Универзитет у Нишу

Електронски факултет

**Стеганографија**

Семинарски рад

Студијски програм: Рачунарство и информатика

Модул: Софтверско инжењерство

Ментор: Студент:

Проф. др Братислав Предић Лазар Најдановић, бр. индекса 1763

Ниш, 2024. година

**Sadržaj**

[**1.** **Увод** 3](#_Toc184405483)

[**2.** **Стеганографија** 4](#_Toc184405484)

[**3.** **Историја стеганографије** 6](#_Toc184405485)

[4. Компоненте стеганографске поруке 6](#_Toc184405486)

[5. Стеганографски приступи 7](#_Toc184405487)

[6. Технике стеганографије 8](#_Toc184405488)

[7. Процес стеганографије слика 10](#_Toc184405489)

[8. Методе стеганографије 11](#_Toc184405490)

[**9.** **Least Significant Bit** 12](#_Toc184405491)

[9.1. LSBу сликама 12](#_Toc184405492)

[9.2. LSBу аудио сигналима 13](#_Toc184405493)

[**10.** **Алати за стеганографију слика** 15](#_Toc184405494)

[**11.** **AForge.NET** 15](#_Toc184405495)

[**12.** **Закључак** 16](#_Toc184405496)

# **Увод**

Основнa семинарског рада је заправо форензика слика. Представља значајну дисциплину унутар дигиталне форензике, фокусирајући се на анализу дигиталних слика како би се откриле и потврдиле кључне информације важне за правне и безбедносне истраге. Фокус ове дисциплине је на провери аутентичности и откривању потенцијалних манипулација, као и на анализи информација садржаних у метаподацима, идентификацији особа или објеката на сликама и сарадњи са сродним подручјима као што су стеганографија и скривени канали.

Основни концепти форензике дигиталних слика су:

* Аутентичност слика
* Детекција манипулације
* Анализа метаподатака
* Идентификација особа и објеката
* Сарадња са другим поддисциплинама

Један од главних циљева форензике слика је утврђивање аутентичности. Овај процес често укључује анализу метаподатака, као што су датум и време снимања, модел уређаја којим је слика забележена и друге идентификационе информације, како би се утврдило да ли је слика оригинална или је била предмет манипулације.

Током форензичке анализе слика, посебан фокус се ставља на детекцију промена или потенцијалних манипулација. Стручњаци користе разне технике, укључујући анализу пиксела (у случају растерских слика), препознавање неправилности у бојама, геометријске анализе, као и друге методе ради идентификације промена на слици.

Метаподаци су кључни део форензичке анализе јер пружају информације о уређају, локацији и времену снимања, омогућавајући проверу аутентичности и реконструкцију догађаја. Поред тога, анализа лица и објеката може бити значајна у криминалистичким истрагама, случајевима нестанака и надзору.

Форензика растерских слика сарађује са поддисциплинама сакривања информација од којих су познатије:

* Стеганографија
* Watermarking
* Сакривени канали

Током овог рада, фокусираћемо се на дисциплину стеганографије.

# **Стеганографија**

**Стеганографија** је дисциплина која се бави скривањем података у другом скупу података тако да се сакривени подаци не могу детектовати.

Реч стеганографија долази од грчких речи steganos и graphein, што у дословном преводу значи скривено писање. Стеганографским техникама тајна се порука скрива унутар неке друге безазлене поруке тако да се постојање тајне поруке не може уочити. Ова знанствена дисциплина позната је од давнина. Херодот је у својим "Причама" спомиње.

Циљ стеганографије је да се сакрије порука унутар слика тако да не дозволи ниједном „непријатељу“ да постоји тајна порука пристуна на слици. Сама стеганографија покушава да сакрије постојање комуникације.

Развој модерних техника стеганографије обухвата коришћење микроскопских слика и микротачака. Француски фотограф Драгон је током Француско-пруског рата (1870–1871) развио технику смањења слика до микроскопских величина, које су скриване у ноздрвама, ушима или испод ноктију. Током Првог светског рата, Немци су користили микротачке за скривене поруке на разгледницама, док су током Другог светског рата микротачке могле да садрже целу страницу текста или чак фотографије.

У савременом добу, са појавом интернета и дигиталних медија, стеганографија је доживела велики процват. Брз развој компјутерских мрежа и дигитализација медија створили су повољно окружење за скривену комуникацију путем стеганографије. Последњих година, стеганографија је осумњичена као могући начин за размену информација и планирање терористичких напада. У складу с тим, развија се и стеганализа, наука која се бави откривањем и декодирањем скривених порука. Стеганографија се сматра компромитованом већ када је откривено само постојање тајне поруке.

Основну структуру стеганографије чине три компоненте:

* Слика
* Порука
* Кључ

Слика представља објекат који ће садржати скривену поруку, док се кључ користи за декодирање/дешифровање скривених порука.

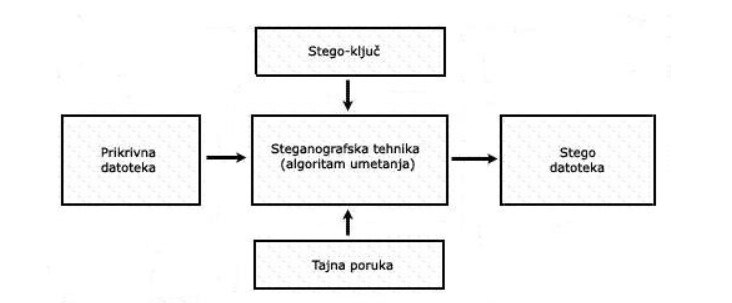
Из тог времена датира једна позната стеганографска метода: носитељу поруке се обрије глава, а онда се на њу утетовира порука коју сакрије нарасла коса. Приматељ једноставно обрије главу носитеља да би дошао до поруке.

Занимљиво је да су се овом техником користили њемачки шпијуни почетком 20. века.

Модерна стеганографија се односи на скривање тајних порука у редундантним деловима скривене датотеке. Дигитална технологија даје превише могућности за примену стеганографије, укључујући и ону најпроширенију - методу скривања информација у дигиталној слици.

Дигиталне датотеке се у рачунару чувају као низови битова, при чему су неки битови битни, док су други мање битни. Редундантни битови не носе информације битне за датотеку, па их можемо неопажено заменити битовима информације коју желимо сакрити. Важно је напоменути да нису све дигиталне датотеке погодне за сакривање тајни. На пример, у извршним верзијама програма сваки бит је битан, па промена само једног бита може изазвати неисправно извршавање програма.

Приликом примене стеганографије често се користи следећи основни принцип. Пошиљалац скривене поруке, означене са "m", насумично одабира безазлену поруку "c" - прикривну датотеку (слику, звук, текст) коју може слободно послати прималцу. Након што је одабрана прикривна датотека, у њу се умеће порука неком стеганографском методом, можда чак и уз употребу тајног кључа "k", те тако од прикривне датотеке "c" настаје стегообјекат "s" Посматрач, који види на први поглед безопасну поруку "s", не сме открити постојање тајне поруке.



Слика 1. – Принцип стеганографског процеса

Како промене на прикривној датотеци не би требале бити видљиве никоме ко не учествује у процесу комуникације, она мора садржавати довољно редундантних битова који могу бити замењени скривеном поруком. У идеалном случају, ни људско око ни рачунар не би требали приметити разлику између изворне прикривне датотеке и стегообјекта.

# **Историја стеганографије**

Први познати примери стеганографије забележени су 440. године пре нове ере, према Херодоту, који описује два случаја скривања порука. Демаратус је упозорио Грке на предстојећи напад тако што је поруку урезао у дрвену подлогу воштане плоче пре него што ју је прекрио воском. Други пример односи се на Хистиаеуса, који је обријао главу свом робу, написао поруку на њој, а затим чекао да му коса израсте како би скривена порука била пренесена без сумње.

Након античких примера, стеганографија се наставила развијати кроз векове. Фило из Византије, у 3. веку п.н.е., експериментисао је са невидљивим мастилом, користећи орахово дрво за писање невидљивог текста, док је бакар-сулфат омогућавао његово откривање. Једна од метода била је и омотавање траке око штапа, где је дебљина штапа била кључна за исправно дешифровање поруке. Тако пренесена трака није откривала поруку на први поглед.

Термин стеганографија први пут се појављује у књизи "Стефанографија" Јоханнеса Тритхемијуса. Књига је била замишљена као дело о магији, али је користила технике криптографије и стеганографије да би сакрила стварни садржај. Касније, 1518. године, објављена је "Полyграпхиа", која је пружила детаљнији увид у праксу стеганографије. Током 17. века, Френсис Бејкон је развио "Бацонову шифру", која се ослањала на различите врсте слова за кодирање тајних порука, чиме је значајно допринео развоју стеганографских техника.

Модерна стеганографија добија замах крајем 19. века са развојем микродотова, који су постали популарни током Другог светског рата. Ове мале тачке садржале су читаве поруке или слике, скривене унутар наизглед обичних текстова. Нови талас развоја стеганографије уследио је деведесетих година прошлог века, када су софтверске апликације омогућиле сакривање података у дигиталним медијима као што су слике, видео записи, аудио датотеке и текстуални документи.

# Компоненте стеганографске поруке

Стеганографска порука састоји се из три основне компоненте које заједно омогућавају сигурно и неприметно преношење тајних података:

* Secret message - представља информацију која се жели сакрити. То може бити било који тип података – текст, слика, видео или бинарне датотеке. Пре него што се угради у cover data, ова порука често бива шифрована како би се додатно заштитила и осигурала тајност чак и у случају откривања.
* Cover data - су медијум у који се тајна порука уграђује. Ова компонента служи као „маскирање“ и може бити различитих врста, укључујући дигиталне слике, аудио записе, видео садржаје или текстуалне датотеке. Квалитет и природа покровних података кључни су за успешност стеганографије – циљ је да стего порука не изазива сумњу приликом преноса или обраде.
* Stego message - је резултат уметања тајне поруке у cover data, који сада садрже скривени садржај, али и даље изгледају неупадљиво. Стего порука мора задржати сличност са оригиналним cover data како би избегла откривање путем анализа или обраде. Током преноса путем мрежа или других канала комуникације, стего порука треба да задржи своју тајновитост и не показује видљиве промене.

Комбинација ових компоненти омогућава безбедну размену информација на начин који не привлачи пажњу. Квалитет стеганографског алгоритма, као и коришћење одговарајућих техника за уметање и екстракцију, кључни су за постизање високе безбедности и поузданости у преносу тајних података. Напредни стеганографски системи често користе додатне технике, попут криптографских метода, како би осигурали да чак и у случају откривања стего поруке, њен садржај остане недоступан неовлашћеним особама.

# Стеганографски приступи

Стеганографски приступи често зависе од тога како се креирају, имплементирају и преносе тајни подаци у оквиру cover data. Два основна приступа која се користе у стеганографији су top-down и bottom-up приступи. Сваки од њих има специфичне методе и поделе које се користе за сакривање информација, од поједностављених решења до сложенијих модела.

**Top-down приступ** представља систематски метод који започиње пројектовањем општег модела за стеганографију, а затим се дели на специфичне технике. Главне категорије су:

* Pure steganography: Овај приступ не користи кључеве за заштиту комуникације. Поверљивост поруке се ослања искључиво на тајност саме методе уметања података, због чега је мање безбедан у поређењу с другим методама. Ако је метода уметања откривена, тајна порука може бити једноставно пронађена. Чиста стеганографија је корисна у ситуацијама када постоји поверење у поверљивост канала, али је подложна компромитовању.
* Private key steganography: Ова метода користи заједнички приватни кључ између пошиљаоца и примаоца. Пре уметања, порука се шифрује помоћу приватног кључа, чинећи је доступном само онима који поседују тај кључ. Овај приступ пружа знатно виши ниво сигурности јер, чак и ако је метода уметања откривена, порука остаје нечитљива без кључа. Приватна кључна стеганографија често се користи у окружењима где је потребно поверење међу комуникационим партнерима и где је кључна контрола приступа информацијама.
* Public key steganography: Ова метода је слична криптографији са јавним кључем. У овом случају, пошиљалац користи јавни кључ примаоца за шифровање поруке која се затим уметне у покровне податке. Само примаоц који поседује одговарајући приватни кључ може дешифровати скривени садржај. Овај приступ нуди висок ниво сигурности и омогућава безбедну комуникацију и између странака које се не познају лично, али захтевају поверење у преносу информација.

**Bottom-up** приступ представља методологију која се фокусира на појединачне аспекте уметања података на основном нивоу. Овај приступ често креће од детаљног разматрања и имплементације једноставнијих техника уметања, попут манипулације појединачним битовима у дигиталним сликама, а затим се надограђује сложенијим техникама и комбинацијама. Bottom-up приступ омогућава дубље разумевање сваког сегмента процеса уметања и често се користи за развијање иновативних стеганографских решења која су отпорнија на детекцију.

У оба приступа, кључни циљ је осигурати да се скривена порука не може открити или компромитовати, било кроз употребу сложених алгоритама, тајних кључева или различитих техника уметања и обраде података.

# Технике стеганографије

Различите технике стеганографије могу се поделити на техничку и лингвистичку стеганографију. Техничка стеганографија користи се за скривање информација унутар других података који нису текстуалног карактера (као што су слике, аудио и видео датотеке), док се лингвистичка стеганографија ослања на скривене податке у датотекама, где модификована датотека и даље веродостојно приказује садржај.

Постоје два главна типа стеганографије:

1. **Лингвистичка стеганографија** обухвата семаграме и отворене кодове.

* Семаграми користе симболе и знакове за скривање порука. Постоје визуелни семаграми, који скривају податке распоредом предмета или објеката, и текстуални семаграми, који користе различите модификације текста, попут промена у размаку, величини или боји фонта.
* Отворени кодови укључују жаргонски код и скривене шифре. Жаргонски код користи унапред дефинисане фразе познате само одређеним особама, док скривене шифре омогућавају откривање порука само уз познавање специфичне методе уметања података. Оне се деле на решеткасте и нулте кодове. Решеткасти шифрари користе шаблоне за сакривање порука, док нулти кодови прате одређено правило уметања (нпр. изузимање одређених редова или речи).

Постоје различите технике уметања информација у датотеке, међу којима су убацивање, замена и генерисање:

* Убацивање: Ова техника скрива податке у мање значајним деловима датотека, често без утицаја на саму функционалност датотеке. Иако оставља "чист" изглед, повећање величине датотеке може изазвати сумњу.
* Замена: Користи замену најмање значајних битова (ЛСБ) у носиоцу података, уз минималан утицај на оригиналну датотеку. Предности су очување величине датотеке, али изазови укључују могућност деградације квалитета и ограничен капацитет.
* Генерисање: Уместо уметања поруке у постојеће податке, креира се потпуно нова датотека са скривеним порукама. Ова техника елиминише потребу за поређењем са оригиналним носиоцем, чинећи откривање теже.

1. **Технолошка стеганографија (заснована на дигиталним медијима)**

Технолошка стеганографија користи дигиталне медије (као што су слике, видео, аудио и други фајлови) за скривање порука. Овај тип стеганографије је постао популаран са развојем рачунара и интернета. Главне методе укључују:

* **Стеганографија у сликама**:
  + **Least Significant Bit (LSB) метод**: Овај приступ користи најмање значајан бит у пикселу слике за скривање података. Промена ових битова је толико мала да је људско око не може уочити. Ово је једна од најпопуларнијих и најједноставнијих метода.
  + **Transform-domain технике**: Подразумавају скривање података у фреквенцијском домену, користећи алгоритме као што су Дискретна косинусна трансформација (DCT), који се користи за компресију JPEG слика. Подаци се уграђују у фреквенцијске компоненте слике, што отежава детекцију скривене поруке.
* **Стеганографија у аудио фајловима**:
  + **Echo hiding**: Користи се техником додавања малих одјека (ехо) у аудио сигнал. Временско кашњење и интензитет ових одјека се прилагођавају тако да не утичу на квалитет звука који људско ухо може да примети.
  + **Phase coding**: Манипулише фазама различитих фреквенцијских компоненти у аудио сигналу да би се скрили подаци, што је веома отпорно на детекцију и често коришћено у аудио сигналима.
* **Стеганографија у видео фајловима**:
  + **LSB у видео кадровима**: Користи се слично као и за слике, али овде се поруке могу скривати у појединачним кадровима видео записа. Скривена порука се дели између различитих кадрова, што је чини још тежом за откривање.
  + **Motion vector modulation**: Скрива поруке манипулишући векторима кретања у видео кодецима, као што су MPEG. Ово укључује промене у векторима кретања у оквиру компресије видео фајлова.
* **Стеганографија у мрежном саобраћају**: Скривање података у различитим аспектима мрежног саобраћаја, као што су поља заглавља или временска кашњења између пакета, што може омогућити пренос скривених информација без привлачења пажње.

Стеганографске технике могу се комбиновати како би се постигла већа тајност и отпорност на анализу, што је од кључног значаја за различите сврхе, укључујући заштиту комуникације и скривање података у дигиталном окружењу.

# Процес стеганографије слика

Стеганографија слика је процес скривања тајних информација унутар дигиталних слика, на начин који их чини непрепознатљивим голим оком, чиме се омогућава сигурна комуникација или заштита података. Основни кораци у овом процесу укључују:

* Избор слике: Први корак је одабир слике која ће послужити као носилац података. Ова слика треба да буде довољно велика да може примити скривене информације, а да се не примете промене.
* Припрема и трансформација слике (опционо): Понекад је корисно трансформисати слику пре него што се подаци сакрију у њој. На пример, применом дискретне косинусне трансформације (ДЦТ) или дискретне таласне трансформације (ДWТ) могуће је ефикасније дистрибуирати скривене податке и повећати сигурност стеганографије.
* Избор методе стеганографије: Постоји неколико техника стеганографије које се могу применити на слике, а најчешће су замена битова (ЛСБ - Леаст Сигнифицант Бит), уметање података у боје пиксела, као и коришћење специфичних трансформација као што су ДЦТ или ДWТ. Свака од ових техника има своје предности и мане у зависности од врсте слике и количине података које треба сакрити.
* Скривање информација: У овом кораку, одабрана тајна порука се кодира и убацује у слику. То може бити текстуална порука, мала слика, или било који други облик података. Коришћењем одабране методе, подаци се дискретно интегрирају у слику, тако да промене не буду видљиве голим оком.
* Чување резултујуће слике: Када су подаци успешно сакривени, резултат је нова слика која може бити сачувана у жељеном формату. У неким случајевима, слика може бити преименована или сачувана у другом формату како би се смањила могућност детекције.

Важно је напоменути да стеганографија слика захтева пажљиво планирање. Осим што је потребно користити ефикасне методе скривања, такође је потребно узети у обзир могуће технике детекције стего-порука. Различите анализе и алати могу открити постојање скривених података, стога је важно користити методе које омогућавају високи степен сигурности и неприметности.

# Методе стеганографије

У стеганографији слика, користе се различите технике за скривање информација у дигиталним сликама. Свака од ових метода има своје предности у погледу ефикасности и неприметности. Ево неколико најзначајнијих и најчешће коришћених метода стеганографије слика:

* **Least Significant Bit (LSB) стеганографија**: Ова метода користи најмање значајне битове пиксела слике да сакрије податке. Мале промене у овим битовима нису видљиве голим оком, чинећи ову технику врло популарном због своје једноставности и ефикасности.
* **DCT (Discrete Cosine Transform) скривање**: ДЦТ користи фреквенцијску трансформацију блокова пиксела у слику. Информације се скривају модификацијом одређених коефицијената ДЦТ-а, чиме се постигнут високи степен сигурности без утицаја на изглед слике.
* **DWT (Discrete Wavelet Transform) скривање**: Ова метода користи таласну трансформацију за слику, расподељујући је у више нивоа фреквенције. Подаци се затим скривају у коефицијентима трансформације, што омогућава већу отпорност на компресију и друге технике детекције.
* **Методе засноване на боји:** Ове методе користе боје пиксела за скривање информација. На пример, информације се могу скривити у засићењу боје или њеним нијансама, што чини промене невидљивим, док слика остаје визуелно непромењена.
* **Методе засноване на текстури:** Ове технике користе карактеристике текстуре слике, као што су градијенти или статистички подаци, за интеграцију скривене поруке. Ове методе су корисне у случајевима када је потребна додатна сигурност, јер мењају текстуралне карактеристике слике, а не само боје или пикселе.

# **Least Significant Bit**

**LSB стеганографија (Least Significant Bit)** је техника која се користи за скривање података унутар дигиталних фајлова тако што се мењају најмање значајни битови њихових елемената. LSB је један од најједноставнијих и најчешће коришћених метода стеганографије због своје једноставности и могућности да неприметно сакрије информације унутар различитих типова медија као што су слике, аудио и видео фајлови.

Како функционише LSB стеганографија?

У дигиталним фајловима, подаци се чувају као низ бинарних бројева (битова), при чему сваки елемент фајла (нпр. пиксел у слици или аудио узорак) има своју бинарну репрезентацију. **Најмање значајан бит** је последњи бит у бинарној репрезентацији неког податка и он има најмањи утицај на стварну вредност тог податка. Промена овог бита има минималан ефекат на коначни изглед или звук медија, што га чини идеалним местом за скривање информација.

Кораци у LSB стеганографији

1. **Припрема поруке за скривање**: Порука која треба да се сакрије (текст, слика, или било који други податак) претвара се у бинарни облик.
2. **Избор медија за скривање**: Изабрани медиј (слика, аудио или видео) служи као "покривајући фајл" у којем ће се подаци сакрити.
3. **Промена LSB-ова**: Сваки бит из поруке замењује најмање значајан бит одговарајућег елемента покривајућег фајла. На тај начин, сваки бит поруке "уђе" у медиј без значајне промене његове структуре.
4. **Генерисање новог фајла**: Резултујући фајл са сакривеним подацима изгледа (или звучи) исто као оригинални фајл, али садржи додатне информације.

## LSBу сликама

Најбољи тип сликовне датотеке за скривање информација је 24-битна (битмап) слика. Када је слика високог квалитета и резолуције лакше је сакрити информације.

На пример, уколико желимо да сакријемо поруку у сваки бајт 24-битне слике, можемо променити 3 бита у сваки пиксел (1 бит у канал сваке боје). Слика димензија 1024x768 пиксела може сакрити 1024 \* 768 \* 3 = 2359296 битова информација, што је 288 KB информација.

Претпоставимо да желимо да сакријемо слобо А. Његов ASCII еквивалент износи 65(10), што је бинарно 01000001(2). За скривање су нам довољна 3 бита. Нека су ти пиксели

(00100111, 11101001, 11001000)

(00100111, 11001000, 11101001)

(11001000, 00100111, 11101001)

Уметањем бинарне вредности слова А у три пиксела даје нам

(0010011**0**, 11101001, 11001000)

(0010011**0**, 11001000, 1110100**0**)

(11001000, 00100111, 11101001).

Само су подебљани битови (3 бита од 9 најмање значајних) променили вредност.

У просеку се користећи ову технику промени само половина најмање значајних битова. Пиксел који се највише променио, променио се за две нијансе, што је у односу на 16,7 милиона нијанси занемарљиво за људско око.

Дакле, ако желимо да сакријемо тајну поруку унутар неке сликовне датотеке, први морамо да пронађемо датотеку. Након одабира датотеке и тајне поруке, бирамо подскуп најмање значајних битова датотеке. Број битова у одабраном скупу одговара броју битова тајне поруке. Тада се неким редоследом сваки тајни бит замењује битом тајне поруке, све док сви не буду замењени.

У најједноставнијем случају LSB технике тајни битови се поставе на најмање значајни бит сваког пиксела по реду.

Да би реконструисао поруку, приматељ мора знати подскуп најмање значајних битова у које је порука сакривена. Техником обрнутом од уметања, „извлачи“ најмање значајне битове, и слаже их правим редоследом, где на тај начин добија поруку.

## LSBу аудио сигналима

**LSB стеганографија у аудио сигналима** подразумева убацивање скривених података у најмање значајне битове дигиталних аудио узорака. Аудио фајлови се састоје од низа узорака који представљају амплитуду звука у одређеном тренутку. Променом најмање значајног бита у сваком узорку, могуће је сакрити информације на начин који није перцептивно приметан за људско ухо.

Како функционише LSB стеганографија у аудио сигналима

1. **Претварање аудио сигнала у дигитални формат**: Аудио сигнал се претвара у дигитални формат (нпр. WAV) који се састоји од низа узорака. Сваки узорак може бити представљен са 16 или 24 бита у зависности од резолуције. У стеганографији са LSB-ом, најчешће се користе аудио формати без губитака (као што је WAV) јер се подаци могу лакше сакрити и остати непромењени.
2. **Припрема поруке за убацивање**: Садржај који желимо да сакријемо (нпр. текстуална порука) се претвара у бинарни формат. На пример, реч "HI" у ASCII коду је 01001000 01001001.
3. **Избор узорака за убацивање**: Порука се убацује у најмање значајне битове узорака аудио сигнала. Најмање значајан бит сваког узорка је бит који има најмањи утицај на стварну вредност узорка, а самим тим и на звучни сигнал.
4. **Процес убацивања**: Приликом убацивања података, LSB метод мења само најмање значајан бит сваког узорка:
   * Узорак се чита и његова вредност се претвара у бинарни формат.
   * Најмање значајан бит узорка се замењује са једним битом из поруке.
   * Нови узорак са изменом се поново складишти у аудио сигнал.

**Пример**: Ако узорак има бинарну вредност 10101100 01110101, и желимо да сакријемо бит 1, променићемо најмање значајан бит првог бајта у 10101101. Резултујући узорак ће изгледати овако: 10101101 01110101.

1. **Чување измењеног аудио сигнала**: Аудио сигнал са сакривеном поруком се чува као нови фајл. Промена једног бита у узорку има минималан утицај на стварну амплитуду звука, што значи да је скривена порука неприметна за људско ухо.

Пример коришћења LSB-а у аудио сигналу

Замислите аудио сигнал представљен низом 16-битних узорака:

11001010 10011011,

10110100 11010011,

01101011 00101001...

Ако желимо да сакријемо слово 'A' (01000001 у бинарном формату), LSB техника би променила најмање значајне битове ових узорака:

1. Први узорак пре измене: 11001010 10011011  
   Први бит поруке је 0, тако да најмање значајан бит остаје 0.
2. Други узорак пре измене: 10110100 11010011  
   Други бит поруке је 1, тако да најмање значајан бит постаје 1, што даје нови узорак 10110101 11010011.

Процес се наставља све док сви битови поруке нису убачени у аудио сигнал.

# **Алати за стеганографију слика**

Постоји неколико популарних алата за стеганографију помоћу слике који се често користе за скривање информација у дигиталним сликама. Ови алати обично пружају различите функционалности и могућности прилагођавања у зависности од потреба корисника. Ево неколико најпознатијих алата за стеганографију слика и како се користе:

* **OpenCV**: je моћна библиотека за обрада слика у Pythonu и C++. Омогућава лако приступање пикселима слике, што је кључно за имплементацију LSB стеганографије. С њом можете манипулирати сликама и скривати податке модификовањем најмање значајних битова пиксела.
* **Python Imaging Library (PIL)**: сада позната као Pillow, је популарна библиотека у Pythonu која омогућава једноставно учитавање, обрада и манипулација сликама. С њом можете лако имплементирати LSB технику како би сакрили поруке у сликама.
* **Matplotlib**: Иако је примарно алат за визуализацију података, Matplotlib омогућава и основну обрада слика, што је корисно за постављање LSB метода у комбинацији са другим библиотекама за рад са сликама.
* **AForge.NET**: је .NET библиотека која пружа алате за обрада слика, видео записа, препознавање објеката и многе друге функционалности. За LSB стеганографију, она омогућава приступ пиxел-левел манипулацији и лако интеграцију у апликације базиране на . NET платформи.
* **StegoTuring**: је специјализован алат за стеганографију који имплементира различите технике скривања података у дигиталним медијима, укључујући LSB. Користи се за едукацију и практичну примену стеганографских метода, а може обрадити слике, текстове и друге формате.

# **AForge.NET**

AForge.NET је open-source библиотека заснована на .NET платформи, намењена првенствено за апликације у областима обраде слика, анализе видео сигнала, вештачке интелигенције и роботике. Ова библиотека пружа бројне алате и функционалности који су веома корисни за имплементацију стеганографских техника, посебно у раду са сликама.

Једна од основних предности AForge.NET библиотеке је њена способност да ефикасно манипулише сликама на нивоу пиксела. AForge.NET омогућава овакву директну манипулацију сликама кроз своје класе и методе за рад са bitmap објектима. На пример, библиотека омогућава лако учитавање слике у меморију, приступ пикселима кроз индексе, као и модификацију RGB вредности пиксела, што су кључни кораци у стеганографији.

Још једна предност AForge.NET библиотеке је њена подршка за широк спектар формата слика, укључујући BMP, JPEG и PNG, што омогућава рад са различитим типовима носилаца тајних података. BMP формат је нарочито популаран у стеганографији због своје једноставне структуре која омогућава прецизну контролу над пикселима без губитака квалитета. AForge.NET олакшава конверзију и обраду слика у овом формату, чинећи је погодном за експерименте и имплементацију алгоритама.

Поред манипулације пикселима, AForge.NET нуди и функционалности за анализу и обраду слика које могу бити корисне за стеганографију. На пример, технике филтрирања и трансформације које библиотека подржава могу се користити за унапређење слике пре уграђивања тајних података, што доприноси бољој неприметности скривених информација. Такође, алат за екстракцију информација може користити методе библиотеке за детекцију и анализу пиксела ради издвајања података из слике-носиоца.

Једна од главних предности коришћења AForge.NET у односу на друге библиотеке је њена једноставна интеграција са .NET окружењем и богата документација. Библиотека омогућава брзо прототиписање и развој апликација, што је корисно за истраживачке пројекте и семинаре. Такође, захваљујући њеној модуларној структури, корисници могу лако комбиновати основне функционалности библиотеке са сопственим алгоритмима за стеганографију.

AForge.NET се може сматрати одличним избором за имплементацију стеганографских техника због своје једноставности, флексибилности и подршке за детаљну манипулацију сликама. Њена примена у овом домену може се искористити за различите сврхе, од основних едукативних примера до развоја сложенијих система за заштиту података путем скривених порука у дигиталним сликама.

# **Закључак**

Стеганографија слика, са посебним фокусом на методу коришћења најмање значајних битова (LSB) и имплементацију кроз AForge.NET библиотеку, пружа снажан оквир за скривање информација унутар дигиталних слика на начин који остаје скривен од људског ока. Током рада, истражена је примена LSB технике као једноставног, али ефективног приступа за манипулацију пиксела, омогућавајући сигурно уграђивање порука у слике без видљивих промена у њиховом изгледу. AForge.NET библиотека, као алат за обраду слика, омогућила је практичну реализацију ових операција и илустрацију стварних примена.

Примена LSB стеганографије има бројне корисне аспекте, укључујући заштиту приватности, размену осигураних информација и уградњу водених жигова за дигитална ауторска права. Ипак, као и све технологије које омогућавају скривање података, овај приступ није без изазова. Потенцијал за злоупотребу остаје стварна претња, јер се може користити за преношење штетног или илегалног садржаја. Зато је кључно осигурати да примена стеганографских техника буде етички и правно усклађена.

Даљи развој ове области може се надовезати на истраживање нових алгоритама, веће отпорности на напредне методе откривања и оптимизацију LSB технике, како би се додатно повећала ефикасност и сигурност решења. Користећи платформе попут AForge.NET, могућности за унапређење и прилагодбу стеганографских решења остају широко отворене, пружајући темеље за још софистицираније примене у будућности.