Razvoj alata za steganografiju

Nikola Fejsov, Miloš Krstić, Ivan Tubin

***Sadržaj* — Rad se bavi mogućnošću primene steganografije za prenošenje slika. U ovu svrhu, korišćen je steganografski program koji su autori sami napravili. Prikazani su rezultati obrade slike ovim programom i neki njegovi nedostaci.**

***Ključne reči* — Steganografija, Turbo Pascal.**

I. UVOD

ISTRAŽIVANJE obavljeno za ovaj rad počiva na potrebi da se razvije jednostavan alat za steganografsku obradu slike, za korisnike kojima nije neophodna velika kriptografska vrednost, ali im treba određeni nivo tajnosti prilikom komunikacije.

Steganografija je naučna disciplina koja se bavi prikrivenom razmenom informacija. Reč steganografija potiče od grčkih reči "steganos" i "graphein", što u bukvalnom prevodu znači "skriveno pisanje".

Osnovni princip steganografije zasniva se na korišćenju medija koji je dostupan široj populaciji, unutar koga se umeće informacija koju želimo da sakrijemo. Savremena steganografija, zasnovana na mogućnostima digitalne tehnologije, uglavnom je usmerena na skrivanje tajne poruke unutar sadržaja nekog multimedijalnog fajla, npr. slike, audio ili video fajlova. Multimedijalni fajlovi po pravilu sadrže neiskorišćene bite koji se na različite načine koriste kako bi se u njima prikrila skrivena poruka. Prednost ovakvog načina prikrivanja informacija se ogleda u tome da se razmena istih obavlja bez izazivanja sumnje da komunikacija uopšte postoji. Steganografija nudi širok spektar mogućnosti primene, od skrivene razmene informacija u privatne i poslovne svrhe, sve do zaštite autorskih prava u obliku vodenog pečata. Ipak, zbog svog suštinskog principa "nevidljivosti" informacija, često se koristi i prilikom ilegalnih aktivnosti. Steganografija podrazumeva prikrivanje tajne poruke, ali ne i činjenice da dve strane međusobno komuniciraju. Zbog toga proces steganografije obično uključuje umetanje skrivene informacije unutar nekog prenosnog medija. Takav medij se naziva nosilac i ima ulogu prikrivanja postojanja skrivene informacije. Skrivena poruka i nosilac zajedno čine jednu celinu koja se naziva stego ili steganografski medij. Radi veće kriptografske vrednosti, skrivena informacija se pre umetanja u nosilac može kriptovati.

Nikola Fejsov, Vojna akademija u Beogradu, Srbija (telefon: 381-64-6728669; e-mail: fejsov@sbb.rs).

Miloš Krstić, Vojna akademija u Beogradu, Srbija; (telefon: 381-64-3061626; e-mail: miloskrstic30130@gmail.com).

Ivan Tubin, Vojna akademija u Beogradu, Srbija; (telefon: 381-65-6473197e-mail: waves_styler@yahoo.com).

II. RAZVOJ STEGANOGRAFIJE

Početak primene steganografije nalazimo još u starom veku, u grčkoj i rimskoj civilizaciji. Koristile su se razne tehnike, od upisivanja tajne poruke na drvenu podlogu ispod voska, preko tetoviranja na obrijanoj glavi glasnika pa sve do upotrebe raznih vrsta nevidljivog mastila. Razvojem tehnologije javljale su se nove metode steganografije, kao što su mikrofilm i nulta šifra.

Ulaskom u informatičko doba, razvojem digitalne tehnologije i porastom količine podataka koji se nalaze na računarima i internetu, steganografija takođe ulazi u novo doba. Razvijaju se steganografski alati koji omogućavaju skrivanje doslovce bilo koje forme tajne poruke unutar nekog multimedijalnog nosioca. Ipak, najčešći nosioci tajnih poruka su slike i zvučni zapisi.

Kao i razne druge sigurnosne metode i alati, steganografija se može koristiti u različite svrhe, kako legalne tako i ilegalne. U legalnu primenu uglavnom spada korišćenje steganografije za umetanje vodenih pečata sa ciljem zaštite autorskih prava nad multimedijalnim sadržajem. Ipak, steganografija se primarno koristi za zaštitu tajnosti važnih informacija, njihovu zaštitu od potencijalne sabotaže, neovlašćenog pristupa ili krađe. Ilegalna upotreba steganografije uglavnom se vezuje za krađu poverljivih podataka, za industrijsku špijunažu, razmenu pornografskog sadržaja, krađu identiteta, terorizam…

III. TEHNIKE STEGANOGRAFIJE

Steganografija se deli na tehničku i lingvističku steganografiju.

Tehnička stenografija koristi naučne metode za skrivanje poruka, kao što su upotreba nevidljivog mastila, mikrofilmova i slično.

Lingvistička steganografija obuhvata tehnike koje skrivaju tajnu poruku na način da nosilac naizgled predstavlja bezazlen podatak. Lingvistička steganografija deli se na semagrame i otvorene kodove.

Semagrami se služe različitim simbolima i znakovima za skrivanje tajnih poruka. Postoje vizuelni i tekstualni semagrami.

Vizuelni semagrami zasnivaju se na principu upotrebe svakodnevnih predmeta i objekata pri skrivanju poruka, koristeći njihov položaj u prostoru za generisanje tajne poruke.

Tekstualni semagrami koriste razne modifikacije teksta nosioca za prikrivanje informacija, kao što su dodavanje suvišnih razmaka, promena veličine ili boje fonta i slično.

Otvoreni kodovi koriste razne tipove prenosa tajne poruke koja se nalazi skrivena u nosilac koji predstavlja

sredstvo neskrivene, tj. otvorene komunikacije. Otvoreni kodovi se dele na žargonski kod i skrivene šifre.

Žargonski kod se zasniva na upotrebi žargona, tj. jezika koji razume samo određeni broj ljudi. Žargonski kod koristi predefinisane fraze koji onome kome su upućeni predstavljaju tačno određene pojmove.

Skrivene šifre predstavljaju steganografsku tehniku kod koje se tajna poruka može izdvojiti iz nosioca samo ako je poznata tehnika koja je korišćena za njeno umetanje. Skrivene šifre se dele na rešetkaste šifre i nulte kodove.

Rešetkaste šifre temelje se na predlošcima koji se koriste za prikrivanje poruke nosioca.

Nulta šifra koristi se za skrivanje informacija tako da se usvoji neko pravilo za umetanje unutar nosioca, npr. izdvaja se svaki treći znak, ili svaka druga reč u parnom redu.

IV. STEGANOGRAFSKE TEHNIKE BAZIRANE NA SUPSTITUCIJI

Osnovni princip tehnika baziranih na supstituciji jeste zamena redundantnih delova slike s tajnim podacima. Kako je za razumevanje ovog principa bitno poznavanje strukture steganografskog nosioca, sledi kratak opis RGB (eng. Red-Green-Blue) sistema.

Unutar RGB sistema, svaka boja se prikazuje pomoću relativnog intenziteta svake od 3 postojeće komponente – crvene, zelene i plave. Nedostatak svih komponenti rezultira pojavom crne, dok prisustvo svih komponenti daje belu boju. Svaka RGB komponenta određena je jednim oktetom, tj. nizom od 8 bita, tako da vrednost intenziteta svake od tri boje može varirati od 0 do 255. Pošto RGB sistem sadrži 3 komponente, doticnom metodom prezentacije, dobija se 24-bitna shema koja podržava 16.777.216 jedinstvenih boja. To znači da je svaki piksel unutar slike kodiran s 24 bita.

Supstitucija bita najmanje vrednosti (eng. least significant bit; LSB) najčešca je steganografska tehnika korištena u radu s multimedijalnim fajlovima. Pojam “bit najmanje vrednosti” vezan je uz numeričku vrednost bita u oktetu. Bit najveće vrednosti je onaj s najvećom aritmetičkom vrednošću, a bit najmanje vrednosti onaj s najmanjom aritmetičkom vrednošću. Zato promena bita najmanje vrednosti ima najmanji učinak na promenu ukupne vrednosti okteta, a promena bita najmanje vrednosti u svim oktetima koji čine multimedijalni fajl ima najmanji učinak na promenu izgleda samog fajla. Opisani princip još je efikasniji zbog činjenice da ljudsko oko nije dovoljno osetljivo za primećivanje takvih promjena u boji.

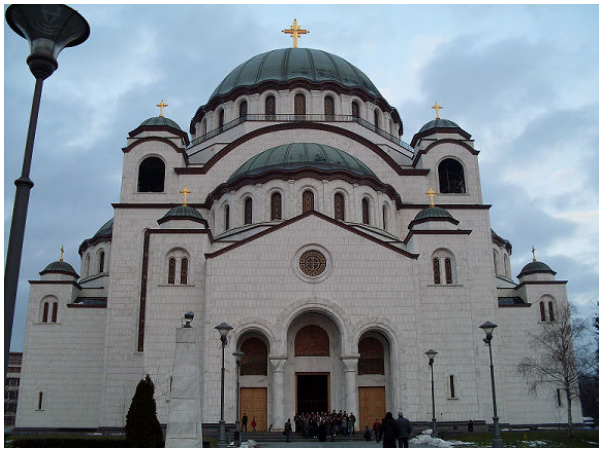
Ideja steganografske tehnike supstitucije bita najmanje vrednosti bazira se na rastavljanju tajne poruke na bitove koji se potom smeštaju na mesto bita najmanje vrednosti u odabranim oktetima.

V. 4-BITNA LSB SUPSTITUCIJA

Autori su za potrebe ovog rada razvili steganografski alat koji sakriva jednu sliku, koja predstavlja tajnu poruku, u drugu sliku, nosilac, upotrebom 4-bitne LSB supstitucije. Osnovna zamisao jeste da se 4 bita više vrednosti, odnosno biti 5-8, iz oktava slike koja predstavlja tajnu poruku, smeste na mesta bita niže vrednosti, odnosno bite 1-4, u oktavama slike koja predstavlja nosilac. Budući da se grupa od 4 bita menja sa grupom od 4 bita, moguće je učešljati tajnu poruku koja je istih dimenzija kao slika-nosilac, bez drastičnog gubitka kvaliteta slike-nosioca.

Za izradu programa, korišćen je programski jezik Turbo Pascal 7.0. Iako je ovaj programski jezik prevaziđen, za potrebe bazične steganografske obrade slike je izuzetno pogodan zbog svoje jednostavnosti.

Na sl. 1. prikazana je slika-nosilac, pre umetanja tajne poruke.

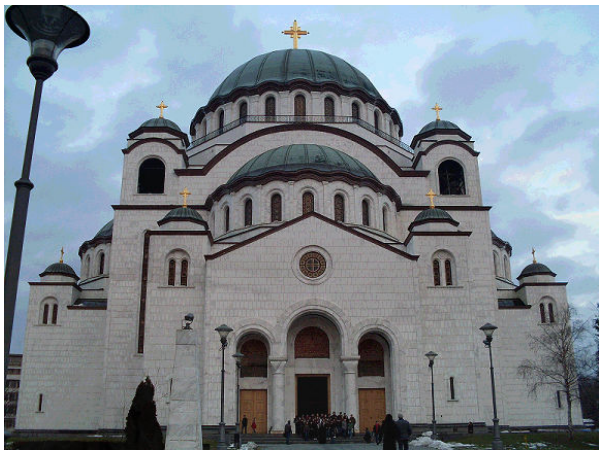


Sl. 1. Slika-nosilac

Na sl. 2. prikazana je tajna poruka, koju smo upotrebom steganografskog alata utisnuli u sliku-nosilac.

Sl. 2. Tajna poruka

Posle pokretanja programa, tajna slika je opisanom metodom supstitucije utisnuta u sliku-nosilac, i dobijen je stego, koji je neznatno izmenjen u odnosu na početnu sliku-nosilac. Stego je prikazan na sl.3.



Sl. 3. Stego

Stenografski medij, koji je prikazan na sl. 3., od originalne slike nosioca se razlikuje u nijansama koje ljudsko oko teško može da detektuje. Ovo je posebno izraženo ako posmatrač nema originalnu sliku sa kojom bi uporedio stego, što je uglavnom slučaj.

Na sl. 4. nalazi se tajna poruka posle izdvajanja iz steganografskog medija.

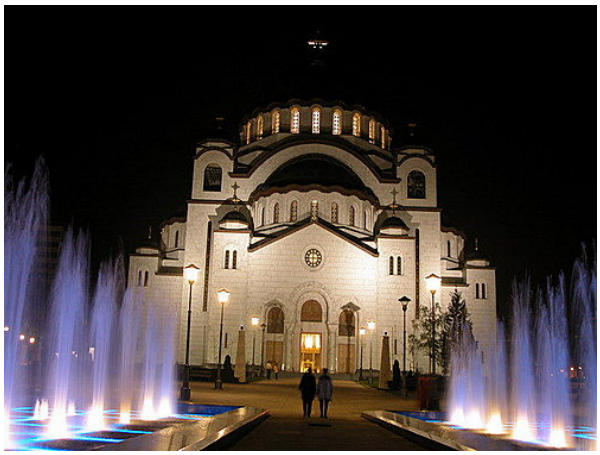
Sl. 4. Tajna poruka izdvojena iz stega

Primećuje se da je tajna poruka pretrpela određenu degradaciju kvaliteta, iako se sadržaj poruke i dalje može „pročitati“ sa zadovoljavajućom tačnošću.

VI. Problemi metode supstitucije

Prilikom testiranja programa, došlo se do određenih zaključaka vezanih za kvalitet steganografskog medija. Kada je korišćena tajna poruka na kojoj preovladava crna, odnosno tamne boje, stego je bio različitog kvaliteta. U zavisnosti od izbora slike-nosioca, kvalitet stega je varirao od vrlo dobrog do ozbiljno degradiranog, i prisustvo tajne poruke postajalo je vidljivo u nekim slučajevima. Na sl. 5. prikazana je loše odabrana slika-nosilac, a na sl. 6. tajna poruka na kojoj preovladavaju tamnije boje.

Sl. 5. Loše odabrana slika-nosilac



Sl. 6. Tajna poruka u tamnim bojama

Kao što se vidi na sl. 7., stego je pretrpeo ozbiljne degradacije. Tajna poruka nije vidljiva u potpunosti, ali se uočava njeno prisustvo, što predstavlja ozbiljan problem, budući da je osnovna zamisao da komunikacija bude neprimetna.

Sl. 7. Stego

Metodom pokušaja i pogrešaka, izabrana je slika-nosilac

koja ne ugrožava tajnost komunikacije kao prethodna. Ona je prikazana na sl. 8., a na sl. 9. je prikazan stego koji se dobije korišćenjem ove slike-nosioca.

Sl. 8. Podobno izabrana slika-nosilac

Sl. 9. Stego podobno izabrane slike-nosioca

Vidimo, sa sl. 9., da se pogodnim odabirom slike-nosioca, može dobiti zadovoljavajući kvalitet stega. Problem kvaliteta stega se može poprilično jednostavno rešiti, kao što se vidi, uz uslov da imamo na raspolaganju dovoljan broj slika koje bi mogle da posluže kao nosioci.

VII. ZAKLJUČAK

Ovaj rad predstavlja ulazak u područje stenografije i obrađuje problem steganografske obrade slika u BMP formatu. Budući da JPEG slike koriste diskretnu kosinusnu transformaciju kao metod prikaza piksela, nad slikama ovog formata nije moguće na jednostavan način izvršiti obradu. U daljem razvoju primenjenog programa pažnju bi svakako trebalo posvetiti implementaciji modula za rad sa JPEG formatom slika, kao i uvođenje video fajlova kao nosilaca tajnih poruka.

LITERATURA

[1] An Overview of Steganography for the Computer Forensics Examiner, Gary C. Kessler, http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm

[2] Steganography Revealed, Kristy Westphal, http://www.securityfocus.com/infocus/

[3] Wikipedia, http://en.wikipedia.org/wiki/Steganography

[4] Steganography, Neil F. Johnson, George Mason University, http://www.jjtc.com/stegdoc

ABSTRACT

Possibilities of using steganography for image transfering is subject of this work. For this purpose, steganography tool was developed by authors. Results of image processing are shown, together with several disadvantages.

DEVELOPING TOOLS FOR STEGANOGRAPHY

Nikola Fejsov, Miloš Krstić, Ivan Tubin