Univerzitet u Nišu, Elaktronski fakultet

Katedra za računarstvo

**Video steganografija**

Student : Saška Radenković 1132

Profesor : Prof. dr Bratislav Predić

Sadržaj

[Uvod 3](#_Toc63615867)

[Steganografija 4](#_Toc63615868)

[Uvod u steganografiju 4](#_Toc63615869)

[Istorija steganografije 5](#_Toc63615870)

[Vrste steganografije 5](#_Toc63615871)

[Steganografija medija 6](#_Toc63615872)

[Kodiranje tajnih poruka u tekstu 6](#_Toc63615873)

[Kodiranje tajnih poruka na slikama 6](#_Toc63615874)

[Kodiranje tajnih poruka u audio 8](#_Toc63615875)

[Upotreba steganografije 9](#_Toc63615876)

[Primena i rezultati 10](#_Toc63615877)

[Video steganongrafija 11](#_Toc63615878)

[Osnovni model 12](#_Toc63615879)

[Tehnika najmanje značajnog bita (LSB) 13](#_Toc63615880)

[Masking and Filter method 15](#_Toc63615881)

[Talasna transformacija 17](#_Toc63615882)

[Redundant Pattern Encoding 18](#_Toc63615883)

[Encrypt and Scatter 18](#_Toc63615884)

[Neparna/Parna (ODD/EVEN) distribucija piksela 19](#_Toc63615885)

[GLM metod 22](#_Toc63615886)

[Rezultat implementacije metode parna/neparna distribucija piksela 25](#_Toc63615887)

[Zaključak 26](#_Toc63615888)

[Reference 27](#_Toc63615889)

# Uvod

Steganografija je tehnika skrivanja tajnih podataka u običnoj, ne-tajnoj datoteci ili poruci kako bi se izbeglo otkrivanje , tajni podaci se zatim izvlače na odredište. Upotreba steganografije može se kombinovati sa šifrovanjem kao dodatni korak za skrivanje ili zaštitu podataka. Reč steganografija izvedena je iz grčkih reči steganos (što znači skriven ili pokriven) i grčkog korena grafa (što znači pisati). Steganografija se može koristiti za prikrivanje gotovo bilo koje vrste digitalnog sadržaja, uključujući tekst, sliku, video ili audio sadržaj. Podaci koje treba sakriti mogu se sakriti u gotovo bilo kojoj drugoj vrsti digitalnog sadržaja. Sadržaj koji se steganografijom skriva - zvan skriveni tekst - često se šifrira pre nego što se uključi u bezazlenu naizgled naslovnu tekstualnu datoteku ili tok podataka. Ako nije šifrovan, skriveni tekst se obično obrađuje na neki način kako bi se povećala poteškoća u otkrivanju tajnog sadržaja.

Steganografijom se bave oni koji žele da prenesu tajnu poruku ili kod. Iako postoji mnogo legitimnih upotreba steganografije, pronađeno je i da programeri zlonamernog softvera koriste steganografiju da zaklone prenos zlonamernog koda.

U savremenoj digitalnoj steganografiji podaci se prvo šifruju ili zamućuju na neki drugi način, a zatim se pomoću posebnog algoritma ubacuju u podatke koji su deo određenog formata datoteke kao što je JPEG slika, audio ili video datoteka. Tajna poruka se može ugraditi u obične datoteke podataka na mnogo različitih načina. Jedna od tehnika je sakrivanje podataka u bitovima koji predstavljaju iste piksele u boji koji se ponavljaju redom u datoteci slike. Primenom šifrovanih podataka na ove suvišne podatke na neki neupadljiv način, rezultat će biti slikovna datoteka koja izgleda identično originalnoj slici, ali koja ima obrasce „šuma“ regularnih, nešifrovanih podataka.

Softver za steganografiju koristi se za izvršavanje različitih funkcija u cilju sakrivanja podataka, uključujući kodiranje podataka kako bi se pripremio za skrivanje u drugoj datoteci vodeći računa o tome koji bitovi naslovne tekstualne datoteke sadrže skrivene podatke, šifrujući podatke u bitovima i izvlačenje skrivenih podataka od strane predviđenog primaoca.

U poglavljima koja slede u nastavku rada biće prikazana istorija I razvoj steganografije , tipovi steganografije. Detalno je obrađena video steganografija i predstavljane su metode za skirvanje/mapiranje podataka unutar video snimaka i slika.

# Steganografija

. Steganografija se može posmatrati kao sličan proces kriptografiji. Obe tehnike su korišćene kroz istoriju kao sredstvo za zaštitu informacija. Izgleda kao da ove dve tehnologije konvergiraju dok se ciljevi te dve tehnologije razlikuju. Kriptografske tehnike "*skroluje*" poruke tako da ako se presretnu, poruke se ne mogu razumeti. Steganografija, u suštini, "*kamuflira*" poruku da sakrije svoje postojanje i učini da izgleda "*nevidljivo*" prikriva tako činjenicu da se poruka šalje u potpunosti. Šifrovana poruka može da privuče sumnju dok nevidljiva poruka neće. Pored skrivanja podataka radi poverljivosti, ovaj pristup skrivanja informacija može se proširiti i na zaštitu autorskih prava za digitalne medije kao što su audio, video zapisi i slike.

## Uvod u steganografiju

Steganografija (Stego kako se često naziva u IT zajednici) bukvalno znači, "*skriveno pisanje*" koje potiče iz grčkog jezika. Steganografiju definiše Markus Kan na sledeći način: "**Steganografija je umetnost i nauka komunikacije na način koji krije postojanje komunikacije. Za razliku od Kriptografije, gde je neprijatelju dozvoljeno da otkriva, presreće i menja poruke bez mogućnosti da naruši određene bezbednosne prostorije garantovane kriptosistemom, cilj Steganografije je da sakrije poruke unutar drugih bezazlenih poruka na način koji ne dozvoljava nijednom neprijatelju da uopšte otkrije da je prisutna druga poruka**". U digitalnom svetu, Steganografija i Kriptografija su namenjene zaštiti informacija od neželjenih strana. Obe tehnike su odlična sredstva kojim se ovo postiže ali nijedna tehnologija sama nije savršena i obe mogu biti slomljene. Preporuka je korišćenje obe tehnike kako bi se prevazišli nedostaci, a bezbednost podigla na veći nivo. Steganografske tehnologije su veoma važan deo budućnosti internet bezbednosti i privatnosti na otvorenim sistemima kao što je Internet. Steganografska istraživanja su pre svega vođena nedostatkom snage u kriptografskim sistemima na svoju ruku i željom da imaju potpunu tajnost u okruženju otvorenih sistema. Steganografija se može koristiti za skrivanje važnih podataka unutar drugog fajla tako da samo strane koje razmenjuju poruku znaju da postoji tajna poruka. Pomoću steganografije informacije se mogu sakriti u podacima kao što su slike, audio datoteke, tekstualne datoteke, video zapisi i prenos podataka.

## Istorija steganografije

Steganografija je prisutna u mnogim oblicima još od vremena grčkog carstva. Reč **steganografija** potiče od grčkih steganosa, skrivenih ili pokrivenih, dok **grafein** služi za pisanje. Zanimlljivost : *Herodotus, grčki istoričar snimio je priču o robu koji se koristi kao medijum za prenos skrivene poruke.Glava roba je bila obrijana i poruka istetovirana na goloj lobanji nakon čega je kosi dozvoljeno da ponovo izraste.Rob je poslat primaocu poruke koji je obrijao glavu roba da bi otkrio poruku.*

Lord Robert Baden-Pauel, kao izviđač Za Britance tokom Boer rata obeležio je položaje artiljerijskih baza Boer ugrađujući mape u crteže leptira. Izgledajući nevino za neobaveznog posmatrača, određene oznake na krilima su zapravo bile položaji neprijateljskih vojnih posada. Osa i saveznički špijuni koristili su nevidljiva mastila koja sadrže voćni sok ili urin za prenos poruka koje bi se otkrile kada se zagreju ili kada su u prisustvu ultraljubičastog svetla.

Sredinom devedesetih brojne starije tehnike skrivanja poruka unutar drugih poruka, pa čak i slika, postale su popularnije kod pojave modernog softvera i moćnih računara. Bez obzira na tehniku koja se koristi, ključna sličnost u svim slučajevima bila je da su poruke bile sakrivene u običnom prikazu.

## Vrste steganografije

U osnovi se koriste 3 vrste steganografskih protokola:

1. Čista steganografija - Pure Steganography
2. Stgeanografija tajnog ključa – Secret Key Steganography
3. Steganografija javnog ključa – Public Key Steganography

Čista steganografija je definisana kao steganografski sistem koji ne zahteva razmenu šifre kao što je stego-ključ. Ova metoda steganografije je najmanje sigurno sredstvo za tajnu komunikaciju jer se pošiljalac i primalac mogu osloniti samo na pretpostavku da nijedna druga strana nije upoznata sa ovom tajnom porukom.

Tajni ključ Steganografija je definisana kao steganografski sistem koji zahteva razmenu tajnog ključa (stego-ključ) pre komunikacije. Tajni ključ steganografije uzima naslovnu poruku i ugrađuje tajnu poruku unutar nje pomoću tajnog ključa (stego-ključ). Samo stranke koje znaju tajni ključ mogu da preokrenu obraditi i pročitati tajnu poruku. Secret Key Steganografija razmenjuje stego-ključ, što ga čini podložnijim presretanju. Prednost kod steganografije tajnog ključa je čak i ako je presretnuta samo strane koje znaju tajni ključ mogu izvući tajnu poruku.

Steganografija javnog ključa uzima koncepte iz kriptografije javnog ključa. Steganografija javnog ključa je definisana kao steganografski sistem koji koristi javni ključ i privatni ključ za obezbeđivanje komunikacije između strana koje žele tajno da komuniciraju. Pošiljalac će koristiti javni ključ tokom procesa kodiranja i samo privatni ključ, koji ima direktan matematički odnos sa javnim ključem, može da dešifruje tajnu poruku. Steganografija javnog ključa pruža robustniji način implementacije steganografskog sistema jer može da koristi mnogo robusniju i istraženu tehnologiju u kriptografiji javnog ključa. Ima više nivoa bezbednosti u tome što neželjene strane prvo moraju da posumnjaju u upotrebu Steganografije, a zatim bi mogle da pronađu način da razbiju algoritam koji koristi sistem javnih ključeva pre nego što presretnu tajnu poruku.

## Steganografija medija

Osnovni oblici steganografije su:

1. Kodiranje tajnih poruka u tekstu
2. Kodiranje tajne poruke u slikama – video snimcima
3. Kodiranje tajne poruke u audio snimku

### Kodiranje tajnih poruka u tekstu

Kodiranje tajnih poruka u tekst može biti vrlo izazovan zadatak. To je zato što tekstualne datoteke imaju vrlo mala količina suvišnih podataka koje treba zameniti tajnom porukom.. Postoje brojne metode pomoću kojih se postiže tekst zasnovan na Steganografiji. Kodiranje sa linijskim pomakom podrazumeva zapravo pomeranje svakog reda teksta vertikalno gore ili dole za samo 3 centimetara. U zavisnosti od toga da li je linija nagore ili nadole sa nepokretne linije, izjednačila bi se sa vrednošću koja bi se ili mogla kodirati u tajnu poruku. Kodiranje sa pomeranjem reči funkcioniše na sličan način na koji funkcioniše kodiranje sa pomeranjem redova, samo što se koriste horizontalni razmaci između reči kako bi se izjednačila vrednost za skrivenu poruku. Ovaj metod kodiranja je manje vidljiv od kodiranja sa pomeranjem linije, ali zahteva da format teksta podržava promenljivi razmak. Kodiranje specifično za funkciju uključuje kodiranje tajnih poruka u formatirani tekst promenom određenog teksta poput vertikalne / horizontalne dužine slova kao što su b, d, T itd. Ovo je ubedljivo najteže kodiranje teksta, jer svaka vrsta formatiranog teksta ima veliku količinu karakteristika koje se mogu koristiti za kodiranje tajna poruka.

### Kodiranje tajnih poruka na slikama

Kodiranje tajnih poruka na digitalnim slikama je ubedljivo najšire korišćeno od svih metoda u digitalnom svetu današnjice. To je zato što može da iskoristi ograničenu snagu ljudskog vizuelnog sistema (HVS). Skoro svaki čisti tekst, šifrovani tekst, slika i bilo koji drugi medij koji se može kodovati u protok može biti sakriven u digitalnoj slici. Dve popularnije tehnike digitalnog kodiranja slika koje se danas koriste su najmanje značajne bit (LSB) tehnike kodiranja i maskiranja i filtriranja.

Najmanje značajno kodiranje bitova (LSB) je ubedljivo najpopularnije od tehnika kodiranja koje se koriste za digitalne slike. Pomoću LSB-a svakog bajta (8 bitova) na slici za tajnu poruku možete da uskladištite 3 bita podataka u svakom pikselu za 24-bitne slike i 1 bit u svakom pikselu za 8-bitne slike. Mnogo više informacija može da se uskladišti u 24-bitnu datoteku slike. U zavisnosti od palete boja koja se koristi za naslovnu sliku (ili, sve sivo), moguće je uzeti 2 LSB-a iz jednog bajta bez mogućnoti da ljudski vizuelni sistem (HSV) bude u stanju da uočite razliku.

*Na primer, sledeća koordinatna mreža se može predstaviti preko 3 piksela 24-bitne slike, koristeći 9 bajta memorije:*

**(00100111 11101001 11001000)**

**(00100111 11001000 11101001)**

**(110010000 00100111 11101001)**

*Kada se skriva karakter A, koji ima binarnu vrednost 10000001, umeće se sledeći rezultati :*

**(00100111 11101000 11001000)**

**(00100110 11001000 11101000)**

**(11001000 00100111 11101001)**

Potrebno je promeniti samo tri bita da bi se znak uspešno umetnuo.U proseku samo polovina bitova na slici će morati da se izmeni da bi se sakrila tajna poruka koristeći maksimalnu veličinu korice. Dobijene promene koje su napravljene u najmanje značajnim bitovima su premale da bi ih ljudsko oko prepoznalo, tako da je poruka efikasno sakrivena. Dok korišćenje 24-bitne slike daje relativno veliku količinu prostora za skrivanje poruka, takođe je moguće koristiti 8-bitnu sliku kao izvor naslovne strane. Zbog manjeg prostora i različitih svojstava, 8 bitnih slika zahteva pažljiviji pristup. 24-bitne slike koriste 3 bajta za predstavljanje piksela, 8 bita koristi samo jedan. Promena LSB tog bajta rezultiraće vidljivom promenom boje, jer će biti prikazana druga boja u dostupnoj paleti. Zato je potrebno pažljivije i poželjnije izabrati naslovnu sliku u sivim tonovima, jer ljudsko oko neće detektovati razliku između različitih sivih vrednosti tako lakih kao kod različitih boja. Jedini problem sa ovom tehnikom je što je veoma podložna napadima kao što su promene slike i oblikovanje (ili, menjanje iz . GIF za . JPEG). Tehnike maskiranja i filtriranja za kodiranje digitalnih slika kao što je Digitalno vodeno žigosanje (.- integrisanje logotipa preduzeća na tu veb sadržaj) je popularnije kod tehnika gubitašne kompresije kao što je (. JPEG).Ova tehnika zapravo proširuje podatke o slici maskiranjem tajnih podataka preko originalnih podataka za razliku od skrivanja informacija unutar podataka. Lepota tehnika maskiranja i filtriranja je u tome što su imune na manipulaciju slikom .

### Kodiranje tajnih poruka u audio

Kodiranju tajnih poruka u audio zapisu je najizazovnija tehnika koju treba koristiti kada se koristi Steganografija. Ljudski auditivni sistem (HAS) ima tako dinamičan opseg da može da sluša preko. Tri popularnija metoda kodiranja za skrivanje podataka unutar audio zapisa su:

1. Nisko-bitno kodiranje - Low-bit encoding
2. Fazno kodiranje - Phase-coding
3. Širenje spektra - Spread spectrum

Nisko-bitno kodiranje ugrađuje tajne podatke u najmanje značajan bit (LSB) audio datoteke. Kapacitet kanala je 1KB u sekundi po kilohercu (44 kb/s za uzorak sekvence od 44 KHz). Ovaj metod je jednostavan za uključivanje ali je veoma podložan gubitku podataka zbog buke kanala i ponovne procene. Fazno kodiranje zamenjuje fazu početnog audio segmenta referentnom fazom koja predstavlja skrivene podatke. O ovome se može razmišljati, kao o nekoj vrsti šifrovanja za audio signal pomoću onoga što je poznato kao Discrete Fourier Transform (DFT), što nije ništa drugo do algoritam transformacije za audio signal. Rašireni spektar kodira zvuk preko skoro celog frekventnog spectra .Zatim prenosi zvuk preko različitih frekvencija koje će se razlikovati u zavisnosti od toga koji se metod širenja spektra koristi. Direct Sequence Spread Spectrum (DSSS) je jedan takav metod koji širi signal množenjem izvornog signala nekim pseudo slučajnim nizom poznatim kao (CHIP). Brzina uzorka se zatim koristi kao brzina čipa za komunikaciju audio signala.

Tabela 1 prikazuje tipove steganografije:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Sr.  No. | **Steganography Techniques** | **Cover Media** | **Embedding**  **Technique** | **Advantages** |
| 1. | Binary File Technique | Binary file | watermark can be  embedded by making changes to  the binary code  that does not affect  the execution of the file | Simple to  implement |
| 2. | Text Technique | Document | To embed  information inside  a document we can  simply alter some  of its characteristics.i.e.  either the text formatting or characteristics of the characters | Alterations not  visible to the  human eye |
| 3. | Image Hiding:   1. LSB | Image | It works by using  the least significant bits of each pixel in one image to hide the  most significant  bits of another. | Simple & easiest  way of hiding  information. |
|  | 1. DCT |  | Embeds the information by altering the  transformed DCT  coefficients. | Hidden data can  be distributed  more evenly  over the whole  image in such a  way as to make  it more robust. |
|  | 1. Wavelet Transform |  | This technique works by taking many wavelets to  encode a whole image | Coefficients of  the wavelets are  altered with the  noise within  tolerable levels |
| 4. | Sound Technique | MP3 file | Encode data as a  binary sequence  which sounds like  noise but which  can be recognised  by a receiver with  the correct key | Used for  watermarking by  matching the  narrow  bandwidth of the  embedded data  to the large  bandwidth of the  medium |
| 5. | Video Technique | Video file | A combination of  sound and image  techniques can be  used | The scope for  adding lots of  data is much  greater |

## Upotreba steganografije

1. Steganografija može biti rešenje koje omogućava slanje vesti i informacija bez cenzure i bez straha od presretanja i vraćanja poruka do pošiljaoca.

2. Moguće je jednostavno koristiti steganografiju za skladištenje podataka na lokaciji. Na primer, nekoliko izvora informacija poput naših podataka o privatnom bankarstvu, neke vojne tajne, može se čuvati u izvoru izvora. Kada se od nas zatraži da otkrijemo tajne podatke u našem izvoru pokrića, lako možemo otkriti svoje bankarske podatke i biće nemoguće dokazati postojanje vojne tajne u njemu.

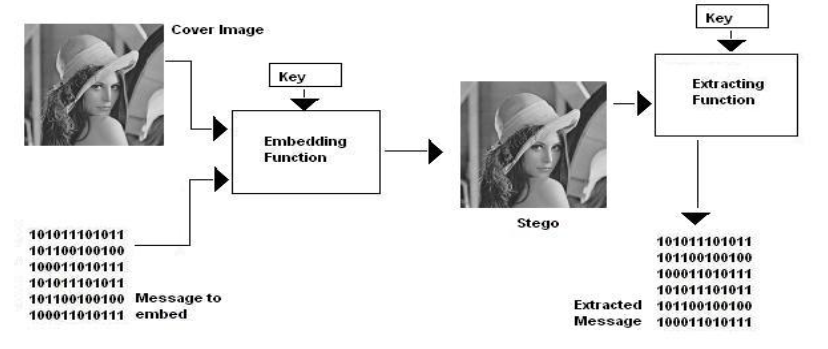
3. Steganografija se takođe može koristiti za primenu vodenih žigova. Iako koncept vodenog žiga nije nužno steganografija, postoji nekoliko steganografskih tehnika koje se koriste za čuvanje vodenih žigova u podacima. Glavna razlika je u nameri, dok svrha steganografije skriva informacije, vodeni žig samo proširuje izvorni izvor dodatnim informacijama. Budući da ljudi neće prihvatiti primetne promene na slikama, audio ili video datotekama zbog vodenog žiga, mogu se koristiti steganografske metode da se to sakrije.

4. Elektronska trgovina omogućava zanimljivu upotrebu steganografije. U trenutnim transakcijama e-trgovine, većina korisnika zaštićena je korisničkim imenom i lozinkom, bez stvarnog načina da se utvrdi da li je korisnik stvarni vlasnik kartice. Biometrijsko skeniranje otiska prsta, u kombinaciji sa jedinstvenim ID-ovima sesija ugrađenim u slike otiska prsta putem steganografije, omogućavaju vrlo sigurnu opciju za otvaranje verifikacije transakcija e-trgovine. 5. Uparen sa postojećim komunikacionim metodama, steganografija se može koristiti za obavljanje skrivenih razmena. Vlade su zainteresovane za dve vrste skrivenih komunikacija: one koje podržavaju nacionalnu bezbednost i one koje to ne čine. Digitalna steganografija pruža ogroman potencijal za obe vrste. Preduzeća mogu imati slične probleme u vezi sa poslovnom tajnom ili informacijama o novim proizvodima.

6. Prenos osetljivih podataka je još jedna ključna upotreba steganografije. Potencijalni problem kriptografije je taj što prisluškivači znaju da imaju šifrovanu poruku kada je vide. Steganografija omogućava prenos osetljivih podataka pored prisluškivača, a da oni ne znaju da su ih prošli osetljivi podaci. Ideja upotrebe steganografije u transportu podataka može se primeniti na skoro svaki način prenosa podataka, od e-pošte do slika na Internet veb lokacijama.

## Primena i rezultati

Svi pristupi steganografiji imaju jedno zajedničko da tajnu poruku kriju u fizičkom objektu koji se šalje. Sledeća slika prikazuje postupak steganografije, slika se prenosi u funkciju za ugrađivanje sa porukom na kodiranje rezultira steganografskom slikom koja sadrži skriveno poruku. Ključ se često koristi za zaštitu skrivene poruke. Ovaj ključ je obično lozinka, pa se ovaj ključ koristi i za šifrovanje i dešifrovanje poruka pre i posle ugradnje. Tajne se mogu sakriti u svim vrstama naslovnih informacija: tekst, slike, audio, video i još mnogo toga. Međutim, postoje alati na raspolaganju čuvajte tajne u gotovo bilo kojoj vrsti pokrivača. Najviše važno svojstvo pokrivnog izvora je količina podataka koja može biti uskladišten u njemu, bez promene uočljivih svojstava poklopac.



*Slika 1 : Proces skrivanja teksta*

# Video steganongrafija

Tehnike steganografije zasnovane na slikama i video snimcima su uglavnom klasifikovane u prostorni domen i frekventni domen. Dva važna parametra za procenu performanse ovog sistema su kapacitet i neprimetnost. Kapacitet se odnosi na količinu podataka koja može biti sakriveni u medijumu za pokrivanje tako da nema bitnih izobličenja. Neprimetnost ili transparentnost predstavljaju nevidljivost skrivenih podataka u naslovnom mediju bez pogoršavanja perceptivnih kvaliteta ugrađivanjem podataka. Steganografija u video zapisu može se podeliti na dva glavne klase. Jedna je ugrađivanje podataka u nekompresovanu sirovu sliku/ video, koji se kasnije kompresuje. Druga pokušava da ugradi podatke direktno u

kompresovani video tok. Problem prvog je kako učiniti da se ugrađena poruka odupre video kompresiji. Postoji mnogo metoda vezanih za šifrovanje slike gde je poruka tajno sakrivena unutar slike. Uobičajeni pristupi uključuju :

1. **Least significant bit insertion (LSB)**
2. **Masking and filtering**
3. **Redundant Pattern Encoding**
4. **Encrypt and Scatter**
5. **Odd/Even method**

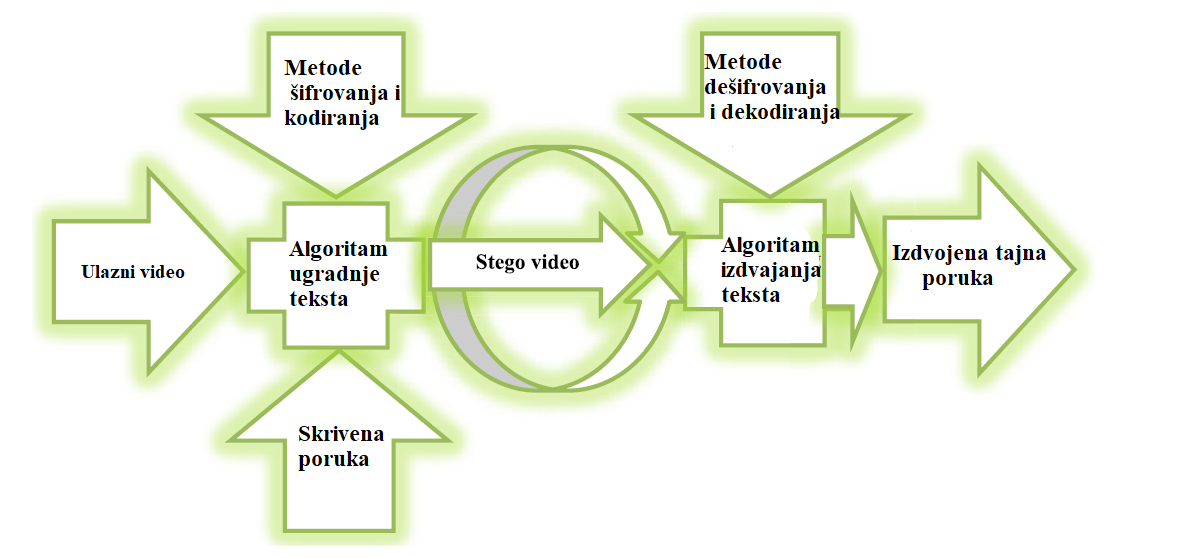
Postoje razne tehnike ugrađivanja koje nam omogućavaju da sakrijemo tajnu poruku u datom objektu. Tehnike steganografije moraju da zadovolje sledeće zahteve:

* **Tajnost**: Izdvajanje skrivenih podataka sa medijuma domaćina ne bi trebalo da bude moguće bez znanja odgovarajućeg tajni ključ koji se koristi u postupku izvlačenja.
* **Neprimetnost**: Nakon ugradnje podataka u medijum, ono treba da bude neprimetan sa originalnog medija.
* **Veliki kapacitet:** Maksimalna dužina skrivene poruke koje se mogu ugraditi mogu biti što duže.
* **Otpor**: skriveni podaci bi trebali moći da prežive kada medijumom domaćina je manipulisano, na primer sa gubitkom šema kompresije.
* **Tačno izdvajanje**: izdvajanje skrivenih podataka iz medijum treba da bude tačan i pouzdan.

Digitalni video sadrži skup okvira (slika) koji se reprodukuju sa fiksnom brzinom kadrova na osnovu video standarda. Kvalitet digitalnog video zapisa zavisi od kombinacije parametara poput fps (broj frejmova u sekundi), broja piksela u kadru i veličine kadra. Standard parametra fps su vrlo uobičajeni video formati, čija je vrednost između 24 i 30 fps. Svaka slika u video zapisu naziva se frejm koji sadrži broj piksela koji imaju tri ili četiri kombinacije boja poput RGB (crvena, zelena, plava) ili CMIK (cijan, magenta, žuta, crna). Preostale boje sastoje se od mešavine ovih osnovnih boja. Digitalne slike se koriste za steganografiju zbog slabosti HVS-a (ljudskog vizuelnog sistema) koji ima malu osetljivost kod slučajnih promena obrazaca. Zbog ove slabosti tajna poruka može se sakriti u video ili sliku I da pritom ne bude primećena.

## Osnovni model

Na datoj slici je prikazan jednostavan prikaz ugradnje i ekstrakcije u video steganografiji. Tajna poruka je ugrađena u digitalni video pomoću tehnike ugrađivanja podataka.



Slika 2 : Dijagram procesa skrivanja i ekstrakovanja testa iz videa

Kada se tada proizvede stego objekat, on će se putem nekog javnog komunikacionog kanala poslati primaocu. Proces izdvajanja je jednostavno obrnut od postupka ugradnje. Primalac mora da dekodira stego objekat da bi video tajnu poruku primenom algoritma / tehnike izdvajanja.

Opšti princim procesa ugradnje i izdvajanja skrivenog teksta:

**Algoritam umetanja**

1. Usnos video datoteke
2. Unos teksta koji se ugrađuje
3. Podeliti video u frejmove.
4. Odrediti bajtove (na osnovu tehnike koja se koristi) koji će biti modifikovani
5. Regenerisanje videa iz okvira.

**Algoritam izdvajanja**

1. Unos stego video datoteke.
2. Čitanje potrebne poruku iz stego videa.
3. Deljenje videa u okvire.
4. Pronalaženje odgovarajućih bitova (na osnovu korišćene tehnike)
5. Regenerisati video okvire

## Tehnika najmanje značajnog bita (LSB)

Podaci se skrivaju u video datoteci uz pomoć algoritma najmanje bitnog bita (LSB). LSB tehnika kodiranja ima prednost male računske složenosti i vrlo velike brzine protoka Svaki piksel ima 3 bita tajne poruke : po jedan u svakoj RGB komponenti. Za skrivanje tri bita poruke u boji svakog piksela koristimo 24-bitnu sliku poput BMP (Bitmap). 3 piksela 24-bitne slike dati su u nastavku:

**(00100110 11101000 11001001)**

**(00100111 11001001 11101001)**

**(11001000 00100111 11101001)**

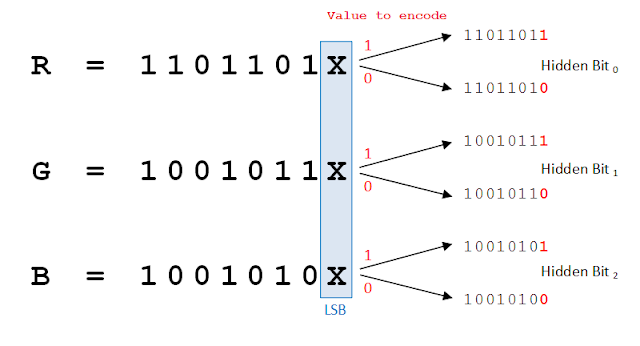
Karakter „a“ ima ASCII vrednost 97 u decimalnom i ekvivalentna binarna vrednost to je **1100001**. Postupak ugradnje :

**(00100111 111010001 1001000)**

**(00100110 110010000 1101000)**

**(11001001 001001111 1101001)**

LSB tehnikom dobija se mala razlika u bojama video snimka. Ljudskom oku bi bilo izuzetno teško da uoči razliku.



Slika 3 : Princip rada LSB-a

## Masking and Filter method

Metoda maskiranja i filtriranja obično je ograničena na 24-bitne slike. Ova metoda koristi određene algoritme maskiranja ili matematičke formule za odabir određenih piksela sa slike naslovnice. Izabrani pikseli se mogu koristiti za ugradnju tajnih informacija nakon odgovarajuće prethodne obrade. Stoga ugrađene tajne informacije izgledaju kao sastavni deo naslovne slike. Korišćenjem odgovarajućeg filtera (matematički izraz) za odabir piksela, povećava se sigurnost steganograpofske metode slike i kapacitet ugrađivanja može se povećati.

Tehnike maskiranja i filtriranja sakriva informacije na način sličan vodenim žigovima na stvarnom papiru i ponekad se koriste kao digitalni vodeni žigovi. Maskiranje slika podrazumeva promenu osvetljenosti maskiranog područja. Što je promena osvetljenosti manja, to je manja šansa da se ona može detektovati. Tehnike maskiranja su pogodnije za upotrebu u JPEG slikama sa gubitkom od umetanja LSB-a zbog njihovog relativnog imuniteta na operacije slike kao što su kompresije.

**Algoritam za ugrađivanje teksta - filter metoda:**

**Ulaz**: Tajna tekstualna poruka, slika u kojoj se skriva poruka.

**Izlaz**: ugrađena (Stego) slika.

1. Izaberite skup piksela za nosače slika pomoću matematičke funkcije

2. Vrednosti nivoa sive / crvene boje pikseli se obrađuju.

3. Pretvorite tajne tekstualne informacije u bit tok (ASCII kodiranje).

4. Ako je prvi bit u toku tekstualnih bitova nula, tada vrednost prvog piksela nije

izmenjen.

5. Ako je prvi bit jedan, onda prvi piksel je napravljen tako da bude neparan

dodajući 1 pikselu

6. Ponoviti gore logiku dok se ne dođe do kraja teksta

7. Modifikovani pikseli se vraćaju u originalnu naslovnu sliku da bi se dobila Stego Image.

**Algoritam za oslobađanje teksta – filtr metoda:**

**Ulaz**: ugrađena (Stego) slika, ključ.

**Izlaz**: Tajna tekstualna poruka.

1. Identifikujte specifične piksele u stego-u slika korišćenjem iste matematičke funkcije .

2. Ispitajte vrednosti piksela. Ako je vrednost piksela neparna, onda je ugrađeni tekst bit bio jedan.

3. Ako je vrednost piksela parna, tada je ugrađeni tekst bio nula.

4. Na osnovu gornjeg tumačenja, dohvatiti tok bitova teksta.

5. Pretvorite tok bitova u ASCII.

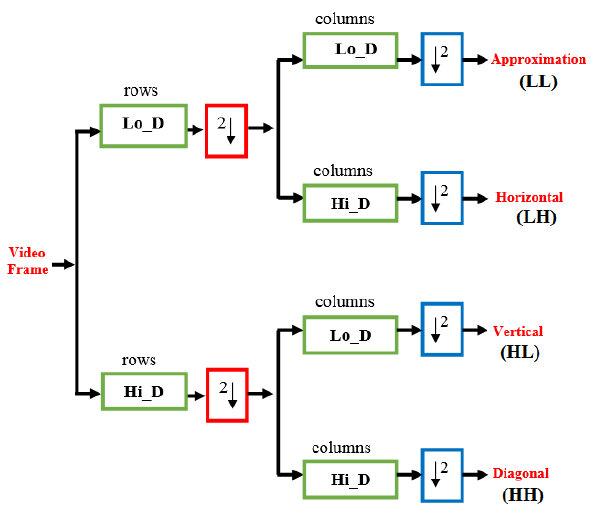
Talasna transformacija

Upotreba talasa u stenografskom modelu slike leži u činjenici da talasna transformacija jasno razdvaja informacije o visoku frekvenciju i informacije o niskoj frekvenciji u odnosu na piksel po piksel. Discrete Wavelet Transform (DWT) je poželjnija u odnosu na Discrete Cosine Transforms (DCT) jer slika u niskoj frekvenciji na različitim nivoima može ponuditi bolju rezoluciju. Dekompozicija DWT rezultira u četiri klase ili koeficijentna opsega koja su : aproksimacioni opseg (LL), vertikalni opseg (LH), vodoravni opseg (HL) i dijagonalni opseg detalja (HH). Aproksimacioni opseg sastoji se od koeficijenta niskog frekventnog talasa, koji sadrži značajan deo slike prostornog domena. Ostali opsezi sastoje se od koeficijenta visoke frekvencije, koji sadrže ivice detalja slike prostornog domena.

Pretvaranje video okvira u frekventni domen kao što su DWT i DCT transformacije poboljšaće robustnost steganografske metode od napada, stoga će se očuvati neprimetnost stego video zapisa.

DWT I DCT transformacije su dobro poznati metodi koji konvertuju digitalne podatke iz prostornog domena u domen transformacije.

Slika 2 ilustruje prvi nivo dvodimenzionalnog DWT raspadanja koji prikazuje svaki od LL, LH, HL i HH opsega.



Slika 4 : primena DWT radi dobijanja 4 opsega

## Redundant Pattern Encoding

Redundant Pattern Encoding predstavlja modifikaciju LSB algoritma. U LSB metodi postoje praznine, zbog toga će LSB metoda biti izmenjen tako da pokriva praznine . Redundant Patterrn Encoding širi poruku na svaku zakrpu piksela na slici.Metod za generisanje sekvenci brojeva koji su blizu prirode nasumičnih brojeva, koristi se za izbor dve oblasti slike (Zakrpa A i zakrpa B).

Proces umetanja poruka : Modifikacija algoritma LSB metoda pomoću metoda RPE obavlja se u fazi izbora oblasti slike, raspodeli zakrpe A i zakrpe B i u fazi distribucije poruka.

**Postupak umetanja:**

**1**.**Izabor veličine piksela slike.** U ovom procesu sistem će otkriti veličinu piksela na slici, a zatim će sistem odabrati područje slike u 2 zakrpe.

**2**. **Distribucija zakrpe A i zakrpe B**. U ovom procesu zakrpa će biti podeljena na 2, zakrpa A i zakrpa B na osnovu širine slike kao mesta za čuvanje poruka. Svako polje je slično 1 piksel, svaki piksel se sastoji od RGB gde R ima 1 bajt, G ima 1 bajt, a B ima 1 bajt, tako da RGB ima ukupno 3 bajta. Zakrpa A ima 16 piksela, dakle: 3 bajta k 16 = 48 bajtova. Dobija se rezultat od 48 bajtova, što znači da je veličina zakrpe A, svaki 1 bajt se sastoji od 8 bitova, dakle: 48 k 8 = 384 bita. Tako u zakrpi A dobijamo 384 bita, pri čemu je 384 bita kapacitet skladištenja poruka u zakrpi A. Zakrpa B je ista kao i izračun u zakrpi A koja ima kapacitet za skladištenje poruka od 384 bita.

**3.** **Konverzija RGB vrednosti u binarne**. U procesu konverzije, vrednost piksela će se promeniti u RGB gde svaki RGB ima vrednost 255 i biće promenjena u binarnu gde će se u poslednji bit umetnuti poruka.

**4. Pretvoranje poruke u binarnu.** Ovaj postupak je pretvaranje ASCII u binarni pri čemu će svaki bit u ASCII koji je pretvoren u binarni biti umetnut u vrednost bita na RGB slici.

**5. Širenje stego-teksta na zakrpu A i zakrpu B.** U ovom procesu sistem čuva svaki bit karaktera poruke u najdesniji bit na slici, kao što je širenje metodom LSB na 2 zakrpe, naime zakrpe A i zakrpe B, koje su podeljene prema koraku 1.

## Encrypt and Scatter

Tehnika šifrovanja i rasejanja je tehnika koja se najviše koristi u steganografiji slika. Pokušava da oponaša beli šum. Vhite Noise Storm je kombinacija praksi širenja spektra i skakanja frekvencija. Princip Vhite Noise Storm-a je da tajnu poruku rasipa da se sakrije preko slike.

## Neparna/Parna (ODD/EVEN) distribucija piksela

Da bi steganografska metoda bila bolja mora se rešiti efikasna tri pitanja (sigurnost, kapacitet i neprimetnost). Najvažniji pitanje je neprimetnost, koja pokazuje kako teško je odrediti i razlikovati postojanje skrivene poruke, to se postiže pomoću šema distribucije neparnih / parnih piksela. Drugo važno pitanje u steganografiji je sigurnost. Poslednje pitanje je kapaciteta, što je maksimalan podatak koji se može bezbedno sakriti na slici sa visokim kvalitetom slike i neprimetnosti.

Standardne tehinike za steganografiju obično stresiraju određene bitove. Ugradnja poruke ili mapiranje se vrši na standardnim pozicijama kao što je kod LSB tehnike to bit najmanje težine , dok se kod Parvinderetove tehnike manipulacija vrši nad 6. I 7. bitom. Ovakav tip tehnika čini stegoanalizu veoma jednostavnom. Promene nad piskelima (ili kanalima piksela) koje ne menjaju tačno određene bitove već ceo piksel ili kanal pružaju veću sigurnost i teže ih je otkriti.

Primer promene vrednosti piksela iz neparne u parnu vrednost (iz parne u neparnu) :

**100000111010101110100111 – 1 = 0100000111010101110100110**

**Algoritam umetanja**

**Ulaz**: Tajna tekstualna poruka, video u kome se skriva poruka.

**Izlaz**: ugrađen tekst u (Stego) video

1. Usnos video datoteke
2. Unos teksta koji se ugrađuje
3. Podeliti video u frejmove.
4. Odrediti piksele (na osnovu tehnike koja se koristi) koji će biti modifikovani
5. Uzeti bitove poruke koji će se ugraditi u jedan frejm primenom tehnike neparno/parno

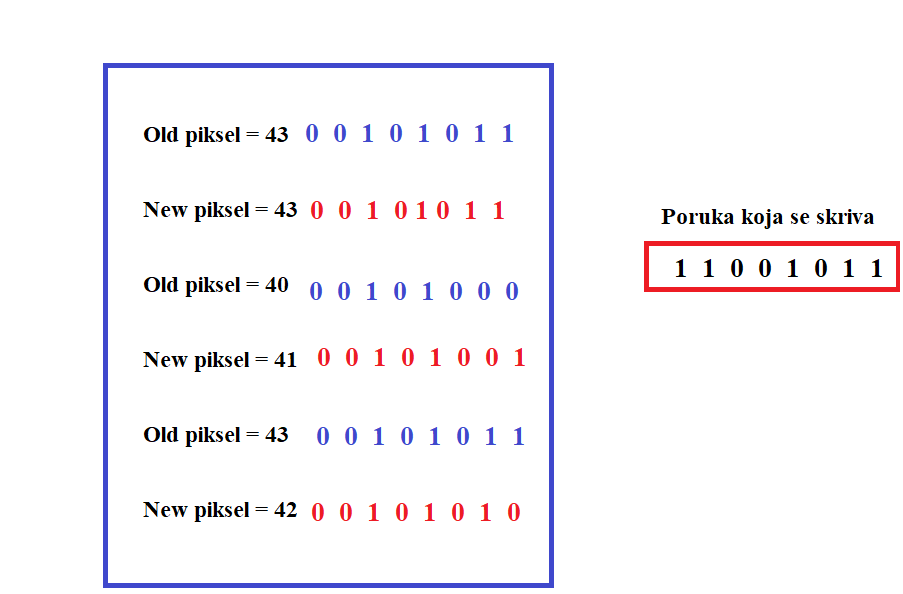
* Tehnika neparno parno :
  + Ako je tajna poruka (bit) 0 , a piksel (kanal) je paran ne treba menjati piksel (kanal)
  + Ako je tajna poruka 0 , piksel (kanal) je neparan onda oduzeti 1 (pixel - 1) i pretvoriti ga u paran
  + Ako je tajna poruka 1 , a piksel (kanal)je neparan ne treba menjati piksel
  + Ako je tajna poruka 1 , piksel (kanal) je paran onda oduzeti 1 i pretvoriti ga u neparan

1. Regenerisanje videa iz okvira.

**Algoritam izdvajanja**

1. Unos stego video datoteke.
2. Čitanje potrebne poruku iz stego videa.
3. Deljenje videa u okvire.
4. Pronalaženje odgovarajućih bitova (na osnovu korišćene tehnike)
5. Regenerisati video okvire

Prilikom izbora piksela na koje će biti mapirane vrednosti biranih poruka iz skupa piksela se izbacuje granična vrednost koju predstavljaju pikseli čija je vrednost za RGB : 000 , jer oduzimanje jecinice od piksela čija je vrednost 0 dovode do negativnigh vrednosti piksela.



Slika 5 : odd/never tehnika

Neparna/Parna distribucija piksela postiže veći stepen neprimetnosti pri ubacivanju koda u odnosu na LSB tehniku.

Sledeći pseudo kod predstavlja algoritam koji obezbeđuje znatno veči nivo kapaciteta i sigurnosti.

**Modifikacija odd/never metode:**

**Ulaz**: Originalni video

**Izlaz**: Stego video.

1. Unos video datoteke
2. Unos teksta koji se umeće
3. Huffmanovo kodiranje nad tajnom porukom
4. Podeliti video snimak na frejmove
5. Odrediti broj znaka koji se umeće u frejm
6. Frejm deliti na blokove 8x8
7. Generisanje slučajnog broja pomoću Henon funkcije
8. Pomoću generisane vrednosti izabrati jedan od blokova (8x8)
9. Ponovo korišćenjem Henanove funkcije sa drugim koeficijentom odrediti nasumične vrednosti piksela
10. Uzeti bitove poruke koji će se ugraditi u jedan frejm primenom tehnike neparno/parno

* Tehnika neparno parno :
  + Ako je tajna poruka (bit) 0 , a piksel je paran ne treba menjati piksel
  + Ako je tajna poruka 0 , piksel je neparan onda oduzeti 1 (pixel - 1) i pretvoriti ga u paran
  + Ako je tajna poruka 1 , a piksel je neparan ne treba menjati piksel
  + Ako je tajna poruka 1 , piksel je paran onda oduzeti 1 i pretvoriti ga u neparan

1. Regenerisati video snimak iz okvira

.

Hafmanova tehnika kodiranja omogućava kompresiju tajne tekstualne poruke pre ugradnje. Kodiranje tajne poruke pre ugradnje pomaže u povećanju sigurnosti (kako bi neko pročitao poruku potrebno je da je dekodira što može uraditi samo ukoliko zna kojom tehnikom je kodirana) I u kapacitetu smeštanja poruke. Rezultat Huffmanovog kodiranje je nova kodirana poruka koja rezultuje manjom dužinom u odnosu na prvobitnu poruku.

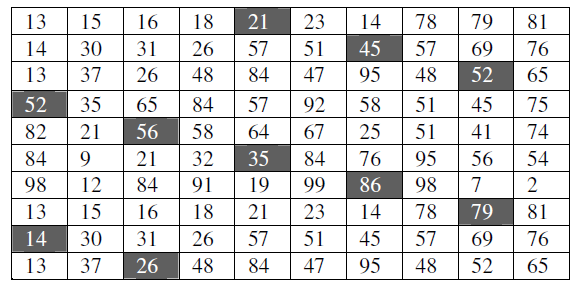
Segmentiranje bolokova , odnosno nasumicno biranje jednog od blokova frejma Henon funkcijama u kome će biti ugrađena poruka pruža dodatni nivo bezbednosti jer izvlačenje teksta neće biti moguće ukoliko ne znamo koji blok je korišćen za skrivanje poruka. Duplu sigurnost omogućava druga primena Henon funkcije za nasumičan izbor piksela u kojima će se skrivati bit simbola.

### GLM metod

Tehnika modifikacije sivog tona (GLM) zasniva se na modifikaciji sivih tonova slike. Promena vrednosti sivog tona za 1 pravi male izmene tako da čovek no može primetiti razliku.

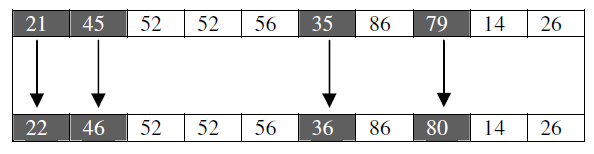
Modifikacija nivoa sive je definisana kao tehnika u kojoj se vrednosti nivoa sive u pikselima slike menjaju . Svaki piksel ima različitu vrednost nivoa sive boje koja može imati neparnu ili parnu vrednost. Ova neparna ili parna vrednost nivoa sive boje je na odgovarajući način modifikovana da predstavlja binarne podatke.

Potrebno je izabrati piksele koji će biti modifikovani. Za izbor pozicije mogu se koristiti različite matematičke funkcije kao što je na primer : **x +5 %** w , gde x predstavllja broj redova slike a w širinu slike na osnovu broja piksela.



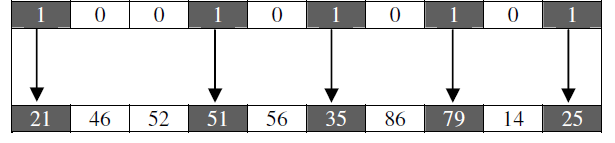
Slika 6 : Izbor piksela primenom funkcije **x +5%w**

Prilikom izbora određenih piksela koji će biti modifikovani matematičkom funkcijom potrebmo ih je svesti na isti nivo sive boje tako što će pikseli koji imaju neparnu vrenodt postati paran dodavanjem jedinice.



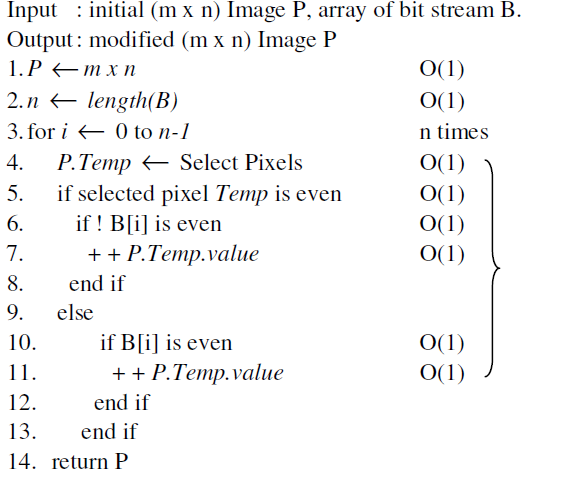
Slika 7: Predstavljanje piksela preko istih (parnih) vrednosti sive boje

Mapiranje teksta (binarne poruke) na piksele vrši se metodom parni/neparnni gde se bit koji ima vrednost 1 predstavlja neparnom vrednosću pixela tako što se oduzme 1 od trenutne (parne) vrednosti piksela , dok je za bit 0 vrednost piksela već podešena na parnu i ne vrše se nikakve dodatne operacije.



Slika 8 : Vrednosti piksela nakon mapiranja poruke **1001010101**

**Primer pseudo koda za implementaciju GLM algoritma:**



Slika 9 : implementacija GLM metode

Naučna podrška ovoj tehnici je mapiranje informacionih podataka unutar prostornog domena slike izmenom vrednosti sivog nivoa piksela. Korišćen je koncepta neparnih i numerisanih sivih vrednosti može se koristiti za mapiranje binarnih podataka. Složenost algoritma je reda O(n). Menjanje vrednosti sivog nivoa za jednu jedinicu ne bi u velikoj meri promenilo statistiku slike.

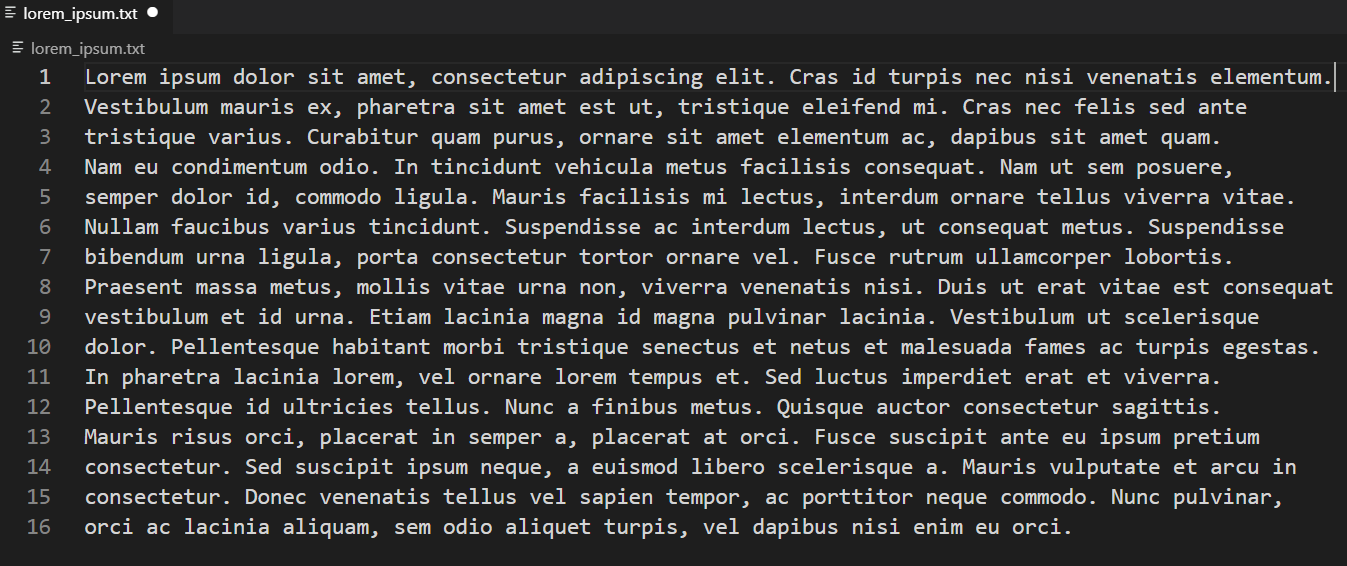
### Rezultat implementacije metode parna/neparna distribucija piksela

Implementirana je metoda parne/neparne distribucije piksela. Distribucija je izvršava nad kanalima piksela. Izabrani pikseli se dele na kanale i unutar kanala vrši se mapiranje vrednosti poruke. Poruka je predstavljena binarnom notacijom.

Video snimak se deli na frejmove (30 frejma po sekundi) u koje se zatim umeće deo tekstualne poruke predstavljene binarno. Implementacija je izvršena tako da se poruka deli u blokove od 250 karaktera (binarnih vrednosti) koji se zatim mapiraju unutar jednog frejma. Pikseli koji se ne uzimaju u obzir za mapiranje su oni pikseli čije su vrednosti RGB kanala 000. Bitovi se skrivaju redom u ne-nulte piksele , mapiranjem 1 bita na 1 kanal (3 bita poruke po pikselu.)

Slika 10 : Primer jednog frejma pre i nakon skrivanja podataka



Slika 11 : Tekst koji se umeće/mapira unutar video snimka

# Zaključak

Steganografija ima svoje mesto u bezbednosti. Nije namenjena za zamenu kriptografije, već za dopunu. Sakrivanje poruka metodama steganografije smanjuje mogućnost otkrivanja poruke. Međutim, ako je to poruka je takođe šifrovana, ako se otkrije, takođe mora da se razbije (još jedan sloj zaštite). Steganografija se ne odnosi samo na digitalne slike već i na druge medije (datoteke poput glasa, drugog teksta i binarnih datoteka, drugi mediji poput komunikacionih kanala, lista se može trajati i dalje).

Video steganografija zasniva se na deljenju video snimka na frejmove I primenu steganografije nad slikokm. Njkorišćeniji metod je LSB algoritam , međutim njegova zaštita nije velika. Standardne metode često koriste princim ugradnje bitova tako što stresiraju određene bitove kao što je to 8. Bit kod LSB tehnike. Ovakvi metodi se mogu lakes otkriti nego metodi koji menjaju ceo pikel ili kanal.

Tri glavne karakteristike koje steganografija mora da ispznjava su : sigurnost, kapacitet i neprimetnost. Najvažniji pitanje je neprimetnost, koja pokazuje kako teško je odrediti i razlikovati postojanje skrivene poruke. Drugo važno pitanje u steganografiji je sigurnost. Poslednje pitanje je kapaciteta, što je maksimalan podatak koji se može bezbedno sakriti na slici sa visokim kvalitetom slike i neprimetnosti.

Korišćenje steganografije uz kriptovanje podataka smanjuje obim poruke koji se skriva i povećava nivo zaštite šifrovanje teksta.

Neke od tehnika koje se koriste su : LSB , HLSB , SLSB, Tehnike transformacije : DWT, DCT. Tehnike enkriptovanja i rasipanja, maskiranje i filtriranje kao i parna/neparna distribucija piksela.

# Reference

[1] JAMMI ASHOK, S.MUNISHANKARAIAH, K.SRINIVAS , STEGANOGRAPHY: AN OVERVIEW (2010) Link:<https://www.researchgate.net/publication/50366231_STEGANOGRAPHY_AN_OVERVIEW>

[2] Ms. Pooja Vilas Shinde , Dr.Tasneem Bano Rehman , A Survey : Video Steganography techniques

Link:<https://www.researchgate.net/publication/329572494_A_Survey_of_Video_Steganography_Techniques>

[3] Gat Pooja Rajkumar , Virendra S Malemath , Video Steganography: Secure Data Hiding Technique Link:<https://www.researchgate.net/publication/320900395_Video_Steganography_Secure_Data_Hiding_Technique>

[4] Bharti Chandel , Shaily Jain , Gurumukhi Text Hiding using Steganography in Video

Link:<https://www.researchgate.net/publication/303318885_Gurumukhi_Text_Hiding_using_Steganography_in_Video>

[5] Er Gursukhmani , Sugandha Sharma , CASE STUDY OF HIDING A TEXT USING VIDEO STEGANOGRAPHY

Link : <https://www.researchgate.net/publication/333618583_CASE_STUDY_OF_HIDING_A_TEXT_USING_VIDEO_STEGANOGRAPHY>

[6] Minkyung Kwak , Youngho Cho , A Novel Video Steganography-Based Botnet Communication

Link : <https://www.researchgate.net/publication/348266746_A_Novel_Video_Steganography-Based_Botnet_Communication_Model_in_Telegram_SNS_Messenger>

[7] Ramadhan J. Mstafa , A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC

Link : <https://ieeexplore.ieee.org/document/7893733>

[8] MOHAMMED MAHDI HASHIM, MOHD SHAFRY MOHD RAHIM , IMAGE STEGANOGRAPHY BASED ON ODD/EVEN PIXELS DISTRIBUTION SCHEME AND TWO PARAMETERS RANDOM FUNCTION

Link : <https://core.ac.uk/download/pdf/225547724.pdf>

[9] Elizabeth Chang , Grey level modification steganography for secret communication

Link:<https://www.researchgate.net/publication/4137627_Grey_level_modification_steganography_for_secret_communication>

[10] Ahmad T. Al-Taani , Abdullah M. AL-Issa , A Novel Steganographic Method for Gray-Level Images

Link: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.309.1495&rep=rep1&type=pdf>