsolutnu sigurnost. Međutim, ovakva rešenja imaju određene nedostatke koji ih čine neefikasnim u realnim uslovima.

Jedan od načina ostvarivanja bolje zaštite jeste i ranije pomenuta upotreba sopstvenih algoritama. Na ovaj način se napadaču proces razbijanja šifrata znatno otežava usled nepoznavanja algoritma kojim je izvršeno šifrovanje odnosno kojim se vrši dešifrovanje.

Pristup koji će u ovom radu biti razmatran zasniva se na upotrebi steganografije uz korišćenje sopstvenog šifarskog simetričnog sekvencijalnog algoritma. Upotrebom steganografije moguće je potencijalnim napadačima znatno otežati proces razbijanja šifrata jer se od njih, pored originala sadržaja, skriva i informacija da je do komunikacije uopšte i došlo. U radu će ceo koncept biti razmotren na primeru Web galerije slika uz korišćenje ranije razvijenog šifarskog algoritma [1,2].

II. STEGANOGRAFIJA, POGODNI SADŽAJI I FORMATI

Jedan od glavnih problema pri korišćenju steganografije jeste neefikasnost, odnosno, loš odnos korisne/prenete količine podataka. Iz tog razloga, bezbednosna rešenja bazirana na steganografiji najčešće podrazumevaju primenu u okruženjima sa velikim mrežnim protocima podataka. U skladu sa ovim kriterijumom, najpodesnije nosioce sadržaja predstavljali bi obimni multimedijalni sadržaji (sadržaji velike bitske dužine).

Jedan od važnih zahteva pri odabiru nosećeg formata i razvoju rešenja zavisi i od toga da li format omogućava čuvanje podataka sa ili bez gubitaka. U slučaju da odabrani format omogućava čuvanje podataka sa određenim gubicima rešenje mora biti takvo da se umetanje skrivenog sadržaja vrši tek nakon formatiranja nosećih podataka, tj. ostvarivanja gubitaka. U protivnom, ukoliko format omogućava čuvanje podataka bez gubitaka, umetanje skrivenog u noseći sadržaj moguće je i pre i nakon formatiranja podataka.

Za potrebe ovog rada razvijeno je rešenje koje koristi PNG (*Portable Network Graphic*) i JPEG (*Joint Photographic Experts Group*) formate slika.

PNG format omogućava čuvanje slika bez gubitaka u obliku mapa bitova (engl. bitmap). Pored ostalih mogućih kanala (indeksirane boje, crno-bela i sl.) PNG format podržava dve značajne kombinacije korišćenja kanala:

1. Red + Green + Blue
2. Red + Green + Blue + Alpha channel

U ovim režimima je za svaki od kanala moguće koristiti po 8/16 bitova što omogućava korišćenje 24/48 bitova po

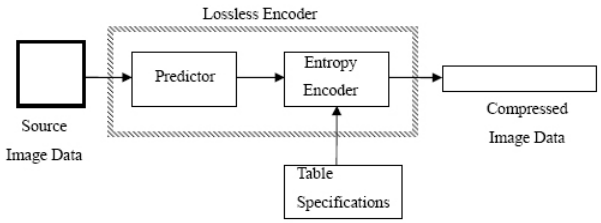
M. Veinović, Univerzitet Singidunum Beograd, Srbija (telefon: 381-11 3093227; e-mail: mveinovic@singidunum.ac.yu).

A. Jevremović, Univerzitet Singidunum Beograd, Srbija (telefon: 381-11 3093265; e-mail: ajevremovic@singidunum.ac.yu).

G. Šimić, Vojna Akademija Beograd, Srbija (telefon: 381-11 3603654; e-mail: gsimic@singidunum.ac.yu).

pikselu za slike sa RGB kanalima, odnosno, 32/64 bita po pikselu za slike sa RGB+alfa kanalima. Ovakve karakteristike (broj kanala, bitova i rad bez gubitka kvaliteta) čine PNG format pogodnim za steganografske operacije, kako zbog visokog koeficijenta iskorišćenosti piksela, tako i zbog mogućnosti umetanja skrivenog sadržaja i pre i nakon formatiranja nosećeg sadržaja slike.

JPEG format je poznat po svojoj efikasnosti u pogledu malog zauzeća prostora na mediju za skladištenje. Ova efikasnost se bazira na delimičnom gubitku podataka (niži kvalitet) i primeni algoritama za kompresiju. Za potrebe ovog rada korišćen je režim koji se ređe sreće u praksi a u kome ne dolazi do gubitka informacija (engl. lossless).



Sl. 1 – JPEG kodiranje bez gubitaka

Važno je napomenuti da lossless JPEG format koristi potpuno drugačiji pristup od standardnog JPEG formatiranja.

III. Sopstveni šifarski algoritam

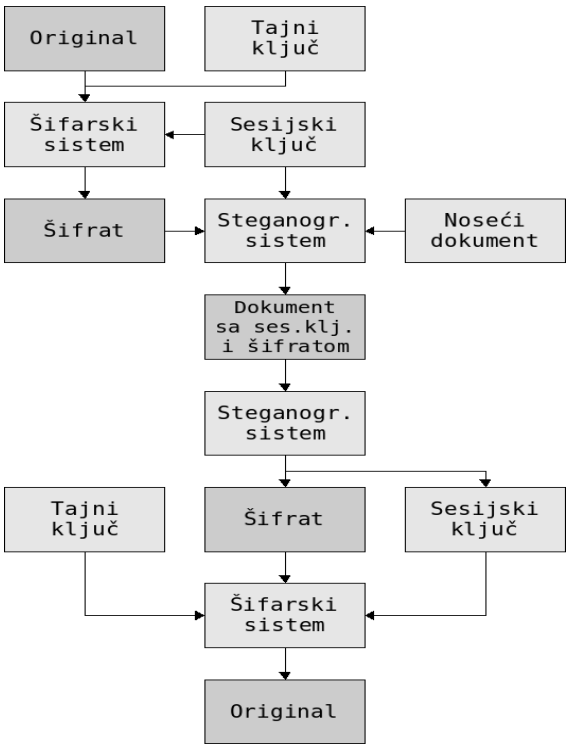
Za potrebe analize rešenja predstavljenog u ovom radu korišćen je realan simetrični sekvencijalni šifarski algoritam koji je inicijalno razvijen za potrebe ranijih radova autora [1,2]. Karakteristike sopstvenog algoritma su u skladu sa savremenim kriptološkim zahtevima. U odnosu na komercijalno dostupan AES algoritam primenjuju se simetrični ključevi znatno većih dužina.

Karakteristike algoritma nisu u prvom planu ovoga rada s obzirom na to da se on koristi pre svega za poboljšanje rešenja i predstavljanje koncepta. Sa druge strane, mogućnost sopstvene realizacije algoritma omogućava profesionalnim korisnicima potpuno poverenje u kriptološki kvalitet realizovanog rešenja. Obezbeđeni dovoljni memorijski resursi za realizaciju sopstvenog algoritma i implementacija simetričnih ključeva zahtevane dužine (znatno više od 256 bitova) predstavljaju dovoljne stepene slobode za svakog profesionalnog korisnika sistema zaštite.

Vreme za realizaciju funkcija šifrovanja i dešifrovanja nije od interesa u ovakvim sistemima, ali se zahteva efikasna realizacija kriptoloških struktura algoritma.

IV. Model rešenja

Ko što je u uvodnom delu rada napisano, rešenje opisano u ovom radu se bazira i na kriptografskim i na steganografskim funkcijama, odnosno, interno razvijenim kriptografskim i steganografskim algoritmima. Pregled kompletnog procesa i puta podataka koji se štite dat je na slici 2.

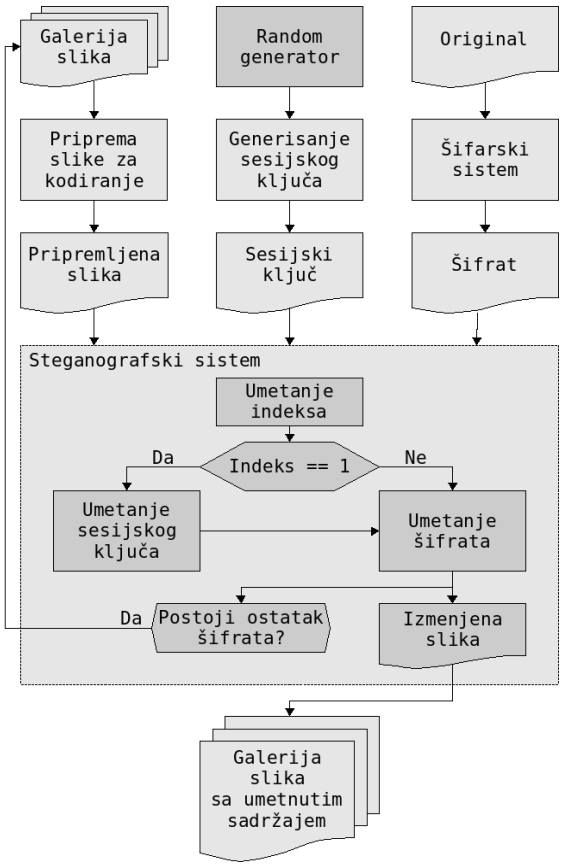


Sl. 2 – Put podataka koji se štite kroz sistem

Rešenje podrazumeva upotrebu standardnog procesa šifrovanja podataka simetričnim sekvencijalnim algoritmom (uz generisanje sesijskih ključeva) sa tom razlikom što se sesijski ključ i šifrat ne šalju direktno primaocu već se isporučuju steganografskom sistemu. Steganografski sistem prihvata sesijski ključ (fiksne dužine) i utiskuje ga na sam početak nosećeg dokumenta (slike). Nakon utiskivanja sesijskog ključa, steganografski sistem nastavlja sa utiskivanjem šifrata u noseći dokument. U slučaju da je bitska dužina šifrata veća od bitske dužine prostora za utiskivanje kod nosećeg dokumenta, steganografski sistem uzima sledeći noseći dokument. Na slici 2. je prikazan kompletan proces sa upotrebom više nosećih dokumenata (galerije slika).

Tajni ključ se nalazi kod korisnika i ne prenosi se kroz razmatrani sistem. Ključ se čuva se na odgovarajućem medijumu. Najpogodniji medijum za ovu namenu je *smart* kartica na kojoj se često mogu naći i drugi kriptološki parametri šifarskog sistema. Pogodnim generisanjem ključeva mogu se realizovati parovi tajnih ključeva (za tajno komuniciranje samo dva učesnika) ili više identičnih ključeva ukoliko je u prijem istog dokumenta uključeno više krajnjih korisnika. Posle određenog vremena vrši se zamena ovih ključeva kod krajnjih korisnika. Ako krajnji korisnici koriste *smart* kartice, generišu se i distribuiraju nove, a stare se uništavaju.

Sesijski ključ nije tajan, ali se zahteva da i on bude generisan na slučajan način. Za svaku novu informaciju koja se prenosi šifrovano steganografskim sistemom neophodno je generisati drugi sesijski ključ. Sve ovo je u skladu sa dobro poznatim klasičnim simetričnim šifarskim sistemima.



Sl. 3 – Proces kodiranja sadržaja u noseću sliku

Još jedna osobina steganografskog sistema koju treba napomenuti jeste i utiskivanje indeksa u noseće dokumente. Ovi indeksi su značajni kod prenosa šifrata koji su utisnuti u više dokumenata jer se na osnovu njih vrši ponovno spajanje delova šifrata po odgovarajućem redosledu.

Dešifrovanje na strani primaoca podrazumeva posedovanje korišćenih steganografskih i kriptografskih sistema (algoritama) i posedovanje tajnog ključa kojim je izvršeno šifrovanje. Procesu dešifrovanja prethodi proces iščitavanja sesijskog ključa i šifrata iz nosećih dokumenata (steganografski sistem) nakon čega se primenjuje standardna procedura dešifrovanja.

Značajan korak celokupnog procesa predstavlja i priprema slike za utiskivanje sadržaja koji se skriva. U okviru tog koraka se vrednost svakog kanala (u ovom slučaju R, G i B ili R, G, B i Alpha kanali) svih piksela fotografije dovodi na parnu vrednost putem postavljanja bita najmanje vrednosti na nulu. Ovakva priprema fotografije omogućava da se na vrednosti poslednjih bitova kanala redno utiskuju bitovi dokumenta koji se utiskuje.

V. Analiza efikasnosti rešenja

Efikasnost kriptografskih rešenja se može određivati na osnovu više parametara – kvalitet generatora slučajnih brojeva, opterećenje procesora koji izvršava šifrovanje, i sl. Međutim, specifičnost rešenja opisanog u ovom radu, ogleda se pre svega u primeni steganografije. U skladu sa tim, neki od kriterijuma vezanih za kriptografiju gube na značaju. Npr. opterećenje procesora, pre svega iz razloga što kod ovakvog sistema ne postoji direktna komunikacija, tj. potreba za velikim protokom u realnom vremenu.

Sa druge strane, jedan od glavnih kriterijuma efikasnosti steganografskih sistema jeste odnos sadržaja koji se skriva i nosećeg sadržaja [3]. Na primeru Web galerije slika – fotografija – mogu se razmatrati fotografije napravljene savremenim digitalnim foto aparatima u standardnoj veličini:

1.920 x 2.560 = 4.915.200 piksela

S obzirom na to da se za svaki od kanala podrazumeva po jedan bajt, i to da kod fotografija najčešće nije prisutan Alpha već samo R, G i B kanali, za skladištenje 4.915.200 piksela je bez optimizacija formata potrebno 14.745.600 bajtova, odnosno, 117.964.800 bitova. Korišćenjem svakog osmog bita za čuvanje sadržaja dokumenta koji se utiskuje dobija se rezultat od 1.843.200 bajtova (1,76MB) za utiskivanje skrivenog sadržaja. Ovakva računica na primeru slike 4., čija originalna veličina u PNG formatu iznosi 5.380.635 bajtova (5,1MB), ukazuje na to da je ostvareni koeficijent iskorišćenja 34 procenta:

1.843.200 / 5.380.635 = 0,34256179

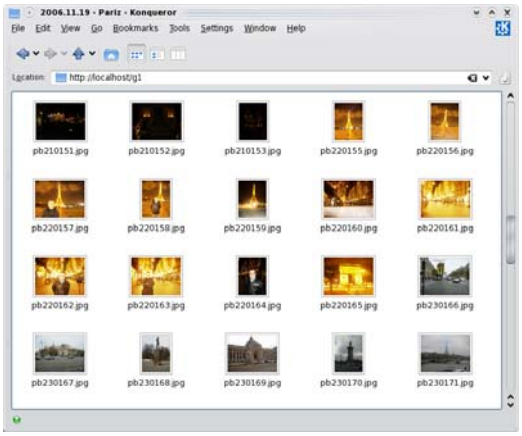
Sledeći kriterijum kod procene efikasnosti steganografskih rešenja jeste stepen izmene nosećeg dokumenta.

Sl. 4 – Skenirana fotografija nosilac

Kvalitetna steganografska rešenja moraju omogućiti takvo utiskivanje skrivenog sadržaja da se na osnovu krajnjeg rezultata (slike, video materijala i sl.) ne može javiti sumnja da je materijal izmenjen. Rešenje predstavljeno u ovom radu podrazumeva verovatnoću od 50% pomeraja vrednosti svakog kanala za vrednost od 0,390625% (1/256), odnosno tri nijanse po pikselu (3/16.777.216). Vizuelna reprezentacija rezultata je data na slikama 4. i 5. gde je slika 5. rezultat umetanja skrivenog sadržaja u sliku 4.

Sl. 5 – Izgled fotografije nakon kodiranja sadržaja

Nakon umetanja skrivenog sadržaja u slike nosioce, sledeći korak predstavlja kreiranje galerije slika i njeno objavljivanje na Internetu (slika 6.).



Sl. 6 – Izgled Web galerije u pretraživaču

VI. ZAKLJUČAK

U ovom radu je predstavljen model kriptografsko-steganografskog rešenja razvijenog u cilju omogućavanja zaštićene i skrivene komunikacije posredstvom Web galerije slika.

U kriptografskoj komponenti korišćen je sopstveni algoritam s tim da je moguće upotrebiti bilo koji javni (AES, 3DES i sl.). ili interno razvijeni algoritam. Struktura i kvalitet šifarskog algoritma nisu detaljnije razmatrani a više detalja o njima mogu se naći u ranijim radovima [1,2].

U radu nisu razmatrane mogućnosti poboljšanja efikasnosti rešenja kroz primenu algoritama za kompresiju podataka kao i upotrebu formata podataka koji podrazumevaju određene gubitke kvalitete.

LITERATURA

[1] Jevremović A., Veinović M., „IPsec - analiza uticaja algoritma za šifrovanje na saobraćaj u LAN mrežama“, 14. telekomunikacioni forum Telfor 2006., Beograd, 2006., CD izdanje;

[2] Veinović M., Jevremović A., Šimić G., „Analysis and implementation of custom cipher algorithm for IPsec under Linux OS“, International Journal of Computer Science and Network Security, Vol. 8 No. 7, July 2008;

[3] Katzenbeisser S., Petitcolas F., „Information hiding“, ISBN 1-58053-035-4;

ABSTRACT

This paper represents the solution model of the encrypted data secret transfer. The solution is based on the usage of custom cipher and steganographic algorithms. The Web galery pictures are used as default data holder. The solution includes *png* and *jpeg* picture formats without lusing of the picture's quality.

Usage of custom cipher and steganographic algorithms on the Web galery of pictures

Mladen Veinović, Aleksandar Jevremović, Goran Šimić