DOI: https://doi.org/10.12700/btsz.2025.7.4.95

STEGANOGRAPHIC MODELS AND TECHNICAL APPROACHES TO ENCRYPTING DATA EMBEDDED IN IMAGES

SZTEGANOGRÁFIAI MODELLEK, KÉPBE INTEGRÁLT ADATOK TITKOSÍTÁSA ÉS TECHNIKAI MEGKÖZELÍTÉSE

OLÁH Róbert[1] – LŐCSEI Anikó[2]

Abstract

The review of image encryption techniques aims to examine the computer-based analysis of digital images, as well as the theoretical and practical implementation of procedural methods. Image encryption methods are explored with regard to automated image analysis, noise reduction techniques, edge detection, and image classification. The presentation of imaging models related to these methods is interpreted through the analysis of image processing algorithms. The primary research focus is on the depiction of applied code snippets and models that contribute to the practical understanding of the presented methods. The functionality of encrypting data within images is demonstrated through various algorithms, which illustrate not only traditional techniques but also modern machine learning-based approaches. The objective of the research is to demonstrate, based on steganographic image encryption methods, how image processing algorithms facilitate the encryption of information within images, and to contribute to the future development of encryption techniques by introducing the latest research topics.

Keywords

steganography, image encryption, digital image processing, edge detection, noise reduction

Absztrakt

A képtitkosítási technikák vizsgálata a digitális képek számítógépes elemzését, az eljárási technikák elméleti és gyakorlati megvalósításának bemutatását célozza. A képtitkosítási módszerek az automatizált képelemzést, zajszűrési technikákat, a kép éleinek detektálását és képosztályozási technikák elemzését ismertetik. A módszerekhez kapcsolódó képalkotó modellek bemutatása a képfeldolgozó algoritmusok elemzésével értelmezhető. Az elsődleges kutatási szempontok azok az alkalmazott kódrészletek, illetve modellek ábrázolása, amelyek a bemutatott módszerek gyakorlati értelmezéséhez járulnak hozzá. A képben szereplő adatok titkosításának működőképességét szemléltetik a különféle algoritmusok, amelyek, a hagyományos módszerekkel szemléltetik a modern gépi tanuláson alapuló megközelítéseket is. A kutatás célja a szteganográfiai képtitkosítási módszerek alapján bemutatni, hogy a képfeldolgozó algoritmusok alkalmazásával hogyan válik lehetővé a képben lévő információk titkosítása, legújabb kutatási témák ismertetésével hozzájáruljon a titkosítási eljárások jövőbeli fejlesztéséhez.

Kulcsszavak

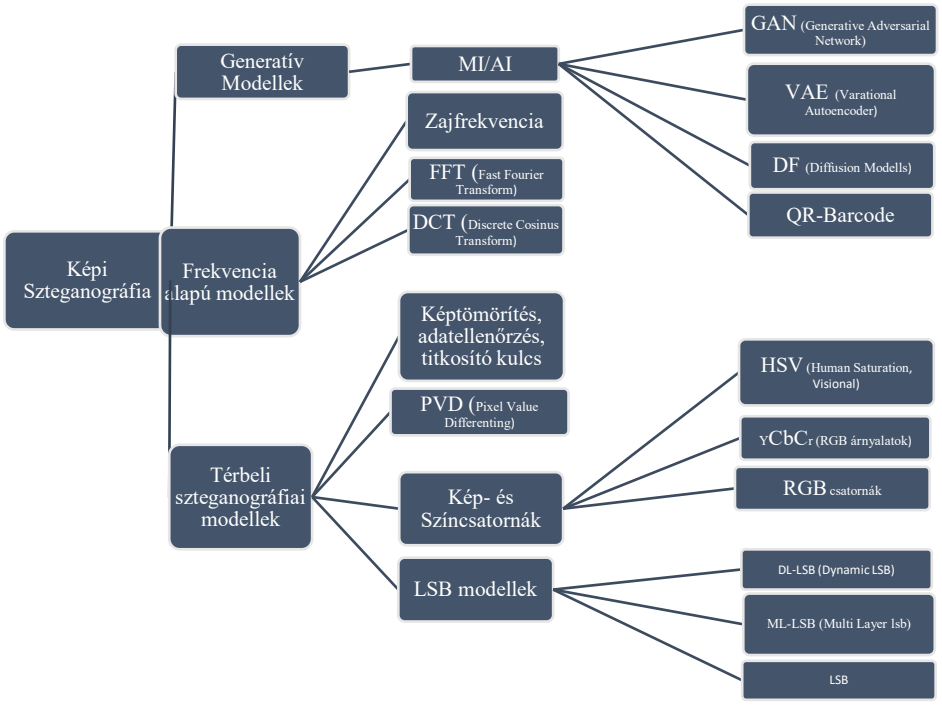
szteganográfia, képtitkosítás, digitális képfeldolgozás, élkiemelés, zajcsökkentés

[1] olah.robert@eotvostechnikum.hu | ORCID: 0009-0007-9134-9521 | IT teacher, Educational Center of Érd | Informatika oktató, Érdi Tankerületi Központ

[2] locsei.aniko@bparchiv.hu | ORCID: 0009-0005-7070-1982 | chief archivist, Budapest City Archives | főlevéltáros, Budapest Főváros Levéltára

BEVEZETÉS

A kezdetlegesen alkalmazott, de jelen időben már generatív technikával is rendelkező képtitkosítási eljárás a digitális adatvédelem és biztonsági során is jelentős szerepet kap. Az adatbiztonság fontosságával a képek titkosítási technikái és a digitális információk védelmének kutatási területei folyamatosan frissülnek. A technológiai területeken megvalósuló fejlődés lehetővé teszi a folyamatosan fejlődő gépi tanulás alkalmazásával szükségessé vált hagyományos és a kortárs képtitkosítási technológiák időrendszerű vizsgálatát. A képi információk titkosítási módszereinek áttekintésével lehetővé válik a modellek elméleti és gyakorlati megközelíthetősége és a képek biztonságos adatkezelése. A képek információbiztonsági szerepe és a digitális adatvédelem hozzájárul a szteganográfiai modellek új fejlesztéséhez és technológiai megoldásához. A mellékelt ábra alapszintektől a felső szintekig ismerteti a képi rejtési technikákat és a hierarchia felső szintjén lévő Mesterséges Intelligencia generatív modelljeit, ahol az intelligens adatbeágyazású MI/AI képbe integrált információk beágyazását ismertetjük. A térbeli módszerek során a Least Significant Bit (LSB), annak továbbfejlesztett rétegelt, multi layer ML-LSB és az adatptív dinamikus LSB modellek elemezzük. A térbeli modelleket kiegészítjük a kép-és színcsatornák váltakozási, a képpont módosítási eljárással a Pixel Value Differencing-gel (PVD). A frekvenciaalapú technikák alkalmazása mellett a koszinusz-függvény alapú Discrete Cosine Transform (DCT) és a Fourier alapú transzformációs modellek zaj- és frekvencia alapú megközelítését és a mindennapok során használt QR-Barcode képen belüli adatok vonalkód, vagy leolvasási technikát is bemutatjuk.



1. Ábra: a tanulmányban szereplő modellek folyamatábrája LSB legalsó szintjeitől a Generatív-AI modellekig, saját szerkesztés

A SZTEGANOGRÁFIA EREDETE FELHASZNÁLÁSI TERÜLETEI

A képi információk elrejtésének korai technikái és fejlődése

A szteganográfia szó elsődleges források szerint görög eredetű *s*tegein *„**στεγεῖν**”* igéből származik, melynek jelentése, hogy "fedni, rejteni", míg a szintén görög eredetű graphē *„γραφή”* szó a leíró tudományok általános neve, és azt jelenti, hogy "írni"[1]. Hérodotosz, görög történetíró nyomán feljegyzett történet a fogvatartott Demaratosz, spártai király nevéhez köthető. A perzsák általi hadműveletről, nyílt üzenetet nem küldhetett. Xerxész, perzsa király általi támadás hírét egy fatáblára vésve juttatta el, amelyet viasszal fedett le. A táblán lévő üzenet a hő hatására lett látható[2]. A kommunikáció fejlődésével új lehetőségek nyíltak meg az adatok képi titkosításához. A papiruszt felváltó pergamen új távlatokat jelentett a steganogramok elrejtéséhez, amely a szteganográfiai algoritmusok létrejövetelét eredményezte. A Kínában feltalált vízjelezett papírt, amely egyfajta eredet-hitelesítési és hamisítás elleni védelmi szerepet töltött be, Európa céhes iparágaiban és kereskedelmi forgalomban vagy okleveleken használták. A középkori módszerek közé tartozott az akrosztichon, a rejtett üzeneteket sorok vagy fejezetek kezdőbetűi tartalmazták. Az ipari forradalom idején újabb kommunikációs formák, az újságok töltötték be a titkos adathordozók szerepét, újságkódok nyomán lyukasztással emelték ki a betűket. A 20. század háborús időszakában a szteganográfia jelentős változáson ment keresztül. Az első világháború során az ún. láthatatlan tinták használata jelentette képi titkosítást, amelyek speciális vegyszerek, fényforrás segítségével váltak olvashatóvá. A második világháború során továbbfejlesztették a módszert mikrofilmek és azok mikro pontjainak használatával, amelyeken kisméretű üzeneteket rejtettek el. Katonai hírszerzés eszközeként szabad szemmel nem voltak láthatók az információk.[3] A szteganográfiát leginkább katonai parancsok, diplomáciai információk és kémkedési adatok elrejtéséhez használták információbiztonsági alapon, a szembenálló fél megtévesztéséhez. Az alábbi műszerek a képi információ kezelésének és vizualizációjának történeti előzményeit szemléltetik, a képi információk mechanikai adatfeldolgozásától a digitális grafikus rendszerekig.

2. Ábra: Lyukkártya és leolvasókészülék (IBM, 1950-1960):A képi információ kódolásának korai formája, ahol az adat mintázatban jelent meg, MKKM Műszaki Tanulmánytár, saját kép

3. Ábra: Telesis grafikus munkaállomás (Angliai modell Elektronikus Mérőkészülékek Gyára, 1985): A munkaállomás (1980) a CAD-CAM szoftverek és a digitális plotterek segítségével precízen kezelte a képi adatokat, lehetővé téve azok manipulálását, hogy az információk rejtett módon kerüljenek beágyazásra a digitális képekbe, MKKM Műszaki Tanulmánytár, saját kép

A képi adatok titkosítása és a mesterséges intelligencia (MI/AI- generatív modellek)

A létező szteganográfiai rendszerek a szöveg (PDF), a hang (visszhang alapú módszer), illetve a hálózati (IP fejlécekben rejtett információ) alapú eljárások közül jelen tanulmányban a képi szteganográfiai modelleket ismertetjük. A képi szteganográfia módszere eltérő a szintén rejtett információátadási technikával, a kriptográfiával, amely az üzenet értelmezhetőségét védi, annak visszafejtése egy megfelelő kulccsal lehetséges. A szteganográfia egy látható képen belül magát az üzenetet rejti el, legfőbb célja, hogy az információt semmilyen eszközzel ne lehessen azonosítani. A folyamat hatékonyságát az alábbi tényezők alapján korábbi kutatások és a mai gyakorlat is figyelembe vesz:

- **láthatósági intenzitás** (PER), amely a rejtett adat észlelhetőségét jelzi, túl sok adat beágyazásánál a kép minősége romlik
- **felfedhetőség** (DET), amely a képben titkosított adatok észlelhetőségét jelenti
- **erősségi faktor** alapján (STR), amely a képek feldolgozása során való sértetlenségét és tartósságát biztosítja
- **kompatibilitás** (COMP) és a **fájlformátum-függőség** (DEP) olyan tényezők, amelyek a titkosítás módszereinek alkalmazhatóságát és a képi formátumok közötti eltéréseket is figyelembe veszik
- **domain típus** (DOM) meghatározza, hogy az információk a képen térbeli vagy transzformációs tartományban kerülnek elrejtésre, ami különböző biztonsági szintet biztosít

A képbe ágyazott információ a kivonási folyamat során visszaállíthatjuk megfelelő kulcs, vagy algoritmusok alkalmazásával. Bizonyos rendszerek automatikus titkosítási módszert alkalmaznak, így az üzenet is titkosítottá, illetve visszafejthetővé válik.[4]

A mesterséges intelligencia képi alkotások algoritmusa

A mesterséges intelligencia napjaink egyik legfontosabb fejlődési területe. A mesterséges intelligencia alkalmazások már részben az életünk részévé vált. Ebben a publikációban azokat az algoritmusokat tárgyaljuk, amely alkalmazható a digitális képfeldolgozásra, amely hatással van a képi objektumok felismerésére is, az adott kép információ elrejtésében és visszafejtésében.

A diffúziós modellek (*Stable Diffusion*, *DALL·E 3*, *Midjourney)*

A diffúz modellek (különösen a Stable Diffusion) alkalmasak a képfelismerésre, osztályozásra, képelemzésre, és az adott objektum beazonosítására, többféle modellt vizsgáltunk meg.

Generatív modell:

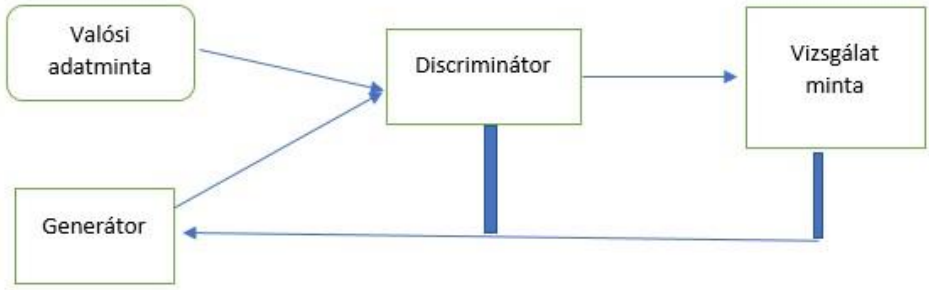
- GAN (Generative Adversarial Network)
- VAE (Variational Autoencoder)
- Diffusion modellek (pl. *Stable Diffusion*, *DALL·E 3*, *Midjourney*)

A generatív modell alkalmas új képek létrehozására és az adott képnek az elemzésére. A GAN modell egy neurális hálózati rendszer, amely alkalmas képgenerálásra és képfelismerésre. A GAN működése egy véletlenszerű rajzból egy valósághoz hasonló képet próbál létrehozni. A diszkriminátor szerepe pedig annak eldöntése, hogy kép valós vagy hamis a képosztályzás segítségével. A GAN a neurális hálózatoknak van egy olyan osztálya, amelyet a felügyelet nélküli tanulásra használnak.

Működése:

- Generatív: Ez valószínűségi modell felhasználásával írja le az adatok generálásának módját
- Adverzális: Itt történik a modell betanítása
- Neurális hálózat: Az MI algoritmusok használata

A Generative Adversarial Network tartalmaz generátort és egy diszkriminátort. A generátor mintákat generál, ami lehet a képi információ, ami lehet igazi vagy hamis.



4. Ábra: Generative Adversarial Network, saját szerkesztés

A diszkriminátor a fenti ábra alapján ez a Generative Adversarial Network versenyalapon működik. Az adatok elosztása rögzítve van, betanított állapotban célja az, hogy a diszkriminátor hibázásának a valószínűségét maximálisan növelje.

Ezzel szemben a dikszkriminátor becsléssel azt vizsgálja, hogy a kapott adatok tanulóadatok-e, és az adatok származását elemzi, hogy azokat honnan kapta. Megállapítottuk, hogy mindkét modell versenyalapon működik mert egymás jutalmát próbálják minimalizálni, de a modellek a saját jutalmukat pedig maximalizálni kívánják.[5]

TÉRBELI SZTEGANOGRÁFIAI MODELLEK

Képi információk titkosítása bit szintű képmódosítás alapján; Least Signification Bit

A képi szteganográfia legelterjedtebb adatrejtési technikája a LSB módszer, amely újabb fejlesztések nyomán egy másik algoritmussal párosítva hatékonyabb eredményeket közvetít. A kutatás során vizsgáltuk, hogy a hagyományos LSB-t a F4 (Filtering szűrési) algoritmussal, egy fejlettebb technikával párosították, amely titkosított adatokat a kép minőségének megőrzése mellett biztosította. Ennek eredményeképpen a LSB-ben (a kép legkisebb információegysége), az adatrejtés a több színcsatornából (RGB) álló látható fedőkép térbeli tartományának, vagyis képszínek manipulációjával valósul meg. A titkosított adatok úgy ágyazódnak be, hogy a képen látható változás minimális marad.

A LSB módosításakor az adatrejtés során a kép pixeleiben használt bitek számát a K-érték határozza meg. Ha a K-érték nő, akkor a bitek is jobban váltakoznak, így rejthető el nagyobb mennyiségű adat, változhat meg jobban egy kép minősége és válhat könnyebbé a titkosított adat észlelhetősége is. K = 1 (csak az egyes pixel, az LSB módosítása történik meg) K = 2 (az LSB és a 2. legkisebb bit is változik, így nagyobb mennyiségű adat rejthető el, de a kép minősége torzulhat.

- Az elrejtendő információ K-bites egységei meghatározott sorrendben kerülnek beágyazásra a kiválasztott fedőkép pixeleinek legkisebb helyiértékű bitjeibe.
- A fedőkép a RGB színmodell három csatornából épül fel, ahol mindegyik csatorna meghatározott (6, vagy 8) bites értékkel jellemzi a színintenzitást; ezek legkisebb bitjei használhatók az adatrejtésre.
- A LSB helyettesítése egy algoritmus alapján történik, ahol az elrejtendő üzenet bitekre bontva kerül titkosításra, így az összes képpont legkisebb helyiértékű bitje a titkos üzenet egy-egy bitjével kerül helyettesítésre. Bináris formátumú kódolás esetén a számítógép adatként, pl. képpont-értékként kezel és értelmez, a kép vizuálisan nem változik, de az információ rejtve marad.
- A visszafejtés során a LSB-bitek kiolvasásával az üzenet visszaállíthatóvá válik; a módszer előnye, hogy a módosított kép azonos marad az eredetivel.[6]

Többrétegű bitrejtési módszer értékelése, Multi Layer LSB (ML-LSB)

A képi titkosítás hatékonyságát és adatbiztonsági funkcióját a Friedrich-modellel, három kritérium alapján szemléltethetjük: a megfelelő kapacitás, robusztusság és a vizuális észlelhetőségi faktor alacsony szinten tartásával. A robusztusság (ellenállóság): a képben lévő titkos adat sértetlenségét külső manipulációk (tömörítés, átméretezés, zajok hozzáadása), a kapacitás pedig a biztonságosan elrejthető adatok mennyiségét határozza meg. LSB esetén: csak az utolsó bitet használja, egy rétegben 1 bit/pixel kapacitást biztosít (512×512 kép esetén kb. 32 KB), míg a ML- LSB több réteg alsó bitet használ, így nagyobb adat rejthető el (64 KB), de a kép torzulása is növekszik. Az észlelhetőség: a rejtett információ láthatósága LSB esetén kevesebb bit módosul, nehezen észlelhető, míg a MLSB több

réteg bitet változtat, a felismerhetőség kockázata nő, a változás sima képeken könnyebben, míg zajos részletgazdag képeken nehezen észlelhető. A többrétegű LSB több LSB réteget alkalmaz az adat elrejtéséhez, hogy növelje a hordozó biztonságát és adatkapacitását (10 KB helyett 12 KB). A többrétegű LSB-t matematikai modellel ábrázolhatjuk *s* és *k* rétegek számításával:

Változók	Rétegek mutatói	eredmény s=1	eredmény s=2
s	beágyazódási szintek	s=1	s=2
b	pixel színmélység értéke	b=24 bit	b=24 bit
a	bitek/pixel száma	a=1	a=2
m	sorok száma	512 pixel	512 pixel
n	oszlopok száma	512 pixel	512 pixel
k	rétegek száma	1 db	1 db
C'	C' (egyrétegű kapacitás)	32 KB	64 KB
C	C (többrétegű kapacitás)	32 KB	192 KB
K%	K% (kapacitás növekedés)	0%	200%
r	r (adat arány)	4.17%	25 % adat

1. Táblázat: Egy 512x512 színes, 24 bites kép egyenletek alapján számolt értékei, forrás: "Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach", saját szerkesztés

- Beágyazási szintek **s**: egy adott kép titkosításához szükséges rétegek száma, figyelembe véve a kép méretét, a használt beágyazott biteket „a" és a pixelbitek „b" számát adja meg, M a képméret, N az adatmennyiség, k a rétegek száma, alapján:

$$s = log_b^a\ (M, Nk)$$

- Többrétegű módszer c: a képletben **c** az elrejtett adat teljes mennyisége, **s** a titkosítási rétegek száma és az előzőekben említett paraméterek összeadása alapján, a kapacitás növekményét mutatja a titkosítási rétegek számának növelésével:

$$c = \sum_{n=1}^{s} \left(MNk \left(\frac{b}{a}\right)^n \right)$$

- Az egyrétegű titkosítás(C'): a fedőadat kapacitása mutatja, a beágyazható adat mennyiségét mutatja egy egyrétegű módszer alkalmazása esetén:

$$C' = MNk \left(\frac{b}{a}\right)$$

- Kapacitásnövekedés mértéke-K% aránya: a kapacitás növekedését mutatja meg, amit az ML-LSB módszer alkalmazásával érhetünk el az alap LSB módszerhez képest:

$$K = \frac{C - C'}{C'}\ x100$$

- Rejtett adat aránya: a képlet a rejtett adat arányát mutatja meg a teljes fedőadathoz képest:

$$r = \frac{C}{MNK} x100$$

A képi adatstruktúrához kötött értelmezést az egyenletben szereplő változók segítik az egy és többrétegű LSB leírásánál.[7]

Képi titkosítás adaptív pixel értékekkel-Dinamikus LSB (D-LSB)

A LSB továbbfejlesztett, adaptív változata a D-LSB, amellyel a kép a vizuális minőséget őrizhetjük meg, míg a rejtett adat mennyiségét maximalizálhatjuk. A dinamikát a kép egyes részeibe rejtett adatok bitjeinek cseréje jelenti LSB legkisebb utolsó bitjei helyett. A LSB dinamikája a pixel kontrasztjában keresendő, amelyben nem társul minden adott pixelhez ugyanannyi bit, ezért alacsony kontrasztnál több, magasabb esetén kevesebb kép vizuális minőségét befolyásoló bit változik. A D-LSB módszert összehasonlítottuk a LSB alapú Binary Image Text-tel (BITS), adattitkosítási módszerrel, melyben az elrejtett információt a kép különböző részein helyezi el. A D-LSB mellőzi a statikus szabályszerűséget, a BITS fix elhelyezési mintát követ, ahol az elrejtési módszer nem adaptív, meghatározott struktúrát követ. A D-LSB módszerekben az elrejtett információ helye nem fix, a titkos üzenet jellemzői vagy a képpontok tulajdonságai alapján változik. A BITS technikában az információ a kép különböző részein helyezkedik el, az éles átmenetek nem látszanak, a detektálhatóság csökkentett mértékű, de az elrejthető adatmennyiség növelhetővé válik. A szakértők a módszert a Wavelet Obtained Weights (WOW) szteganográfiai algoritmusokkal fejlesztették tovább, amely intelligensen alkalmazkodik a kép helyi kontrasztjához, ezáltal megőrizve vizuális minőségét és biztosítva a beágyazott információk integritását. Mindenre kiterjedő, alapos tesztelést követően a csúcsjelzés-zaj arány (PSNR), a strukturális hasonlósági index mérés (SSIM), a bit hibaarány (BER) és az átlagos négyzet alakú hibamérés során (MSE) – 87 %-os megközelítést ért el a stego-kép az eredeti képhez való viszonyításkor.[8]

LSB típusa	Tulajdonság	Előny	Hátrány
LSBT	üzenet bitek legkevésbé jelentős bitekbe kerülnek	egyszerű, gyors	Kevés adat rejthető el, könnyen kimutatható.
ML-LSB	üzenetbitek több rétegben helyezkednek el a képpontokban	több adat rejthető el	képminőség romlása láthatóbb
D-LSB	üzenetbitek dinamikusan, adattípusnak megfelelően helyezkednek el (adaptív rendszere miatt hatékonyabb)	több adatrejtés, jobb minőség	bonyolult, lassabb művelet

2. Táblázat: A képi szteganográfia térbeli LSB modellek összehasonlításáról, saját szerkesztés

Kép- és színcsatornák váltakozása (HVS, YCbCr, RGB)

Vizsgálatunk a képi szteganográfia legfontosabb alapjaira, a kép élességére és az abban elrejtett információ láthatatlanságára összpontosít. A kép a színcsatornák váltakozása és manipulációja révén a humán vizuális rendszer (HVS) érzékenységéhez igazodik. A HSV modell kis méretű képeknél jobb vizuális eredményt ad, mint a YCbCr, mert a módosítás

kevésbé torzítja a minőséget. A fényerő (Value) különválik a színektől (Hue Saturation), így a rejtett információ kevésbé torzítja a képet. A YCbCr modellben Y – luminancia, fényerősség, Cb (Blue Chroma –kék, illetve Cr –Red Chroma- vörös színárnyalatok, amelyek a fényerőt és a színárnyalatokat külön kezelik. A modell hatékony az információ elrejtésére, de a színcsatornák energiaszintje érzékeny, kisebb színinformációkal rendelkező képeknél torzításokat okoz. Az RGB modell nagyobb formátumú képek esetében energiahatékonyabb és stabilabb.[9] A különböző színmodellek a beágyazás során módosult változatokat mutatnak. A RGB – minden csatornája (vörös, zöld, kék) egyenlő szerepet kap a nagyobb képeken stabilabb teljesítményű, minimális torzulási eredménnyel. A három csatornás módszerben az egyik csatorna utolsó két LSB-je jelzi, hogy a további két csatorna tartalmaz-e adatot. A csatornák sorrendje minden 3. pixelnél ismétlődően változik. A módszer hátránya, hogy a kapacitás a jelzőbit értékétől, átlagosan 3 bit/pixel értéktől függ.

Pixel sorszáma	R-csatorna	G-csatorna	B-csatorna
1	I	adattároló 1.	adattároló 2.
2	adattároló 1.	I	adattároló 2.
3	adattároló 1.	adattároló 2.	I

3. Táblázat: RGB csatornák beosztása pixelindikátorok szerint. I = Indikátor csatorna, adattároló 1, 2 = a pixel azon csatornái, ahol a titkosított adat el van rejtve, saját szerkesztés

A módszer továbbfejlesztett változata a Triple-A algoritmus, amely az AES szimmetrikus titkosítást és pszeudorandom számgenerátort (PSNG) használja a színcsatornák véletlenszerű kiválasztásával. Két véletlenszám (Seed1, Seed2) határozza meg a beágyazás helyét és a beilleszthető bitek számát, így a biztonság és kapacitás egyaránt növekszik.[10]

PVD (Pixel Value Differencing), a képpont alapú értékkülönbségek a szteganográfiában

A ML-LSB és DLSB módszerek utáni leghatékonyabb eljárás az adatelrejtést és a kép minőségének megőrzését illetően a PVD. Módosított változataival a képek pixelértékein belüli hatékony dinamikus adatrejtést tehetjük lehetővé. Fejlesztett változata a hibrid PVD és az LSB technikák kombinációja, így a bitek szélterületeinek kihasználásával a beágyazási kapacitás is hatékonyabbá vált. A TPVD (három-pixel érték technikájú alkalmazás) a meglévő értékek különbségéttől teszi függővé a beágyazás minőségét. A hagyományos PVD statikus alapú módszer értékerősségét fokozta a PVD flexibilis változata a MFPVD (Modified Flexible PVD), amelynek legfőbb tulajdonsága a rugalmas paraméterek, a képi minőség és színpontosság megőrzése. A fejlesztési eredmények ellenállók a képbe integrált adatok megfejtésekor a RS (Regular Sampling) rendszerességen alapuló elemzés során. A PVD célja hogy a pixel értékeiben hatékonyan megőrizze a beágyazott információt, mert a hatékonyságot vizsgáló módszerek, például a Wavelet Steganalízis (WS) és a PDH (Pixel Differenciás Hisztogram) a képen belüli apró eltéréseket és a színek közötti eltérő mintákat ismerik fel. A kezdetleges PDH a pixelérték különbség sebezhetőségét méri. MatlabR2018 segítségével létrehozott kísérleti környezetben 1000-10000 véletlenszerű kép válogatásával a képosztályokat négy osztályra csoportosították, gyanús-stego kép, valódi-borítókép és ezek kevert változatai alapján.[11]

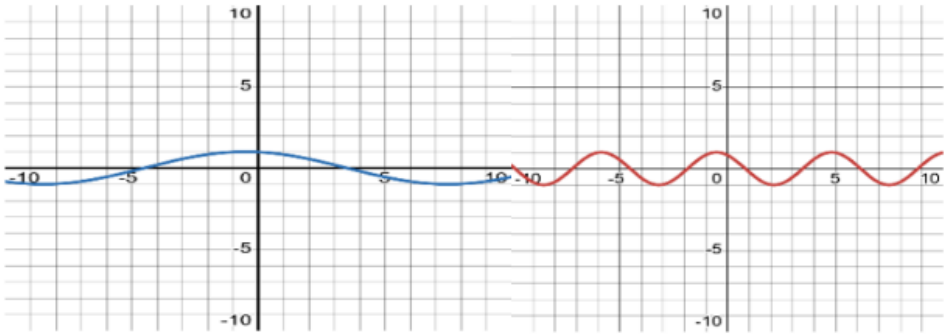
Az adatok biztonságos beágyazása a stego-kép magas vizuális minőségétől függ. Az adatok kinyerését egy indikátor pixeltől (IP), tehetjük függővé. Az IP egy kulcsjelző

pixel, ami megmutatja, hogy *honnan és hogyan* tudjuk az adatokat kinyerni. A borítóképbe való beágyazása előtt a titkos adatoknak megfelelő pixelek sorrendje módosul és átrendeződik. Adatbiztonsági szempontokat figyelembe véve a képpontok sorrendjét és beágyazás szempontjából fontos paramétereit egy Genetikai Algoritmussal (GA) optimalizáltan módosítjuk és rendezzük át. A folyamat célja a legalkalmasabb képi pixelpozíciók kiválasztódása. A legújabb fejlesztések algoritmusok és keresztezett PVD módszerek alapján, így a GA-IPVD egy, amely a beágyazott adatok biztonságos rejtésére összpontosít és garantálja a kép minőségét. A módszer a különböző stego-támadásokkal szemben ellenállást mutatott, beleértve a hisztogramot (PDH), valamint a rendszeres és egyedülálló (RS) elemzéseket.[12]

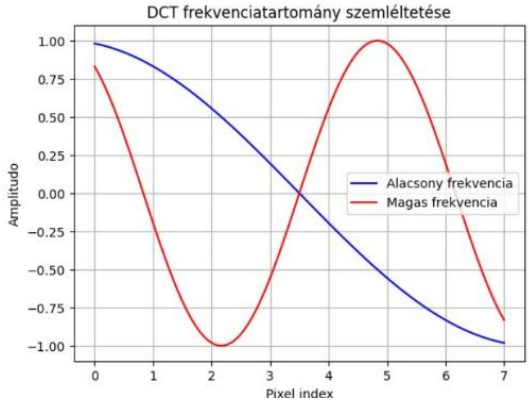
FREKVENCIA-ALAPÚ KÉPREJTÉSI MODELLEK

Diszkrét Cosinus Transzformáció, Fast Fourier Transzformáció, zajfrekvencia

Míg a PVD a képpontok intenzitáskülönbségeire épít, addig a transzformációs modellek frekvenciatartománybeli feldolgozással növelik a hatékonyságot, ahol az együtthatók viszonya és a referencia-minták biztosítják a stabil adatbeágyazást. A DCT az 1970-es évek végétől ismert képtömörítési eljárás. A szakértők a transzformációs technikát a 8x8 soros blokkokra alkalmazták, ahol a kiválasztott együtthatókat rendezett párokba csoportosították. Minden párba egyetlen vízjel-bitet kódoltak referenciaminták alapján: ha az első együttható nagyobb a másodiknál, 1 bitet, ha kisebb, 0 bitet jelöl, egy minta két együtthatója 1 és −1. Az együtthatók értéke a képpel összevetve jut eredményre, az előjelek mutatják, hogy az első együttható nagyobb-e a másodiknál. A Watson (David J. Watson) perceptuális modellje az észlelési kísérletben elsőként a referencia mintát alakítja át DCT-ben, ahol a kép ábra-komplexitás, színek, és fényerősség frekvenciájával optimalizál egy képet. A módosított komponensek szabályozzák, hogy hol tudjuk jobban elrejteni az adatot, amelyek a formált mintát a térbeli tartományba helyezik vissza, hogy azt a képbe ágyazhassák. Nem lineáris adatnyerési folyamat, így a Gauss-féle (harang-görbe) eloszlással a középtartományban lévő adatokban a kódolt bitek statisztikai módszerekkel könnyen kinyerhetők.[13] A DCT a kétirányú koszinusz függvények kombinációját használja a 8×8-as blokk frekvenciáinak bemutatására. Az ábrák a blokk komponenseit szemléltetik, az x- és y-irányú koszinuszokat külön hullámként:



5. Ábra: kétirányú függvények hullámábrázolása, a bal oldalon lágy, alacsony frekvenciájú, míg a jobb oldalon egy zajosabb, magasabb frekvenciájú hullámok különbsége a frekvencia növekedésében rejlik, amely a DCT alkalmazásával érzékelhető, desmos-graph: saját szerkesztés



6. Ábra: A mindkét irányban (x és y) ábrázolt koszinusz függvények mutatják, hogyan hatnak a különböző frekvenciák az 8×8-as blokk komponenseire a diszkrét koszinusz transzformáció során, jupyterlite.github.io/demo/lab/index- Python kernel backed by Pyodide: saját szerkesztés

A DCT-transzformáció az egyik legelterjedtebb frekvencia-alapú módszer a sztenográfiában, energia-tömörítési tulajdonságával a jel energiáját néhány jelentős együtthatóban koncentrálja. A jelentéktelenebb együtthatókat felhasználhatjuk a titkos adatok elrejtésére a jel minőségének romlása nélkül. A DCT a kép az alacsony frekvenciákat a térbeli tartományából a frekvenciatartományba, míg a nagyfrekvenciás összetevőket a kisebb és kevésbé érzékelhető értékekre állítja, így biztonságosan módosíthatjuk a titkos adatok beágyazására. A kép vizuális érzékeléséért felelős nagyfrekvenciás, rejtett adatokat tartalmazó együtthatók módosíthatók anélkül, hogy a változás észlelhető lenne. A következő képletek a DCT alkalmazását mutatják a jelek frekvenciakomponensekre bontásakor, a titkos információk különböző frekvenciákba való beágyazásánál. Elsőként egydimenziós DCT képletet használunk, a jel frekvenciakomponensekre való bontásához, egy sor vagy oszlop itt N a minták száma (azaz a jel hosszúsága), **k** az adott frekvenciaindex:

$$\mathrm{X}[k] = \sum_{n=0}^{N-1} x[n] \cos\left[\frac{\pi}{N}\left(n+\frac{1}{2}\right)k\right], \quad ahol\ k = 0,1,\dots,N=-1$$

A kétdimenziós DCT, amelyet képek esetén alkalmazunk, az alábbi módon számíthatjuk ki a képi frekvenciákat:

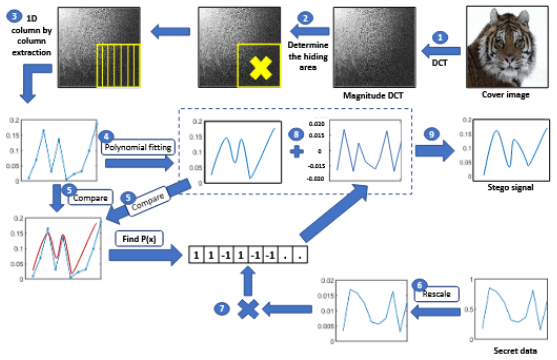
- M **és** N a bemeneti kép dimenziói:
- u**,** v a frekvenciaindexek
- x,y = eredeti kép képpontjainak értékei:

$$\mathrm{X}[\mathrm{u},\mathrm{v}] = \sum_{\mathrm{x}=0}^{\mathrm{M}-1}\sum_{\mathrm{y}=0}^{\mathrm{N}-1} \mathrm{x}\left[\mathrm{x},\mathrm{y}\right] \cos\left[\frac{\pi}{\mathrm{M}}\left(\mathrm{x}+\frac{1}{2}\right)\mathrm{u}\right] \cos\left[\frac{\pi}{\mathrm{N}}\left(\mathrm{y}+\frac{1}{2}\right)\mathrm{v}\right]$$

Az első summáció **x** indexe, a **x=0** értéktől **M-1**-ig terjed, a második **y** indexét használja, és **y=0** értéktől **N-1**-ig terjed, a summáció az alacsony frekvenciájú jellemzőket, hátteret, éleket mutatja, a koszinuszok a képen változó frekvenciákat.

A titkos adat beágyazásának folyamata oszloponként zajlik. Az algoritmus a 2D-DCT alkalmazásával először a fedő képből kinyeri a DCT koefficienseket, majd a titkos

jelet a polinomiális modellel kombinálja. Az inverz DCT -vel visszaállítja a stego képet, így a titkos információ rejtve marad:



7. Ábra: Az embedding algoritmus, oszlopról-oszlopra haladva. Rabie T.,Baziyad M., Kamel I.: High-Fidelity Steganography: A Covert Parity Bit Model-Based Approach, 9.pp

- 1-4 lépések: fedő kép és titkos információ behelyezése, polinomiális fok és skálázási tényezők megállapítása
- 5-9 lépések: a 2 Dimenziós DCT-t a fedő képre helyezik, majd a titkos képet lecsökkentik a skálázási tényezővel a DCT oszlopok kinyerése után minden oszlopon polinomiális modellezést alkalmaznak, amelyhez hozzáadják a titkos üzenetet
- 11-16 lépések: csoportosítják az oszlopokat és visszahelyezik őket, majd az inverz DCT-t alkalmazzák a stego kép előállításához.[14]

FFT (Fast Fourier Transform) alapú szteganográfia

Az FFT hasonlóan működik a DCT-hez, de a Fourier-transzformációt alkalmazza a képen. Az elrejtett adatokat a kép frekvenciatartományában található magas frekvenciájú komponensekben rejthetjük el, amelyek kevésbé észrevehetők a szem számára.

A Fourier-transzformáció egy olyan matematikai módszer, amely alapján az adott jel vagy függvényt át tudjuk transzformálni időtartományból frekvenciatartományba.

$$F(w) = \sum_{-8}^{8} f(t) e^{-iwt} dt$$

Ahol:

- f(t)f(t)f(t) az időbeli jel,
- F(ω)F(\omega)F(ω) a frekvenciatartományban lévő transzformált jel
- ω\omegaω a szögfrekvencia (ω=2πf)
- i az imaginárius egység.[15]

A képfeldolgozás igen fontos technika, mert többféle alkalmazási területe van, pl. a röntgenfelvételek képi információ vagy fényképezőgéppel elkészített kép képi információ feldolgozása. Vizsgálatunk az adott képi szűrők alkalmazására tér ki, hogy hogyan változik a kép, a jó minőségű megtartása mellett. A Fourier-transzformáció algoritmusai segíthetnek a hatékony képfeldolgozásban. Egy adott kép feldolgozása során többféle képi szűrő algoritmusát alkalmazhatjuk, amelynek keretében fontos a képminőség javulása pl.: a képélesítési algoritmussal és a zaj eltávolításával, ha van a képen. A képfeldolgozásban vizsgált frekvenciatér segít megérteni és megváltoztatni az adott kép frekvenciatartományát. Míg a

képeket a vizualitás szemszöge szempontjából a pixelek érétkei alapján vizsgáljuk, a Fourier transzformációs módszerrel a képet egy frekvencia terében értékelhetjük. Vannak alacsony frekvenciák, amelyeken az adott képet egy lassú és fokozatos átmenetek kísérik, míg ha a magas frekvenciát tekintjük, akkor a képi élek textúrák gyors változásai követhetjük nyomon.

A Fourier-transzformáció igen fontos szerepet játszik, különösen a Fast Fourier Transzformáció a digitális szteganográfiában, amely alapján egy adott frekvenciatartományban a jelet változtathatjuk is az információ elhelyezése vagy kinyerés mentén. A Fourier-transzformáció alkalmazása során a digitalizált kép vagy hang frekvenciakomponensekre bomlik. A frekvenciák lehetnek magas és alacsony szinten. Azt az információt, amit szeretnék elrejteni a magas frekvenciába ágyazzák be, tekintettel arra hogy ez biztonságosabb mert az emberi hallószerv, nem érzékeli megfelelően a változást. Megkülönböztetünk kép és hangalapú titkosítást. A Fourier transzformációnak köszönhetően megkülönböztethetünk képi és hangalapú szteganográfiát. A FAST Fourier Transzformáción alapúló változtatás során, a képi színintenzitások szempontjából kisebb változást tehetünk azokon a képi komponenseken amelyek, a magas interferencia tartományú értékeket képviselik. A kép tartalma nem változik, de a titkosítandó adat rejtve marad a képen. A hangsztenográfia esetében a magas frekvencia hangok változtatására fokuszálunk, van olyan hangminta, amely mint zaj, az emberi érzékszerv a fül nem érzékel, mert egy olyan frekvencia tartományba esik, amely nem hallható, és ott van az a pont, ahol az információ elrejtése valósul meg. Azonban mint mindennek vannak előnyei és hátrányai. Vizsgálva a Fourier algoritmust lehetőségünk van adatokat elrejteni torzulás nélkül, mivel a változások frekvenciatartományban történnek meg. A jelet nem szabad túlzottan módosítani, mert a rejtett adat sérülhet, és a kívánt információ visszanyerése nehezített lesz.

8. Ábra: eredeti kép, Gauss elmosás, gimp, saját szerkesztés

Itt az eredeti képet elsőször a frekvencia tartományba alakítottuk a diszkrét Fourier transzformációval DFT segítségével. A DFT és FFT összehasonlítva az FFT jobb hatékonyságot mutat, a számítási módban is. A Léna-képet (8. ábra) FFT alkalmazásával frekvenciatartományba alakítottuk egy felül áteresztő szűrőt alkalmazva, hogy az alacsony frekvencia összetevőket kiszűrjük, kiemelve az éleket és a képen látható finom részleteket. A képen a magas frekvencia a kép éleit és a zajaikat reprezentálják, a szűrő segítségével megtartunk alacsony frekvenciás képi információkat. A felül áteresztő szűrővel eltávolítottuk a mély

frekvenciákat, ennek köszönhetően a kép élesebb lett, de az alacsony frekvenciájú képi információk komponensei erősebb képi megjelenést adnak, miközben az alacsony frekvenciájú információk megmaradnak. Léna (8. ábra) képét gauss elmosás algoritmusát alkalmazva a képi pixel értékek egy elmosó megjelenést adtak, amely hatékony módszer a kép simítására, és amely a konvulució és a FFT kapcsolatára alapoz. A kép simítása során, a gauss-elmosás célja az, hogy csökkentsük a zaj és a Gauss függvénnyel való konvuluciót, de ez a konvulucios művelet szorzatként jelenik meg ezért hatékonyabb, ha a képet egy egyszerűbb frekvencia tartományba helyezzük, ott végezzük el az adott műveletet majd visszaalakítjuk.

A folyamat lépései:[15]

Fourier-transzformáció - Az adott képet, amit szeretnénk elmosni alkalmazva az FFT (FAST Fourier Transform) átalakítjuk egy frekvencia tartományba, így eredményképpen az adott kép frekvenciakomponenseit.

$$F(u,v)FFT(\{f(x,y)\}$$

A Gauss függvény segítségével megtartjuk a középső és alacsony képi frekvenciákat míg a magas frekvenciákat pedig lépésekben elnyomjuk.

$$H(u,v)=e-\frac{(u^2+v^2)}{2q^2}$$

Ezután a képnek a Fourier spektrumát szorozzuk a Gauss szűrővel

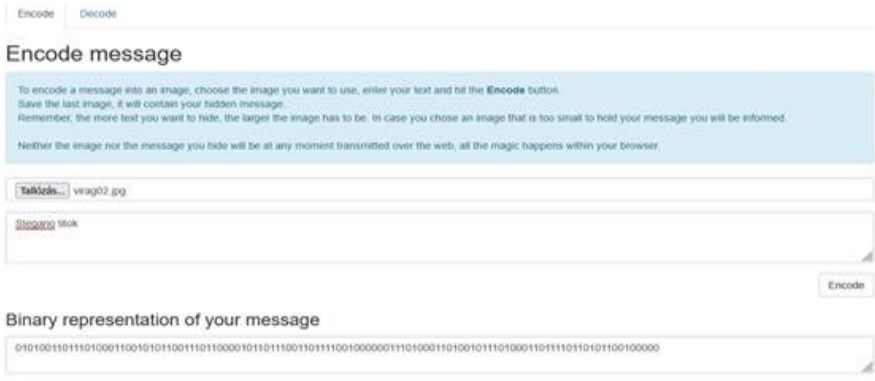
$$G(u,v)=F(u,v)\cdot H(u,v)$$

Végül a kapott eredményt segítségével visszaalakítjuk a képtartományba az úgynevezett inverz FFT segítségével.

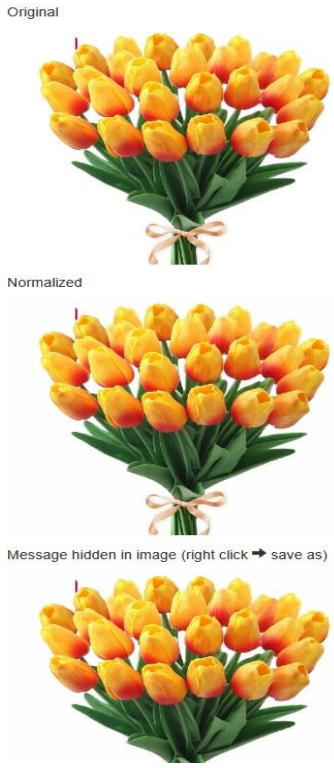
$$g(x,y)=Inverz\ FFT\ G\{(u,v)\}[15]$$

Az eredmény egy elmosott, lágyabb kép lesz, ahol a részletek csökkennek, de a fő struktúrák megmaradnak. A képekre többféle szűrőt, vagy open-cv könyvtárat alkalmazhatunk, amelyek segítségével az algoritmusok olvassák be az adott képet. A könyvtár számtalan algoritmust tartalmaz, amelyet a mémiára, ami lehet kép vagy hangfájl is használhatunk. Az adott képre nem csak szűrőt alkalmazhatunk, hanem információt is be tudunk ágyazni a gyors Fourier-transzformáció segítségével, amely egy digitális szteganográfiának felel meg, ahol a képre elrejteni kívánt információt a frekvencia tartományba rejtjük el. A módszer működhet kép és hangfájlokra is. A titok egyik nyitja az, hogy az FFT a média frekvencia komponenseit olyan mértékben módosítjuk, hogy az emberi érzékszervek pl. fül vagy, szem számára alig észrevehető legyen. Első körben a médiától függetlenül (kép vagy hang) a gyors Fourier transzformációval átalakítjuk, ebben az esetben a médiát (képet) ez a művelet felbontja, ahol az adott pont egy frekvenciát és egy fázist jelent. A következő lépésben az adatbeágyazását tesszük meg, azt az üzenetet, szövegrészt, amit szeretnénk titkosítani, egy középfrekvenciás komponensbe bitenként beágyazzuk. Ezután a Fourier transzformációnak vesszük az inverzét, így visszakaphatjuk a tértartománybeli képet. Az adott képen, hogy a titkosított információt kinyerjük, dekódolós eljárást végzünk és kiolvassuk a bitinformációkat. A beágyazási módszer jól paraméterezhető, a frekvenciasáv, a képen lévő beágyazás mélysége és a visszafejtési kulcs alapján. A módszer előnye abban tükrözik, hogy más módszerhez hasonlóan az információ rejtettebb lesz, hátránya, hogy számításigényes, mert az FFT inverzét is alkalmazni kell, továbbá ismernünk kell a frekvenciasávot, és a kulcsot.

A szteganográfia szempontjából a kép olyan részét használjuk fel, ami nem okoz szemmel látható torzulást. A kép pixelgrafika esetén pixelekből áll, minden egyes pixel adott képpontnak felel meg amely RGB numerikus színértéket képvisel. A szteganográfiai programok elő körben bekérik az eredeti képet, amire szeretnék a titkosítani kívánt információt elrejteni.



9. Ábra: információ kódolása, saját szerkesztés



10. Ábra: képi transzformációk, saját szerkesztés

A rejtett üzenet dekódolását láthatjuk, itt az üzenetet vagy egy szót dekódoltuk.

ASCII Bináris Kódtáblázat (Nagy- és Kisbetűk)

Karakter	ASCII (decimális)	Bináris
A	65	01000001
B	66	01000010
C	67	01000011
D	68	01000100
E	69	01000101
F	70	01000110
G	71	01000111
H	72	01001000
I	73	01001001
J	74	01001010
K	75	01001011
L	76	01001100
M	77	01001101
N	78	01001010
O	79	01001111
P	80	01010000
0	81	01010001
R	82	01010010
S	83	01010011
T	84	01010100
U	85	01010101
V	86	01010110
W	87	01010111
X	88	01011000
Y	89	01011001
Z	90	01011010
a	97	01100001
b	98	01100010
c	99	01100011
d	100	01100100
e	101	01100101
f	102	01100110
g	103	01100111
h	104	01101000
i	105	01101001
j	106	01101010
k	107	01101011
l	108	01101100
m	109	01101101

Karakter	ASCII (decimális)	Bináris
n	110	01101110
o	111	01101111
p	112	01110000
q	113	01110001
r	114	01110010
s	115	01110011
t	116	01110100
u	117	01110101
v	118	01110110
w	119	01110111
x	120	01111000
y	121	01111001
z	122	01111010

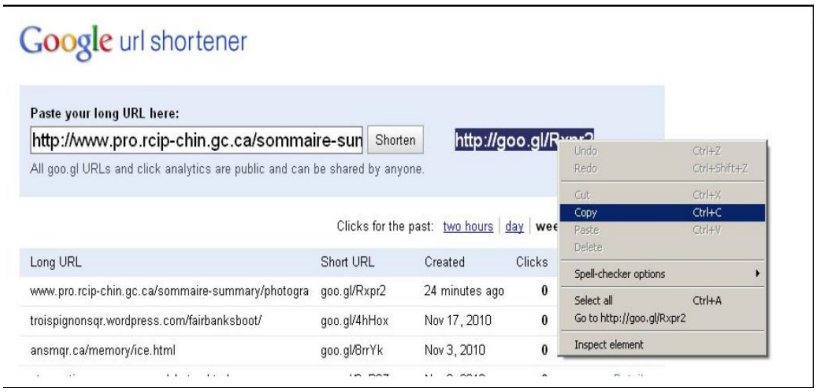
4. Táblázat: Ascii kódtáblázat, saját szerkesztés

ASCII kódtáblázat

A kódtáblázat segítségével történik a titkosítás, azonban a fő komponens a Fourier-transzformáció algoritmusa, amely az adatot átalakítja a frekvenciatartományba, így az adott eredeti jel, amely lehet hang vagy kép, komponensekre bontják. Az eltitkolni kívánt üzenetet elrejthetjük az adott jel frekvencia komponenseiben vagy a frekvencia spektrumánál tesszük meg a módosítást, de csak olyan mértékben, hogy ne legyen ismert. Egy kulcs segítségével végezzük el a frekvenciák módosítását, amely a titkosítani kívánt információt jelenti, csak az tudja visszafejteni, aki a kulcsot ismeri. Ezután vesszük a titkosított üzenetet, amely már el van rejtve a frekvenciák között, ezt az eredeti jelet visszaalakítjuk az időtartományba, és a Fourier-transzformáció inverzének segítségével, így már a kapott média tartalmazza a titkosított információt, amelynek dekódolásához ismerni kell a kulcsot. A Fourier transzformációt alkalmazzák a titkosítási módszereknél, mert lehetővé teszi az adott jel frekvenciatartományában megtehető módosításokat, amelynek köszönhetően el tudjuk rejteni a kívánt információt, amely a jel manipulatív eljárásán alapul.

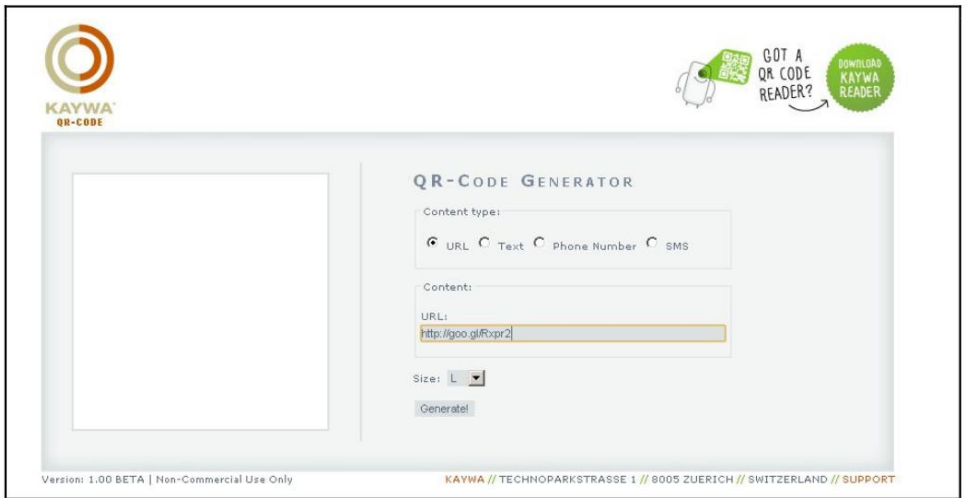
QR-kódok vagy Barcodes a képen belül

A QR-kód egy vonalkód típus, amelyben információt tudunk tárolni, pl.: a termék árát. A szkennerek segítségével tudjuk az információ dekódolni. Kezdetben a logisztikai területén alkalmazták. Bár ez nem egy hagyományos szteganográfiai módszer, a QR-kódok és vonalkódok is tartalmazhatnak titkos adatokat, amelyeket a képen belül rejtünk el. Ezt akkor alkalmazzák, ha a képen egy olyan mintázatot szeretnének elhelyezni, amelyet egy QR-kód vagy vonalkód olvasó képes dekódolni. A QR kód egy beágyazott weblinként működik. Biztonságot is adhat pl.: hogy csak a kódkiolvasás esetén lehet használni a számítógépet. A QR kódokat létre tudjuk hozni webes felületen, kutatásunk során a Kayw weboldallal találkoztunk, ahol a QR kód generátort alkalmazva, lehetőségünk van QR kódot generálni. Első körben a létrehozott tartalom mint információ rövid kódját másoljuk, a goole.gl webes felületen.[16]



11. Ábra: weboldal, forrás: URK weboldal

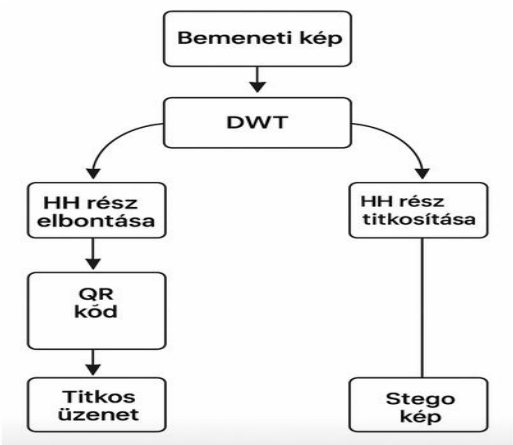
Beillesztjük az URL-t, a https://qrcode.kaywa.com/ weboldalon, kiválasztjuk a 12. ábra méretét, végül megjelenik a QR-kód.



12. Ábra: *QRkód Generátor, forrás: https://qrcode.kaywa.com/*

A fentieket tovább gondoljuk és alkalmazzuk a szteganográfia eljárást akkor a QR kód és a kriptográfiát is kombinálva lehetőségünk van biztonságos környezetű információ beágyazását az adott képbe, amely egy QR kód kép. Ezt a titkosított QR kódot a kép, DWT diszkrét hullámtranszformációs tartományba teszik, a tartományon belül az úgynevezett HH alrészlet legkisebb helyiértékű LSB bitjeibe ágyazzák. A HH Hullámtranszformáció több részre osztható (LL, LH, HL, HH). A HH alrésznek van egy LSB bit síkja és azt a részt módosítják, ennek köszönhetően szinte alig észrevehető lesz az rejtett információ. Hasonlóan a FFT (Fast Fourier Transformation) eljáráshoz, alkalmazzák a DWZ inverzét, visszakapjuk a stego-képet amelyben az információ rejlik.[17]

A titkosított üzenet visszanyerése fordított művelettel történik meg. A módszer a vizsgálat során igen jónak bizonyult, mert alig észrevehető a torzítás.[18] [19]



13. Ábra: folyamatábra, saját szerkesztés

Zaj hozzáadása

Az adatok beágyazása után kis mennyiségű zaj hozzáadása a képhez segíthet elrejteni a módosításokat. A zaj célja, hogy eltorzítsa az eredeti pixelek értékét úgy, hogy az adatok ne legyenek könnyen felismerhetők, de a titkosított üzenet még mindig visszanyerhető marad. A zaj hozzáadása csökkenti a titkosított üzenet minőségét, így érdemes a zaj mértékét gondosan szabályozni.

Degradációs modell

A képi degradációs folyamat egy **degradációs függvény** hatásán keresztül modellezhető, amely az eredeti képen, valamint egy **additív zajkomponensen** működik.

Formálisan a folyamat az alábbi összefüggéssel írható le:

$$g(x,y)=H\{f(x,y)\}+\eta(x,y)$$

- f(x,y) az eredeti (torzítatlan) kép**,**
- H{·} a degradációs operátor vagy átviteli függvény**,** amely jellemzi a torzító folyamatot (pl. elmosódás, mozgás, optikai hibák stb.),
- η(x,y)az additív zajkomponens, amely a képhez szuperponálódik,
- g(x,y) pedig a megfigyelt (degradált) kép[20]

14. Ábra: RGB zaj és Median filter kép, saját szerkesztés

f(x,y(median{g(s,t)}

A medián a **zaj csökkentéséhez** a véletlenszerű zajokat távolítja el, megőrizve a kép fontos részleteit:

- **g(s,t)**: ahol a függvény felvesz egy s és t változót, a kimeneti érték egy numerikus érték
- a **median{g(s,t)}**: a medián függvény a zaj csökkentéséért felel
- **f(x,y,median{g(s,t)})**: x és y azok a pixel pontok koordinátái, ahol a függvényt alkalmazzuk.

A zaj miatt a kép helyreállítása, degradációs függvény statisztikai jellemzőire tekintettel minél pontosabban becsüljük vissza az eredeti képet, ami f(x,y) lenne. Ez egy inverz feladat, amely alapján a degradációs függvény inverzét kell meghatározni, figyelembe véve a környezeti jellemzőket, mint a kép zajának mértéke és torzítása. a kutatásom alapján megállapítottam, hogy az egyik legjobb zajszűrő a medián filter alkalmazása az adott képre, amely a kép pixel intenzitás értékét, amely helyettesítve van a kép szürkeségi szintek mediánjával. Ez a módszer hatékonyan csökkenti a zajt.[21][22]

A median filter képszűrő alkalmazásával kiváló zajcsökkentési képesség érhető el, más filterhez képest arányosan kevesebb elmosodással. A kép vizsgálat alapján hatékonyság tapasztalható impulzuszaj bipoláris és unipoláris zaj esetén.[20]

FELHASZNÁLT IRODALOM

[1] D. Harper, „steganography”, *Online Etymology Dictionary*. [Online]. Elérhető: https://www.etymonline.com/word/steganography

[2] B. Thayer, *Herodotus: The Histories, Book VII, chapters 175–239*. [Online]. Elérhető: https://penelope.uchicago.edu/Thayer/E/Roman/Texts/Herodotus/7d%2A.html

[3] D. Megías, W. Mazurczyk, és M. Kuribayashi, Szerk., *Data Hiding and Its Applications: Digital Watermarking and Steganography*. Basel: MDPI - Multidisciplinary Digital Publishing Institute, 2022.

[4] P. Sharma és S. Goyal, „Steganography Techniques, in: International Journal of Engineering Research & Technology (IJERT)”, köt. 02, 2013, doi: 10.17577/IJERTV2IS4812.

[5] V. Bok, *GANs in Action: Deep Learning with Generative Adversarial Networks*. New York: Manning Publications Co. LLC, 2019.

[6] H. Jaheel, Z. Beiji, és A. L. Jaheel, „Design and Implementation Steganography System by using Visible Image”, *International Journal on Smart Sensing and Intelligent Systems*, köt. 8, sz. 2, o. 1011–1030, jan. 2015, doi: 10.21307/ijssis-2017-793.

[7] A. Qasim Jabbar és D. Roshidi, „Capacity Performance of LSB Method On Multi-Layer Images in Steganography”, *International Journal of Engineering and Techniques*, sz. 5, o. 118–121, 0 2022.

[8] M. S. Abuali, C. B. M. Rashidi, R. A. A. Raof, K. N. F. Ku Azir, S. S. Hussein, és A. Q. Abd-Alhasan, „Enhancing Security with Multi-level Steganography: A Dynamic Least Significant Bit and Wavelet-Based Approach”, *MMEP*, köt. 11, sz. 6, o. 1403–1416, jún. 2024, doi: 10.18280/mmep.110602.

[9] H. Sajedi, Szerk., *Recent Advances in Steganography*. InTech, 2012. doi: 10.5772/2501.

[10] G. Swain, „Classification of Image Steganography Techniques in Spatial Domain: A Study”, *IJCSET*, köt. 5, sz. 3, o. 219–232, 2014.
[11] W.-B. Lin, T.-H. Lai, és K.-C. Chang, „Statistical feature-based steganalysis for pixel-value differencing steganography”, *EURASIP J. Adv. Signal Process.*, köt. 2021, sz. 1, o. 1–18, dec. 2021, doi: 10.1186/s13634-021-00797-5.
[12] F. Akram, A. AbuEl-Atta, és M. M. Selim, „Image Steganography Based on PVD and Knight Tour Algorithm: A Combined Approach”, *BJAS*, köt. 9, sz. 5, o. 97–103, 2024.
[13] I. J. Cox, *Digital watermarking and steganography*, 2nd ed. in The Morgan Kaufmann series in multimedia information and systems. Amsterdam Boston: Morgan Kaufmann Publishers, 2008.
[14] T. Rabie, M. Baziyad, és I. Kamel, „High-Fidelity Steganography: A Covert Parity Bit Model-Based Approach”, *Algorithms*, köt. 17, sz. 8, o. 328, júl. 2024, doi: 10.3390/a17080328.
[15] V. A. Oppenheim és S. A. Wilsky, *Signals and Systems*, köt. Pearson Education. 1983.
[16] „Appendix D: Glossary Introduction, QR Code How-To Guide”. Prepared by the Association of Nova Scotia Museums For the Canadian Heritage Information Network’s (CHIN) Professional Exchange. [Online]. Elérhető: https://www.canada.ca/content/dam/chin-rcip/documents/services/web-interactive-mobile-technologies/codes_qr-qr_codes-eng.pdf
[17] A. Yahya, *Steganography Techniques for Digital Images*. Cham: Springer International Publishing, 2019. doi: 10.1007/978-3-319-78597-4.
[18] L. M. Marvel, C. G. Boncelet, és C. T. Retter, „Spread spectrum image steganography”, *IEEE Trans. on Image Process.*, köt. 8, sz. 8, o. 1075–1083, aug. 1999, doi: 10.1109/83.777088.
[19] C. Y. K, „A HDWT-based reversible data hiding method”, *Journal of Systems and Software*, sz. 82, o. 411–421, 2009.
[20] N. Subash és M. Sucharitha, *DIGITAL IMAGE PROCESSING*. 2021.
[21] V. Hajduk, M. Broda, O. Kovac, és D. Levicky, „Image steganography with using QR code and cryptography”, in *2016 26th International Conference Radioelektronika (RADIOELEKTRONIKA)*, Kosice: IEEE, ápr. 2016, o. 350–353. doi: 10.1109/RADIOELEK.2016.7477370.
[22] R. C. Gonzalez és R. E. Wood, *Digital Image Processing*. in 4.