POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Digital image as a cyber spy: a gray coded secure model to transfer the secret information

Bir siber casus olarak dijital görüntü: gizli bilgileri aktarmak için gri kodlu güvenli bir model

***Yazar(lar) (Author(s))**: Hüseyin Bilal MACİT*[1]

ORCID[1]*: 0000-0002-5325-5416*

To cite to this article: Macit H.B., “Digital Image as a Cyber Spy: A Gray Coded Secure Model to Transfer the Secret Information”, ***Journal of Polytechnic***, *(*): *, (*).

Bu makaleye şu şekilde atıfta bulunabilirsiniz: Macit H.B., “Digital Image as a Cyber Spy: A Gray Coded Secure Model to Transfer the Secret Information”, ***Politeknik Dergisi***, *(*): *, (*).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: 10.2339/politeknik.1567237

Digital Image as a Cyber Spy: A Gray Coded Secure Model to Transfer the Secret Information

Highlights

- *A robust, imperceptible, and high payload data hiding method has been proposed.*
- *Mathematical success was achieved in steganalysis tests.*
- *The entropy value of the secret data was reduced to a value close to 0 with Gray Coding.*

Graphical Abstract

This study proposes an algorithm to hide the secret data in a carrier data in the frequency domain on different bit planes using gray coding to decrease the entropy. The success of the method has been proven by steganalysis tests and statistical metrics.

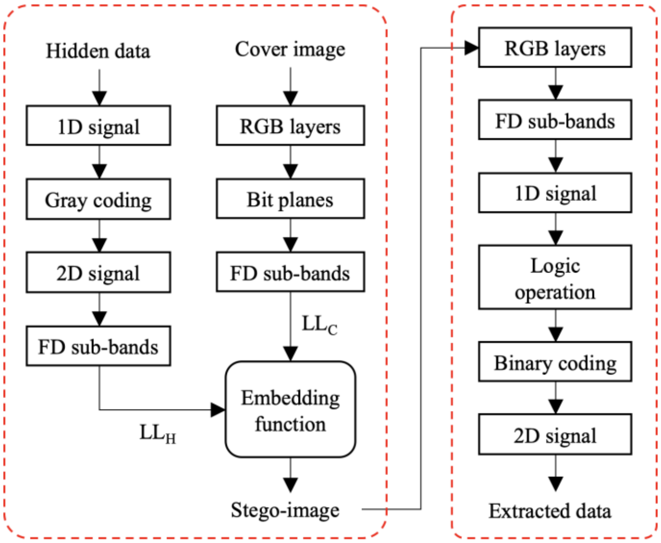

Figure. Flowchart of proposed algorithm

Aim

In this study, it was aimed to design a steganographic algorithm that combines high imperceptibility, robustness and data load features.

Design & Methodology

Discrete Wavelet Transform with Haar was used for frequency domain transformation. The image was processed in 24 parts, 3 color layers and 8 bit planes. Gray coding was applied to the secret data in the range of 2-128 bits.

Originality

When the literature is examined, steganography was performed for the first-time using bit plane slicing, gray coding and frequency domain transformation together.

Findings

In the tests performed with Lena image, after many iterations, the stego-image and cover image matched one-to-one in statistical comparisons such as structural similarity and normalized correlation. The PSNR measurement reached a maximum of 83.47. The extracted data showed a statistical similarity of 0.9979 to the secret data even in the worst case.

Conclusion

It was shown to be successful when compared to the methods in the literature in terms of imperceptibility, robustness and data load.

Declaration of Ethical Standards

The author of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Digital Image as a Cyber Spy: A Gray Coded Secure Model to Transfer the Secret Information

Araştırma Makalesi / Research Article

Hüseyin Bilal MACİT[1*]

[1]Department of Information Systems and Technologies, Bucak ZTYO, Burdur Mehmet Akif Ersoy University, Burdur, Türkiye

(Geliş/Received : 02.10.2016 ; Kabul/Accepted : 26.08.2017 ; Erken Görünüm/Early View : 07.07.2025)

ABSTRACT

The widespread use of the Internet and the ability of data transfer between different types of devices have caused intense multimedia traffic today. More than a hundred thousand image files are transferred per second on Meta group social media platforms alone. In particular, multimedia objects that directly target human perception such as images, audio, and video can be used as cyber spies on the network. Steganography methods are generally used for this. This study proposes an alternative digital image steganography method. The proposed method works in both the frequency domain and bit plane slicing methods, which is unusual. Gray coding is applied to the secret data to obtain minimum entropy. The results of the method are presented with surface graphics and tables by performing many iterations on different gray code lengths and different bit planes. Steganalysis tests have been performed for the applicability of the method in the real world and the results are shown. The method has been compared with some methods in the literature in terms of imperceptibility, robustness, and data load. Despite the high data load, higher scores were obtained than similar methods in structural and perceptual mathematical tests.

Keywords: Cyber spy, image steganography, bit plane slicing, steganalysis.

Bir Siber Casus Olarak Dijital Görüntü: Gizli Bilgileri Aktarmak İçin Gri Kodlu Güvenli Bir Model

ÖZ

İnternetin yaygınlaşması ve veri transferinin farklı türde cihazlar arasında da gerçekleştirilebilir olması, günümüzde yoğun bir multimedya trafiğinin oluşmasına neden olmuştur. Yalnızca Meta grubuna bağlı sosyal medya platformlarında saniyede yüz binden fazla statik görüntü dosyası transferi gerçekleşmektedir. Özellikle görüntü, ses, video gibi doğrudan insan algısını hedef alan multimedya nesneleri ağ üzerinde birer siber casus olarak kullanılabilmektedir. Bunun için genellikle steganografi yöntemleri kullanılır. Bu çalışma, alternatif bir dijital görüntü steganografisi yöntemi önermektedir. Önerilen yöntem, alışılmışın dışında hem frekans alanında hem de bit düzlemi dilimleme yöntemi ile çalışmaktadır. Gizli veriye, minimum entropi elde etmek için gray kodlaması uygulanmıştır. Yöntemin sonuçları, farklı gray kodu uzunlukları ve farklı bit düzlemi dilimleri üzerinde çok sayıda iterasyon gerçekleştirerek yüzey grafikleri ve tablolar ile sunulmuştur. Yöntemin gerçek dünyada uygulanabilirliği için steganaliz testleri yapılmış ve sonuçları gösterilmiştir. Yöntem algılanamazlık, sağlamlık ve veri yükü açısından literatürdeki bazı yöntemlerle kıyaslanmıştır. Yüksek veri yüküne rağmen, yapısal ve algısal matematiksel testlerde benzer yöntemlerden daha yüksek skorlar elde edilmiştir.

Anahtar Kelimeler: Siber casus, görüntü steganografisi, bit düzlemi dilimleme, steganaliz.

1. INTRODUCTION

Information technologies are in every aspect of the social lives of individuals and societies today. Many activities of social life such as shopping, banking, education, communication and transportation are carried out with information processing technologies [1]. As a result of the interconnection of computers, phones and many other devices in the world, a huge amount of information is captured, copied and consumed every day [2]. It is estimated that in 2023, an average of 3.5 million e-mails were sent every second in the world [3], approximately 2500 photos were uploaded to Facebook [4], and 17000 photos were uploaded to Instagram [5]. Also, it is estimated that an average of 4.6 million GB of data is being generated every second in 2024 [6]. Although this increase in the amount of data is beneficial for humanity, ensuring its security has also become a major problem. Data has become susceptible to cyber-attacks such as data breaches and data theft due to the access of many devices via the network [7]. The biggest problem that distributed systems are trying to deal with today is data security [8]. Cryptography and steganography techniques, which are the most important ways to deal with this problem, have gained great importance in recent years [9]. The main purpose of cryptography is to provide a secure exchange of information between the receiver and the transmitter without interference from external factors [10]. Information is encrypted with an algorithm and/or a key that only the receiver and the transmitter know and converted into a form that unauthorized persons cannot read [11]. However, data raises suspicion when an attacker intercepts it in an incomprehensible form in the communication channel [12]. Moreover, if the attacker detects the decryption algorithm and/or the

Sorumlu Yazar (Corresponding Author)
e-posta : hbmacit@mehmetakif.edu.tr

key with cryptanalysis techniques, they can read and change the secret information [13]. In addition, traditional cryptography algorithms have a very high computational cost, especially for large volumes of data [14]. Steganography is the art and the science of hiding the existence of data and has been accepted as a computer science discipline since the 1990s [15]. The word "stegano" means "covered" in ancient Greek [16]. In digital steganographic techniques, secret data is embedded in a multimedia object called "cover" such as another image, audio, video, text, or network protocol [1] in a way that cannot be understood by human perception. This process is called "embedding" [17], and the resulting carrier object is called stego-text, cover data, stego-image, cover-file, etc. [18]. Secret data can be easily transmitted on the network by hiding it in ordinary data that will not attract any suspicion. Steganographic techniques are applied especially in cases where cryptology methods are inadequate, such as in the military, biometrics and health fields, such as transmitting military coordinate data without attracting suspicion and without being intercepted, or hiding retinal images, fingerprints, and patient demographic information in medical images to ensure the security of these images during storage [19]. Content producers and owners also use digital steganographic techniques to protect digital property rights of content [20]. These methods are often called digital watermarking [21]. Figure 1 shows the steganographic system that consists of three basic elements: cover data, secret data, and embedding function (figure 1).

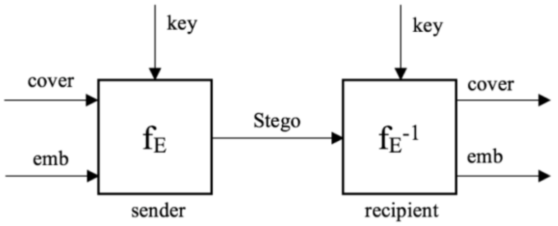

Figure 1. The steganographic system [20]

Secret data refers to the data to be sent to the recipient securely, while cover data refers to the data that carries it and does not attract suspicion. The embedding function includes the algorithm and keys that embeds the secret data in the cover data [22]. The first goal of the embedding function is to find enough space to embed the secret data in the cover data [23]. Also, it should embed the secret-data in a retrievable form. Moreover, all or a part of the secret data should be retrievable even if only a part of the cover data reaches the receiver. Secret data should not be embedded in a section of the cover data such as the file header, because it may be lost with the format change of the cover data. If the cover data is an image, audio or video data, the secret data should be protected against attacks such as cropping, rotation, sampling and filtering [24]. The more the secret data is protected, the more robust the method is. Steganalysis techniques have been developed to determine whether the ordinary data contains any secret data and to capture or destroy the secret data in a conventional way. In particular, statistical steganalysis methods are quite successful and today, new steganography methods are being developed against them [9]. The more anomalies a captured ordinary data contains statistically, the more suspicious it is. For example, a polar bear photo obtained from a recipe sharing site [25]. The success of a steganographic method can be determined by comparing stego-data with cover data. The more similar these two data are to each other, the more imperceptible the stego-data is [26]. Structured Similarity Index (SSIM) and Peak Signal to Noise Ratio (PSNR) metrics are usually used to calculate this similarity [27].

The most popular digital steganography method is digital image steganography due to its high storage capacity and low processing complexity [28]. In this study, a new image steganography technique is proposed and implemented. Image steganography methods are examined in two classes as spatial and frequency domain technics. Spatial domain methods deal with the insignificant areas in the pixels of the image. Let, I is a Red-Green-Blue (RGB) image with m rows and n columns;

$$I(m,n) = \{x_{i,j} | 1 \leq i \leq m, 1 \leq j \leq n\} \quad (1)$$

Each $x_{i,j}$ represents a pixel of I. A binary image represents a pixel with 1 bit, a grayscale image with 8 bits, and an RGB image 3x8 bits as shown in figure 2.

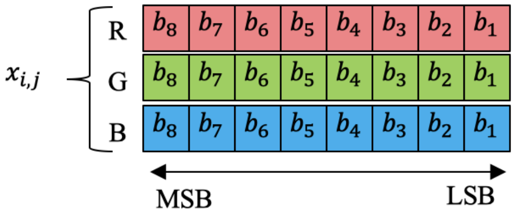
$x_{i,j}$
R
G
B
b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1
b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1
b_8 b_7 b_6 b_5 b_4 b_3 b_2 b_1
MSB
LSB

Figure 2. Binary representation of the pixel value of an RGB image

The numerical value of each layer for pixel $p_{i,j}$ represents the intensity of the corresponding color, and the value range of the pixel is $0 < p_{i,j} < 255$.

$$R, G, B = \{r_{ij}, g_{ij}, b_{ij} | 1 \leq i < m, 1 \leq j < n\},$$
$$r_{ij}, g_{ij}, g_{ij} \in \{0,1,2, \dots, 255\} \quad (2)$$

The Most Significant Bit (MSB) is b_8, because the transformation of b_8 from 0 to 1 or from 1 to 0 changes the pixel intensity value by 128. The Least Significant Bit (LSB) is b_1, because the transformation of b_1 from 0 to 1 or from 1 to 0 changes the pixel intensity value by only 1. A change of magnitude 128 in pixel intensity can be easily perceived by the Human Visual System (HVS), while a change of magnitude 1 cannot be perceived [29]. Therefore, spatial methods change one or more LSB bits to embed the secret data [30]. Another way to work bitwise in digital images is Bit Plane Slicing (BPS). This is a frequently used approach, especially for image compression [31] and data hiding. BPS divides the image into 8 separate layers for each bit from LSB to MSB as shown in figure 3.

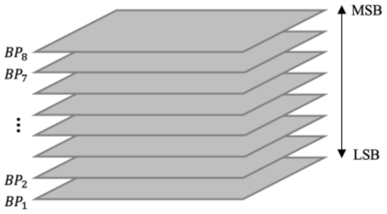

Figure 3. BPS

BP_1 refers to LSB, BP_8 refers to MSB obtained with BPS. For example, A grayscale I image consisting of 8 BPs is expressed as in the equation;

$$I = \sum_{i=1}^{8} BP_i . 2^i \tag{3}$$

In spatial domain hiding methods, the BP_i in which the secret data will be embedded is selected according to the desired imperceptibility/robustness ratio. Let the secret data be D with m rows and n columns;

$$D(m, n) = \{x_{i,j} | 1 \leq i \leq m, 1 \leq j \leq n\} \; x_{ij} \in \{0,1\} \tag{4}$$

Embedding process for stego-image I_S and selected BP x is;

$$I_S = (\sum_{i=1}^{8} BP_i . 2^i) - (BP_x . 2^x) + D(BP_x . 2^x)) \tag{5}$$

In the literature, Lena image has been used as a test image in many image processing studies. In order to compare the results of the proposed method, Lena image has been used as a test image in this study. The results of the classical spatial domain hiding process in each element of the set $BP_i, i \in \{1,2, \ldots ,8\}$ is shown in figure 4.

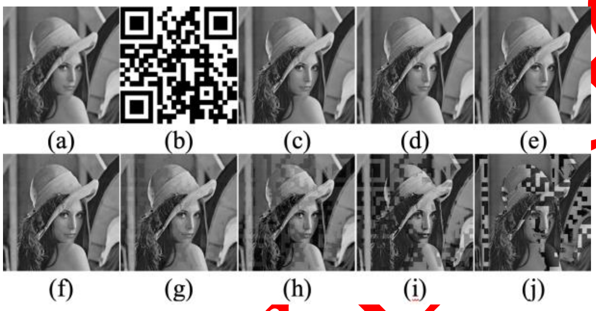

Figure 4. (a) Lena image as the cover data (b) secret data (c) stego-image for BP_1 (d) stego-image for BP_2 (e) stego-image for BP_3 (f) stego-image for BP_4 (g) stego-image for BP_5 (h) stego-image for BP_6 (i) stego-image for BP_7 (j) stego-image for BP_8

As clearly seen in figure 4, the imperceptibility level of the hiding process decreases as we proceed from BP_1 to BP_8. Although spatial domain hiding performed at low BP levels provides high imperceptibility, it is not resistant to attacks such as bit deletion, averaging filtering, [32] and compression algorithms such as JPEG [33]. In the frequency domain, hiding methods treat the image as a signal function and use wavelet transform methods. These methods hide the secret data in a robust but perceptible way. However, in data hiding methods, the detection of hidden data is often not a desired situation. In this study, one of the aims is to make the hidden data imperceptible. Thus, Discrete Wavelet Transform (DWT) which is a mathematical transformation method that divides a signal into four sub-frequencies by applying Low Pass filters (LPF) and High Pass filters (HPF) [34] is used for transformation in the frequency domain. When DWT is applied to a signal, the signal is decomposed into four separate frequency sub-bands (figure 5). The Low-Low (LL) sub-band is approximately the same as the original signal. The High-Low (HL) sub-band is the original signal details with horizontal high frequencies. The Low-High (LH) sub-band is the original signal details with vertical high frequencies. The High-High (HH) sub-band shows the high frequencies [32].

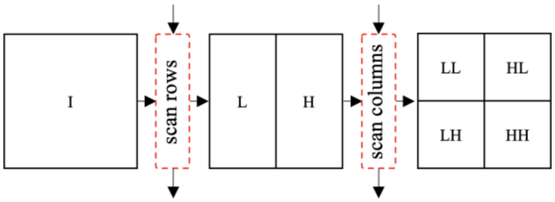

Figure 5. DWT process of a digital image

A significant problem is how to choose the coefficients to which the secret data will be embedded. [35]. If a result in the middle of robustness and imperceptibility is desired, the secret data is embedded in the mid-frequency region, namely the LH and HL bands [36]. However, if more robust result is desired, the secret data is embedded in the HH components [37]. If any compression algorithm will be used, the HH band is not preferred because it cannot protect the secret data. However, this band is robust to some attacks such as cropping, sharpening, contrast modification, histogram equalization, and gamma correction [38]. An important advantage of steganography in the frequency domain is that the image does not need to be separated into color layers. In other words, secret data can be embedded directly into the RGB image. However, when steganalysis is performed by separating the stego image into RGB layers, the same statistical change can be detected in all three layers. In this case, secret information can be captured. While the bit slicing process is a major factor in embedding data in the spatial domain, it has no effect in the frequency domain. For instance, when secret data is embedded in the set $BP_i, i \in \{1,2, \ldots ,8\}$ to the bit-sliced gray scale Lena image, the hidden data can be easily detected with HVS, as clearly seen in figure 6.

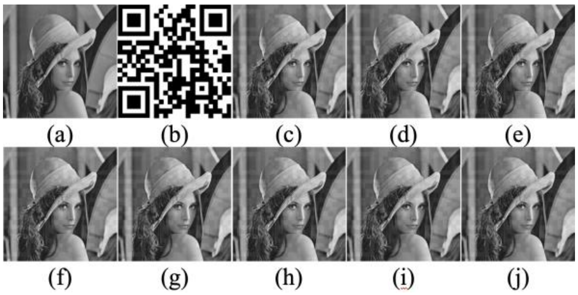

Figure 6. (a) Lena image as the cover data (b) secret data data (c) stego-image for BP_1 (d) stego-image for BP_2 (e) stego-image for BP_3 (f) stego-image for BP_4 (g) stego-image for BP_5 (h) stego-image for BP_6 (i) stego-image for BP_7 (j) stego-image for BP_8

Secret data embedding operation in the set $BP_i, i \in \{1,2,\dots,8\}$ was performed with both classical spatial domain and frequency domain methods and the similarity metric results of the stego-image and the cover image were given in figure 7. As the numerical value of i increases for BP_i in the spatial domain, the stego-image differentiates from the cover image. However, in the frequency domain, the secret data embedding operation always results the same regardless of which element in the set $BP_i, i \in \{1,2,\dots,8\}$ is applied.

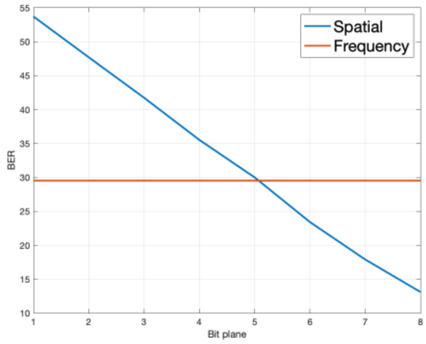

Figure 7. BP-PSNR graph of frequency domain steganography

2. PROPOSED METHOD

Classical data hiding methods in the frequency domain result the same in the entire BP. In this study, a data hiding method is proposed which is aimed to provide high imperceptibility and obtain different results in each BP of the RGB cover image. The method consists of two stages: embedding phase and extracting phase. In order to measure the performance of the method, similarity ratio metrics are applied which are frequently used in the literature. For the presentation of the first results of the method, Lena image was used as the cover image and a QrCode image was used as secret data. The flowchart of the proposed method is shown in figure 8.

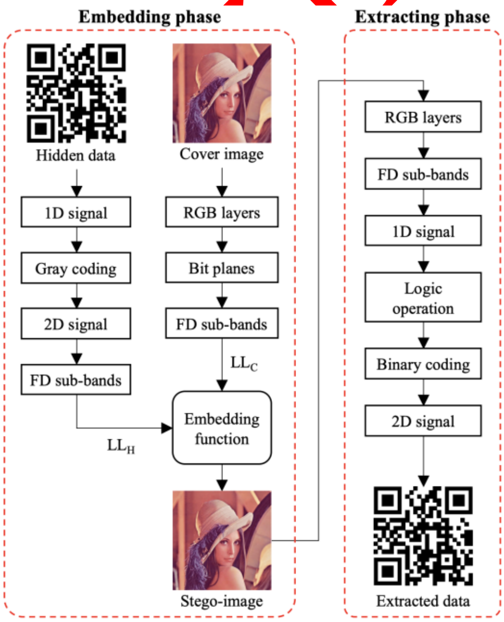

Figure 8. Flowchart of proposed algorithm

2.1. Embedding Phase

This phase is the stage of generating stego image using the cover image, secret data and the proposed function. Let the cover image be C, consisting of m rows and n columns.

$$C(m,n) = \{x_{i,j} | 1 \le i \le m, 1 \le j \le n\} \quad (6)$$

C is divided into R_C, G_C, and B_C color layers consisting of m rows and n columns. Bit slicing is applied to each layer.

$$R_C = \sum_{i=1}^{8} R_C BP_i, G_C = \sum_{i=1}^{8} G_C BP_i, B_C = \sum_{i=1}^{8} B_C BP_i \quad (7)$$

Each BP_i holds the i.BP data of the relevant layer. In the proposed method, it can be predicted which BP will provide more imperceptibility and robustness value. In order to test this, the embedding process is applied one by one for each BP_i and the results are interpreted. In the next step, R_C, G_C, and B_C arrays are converted to the frequency domain to obtain the LL_{Rc}, LL_{Gc}, and LL_{Bc} sub-bands, respectively. The secret data D can be any text, image, sound or content, even an unspecified file. D is treated as an array and if the number of elements is less than C, D is expanded until $D = C$. In the study, D was selected as a digital image of $m.n$ size and the D was converted to a one-dimensional signal in order to visually express the results in the test phase. In order to perform bitwise processing, each element of the D is transferred to a new binary array with an 8-bit equivalent as $D = \{D_1, D_2, \dots D_{mxn}\}$ for each $D_i = \{D_i b_1, D_i b_2, \dots, D_i b_8\}$.

Standard data hiding algorithms do not use any transformation in the secret data during the embedding phase, but advanced algorithms usually use encryption techniques. The more advanced the encryption method, the more processing time it requires. In addition, the encrypted data is usually longer than the secret data as a result of the encryption, which harms the imperceptibility of the stego-data. The proposed method applies Gray Coding (GC) to D for less imperceptibility. GC gives output as a single bit change in multiple bit changes in a data array, as seen in table 1 [39].

Table 1. 3-bit GC

Binary	000	001	010	011	100	101	110	111
GC	000	001	011	010	110	111	101	100

With this feature, GC reduces the sharpness of the array. Changing the i. bit value of any pixel in an image in the binary system causes a change of $\pm 2^{i-1}$ magnitude in the value of that pixel [40]. The fewer binary changes there are in the array, the greater the imperceptibility. GC transformation is applied to the k. element of the secret data array as in equation 8.

$$D_k = D_k b_x \oplus (D_k b_{x+1}) \quad (8)$$

Here, $D_k b_{x+1}$ represents the right shift bit. GC is performed by dividing the secret data into one-dimensional blocks of minimum 2 bits. In this study, GC was applied on 2, 4, 8, 16, 32, 64, and 128-bit blocks to test GC performance.

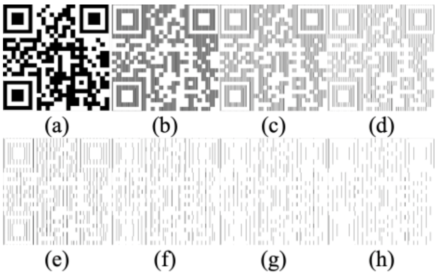

Figure 9. (a) Secret test data D (b) 2bit GC (c) 4bit GC (d) 8bit GC (e) 16bit GC (f) 32bit GC (g) 64bit GC (h) 128bit GC

HVS focuses directly on the edge details of the image. The significant edges of a digital image are only a small part of the entire edge information. This part is called the “salient area” [41]. Frequency domain data hiding algorithms can generate sharp edges in the stego image that can be detected by HVS [42]. The proposed method aims to reduce the sharpness by applying GC to the secret data to prevent this. Let t be the number of neighbors of each pixel $p(i,j)$ of the secret data of $m.n$ pixels:

$$\mu = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\sum_{i-1}^{i+1}\sum_{j-1}^{j+1}p(i,j)}{t}}{m.n} \tag{9}$$

μ refers the mean of unequal neighbor pixel count per pixel. As μ increases, the probability of the block surrounding that pixel being an edge increase. The proposed method has reduced this probability, especially in low-bit GC, as seen in figure 10. In addition, according to the second law of thermodynamics, entropy [43], the entropy of a system gives the uncertainty measure about its structure [44]. The entropy function reaches its maximum value when the probabilities of the results produced by the system are equal to each other. For example, if D is assumed to be a random system, the sum of the probabilities of all pixels of D is equal to 1:

$$\sum_{i=1}^{m}\sum_{j=1}^{n}p_i = 1,\ \text{for each } i,j \rightarrow p_i \geq 0 \tag{10}$$

$$\begin{aligned} H(D) &= H\left(p_{(1,1)},\dots,p_{(i,j)}\right) \\ &= -\sum_{i=1}^{m}\sum_{j=1}^{n}p_{(i,j)}logp_{(i,j)} \end{aligned} \tag{11}$$

$H(D)$ is the entropy of the secret data which is related to the histogram distribution of the image [45] and is inversely proportional to the amount of detail in the image. As the Gray Code Length (GCL) increases, the entropy value decreases, as seen in figure 11.

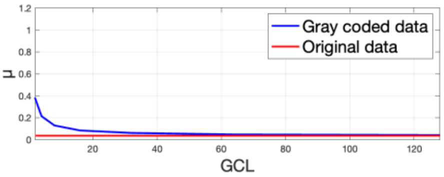

Figure 10. Comparison of mean value of GC vs original data

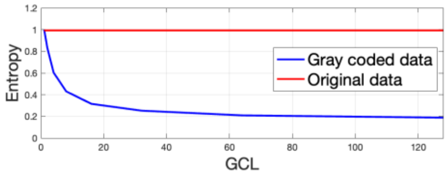

Figure 11. Comparison of entropy value of GC vs original data

Gray coded secret data D_{Gray} is embedded with α strength factor into the sub-bands $LL_{R_CBP_i}$, $LL_{G_CBP_i}$, and $LL_{B_CBP_i}$ which are obtained by frequency transformation of selected BP and stego sub-layers are obtained for each color. For this, by applying the LPF and HPF frequency transformation in equations 10 and 11 to both C and D_{Gray}, the sub-bands $LL_{DR_CBP_i}$, $LL_{DG_CBP_i}$, and $LL_{DB_CBP_i}$ for the secret data, and LL_{CR_C}, LL_{CG_C}, and LL_{CB_C} for the cover data are obtained, respectively. The embedding process is performed as in the equation 12.

$$LL_{S\lambda_C(i,j)} = \left(LL_{D\lambda_CBP_i}.\alpha\right) + \left(LL_{C\lambda_C(i,j)}\right) \quad \{\lambda = R,G,B\} \tag{12}$$

IDWT is applied to obtain the stego-image from the three resulting stego color space sub-bands. The sub-bands are up-sampled at each level, passed through $y'[x]$ and $a'[x]$ filters, and the resulting signals are summed.

$$S_\lambda = \sum_{i=-\infty}^{\infty}(HPF[i]\alpha\left[2.LL_{S\lambda_C(i,j)} - i\right] + LPF[i]y[2.LL_{S\lambda_C(i,j)} - i])\ ,\{\lambda = R,G,B\} \tag{13}$$

The signals obtained in equation 13 are concatenated to obtain the stego image $= (S_R, S_G, S_B)$.

2.2. Extracting Phase

It is not necessary to know which BP the hidden data is embedded in during the extraction phase. This is a great advantage of the proposed method. The only key that the receiver needs to know is the GCL. The receiver divides the S stego-image into S_R, S_G, and S_G color spaces. Each of these may simultaneously contain a piece of hidden information. Therefore, the extraction process in equation 14 is applied to each of the three channels separately and the secret data sequence obtained from the Red, Green and Blue channels is created, respectively:

$$E_\lambda = \sum_{i=-\infty}^{\infty}(HPF[i]\alpha\left[2\left(LL_{S\lambda(i,j)} - \left(\frac{LL_{C(i,j)}}{\alpha}\right)\right) - i\right] + LPF[i]y[2.(LL_{S\lambda(i,j)} - (\frac{LL_{C(i,j)}}{\alpha})) - i]) \tag{14}$$

Theoretically, it is expected that E_R, E_G, and E_B are exactly the same sequences, but in practice this may not be the case. S may have been subjected to various image attacks, such as compression, sharpening, especially in the transmission channel or in the storage phase. The proposed method compares each sequence bitwise, assuming that even in the event of an attack, it will be sufficient for at least two of these three sequences to be correct, as in table 2.

Table 2. Bitwise comparison results of 3-extracted color space data

$i.E_R$	$i.E_G$	$i.E_B$	Estimation
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

The logical expressions of the rows estimated as 1 in Table 2 were collected by equation 15:

$$E_{Gray} = (E_G . E_B) + (E_R . E_B) + (E_R . E_G) + (E_R . E_G . E_B) \quad (15)$$

Equation 15 is simplified with the Karnaugh map:

$$E_{Gray} = E_G(E_B + E_R) + (E_R . E_B) \quad (16)$$

The resulting E_{Gray} is the gray coded secret data. To convert Gray Code to Binary code, first the MSB bit is left as it is and for every kth element in the sequence:

$$Ext_B = {E_{Gray}}_k b_x \oplus \left({E_{Gray}}_k b_{x-1}\right) \quad (17)$$

Here, Ext_B is the binary encoded extracted secret data. In the last stage, Ext_B, is converted to the extracted data $E(m,n)$ consisting of m rows and n columns.

3. EXPERIMENTAL RESULTS

Basically, the similarity of S and E shows the success of the proposed method, and it can be measured by subjective and some objective methods. Subjective methods are based on the HVS and cannot be expressed mathematically [46]. In contrast, objective methods use numerical measures [47]. In this study, PSNR, SSIM, Bit Error Rate (BER) and 2-Dimension Cross Correlation (NC) are used as the objective measurements of the performance of the algorithm. PSNR for single-layer images a and b is calculated in equation 18.

$$PSNR(a,b) = 10log_{10}\left(\frac{255^2}{MSE(a,b)}\right) \quad (18)$$

The number 255 in the equation is the maximum numerical value that an 8-bit pixel can take. MSE stands for Mean Square Error and is calculated in equation 19 [48].

$$MSE(a,b) = \frac{1}{m.n}\sum_{i=1}^{m}\sum_{j=1}^{n}(a_{(i,j)} - b_{(i,j)})^2 \quad (19)$$

As MSE approaches 0, PSNR approaches infinity. For two identical signals, $PSNR = \infty$. SSIM offers a metric closer to HVS [49] and is calculated in the equation 2.

$$SSIM(a,b) = l(a,b)^{\alpha} . c(a,b)^{\beta} . s(a,b)^{\gamma} \quad (20)$$

Here, α, β, and γ, are the three significance parameters. SSIM works as a combination of correlation loss, distortion of luminance and distortion of contrast factors, and these factors are calculated respectively in equations 21, 22, and 23.

$$l(C,C') = \left(\frac{2\mu_C\mu_{C'}+k_1}{\mu_C{}^2+\mu_{C'}{}^2+k_1}\right) \quad (21)$$

$$c(C,C') = \left(\frac{2\sigma_C\sigma_{C'}+k_2}{\sigma_C{}^2+\sigma_{C'}{}^2+k_2}\right) \quad (22)$$

$$s(C,C') = \left(\frac{2\sigma_{CC'}+k_3}{\sigma_C+\sigma_{C'}+k_3}\right) \quad (23)$$

μ_C and $\mu_{C'}$ are the sample means of C and C’, σ_C and $\sigma_{C'}$ are the sample standard deviations of C and C’ respectively. $\sigma_{CC'}$ is the cross-correlation of C and C’ after subtracting their averages. k_1, k_2, and k_3 are small positive constants that stabilize each term. Therefore, samples, correlations or variances close to zero don’t lead to numerical instability [48]. Bit Error Rate (BER) is a bitwise calculation metric which is used to measure the number of bits that change between two signals. In steganography, lower BER value is the indicative of higher imperceptibility and is calculated as in the equation 24.

$$BER = \frac{Number\ of\ bit\ errors}{Total\ number\ of\ bits} \quad (24)$$

The final metric is the correlation coefficient calculation. The more similar the reference sequence and the comparative sequence are, the higher the correlation coefficient value.

$$CC = \frac{\sum_m\sum_n(a-a\prime)(b-b\prime)}{\sqrt{(\sum_m\sum_n(a-a\prime)^2)(\sum_m\sum_n(b-b\prime)^2)}} \quad (25)$$

a' is the mean of the signal a, and b' is the mean of the signal b. The propsed algorithm is tested using Lena image. The input parameters are $\alpha = 0.05$, $GCL = 2^i, \{i = 1,2,\dots,7\}$, and $BPN = 1,2,\dots,8$. The performance metrics results for a total of 56 iterations are shown in the graphs (figures 12-15), where C is the cover image, S is the stego image, D is secret data, and E is extracted data. SSIM and CC are close to HVS perception. As seen in figure 13, the perceptual similarity between D and E is independent of GCL and BP. While the perceptual similarity is high in the range of BP 1-6, it is quite low in 7 and 8. GCL did not show a significant effect on perceptual similarity. As seen in figure 14, the perceptual similarity is quite high for C and S in the first 7 BPs. The change in GCL is effective only in BP 8. PSNR and BER are closer to mathematical, and can be considered meaningless for HVS. As seen in figures 12 and 15, the difference of C and S at high BP is not meaningful for HVS, but meaningful for steganalysis techniques.

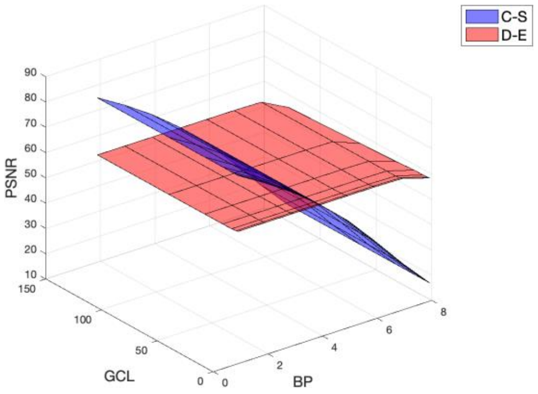

Figure 12. PSNR of C-S and D-E

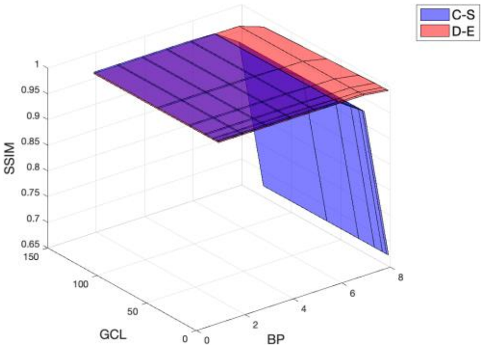

Figure 13. SSIM of C-S and D-E

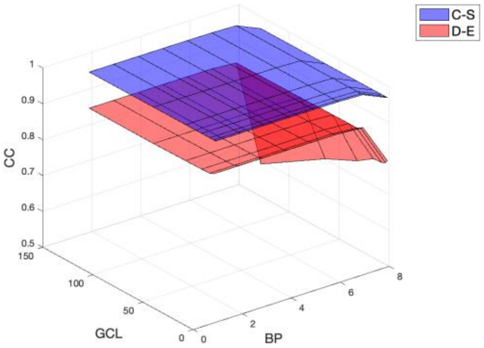

Figure 14. CC of C-S and D-E

As shown in figure 6, in standard frequency conversion methods, it does not matter which BP the transformation is performed on. Therefore, BPS data hiding generally uses spatial methods. However, as seen in figure 13 and 14, the proposed method produced imperceptible results for HVS in the first 5 LSB bit planes, especially when 4-bit and larger GC is applied.

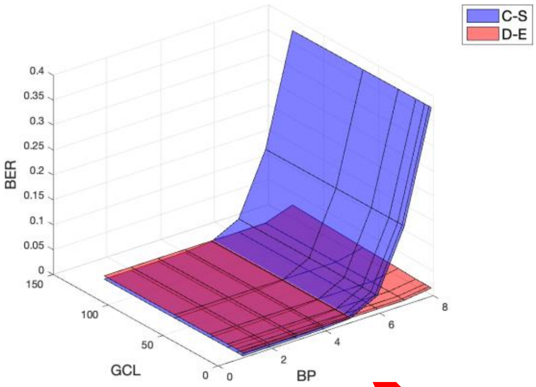

Figure 15. BER of C-S and D-E

In figure 12, it is seen that the PSNR value for cover data decreases as it approaches the MSB. This shows that the proposed method is better for statistical steganalysis only in LSBs. The extracted data is almost the same as the original secret data except for the BP number 8, as seen in figure 15. The proposed method was also tested with 3 more different digital cover images (figure 16) frequently used in the literature and the obtained results are shown in table 3.

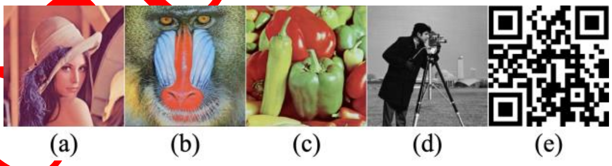

Figure 16. Test images (a) Lena (b) Baboon (c) Peppers (d) Cameraman (e) Secret data

Table 3. The best and the worst results obtained with test images.

		Cover vs stego image						**Hidden vs extracted image**					
		Worst case			**Best case**			**Worst case**			**Best case**		
	Metric	GCS	BPN	Value	GCS	BPN	Value	GCS	BPN	Value	GCS	BPN	Value
Lena	PSNR	all	8	16.4637	all	1	83.4701	128	8	55.0306	2	6	61.4526
	SSIM	all	8	0.6715	all	1-4	1	128	8	0.9807	2	1-6	0.9979
	CC	all	8	0.9673	all	1-4	1	128	8	0.5898	2	6	0.9108
	BER	all	8	0.3753	all	1	<0.00001	128	8	0.0255	2	1-6	0.0058
Baboon	PSNR	all	8	15.8823	all	1	92.1738	128	8	52.6098	2	1,2	61.4490
	SSIM	all	8	0.6771	all	1-4	1	128	8	0.9653	2	1-3	0.9979
	CC	all	8	0.8951	all	1-4	1	128	8	0.2736	2	1,2	0.9107
	BER	all	8	0.3721	all	1	<0.00001	128	8	0.0446	2	1-3	0.0058
Peppers	PSNR	all	8	16.7468	all	1	92.7738	128	8	55.7253	2	1-5	61.4512
	SSIM	all	8	0.7636	all	1-5	1	128	8	0.9841	2	1-6	0.9979
	CC	all	8	0.9459	all	1-6	1	128	8	0.06548	2	1-5	0.9107
	BER	all	8	0.4177	all	1	<0.00001	128	8	0.0217	2	1-5	0.0058
Cameraman	PSNR	all	8	18.3499	all	1	84.6819	128	8	52.0276	2	1	61.4235
	SSIM	all	8	0.8802	all	1-4	1	128	8	0.9559	2	1-4	0.9979
	CC	all	8	0.9581	all	1-5	1	128	8	0.1656	2	1	0.9101
	BER	all	8	0.3717	all	1	<0.00001	128	8	0.0505	2	1-4	0.0059

Table 4. Comparison of proposed method with state-of-the-art data hiding techniques

Paper	**Method**	**H type and size**	**Cover data versus stego data**			
			PSNR	**SSIM**	**NC**	**BER**
-	Proposed	13kB digital image	83.4701	1	1	< 0.00001
[50]	Fuzzy edge detection and LSB	Not given	61.2956	0.9998	-	-
[51]	Hamming Code and Integer Wavelet Transform	256-bit text message	76.54	0.9967	1	0.00005
[52]	Genetic algorithm on frequency domain	1.25kB text message	57.32	0.9861	0.98652	-
[53]	LSB with binary lower triangular matrix	Digital image of uncertain size	52.90	0.9999	-	0.0111
[54]	LSB	Not given	51.19	-	-	-
[55]	Block based Discrete Cosine Transform	20B text message	85.41	0.92346	0.958900	-
[56]	LSB and DES encryption	Not given	52.0235	-	-	-
[57]	LSB improved 1D chaotic map	24576B digital image	42.015941	-	0.829487 ~ 0.909341	-
[58]	LSB after flipping and shuffling	8kB text message	63.1719	-	0.9995	-
[59]	One-time pad encryption and LSB	Undefined sized image	53.2122	0.9532	-	-
[60]	LSB with shifting encrypted hidden data	~2B text message	51.656	0.99982	-	-
[61]	XOR Transposition Encryption and LSB	1kB~4kB text message	57.0260 ~ 63.5195	-	-	-
[62]	Chaos based LSB	Not given	68.37 ~ 68.88	-	-	-
[63]	Random LSB insertion	8kB text message	Mean 65.2244	-	-	-
[64]	LSB with XOR	2kB text message	64.89	-	-	-
[65]	Random selected pixel using secret keys	Not given	49.2668	-	-	-
[66]	Chaotic Particle Swarm Optimization	64×64 RGB image	51.1354	0.9982	-	-
[67]	Canonical Huffman Coding with DWT	Undefined sized image file	54.09	0.98	0.95	-
[68]	Integer Wavelet Transform	Same sized grayscale image with cover	46.041	-	-	-

There is a lot of data hiding studies in the literature. Many of them used the Lena image as the test image. Table 4 recalls state-of-the-art data hiding techniques, and puts our approach back in its place.

The significant output parameters of a data hiding algorithm are payload, robustness and imperceptibility. Table 4 provides comparative information about the payload and imperceptibility of the proposed method. As it is clearly seen, all of these methods except [57] have been tested with less than 8kB data load. However, the proposed work has been tested with 13kB data load, which is ~50% more than the state-of-art. Even with this high data load, the imperceptibility results PSNR, SSIM and NC scores were measured above all other works. Moreover, the proposed method has demonstrated high undetectable performance in the field of data hiding with a BER of one part per million despite this high data load.

3.1. Steganalysis

Steganalysis is an analysis process performed to detect the existence of information hidden by digital steganography and, if possible, to reveal its content. Steganalysis seeks answers to the questions: "Is there any hidden information?", "What is it hiding method?", "Can hidden information be extracted?". It is particularly important for the detection of hidden data leaks, prevention of illegal information transfer, detection of attempts to evade censorship, and detection of spying attempts. Various steganalysis techniques are applied to predict whether any image is a stego-image or not. The most commonly used ones for digital images are histogram analysis, RS steganalysis, and visual attacks. These steganalysis techniques are applied to the stego-image obtained with the proposed method and their results are shown.

3.1.1. Histogram analysis

The comparison of the proposed method based on the best case in table 3 with the classical frequency domain data hiding method is shown in figure 17 and 18. The purple regions in the histogram represent S, and the red regions represent C. The blue regions represent the distance between S and C. It is clearly seen in figure 18 that the S produced by the proposed method cannot be classified as a stego-image by histogram analysis.

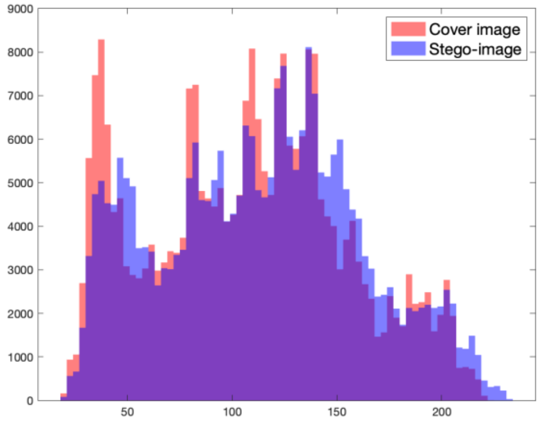

Figure 17. Histogram difference of C vs S using standard frequency domain embedding

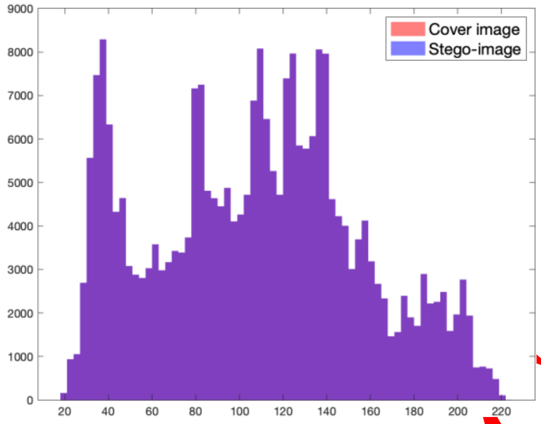

Figure 18. Histogram difference of C vs S using proposed method

3.1.2. RS steganalysis

This method uses sensitive binary statistics generated from spatial correlations of digital images [69], a discrimination function and a flipping operation to identify Regular (R), Singular (S) and Unchanged (U) pixel groups depending on how the flipping changes the value of the discrimination function. The stego-image S is divided into G separate groups, each consisting of k neighboring pixels.

$$f(G) = f(x_1, x_2, \ldots, x_k) \in S \quad (26)$$

Equation 27 is the separator function.

$$f(x_1, x_2, \ldots, x_k) = \sum_{i=1}^{k-1} |x_{i+1} - x_i| \quad (27)$$

Besides, shifting functions S_1 and S_{-1}, and mask M were used for RS steganysis.

$$S_1 : 0 \leftrightarrow 1, 1 \leftrightarrow 2, \ldots, 254 \leftrightarrow 255 \quad (28)$$

$$S_{-1} : -1 \leftrightarrow 0, 0 \leftrightarrow 1, \ldots, 255 \leftrightarrow 256 \quad (29)$$

$$M = [1\ 0\ 1\ 0\ 1] \quad (30)$$

We assume that if $f\big(F(S)\big) > f(S)$; pixel group G is Regular (R), if $f\big(F(S)\big) < f(S)$; pixel group is Singular (S), and if $f\big(F(S)\big) = f(S)$; pixel group is Unchanged (U). We calculated R_{-M}, R_M, S_{-M}, S_M, U_{-M}, and U_M to check if $R_{-M} \cong R_M$ and $S_{-M} \cong S_M$. According to the null-message hypothesis, the closer the values are to 0, the lower the probability of it being a stego-image. RS steganalysis results for both the proposed method and the classical frequency domain data hiding method are shown in figure 19. The proposed method only became distant from 0 for BPs 5, 6, and 7, meaning that the probability of S being identified as a stego-image for the other BP is low. This shows that the method is successful for RS steganalysis.

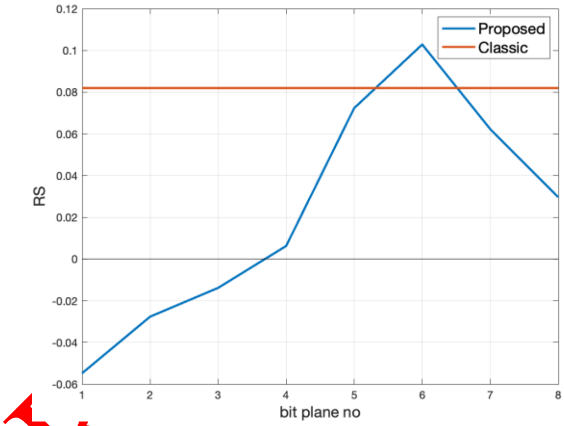

Figure 19. RS steganalysis results of proposed method versus classic method

3.1.3. Visual attacks

The way to permanently destroy confidential data from a stego image is to apply visual attacks. Spatial domain-based methods are weak to those attacks because they change the numerical values of the pixels to hide the confidential data. However, digital signal processing based methods, such as the proposed method, are more effective in protecting it against visual attacks. As a proof, some attack tests were conducted to measure the robustness of the proposed method. These attacks are Gaussian blur, which is a mathematical function used to blur an image, Gaussian noise, which is a random, unpredictable and uniformly distributed signal noise, histogram shifting, which adjusts the distribution of pixel values in a histogram, jpeg compression, which is a lossy compression algorithm that permanently removes some data from the original, the median filter, which is a non-linear digital filtering technique, often used to remove noise from an image, sharpening, which is an image-manipulation technique for making the outlines of a digital image look more distinct, salt and pepper, which is a randomized signal noise, and rotating without cropping attack which rotates the image with 45 ° to a specific direction. The proposed algorithm is tested against these attacks and the results are shown in table 5.

Table 5. Robustness of proposed method against visual attacks

Attack type	Definition	Hidden vs extracted image			
		PSNR	SSIM	NC	BER
No attack	Stego-image is not attacked.	83.4701	1	1	<0.00001
Gaussian blur (Radius: x, y=0.5)	Applies a Gaussian LPF to smooth the signal because the most of the detail remains in the HF bands.	51.7361	0.96733	0.096032	0.054498
Gaussian noise (2%)	Adds random pixel values according to a normal Gauss distribution.	51.3901	0.95886	-0.0043256	0.059017
Histogram shifting (+1)	Shifts all the pixel values by +1 or -1.	51.1349	0.96568	-0.0014261	0.062589
Jpeg compression	Applies a compression using jpeg algorithm which may cause loss of and image quality.	51.5737	0.96435	0.053794	0.056574
Median (percentile 50)	Calculates the median of pixel values in a neighborhood to reduce the noise of the image.	51.5737	0.96435	0.053794	0.056574
Sharpening (Radius=1)	Brings out more details by increasing the difference between the numerical values of pixels in the edge regions.	51.6775	0.96348	0.075477	0.055238
Salt and pepper (2%)	Adds randomly distributed noise on some pixels which makes some of the pixel black and some of them white.	57.9614	0.9954	0.79184	0.012997
Rotating without cropping	Rotating the whole stego-image by 45°.	51.4953	0.94998	0.002952	0.057605

3.1.4. Steganalysis software

There are several steganalysis software that can detect the presence of hidden information in digital images. Some of these are open source, while others are paid. Examples of open source software are StegSpy and Stegdetect [70]. StegSpy can determine if any data is stored in the file and in which file it is stored. Stegdetect is a free steganalysis software that can detect data stored in a JPEG image. The stego-object produced by the proposed method was tested with these softwares that can run many different steganalysis methods. The tests were run repeatedly on all bit-planes. In no case was the stego-object produced by the proposed method identified by these softwares. An example of this is given in figure 20.

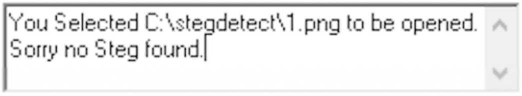
You Selected C:\stegdetect\1.png to be opened.
Sorry no Steg found.

Figure 20. Stegspy steganalysis result

3.2. Complexity

Using mathematical expressions are practical instead of using experimental methods to express the performance of an algorithm. These processes are called algorithm analysis which predicts the runtime and memory requirement of the algorithm. The amount of memory used by the algorithm at runtime is called memory cost. The memory cost of the proposed algorithm is calculated in equation 31:

$$S(n) = mxn\ bytes \tag{31}$$

In addition to S(n), the algorithm keeps 2 integer variables that cycles the loops and 2 for countering size of C. These small sized variables can be ignored for memory cost. Beside space cost, an algorithm requires a finite amount of time to run which is called time complexity. Time complexity is a useful measure in algorithm analysis. The time complexity-GCL graph of the proposed algorithm measured for the Lena image is shown in in figure 21.

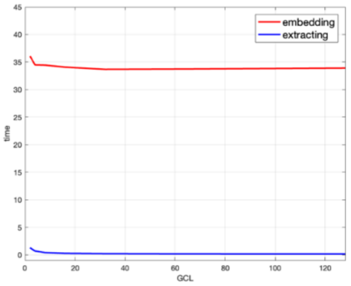

Figure 21. Time complexity-GCL graph

The amount of increase in the time cost calculation of an algorithm in the face of a large number of parameters is called complexity. It is more logical to observe the behavior of the algorithm with similar algorithms as the data size goes to infinity. In the proposed method, $O(mxn)$ is the asymptotic upper bound of the algorithm as m and n go to infinity. In short, the memory cost, time cost and algorithm complexity of the algorithm are directly proportional only to the size of C.

3. CONCLUSION

There are many studies on data hiding in the frequency domain in the literature. Some of them are hybrid studies where cryptography and steganography techniques are used together. Cryptographic methods are less preferred due to high processing load, extra data production and reduced payload. In addition, the requirement of a key for the receiver of the stego-data is a disadvantage of hybrid methods. These methods are sensitive to steganalysis because they create statistical anomalies on the stego-image. Data hiding methods on images usually lose all secret data in image attacks. In this study, a new frequency domain data hiding method is proposed where gray coding is applied to secret data. The biggest advantage of gray coding is reducing the entropy value of the secret data. Thus, the amount of statistical anomaly that will occur in the cover image after the data hiding process is reduced. Gray code length was tested in the range of $2^1, 2^2, \ldots, 2^7$. The best imperceptibility, robustness and complexity results were obtained when the gray code length is 128. However, gray code length is limited by the length of the secret data. The proposed method was tested with various parameters using the most commonly used Lena, Baboon, Peppers, and Cameraman images of the field of image processing in the literature, and the results were shown in graphs and tables. In addition, the results of the common metrics used were compared with some studies conducted in the literature in recent years. The steganalysis performance of the method was tested with RS steganalysis, histogram shifting and various visual attacks, and the results were presented. The proposed method contributed to the literature with its high imperceptibility/robustness results and low processing cost on colored images. However, in today's digital world, digital images up to 8K in size are produced. In future work, it is planned to run longer gray coding on images of these huge sizes. It is predicted that lower time complexity and higher imperceptibility can be achieved when the limit on gray code length is eliminated.

DECLARATION OF ETHICAL STANDARDS

The author of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

AUTHORS' CONTRIBUTIONS

Hüseyin Bilal MACİT: Generated and designed the algorithm, performed experiments and collected results, and wrote the manuscript.

CONFLICT OF INTEREST

There is no conflict of interest in this study.

REFERENCES

[1] Apau R., Koranteng F.N., Gyamfi S.A, "Cyber-crime and its effects on E-commerce technologies", ***Journal of Information***, (5)1: 39–59, (2019).

[2] Park H.S., "Technology convergence, open innovation, and dynamic economy", ***Journal of Open Innovation: Technology, Market, and Complexity,*** (3)4: 24, (2017).

[3] Norquay, J. 2023, "How Many Emails Are Sent Per Day In 2024?", [Online] https://prosperitymedia.com.au/how-many-emails-are-sent-per-day-in-2024, (2024).

[4] Aslam S., "80+ Facebook Statistics You Need to Know in 2023—Omnicore." [Online] https://www.omnicoreagency.com/facebook-statistics/, (2023).

[5] Aslam, S. "Instagram by the Numbers: Stats, Demographics & Fun Facts", [Online] https://www.omnicoreagency.com/instagram-statistics/, (2024).

[6] Duarte, F., "Amount of Data Created Daily", J [Online] https://explodingtopics.com/blog/data-generated-per-day, (2024).

[7] Waseso B.M.P., Setiyanto N.A., "Web phishing classification using combined machine learning methods", ***Journal of Computing Theories and Applications***, (1)1: 11–18, (2023).

[8] Sakr, H.A., El-Afifi, M.I. "A Framework for Confidential Document Leakage Detection and Prevention", ***Nile Journal of Communication & Computer Science***, (7), (2024).

[9] Apau R., Asante M., Twum F., Ben Hayfron-Acquah J., Peasah K.O., "Image steganography techniques for resisting statistical steganalysis attacks: A systematic literature review", ***PLoS ONE,*** 19(9), (2024).

[10] Gautam, D., Agrawal, C., Sharma, P., Mehta M., Saini, P., "An Enhanced Cipher Technique Using Vigenère and Modified Caesar Cipher," ***2nd International Conference on Trends in Electronics and Informatics***, Tirunelveli, India, 1-9, (2018).

[11] Qadir A.M., Varol N., "A review paper on cryptography," ***7th International Symposium on Digital Forensics and Security***, 1–6, (2019).

[12] Sahu A.K., Sahu M., "Digital image steganography and steganalysis: A journey of the past three decades," ***Open Computer Science,*** (10)1: 296–342, (2020).

[13] Stallings W. Brown L., "Computer security: principles and practice". ***Upper Saddle River: Pearson Education***, IV. Edition, ISBN: 978-0133773927, England, (2017).

[14] Al-Batah, M.S., Alzboon, M.S., Alzyoud, M., Al-Shanableh, N. "Enhancing Image Cryptography Performance with Block Left Rotation Operations", ***Applied Computational Intelligence and Soft Computing***, (2024)1: 1-19, (2024).

[15] Westfeld, A., "Steganalysis in the Presence of Weak Cryptography and Encoding", ***5th International Workshop***, Jeju Island, Korea, 19-35, (2006).

[16] Kour J., Verma, D., "Steganography Techniques – A Review Paper", ***International Journal of Emerging Research in Management &Technology***, 3(5): 132-135, (2014).

[17] Macit, H.B., Koyun, A., Güngör, O., "A Review and Comparison of Steganography Techniques", ***4'th International Academic Research Congress***, Alanya, Türkiye, 37-44, (2018).

[18] Kurnaz H., "Hibrit Yaklaşımlı Yeni Bir Seganografi Yönteminin Geliştirilmesi," ***M.S. thesis***, Kocaeli University, Institute of Science, (2019).

[19] Chaum D., "Untraceable Electronic Mail, Return DWTresses and Digital Pseudonyms", ***Communications of the ACM***, 24(2), 84-88, (1981).

[20] Jayaram, P., Ranganatha, H.R., Anupama, H.S. "Information Hiding Using Audio Steganography – A Survey", ***The International Journal of Multimedia & Its Applications***, (3)3: 86-96, (2011).

[21] Macit, H.B., "The Effect of Resolution and Watermark Strength on Multi-level DWT Image Watermarking", ***Düzce Üniversitesi Bilim ve Teknoloji Dergisi***, (12)2: 1178-1191, (2024).

[22] Kutucu, H., Dişli, A., Akça, M., "Çok Katmanlı Steganografi Tekniği Kullanılarak Mobil Cihazlara Haberleşme Uygulaması", ***Akademik Bilişim Konferansı***, Eskişehir, Türkiye, 672-678, (2015).

[23] Liu, B., Xu, E., Wang, J., Wei, Z., Xu, L., Zhao, B., Su, J., "Thwarting Audio Steganography Attacks in Cloud Storage Systems***", International Conference on Cloud and Service Computing,*** Hong Kong, 259-265, (2011).

[24] Rabah, K. "Steganography – The Art of Hiding Data", ***Information Technology Journal,*** 3(3): 245-269, (2004).

[25] Cachin, C., “An information-theoretic model for steganography”, ***Information Hiding 2nd International Workshop***, New York, 306–318, (1998).

[26] Rachid, R.S., “Binary Image Watermarking on Audio Signal Using Wavelet Transform”, ***M.S. thesis***, Çankaya University, Institute of Science, (2014).

[27] Şener, D., Güney, S. “Enhancing Steganography in 256×256 Colored Images with U-Net: A Study on PSNR and SSIM Metrics with Variable-Sized Hidden Images”, ***Review of Computer Engineering Studies***, (11)2: 13-29, (2024).

[28] Poornima R., Iswarya R.J., “An overview of digital image steganography”, ***International Journal of Computer Science & Engineering Survey***, (4)1: 23–31, (2013).

[29] Özdemir B., Doğan N., “Data hiding to the image with bit plane slicing and double XOR”, ***MANAS Journal of Engineering,*** (10)1: 66-72, (2022).

[30] Jebur, S.A., Nawar, A.K., Kadhim, L.E., Jahefer, M.M. “Hiding Information in Digital Images Using LSB Steganography Technique”, ***International Journal of Interactive Mobile Technologies***, 17(7): 167-178, (2023).

[31] Akbar S., Rao K.N., Anand T., “Bit-Plane Slicing Algorithm for Crime Data Security Using Fusion Technologies”, ***International Journal of Recent Technology and Engineering,*** (7): 323-325, (2019).

[32] Abdülkhaev, A., “A New Approach for Video Watermarking”, ***M.S. thesis,*** Gaziantep University, Institute of Science, (2016).

[33] Patel, M., Sajja, P.S., Sheth, R., “Analysis and Survey of Digital Watermarking Techniques”, ***International Journal of Advanced Research in Computer Science and Software Engineering***, (3)10: 203-210, (2013).

[34] Araghi, T.K., Megías, D. “Analysis and effectiveness of deeper levels of SVD on performance of hybrid DWT and SVD watermarking”, ***Multimed Tools App***, (83): 3895–3916, (2024).

[35] Pereira, S., Voloshyoskiy, Y., Pun, T., “Optimal transform domain watermark embedding via linear programming”, ***Signal Process,*** (81)6: 1251-1260, (2001).

[36] Hsieh, M., Tseng, D., Huang, Y., “Hiding Digital Watermarks Using Multiresolution Wavelet Transform”, ***IEEE Trans. on Industrial Electronics,*** 48(5): 875-882, (2001).

[37] Xia, X.G., Boncelet, C.G., Arce, G.R., “A multiresolution watermark for digital images”, ***IEEE International Conference on Image Processing,*** Santa Barbara, USA, 548-551, (1997).

[38] Yavuz, E., “Duruk İmgelerde Damgalama ve Veri Saklama”, ***PhD. thesis,*** Ankara University, Institute of Science, (2008).

[39] Abd-El-Atty, B., El-Affendi, M., El-Latif, A.A.A., “A novel image cryptosystem using Gray code, quantum walks, and Henon map for cloud applications”, ***Complex & Intelligent Systems,*** (9): 609–624, (2023).

[40] Ngyuen, B.C., Yoon, S.M., Lww, H.K., “Multi Bit Plane Image Steganography”, ***5th International Workshop***, Jeju Island, Korea, 8-10, (2006).

[41] Qi, W. Liu, Y., Sirui, G., Wang, X., Guo, Z. “An Adaptive Visible Watermark Embedding Method based on Region Selection”, ***Security and Communication Networks,*** (2021), 1-11, (2021).

[42] Mannepalli, P.K., Richhariya, V., Gupta, S.K. “A robust blockchain-based watermarking using edge detection and wavelet transform”, ***Multimed Tools Appl,*** (2024).

[43] Dinçer G., Entropi Kavramının İstatistikteki Bazı Uygulamaları, ***M.S. thesis,*** Yıldız Teknik University, Institute of Science, (2015).

[44] Shannon, C.E., “A mathematical theory of communication”, ***Bell Systems Technology Journal,*** (27): 379-423, (1948).

[45] Pal, N.R., Pal, S.K., “Entropy: A New Definition And Its Applications”, ***IEEE Transactions on Systems, Man and Cybernetics,*** (21)5: 1260-1270, (1991).

[46] Farrell, J. E., “Image quality evaluation in colour imaging: vision and technology”, Eds: MacDonald, L.W., Luo, M.R., ***John Wiley***, Stanford, (1999).

[47] Cadik, M., Slavik, P., “Evaluation of two principal approaches to objective image quality assessment”, ***8th International Conference on Information Visualisation,*** North Carolina, 513-551, (2004).

[48] Hore, A., Ziou, D., “Image quality metrics: PSNR vs. SSIM”, ***International Conference on Pattern Recognition***, İstanbul, Türkiye, 2366-2369, (2010).

[49] Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P., “Image quality assessment: from error visibility to structural similarity”, ***IEEE Transactions on Image Processing***, (13)4: 600-612, (2004).

[50] Setiadi, D.R.I.M., Rustad, S., Andono, P.N., Shidik G.F., “Graded fuzzy edge detection for imperceptibility optimization of image steganography”, ***The Imaging Science Journal***, (72)6: 693-705, (2024).

[51] Saeidi, Z., Yazdi, A., Mashhadi, S., Hadian, M. Gutub, A., “High performance image steganography integrating IWT and Hamming code within secret sharing”, ***IET Image Process***, (2024)18: 129–139, (2024).

[52] Pramanik, S., “An adaptive image steganography approach depending on integer wavelet transform and genetic algorithm”, ***Multimed Tools App,*** (82): 34287–34319, (2023).

[53] Prasad, S. Pal, A.K., Mukherjee, S., “An RGB Color Image Steganography Scheme by Binary Lower Triangular Matrix”, ***IEEE Transactions on Intelligent Transportation Systems***, (24)7: 6865-6873, (2023).

[54] Dumre, R., Dave, A., “Exploring LSB Steganography Possibilities in RGB Images”, ***12th International Conference on Computing Communication and Networking Technologies***, Kharagpur, India, 1-7, (2021).

[55] Abdel-aziz, M.M., Hosny, K.M., Lashin, N.A., “Improved data hiding method for securing color images”, ***Multimed Tools Appl,*** (80): 12641–12670, (2021).

[56] Kareem, H.R., Madhi, H.H., Mutlaq, KA., “Hiding encrypted text in image steganography”, ***Periodicals of Engineering and Natural Sciences*** (8)2, pp. 703–707, (2020).

[57] Pak, C. Kim, J. An. K., Kim, C., Kim, K., “A novel color image LSB steganography using improved 1D chaotic map”, ***Multimed Tools Appl***, (79): 1409–1425, (2020).

[58] Rahman, S., Masood F., Khan, W.U., Ullah, N., Khan, F.Q., Tsaramirsis, G., Jan, S., Ashraf, “A Novel Approach of Image Steganography for Secure Communication Based on LSwB Substitution Technique”, **Computers, Materials & Continua**, (64)1: 31–61, (2020).

[59] Calanda, F.B., Sison, A.M., Molato, M.R.D., Medina, R.P., “A Modified Least Significant Bit Randomized Embedding Method based on Image Partitioning and Columnar Transposition with Encryption”, ***2nd***

International Conference on Computing and Big Data, New York, 68–72, (2019).

[60] Solak, S., Altınışık, U., “A New Approach for Steganography: Bit Shifting Operation of Encrypted Data in LSB (SED-LSB)*”, **J Inf Tech***, (12)1: 75–82, (2019).

[61] Setyono, A., Ignatius, D.R., Setiadi, M., “Securing and Hiding Secret Message in Image using XOR Transposition Encryption and LSB Method”, ***Journal of Physics,*** (1196): 1-6, (2019).

[62] Mukherjee, S., Sanyal, G., “A chaos based image steganographic system”, ***Multimed Tools Appl***, (77)21: 27851–27876, (2018).

[63] Rajput G.G., Chavan R., “A Novel Approach for Image Steganography Based On Random LSB Insertion in Color Images”, ***International Conference on Intelligent Computing Systems***, Tamilnadu, India, 265–273, (2017).

[64] Chauhan, S., Jyotsna, Kumar, J., Doegar, A., “Multiple layer Text security using Variable block size Cryptography and Image Steganography”, ***3rd International Conference on Computational Intelligence & Communication Technology***, Ghaziabad, India, 1-7, (2017).

[65] Dagar, S., “Highly Randomized Image Steganography using Secret Keys”, ***IEEE International Conference on Recent Advances and Innovations in Engineering***, Jaipur, India, 1-5, (2014).

[66] Jaradat, A., Taqieddin, E., Mowafi, M., "A high-capacity image steganography method using chaotic particle swarm optimization", ***Hindawi Security and Communication Networks,*** (2021)1, 1-11, (2021).

[67] Babu, A.R., Al-Fatlawy, R.R., Veeranjaneyulu, K., Kumar, K.S., "Canonical Huffman Coding (CHC) - Discrete Wavelet Transform (DWT) Method for Image Steganography," ***2024 International Conference on Integrated Circuits and Communication Systems (ICICACS)***, Raichur, India, 1-4, (2024).

[68] Yassin, N.I.R., El-Houby, E.M.F., "Image Steganography Technique Based on Integer Wavelet Transform Using Most Significant Bit Categories." ***International Journal of Intelligent Engineering & Systems***, (15)1, 499-508, (2022).

[69] Fridrich, J., Goljan, M., Du, R., “Reliable Detection of LSB Steganography in Color and Grayscale Images”, ***ACM Workshop on Multimedia and Security***, Ottawa, Canada, 27-30, (2001).

[70] Hassan, M.D., Amin, M.A.M., Mahdi, S.T., "Steganalysis Techniques and Comparison of Available Softwares", ***Proceedings of the 1st International Multi-Disciplinary Conference Theme: Sustainable Development and Smart Planning, IMDC-SDSP-2020***, (2020).