International Journal of Computer Vision and Signal Processing, 1(1), 1-9(2019) ORIGINAL ARTICLE

On a Secure Steganography Approach with Increased Capacity and Security

Aqsa Rashid

Department of Information Security
National University of Science and Technology, Islamabad/Rawalpindi 44000, Pakistan

Department of Computing and Technology
Iqra University, Islamabad 44000, Pakistan

Nadeem Salamat*

Department of Mathematics
Khwaja Fareed University of Engineering and Information Technology, RahimYar Khan 64200, Pakistan

V. B. Surya Prasath

Division of Biomedical Informatics
Cincinnati Children's Hospital Medical Center, Cincinnati OH 45229 USA

Department of Pediatrics, University of Cincinnati, OH USA

Department of Biomedical Informatics
College of Medicine, University of Cincinnati, Cincinnati OH 45267 USA

Department of Electrical Engineering and Computer Science
University of Cincinnati, Cincinnati OH 45221 USA

Abstract

The data security in the digital communication is the major issue in this technological era. There are lots of methods and protocols used for secure communication, steganography is one of them. In this paper, we present the χ Secure Crypto-Stego_System for secure communication. A common 256 bits random key is used at the encryption and embedding phase. The entropy and joint image histograms are used for the evaluation of security measure for the method. Experiments were performed with different embedding rate in the selected cover data set of images. The results that we achieved, are the proof of the fact that the proposed scheme is a good contribution in the scientific community in the field of Information hiding.

IJCVSP
International Journal of Computer Vision and Signal Processing

ISSN: 2186-1390 (Online)
http://cennser.org/IJCVSP

Article History:
Received: 23 June 2018
Revised: 3 December 2018
Accepted: 24 March 2019
Published Online: 27 March 2019

Keywords: Entropy, Joint Histogram, Secure Stego System, Cryptography, Steganography, Crypto-Stego method.

© *2019, IJCVSP, CNSER. All Rights Reserved*

1. Introduction

Revolution in internet provides the easy way of communication between two or more parties; meanwhile, it's a big challenge to secure the information and way of communication over the internet, which is an open network. In order to discourse the security challenges, lots of methodologies have been suggested under cryptography (information encryption) and Steganography (information hiding). Cryptography transforms a secret information in such a way that it converts to an unintelligent communication to observers [1]. But the problem is, it draws attention. Therefore, it is essential to have an imperceptible commu-

*Corresponding author
Email addresses: aqsa.phd@students.mcs.edu.pk (Aqsa Rashid), nadeem.salamat@kfueit.edu.pk (Nadeem Salamat), prasatsa@uc.edu (V. B. Surya Prasath)

nication deprived of observing to anyone in the communication channel. That's why steganography [2] mechanism is required.

The steganography algorithms are classified based on the data embedding and extraction techniques and these classifications are discussed in [3, 4, 5, 6, 7, 8, 9]. These algorithms are also classified on the basis of key used for data embedding algorithm, this includes the pure, private and public key steganography. In recent years, many algorithms have been developed in this field and are categorized as Least Significant Bit based steganography methods, improved Least Significant Bit based methods, adaptive schemes for Least Significant Bit in human visual system etc. Rashid and Rahim [10] provide a comprehensive review of more than hundred algorithms of steganography. The Least Significant Bit (LSB) substitution based methods are described in [11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21]. The improved version of the Least Significant Bit matching stego-system are discussed in [22, 23]. These methods improve the computational complexity of the simple Least Significant Bit matching method. The data is embedded into the pixels using the difference operator in the method proposed by Li et al.[24]. The *pair wise* attacks of the stego systems are analyzed by Chi-Square test [25, 3, 4].

An adaptive scheme for LSB based stenography in the Human Visual System (HVS) is introduced by Stanley [5]. Lie and Chang [26] used luminance and contrast properties of the Human Visual System (HVS) for the stego-system. A comprehensive study of stego attacks on a stego system is found in [6, 7, 3]. The term steganalysis is used to study the methods for detection of hidden messages without the priori knowledge of algorithm and key implemented in the algorithms. The methods which have successfully break embedding algorithms are discussed in [27, 8, 9, 28, 29, 30, 31].

The above cited algorithms for stego systems have some limitations in terms of Type I and Type II Error [20], in terms of attacks (active and passive attacks [22, 23]) and computational complexity [1, 10]. In this paper, we present a crypto-stego system that uses the same, unique 256 bits key for crypto and stego part of the crypto-stego system that have the feature of unnoticeable change in image quality, better security, high embedding rate and less computational complexity.

A stego system is called perfectly secure [21], if the entropy of both the cover and stego images matches completely i.e., the difference is zero. It is called a χ secure stego system, if the entropy difference of the cover and stego objects is close to zero. In this paper, a private key χ-Secure Stego-System is proposed, which uses the unique key for encryption and steganography steps. This method have the features of increased capacity and security. This includes probability of chosen stego attacks, reduces the computational complexity and statistical or probabilistic errors.

The rest of the paper is arranged as follows. Section 2 covers the proposed method and formal presentation of embedding and extraction process. The evaluation of the method is discussed in Section 3. Section 4 includes simulation results and discussion. The paper is concluded in Section 5 and future research directions are discussed.

2. Proposed Secure Crypto-Stego Method

The proposed crypto-stego approach completes its processing in four phases. This is shown in Figure 2. An algorithm is proposed for each phase. The data is first encrypted and then embedded in the image at sender side. The process of encryption and embedding data is described in Algorithm 1 and 2. Both the algorithms performed in a concatenation.

The whole process is reverse to the sender side. first of all, the extraction algorithm extract data from the stego image and second Algorithm 4, for decrypt the data, as a result, the secret message is recovered. The process of transformation of plain text in to cipher text and the cipher text is embedded into the image is performed with the help of the key.i.e, the key is used at every phase, in each algorithm, for encrypting, embedding phases to transfer plain text into cipher text and to find pixel locations. At receiver end, to extract and decrypt data for the recovery of secret message. The algorithms at both ends, use shared secret key. The key length is 256 bits, which is the secure as the description of Data Encryption Standard (DES). This has the 2^{256} possibilities of key compositions. The system for the selection of key dependent random pixels for data embedding is described in equation (1).

$$RP = (65535 \bmod(65535 \bmod \sum_{i=0}^{31} Sk_i^3)) + 1 \qquad (1)$$

The Sk represents the bytes of key, if $RP > 255$ then use an other option for key. The system composed of two modules, the sender and reception position. These modules are explained as the encryption and embedding module and the Extraction and decryption modules. These are explained in the following subsections.

2.1. Encryption and embedding

There are two steps, for the embedding encrypted data in the cover medium. The first algorithm encrypts the data using the stego key. The algorithm can be performed in two ways, block wise or as a whole text. For block wise, The whole binary equivalent of plain text is divided into block of 256 bits and padding is implemented if the BESM is not multiple of 256. The XOR operation is performed on each block, then concatenation is perfumed to complete the encryption. One the other hand, the XOR operation is performed on equal logical statements, so a concatenation is performed on the stego key followed by the XOR operation once as whole. The Formal steps for the encryption

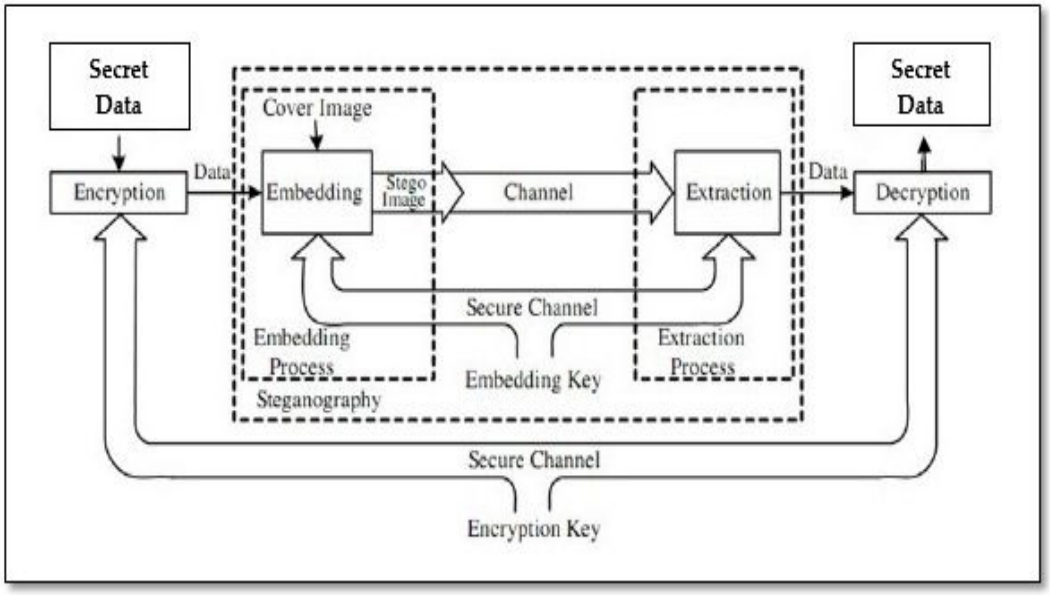


Figure 1: Flow of the proposed ecure crypto-stegno model.

Algorithm 1: Encryption algorithms

Data: Secret message (SM), Stego Key (SK)
Result: Bit Stream (BS) (cipher text)
1 Read secret message (SM);
2 Binary equivalent (BESM) of SM.;
3 Read stego key (SK);
4 Binary equivalent (BESK) of SK;
5 Concatenate BESK till the length of BESM;
6 $BESM \oplus BESK$;
7 Store as bit stream BS;

algorithm are:

The out put of Algorithm 1 is used as the input of the Algorithm 2. Once the data is encrypted, then we need to embed this data into the cover image. This algorithm embeds the encrypted message into cover image. In this algorithm, Pel is used for pixel value of a randomly selected pixel in cover and stego image and TCB represents two consecutive bits from the BS.

2.2. Extraction Process

The extraction process of information from the medium is performed at the receiver end. Once the stego image reached to the receiver, then next step is to extract and decrypt the hidden information. The extraction is given in Algorithm 3. The output of this algorithm is a binary equivalent of the hidden message. Once the hidden information into the stago images is extracted, then the next phase is to decrypt this information. Algorithm 4 decrypt the crypted information using the stego key.

3. Evaluation Methodology

Numerous methods can be found in literature for stego-systems evaluation in terms of perceptibility [32, 33, 34]. For evaluation, three methods are used. One is the visual perception and spatial resolution is checked with the mere visual inspection. Two statistical measures, entropy and joint entropy (histogram) are computed to check randomness in images. Because, if the difference in entropy is low and joint histogram is ideal then all other measure will also give acceptable results.

3.1. Entropy

For efficiency evaluation entropy matrix is used. Mathematical, the entropy is defined as:

$$\chi(d) = \sum_{i=1}^{N} p(d_i) \log\left(\frac{1}{p(d_i)}\right) \tag{2}$$

where N is the number of pixels in an image and $p(d_i)$ is the probability of occurrence of a pixel in an image with value d_i. This definition is inversely related to the randomness of pixel values in an image, higher values are corresponding to the precise results. In this setting, the entropy measure is used to measure the level of security and robustness. Let $\chi(\theta)$ represents the entropy of cover image while $\chi(\phi)$ denotes that of Stego image. The ideal and perfect possibility is both the images have same entropy, i.e., $\chi(\theta) = \chi(\phi)$. However if difference between the two is not very less then system is χ_Secure Stego-system.

3.2. Joint Entropy

The joint entropy, also known as joint histogram creates a two dimensional feature space [35, 36, 37]. This shows

Algorithm 2: Embedding algorithms

Data: Cover Image (CI), BS, Stego key (SK)
Result: Stego Image SI

```
Read cover image (CI);
Read SK;
Read BS ;
while half length of the message bit BS do
    Take two consecutive bits of BS;
    if TCB=00 then
        S=0;
    else
        if TCB=01 then
            S=1;
        else
            if TCB=10 then
                S=2;
            else
                S=3
            end
        end
    end
end
Compute random pixel location by Eq.(1);
Put n = 4;
Compute Pel_SI = Pel_CI − (Pel_CI mod n) + S);
```

Algorithm 3: Extraction algorithms

Data: Stego Image SI, Stego Key SK
Result: Binary sequence S

```
Read SI, SK;
Compute pixel location by equation (1) ;
Compute S by : S = (Pel_SI mod n);
Store results in binary sequence S;
```

the occurrence of combination of a particular feature in both images. The robustness of the method is directly related to the measure of imperceptibility or detectability of hidden data into the medium. This is directly related to the change in images. The joint histogram, $j_\chi(X, Y)$ of two images (X, Y) with a joint distribution $p(x, y)$, is mathematically defined as:

$$j_\chi(X, Y) = \sum_{xinX} \sum_{y \in Y} p(x, y) \log p(x, y) \tag{3}$$

Each entry in this histogram is composed of a set of local features. The linear output of this feature space intuitively shows that there is no change in statistical measures of pixels and the highest level of change in pixels is reflect as the nonlinear and variational output of joint histogram. The joint histogram of two totally dis-similar images is shown in Figure 2(a) and that of similar images is shown in Figure 2(b).

We use the histogram and entropy features of the stego and cover images for the strength evaluation of encryption strength and evaluation of steganography algorithms. These measures are effective for both type of algorithms and equally used for the security analysis and steganalysis.

Algorithm 4: Algorithms for decryption

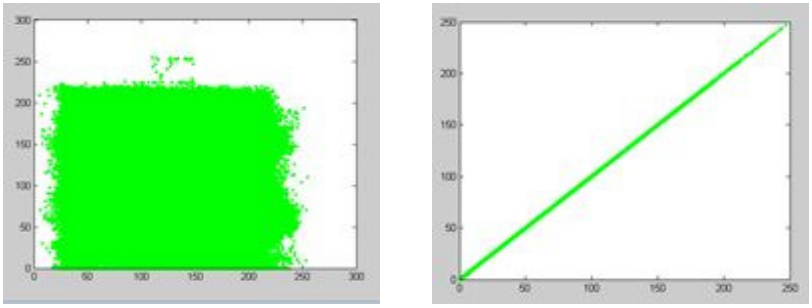
Data: Stego Key (SK), S
Result: Secret Message SM ()

```
Read SK, S ;
Compute BESK, binary equivalence of SK;
while length of the message bit S do
    if s=0 then
        BS=00;
    else
        if s=1 then
            BS=01;
        else
            if s=2 then
                BS=10;
            else
                BS=11
            end
        end
    end
end
Concatenate SK to the length of BS;
SM = BS ⊕ SK ;
Compute plain text from SM ;
```

4. Simulation Results and Discussion

In this section, the proposed method is applied to a set of test image taken from the benchmark databases. For this purpose, we choose two data sets, one is gray scale image and the other is radiographic image data set. A set of five images are chosen at random from each data set. The five gray scale images taken from The USC-SIPI image database are represented in Figure 3. The SIPI Image database is a free online database of ariel, texture and miscellaneous benchmark gray scale and color images. In this discussion, these images are called, Sipi-I (Figure 3(a)), Sipi-II (Figure 3(b)),Sipi-III (Figure 3(c)), Sipi-IV (Figure 3(d)) and Sipi-V(Figure 3(e)). We note that the method can also be potentially used in other images such as aerial [38], and medical images [21, 39].

The second set of experiments is performed on radiographic images, chosen from Medpix images database, which is a free online medical image test database. In these experiments, images are named as Medpix-I (Figure 4(a)), Medpix-II (Figure 4(b)), Medpix-III (Figure 4(c)), Medpix-IV (Figure 4(d)) and Medpix-V (Figure 4(e)). The efficiency of the method is taken into account in both visual perception and in terms of statistical changes. The statistical changes are measured with the shape of joint histograms and the effect of embedding on the entropy of the image.



(a) Two dissimilar Images (b) Two Similar Images

Figure 2: Joint Histograms.

(a) (b) (c) (d) (e)

Figure 3: Test images from USC-SIPI image database.

Table 1: Entropy after embedding 8272 bits data in images Figure 3.

image	$\chi(\theta)$	$\chi(\phi)$	$\chi(\theta) - \chi(\phi)$
Sipi-I	7.455001e+00	7.455165e+00	1.644582e-04
Sipi-II	7.633334e+00	7.633409e+00	7.562311e-05
Sipi-III	7.174150e+00	7.173669e+00	-4.803017e-04
Sipi-IV	7.189197e+00	7.188824e+00	-3.728448e-04
Sipi-V	7.583897e+00	7.584505e+00	6.076858e-04

Table 2: Entropy for cover images in Figure 3, Stego images in Figure 7 and their differences.

image	$\chi(\theta)$	$\chi(\phi)$	$\chi(\theta) - \chi(\phi)$
Sipi-I	7.455001e+00	7.455316e+00	3.158314e-04
Sipi-II	7.633334e+00	7.633387e+00	5.391741e-05
Sipi-III	7.174150e+00	7.173194e+00	-9.560168e-04
Sipi-IV	7.189197e+00	7.189227e+00	3.328143e-04
Sipi-V	7.583897e+00	7.584578e+00	6.807030e-04

On each data set, two tests are performed. In first set of experiments, gray images, represented in Figure 3 are considered as cover images. The 8272 bits of data is embedded into cover images and resulting stego images are represented in Figure 5 for visual comparison. The joint histograms computed as equation (Eq.(3)).

The Joint histograms between images in Figure 5 and Figure 3 are shown in Figure 6. First histogram in this figure is joint histogram between image (Figure 3(a)) and image (Figure 5(a)). Similarly histogram between image (Figure 3(b)) and (Figure 5(b)) is represented by image (Figure 6(b)). The other are also represented in a similar correspondence.

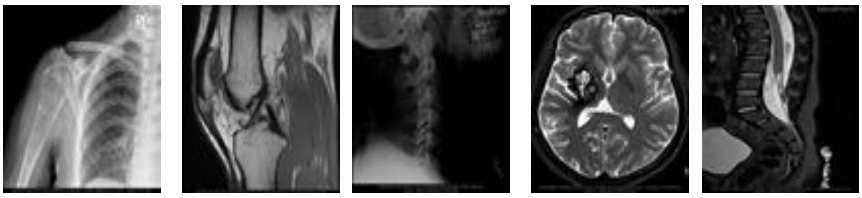
In a similar way, the statistical measure, entropy is also computed as given in equation (2). The first column of Table 1 contains image names, the entropy of original images are denoted in second column of table. Entropy of corresponding stego image is provided in third column of the table. The difference of two entropies is described in fourth column of Table1.

The second experiment is performed on same data set, with increased embedding rate. In this experiment, stego images in Figure 7 are represented after embedding 14704 bits of data into cover images of Figure 3. Visually, both the corresponding pair of images seems to be similar and no visual change is observed in these image pairs.

In Figure 8, joint histogram between each pair of image in Figure 3 and Figure 7 is given. In these histograms, The shape of histogram shows that the image pair is similar and there is no statistical change observed in images after embedding of 14704 bits data in cover image.

The second statistical measure, entropy of images represented in Figure 3 and stego images in Figure 7 and difference between these two entropies is described in Table 2. The difference between two entropies shows that there is a very small change in statistical features of the stego images.

The third set of experiment is performed on radiographic images represented in Figure 4. The images in Figure 9 are the results embedding 8272 bits data in cover images of Figure 4. These results show that there is no

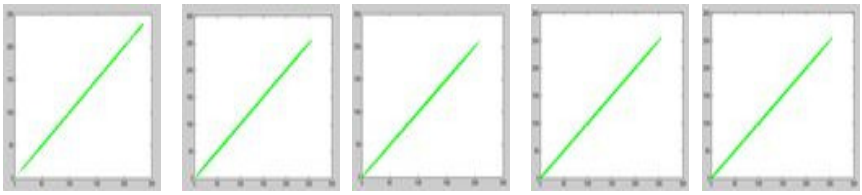


(a) (b) (c) (d) (e)

Figure 4: Test images from Medpix database.

(a) (b) (c) (d) (e)

Figure 5: Stego images after embedding 8272 bits into cover images of Figure 3.

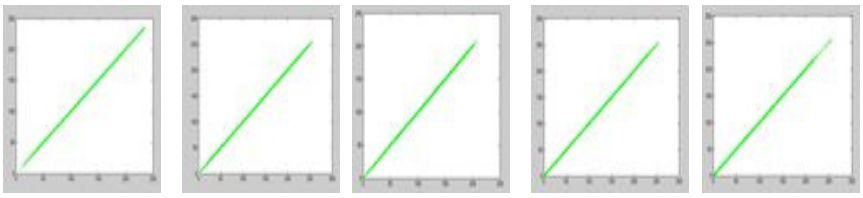


(a) (b) (c) (d) (e)

Figure 6: Joint histogram for images of Figure 3 and Figure 6.

(a) (b) (c) (d) (e)

Figure 7: Stego images after embedding 14704 bits in cover images of Figure 3.



(a) (b) (c) (d) (e)

Figure 8: Joint histograms of images in Figure 3 and Figure 7.

Table 3: Entropy after embedding 8272 bits data in images represented in Figure 4.

image	$\chi(\theta)$	$\chi(\phi)$	$\chi(\theta) - \chi(\phi)$
Medpix-I	7.001516e+00	7.024974e+00	2.345766e-02
Medpix-II	7.266514e+00	7.267353e+00	8.396193e-04
Medpix-III	5.389515e+00	5.399230e+00	9.715365e-03
Medpix-IV	6.981962e+00	6.982392e+00	2.031763e-04
Medpix-V	6.401003e+00	6.401436e+00	4.328055e-04

Table 4: Entropy of original images and after embedding 14704 bits data in images Figure 4.

image	$\chi(\theta)$	$\chi(\phi)$	$\chi(\theta) - \chi(\phi)$
Medpix-I	7.001516e+00	7.039383e+00	3.786650e-02
Medpix-II	7.266514e+00	7.268214e+00	1.700425e-03
Medpix-III	5.389515e+00	5.403955e+00	1.444042e-02
Medpix-IV	6.981962e+00	6.982194e+00	5.609850e-06
Medpix-V	6.401003e+00	6.401552e+00	5.491430e-04

visual change marked in these images.

Figure 10 shows joint histograms between images of Figure 4 and Figure 9. The appearance of joint histograms shows that both images are similar and no spatial change is observed.

The entropies of these images represented in Table 3. The values in fourth column of table shows that there is a small change in the entropy of cover and stago images after embedding 14704 bits of data.

The fourth set of experiments with embedding 14704 bits data into cover images, which are represented in Figure 4. The resulting images are represented in Figure 11. Obliviously both images appears similar and no spatial or resolution change is marked in these images.

The joint histograms between these images of Figure 4 and stego images represented in Figure 11 are computed and results of these histograms are shown in Figure 12. The histograms shows that both images are similar and there is no difference observed in pixel values between these pair of images.

The second type of statistical measure, entropy is computed for each pair of images and results are described in Table 4. The third column shows results of difference between two entropies. The values in this column shows that is a minor change in two entropies.

The cover images represented in Figure 3 appears similar to stego images represented in Figure 5 and Figure 7 after embedding 8272 bits and 14704 correspondingly. Similarly, images represented in Figures 11 and 9 are the results of embedding same data in radiographic images represented in Figure 4. It is observed that change in visual appearance of stego images are imperceptible as compare to that of their corresponding cover images. Joint histograms of these image pairs are shown in Figures 6, 8, 10, and Figure 12. The appearance shape of histograms shown in Figures 6, 8, 10 and Figure 12 provide information that embedding rate does not effect the visual and statistical features of images. The key length shows that the system is secure. The fourth column in Tables 1, 2 3, and Table 4 shows that the change in entropy is minimum and our method of encryption and steganography represents the χ_Secure Stego_System. The method uses embedding rate of two bits per pixel so method is also increased capacity stego_system.

Table 5 summarize the comparison of the proposed method with the methods discussed in the literature review section in the introduction. Table 5 compares the important properties of stego systems i.e., embedding rate which is capacity per pixel, security level, complexity and Image quality after embedding.

5. Conclusion and Future Work

The secure transmission of secret data over the internet or communication channels is the active research topic. The proposed, χ_Secure Stego-System can be used for the communication of such data. This is a crypto-stego model with increased embedding capacity. The secure key is used twice for any cipher text, this results that the security level is almost double. It provides the χ_Secure results. This method uses the pixel by pixel processing for crypto and stego parts that reduces the computational complexity. The method is equally effective for grayscale and colored images. The visual and statistical measure's results with the different embedding rates proves the effectiveness of the method. The prospective applications of the method include tele medicine, secure bank transaction, secret communication, authentication tool, tracking tools, copyright information, strong watermark, etc. The method increases the capacity in terms of embedding rate, 2 bits per pixel for grayscale and 6 bits per pixel for colored images. The future contribution will include the modification in the presented methodology that will increase the capacity in term of embedding rate with the change in the stage medium in an acceptable range. This method will be extended to the audio and video applications in future.

References

[1] J. Shearer, P. Gutmann, Government, cryptography, and the right to privacy, j-jucs 2 (3) (1996) 113–146.

[2] S. Katzenbeisser, F. A. Petitcolas (Eds.), Information Hiding Techniques for Steganography and Digital Watermarking, 1st Edition, Artech House, Inc., Norwood, MA, USA, 2000.

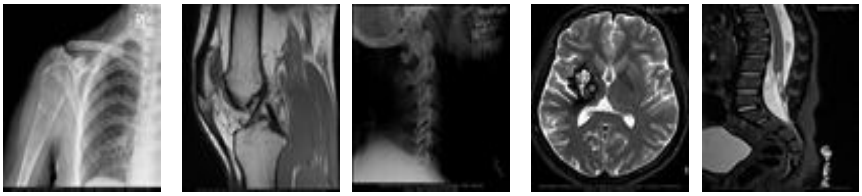
[3] A. Westfeld, A. Pfitzmann, Attacks on Steganographic Systems, Springer Berlin Heidelberg, Berlin, Heidelberg, 2000, pp. 61–76. doi:10.1007/10719724_5.

[4] N. Provos, P. Honeyman, Detecting steganographic content on the internet, Tech. Rep. 01-11, Center for Information Technology Integration,University of Michigan, 535 West William Street,Ann Arbor, MI 48103-4943 (2001).

[5] C. A. Stanley, Pairs of values and the chi-squared attack (May 2005).

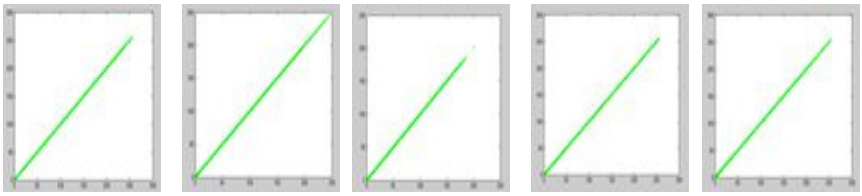
[6] C. Cachin, An Information-Theoretic Model for Steganography, Springer Berlin Heidelberg, Berlin, Heidelberg, 1998, pp. 306–318. doi:10.1007/3-540-49380-8_21.

[7] B. Li, J. He, J. Huang, Y. Q. Shi, A survey on image steganography and steganalysis, Journal of Information Hiding and Multimedia Signal Processing 2 (2011) 142–172.



(a) (b) (c) (d) d (e)

Figure 9: The set of images after embedding 8272 bits in cover images of Figure 4.

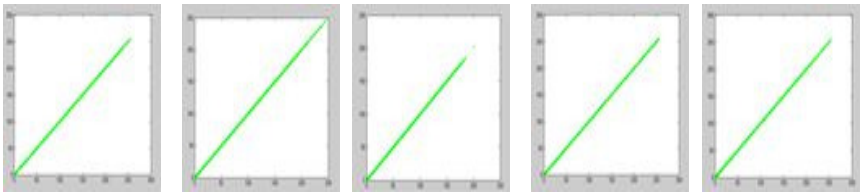


(a) (b) (c) (d) (e)

Figure 10: Joint histograms between images in Figure 4 and Figure 9.

(a) (b) (c) (d) (e)

Figure 11: stego images after embedding 14704 bits in cover images of Figure 4.



(a) (b) (c) (d) (e)

Figure 12: Joint Histograms between images in Figure 4 and Figure 11.

Table 5: Comparison of the Proposed Method with Others Methods

Feature	Substitution	Matching	Adaptive	Proposed
	(LSB)	(LSB)	(HVS)	Method
Capacity	1bpp	1bpp	Mostly 1bpp	2bpp
Security	Single	Single	Songle	Double
Complexity	Medium	Medium	Low	Low
Image Quality	good	good	good	good

[8] J. Fridrich, M. Goljan, R. Du, Detecting lsb steganography in color, and gray-scale images, IEEE MultiMedia 8 (4) (2001) 22–28. doi:10.1109/93.959097.

[9] S. Dumitrescu, X. Wu, Z. Wang, Detection of lsb steganography via sample pair analysis, IEEE Transactions on Signal Processing 51 (7) (2003) 1995–2007. doi:10.1109/TSP.2003.812753.

[10] A. Rashid, M. K. Rahim, Critical analysis of steganography: An art of hidden writing, International Journal of Security and Its Applications 10 (3) (2016) 259–281.

[11] C.-K. Chan, L. M. Cheng, Improved hiding data in images by optimal moderately-significant-bit replacement, Electronics Letters 37 (16) (2001) 1017–1018. doi:10.1049/el:20010714.

[12] R.-Z. Wang, C.-F. Lin, J.-C. Lin, Image hiding by optimal lsb substitution and genetic algorithm, Pattern Recognition 34 (3) (2001) 671 – 683. doi:https://doi.org/10.1016/S0031-3203(00)00015-7.

[13] C.-C. Chang, H.-W. Tseng, A steganographic method for digital images using side match, Pattern Recognition Letters 25 (12) (2004) 1431 – 1437. doi:https://doi.org/10.1016/j.patrec.2004.05.006.

[14] C.-K. Chan, L. Cheng, Hiding data in images by simple lsb substitution, Pattern Recognition 37 (3) (2004) 469 – 474. doi:https://doi.org/10.1016/j.patcog.2003.08.007.

[15] C.-C. Chang, J.-Y. Hsiao, C.-S. Chan, Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy, Pattern Recognition 36 (7) (2003) 1583 – 1595. doi:https://doi.org/10.1016/S0031-3203(02)00289-3.

[16] C.-C. Chang, C.-S. Chan, Y.-H. Fan, Image hiding scheme with modulus function and dynamic programming strategy on partitioned pixels, Pattern Recognition 39 (6) (2006) 1155 – 1167. doi:https://doi.org/10.1016/j.patcog.2005.12.011.

[17] C.-C. Chang, M.-H. Lin, Y.-C. Hu, A fast and secure image hiding scheme based on lsb substitution, International Journal of Pattern Recognition and Artificial Intelligence 16 (04) (2002) 399–416. doi:10.1142/S0218001402001770.

[18] C.-C. Thien, J.-C. Lin, A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function, Pattern Recognition 36 (12) (2003) 2875 – 2881. doi:https://doi.org/10.1016/S0031-3203(03)00221-8.

[19] A. D. Ker, Steganalysis of lsb matching in grayscale images, IEEE Signal Processing Letters 12 (6) (2005) 441–444. doi:10.1109/LSP.2005.847889.

[20] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on lsb matching revisited, IEEE Transactions on Information Forensics and Security 5 (2) (2010) 201–214. doi:10.1109/TIFS.2010.2041812.

[21] A. Rashid, N. Salamat, V. B. S. Prasath, An algorithm for data hiding in radiographic images and ePHI/R application, Technologies 6 (1) (2018) 7. doi:10.3390/technologies6010007.

[22] M. Barni, Steganography in digital media: Principles, algorithms, and applications (fridrich, j. 2010) [book reviews], IEEE Signal Processing Magazine 28 (5) (2011) 142–144. doi:10.1109/MSP.2011.941841.

[23] J. Mielikainen, Lsb matching revisited, IEEE Signal Processing Letters 13 (5) (2006) 285–287. doi:10.1109/LSP.2006.870357.

[24] X. Li, B. Yang, D. Cheng, T. Zeng, A generalization of lsb matching, IEEE Signal Processing Letters 16 (2) (2009) 69–72. doi:10.1109/LSP.2008.2008947.

[25] D.-C. Wu, W.-H. Tsai, A steganographic method for images by pixel-value differencing, Pattern Recognition Letters 24 (9) (2003) 1613 – 1626. doi:https://doi.org/10.1016/S0167-8655(02)00402-6.

[26] W.-N. Lie, L. C. Chang, Data hiding in images with adaptive numbers of least significant bits based on the human visual system, in: Proceedings 1999 International Conference on Image Processing (Cat. 99CH36348), Vol. 1, 1999, pp. 286–290 vol.1. doi:10.1109/ICIP.1999.821615.

[27] J. Fridrich, M. Long, Steganalysis of lsb encoding in color images, in: 2000 IEEE International Conference on Multimedia and Expo. ICME2000. Proceedings. Latest Advances in the Fast Changing World of Multimedia (Cat. No.00TH8532), Vol. 3, 2000, pp. 1279–1282 vol.3. doi:10.1109/ICME.2000.871000.

[28] T. Zhang, X. Ping, Reliable detection of lsb steganography based on the difference image histogram, in: Acoustics, Speech, and Signal Processing, 2003. Proceedings. (ICASSP '03). 2003 IEEE International Conference on, Vol. 3, 2003, pp. III–545–8 vol.3. doi:10.1109/ICASSP.2003.1199532.

[29] P. Lu, X. Luo, Q. Tang, L. Shen, An Improved Sample Pairs Method for Detection of LSB Embedding, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 116–127. doi:10.1007/978-3-540-30114-1_9.

[30] A. D. Ker, Improved Detection of LSB Steganography in Grayscale Images, Springer Berlin Heidelberg, Berlin, Heidelberg, 2005, pp. 97–115. doi:10.1007/978-3-540-30114-1_8.

[31] A. D. Ker, Derivation of error distribution in least squares steganalysis, IEEE Transactions on Information Forensics and Security 2 (2) (2007) 140–148. doi:10.1109/TIFS.2007.897265.

[32] A. Rashid, M. M. S. Missen, N. Salamat, Analysis of steganography techniques using least significant bit in grayscale images and its extension to colour images, Journal of Scientific Research and Reports 9 (2016) 1–14.

[33] K. R. Rasheed, A. Rashid, N. Salamat, S. M. Missen, Experimental analysis of matching technique of steganography for greyscale and colour image, International Journal of Computer Science & Information Technology (IJCSIT) 6 (6) (2014)) 157–166.

[34] A. Rashid, Experimental analysis and comparison of lsb substitution and lsb matching method of information security, International Journal of Computer Science Issues (IJCSI) 12 (1(1)) (2015) 91–100.

[35] D. B. Russakoff, T. Tomasi, Carl oand Rohlfing, C. R. Maurer, Image Similarity Using Mutual Information of Regions, Springer Berlin Heidelberg, Berlin, Heidelberg, 2004, pp. 596–607. doi:10.1007/978-3-540-24672-5_47.

[36] M. Trajkovic, Palette-based histogram matching with recursive histogram vector generation, US Patent App. 09/854,121 (2002). URL `http://www.google.com.af/patents/US20020168106`

[37] D. Mistry, A. Banerjee, A. Tatu, Image similarity based on joint entropy (joint histogram), in: International Conference on Advances in Engineering and Technology, 2013.

[38] Z. R. Mahayuddin, A. S. Saif, Fast and effective motion model for moving object detection using aerial images, International Journal of Computer Vision and Signal Processing 8 (1).

[39] M. Nii, Y. Kato, M. Morimoto, S. Kobashi, N. Kamiura, Y. Hata, S. Imawaki, T. Ishikawa, H. Matsubayashi, Ovarian follicle classification using convolutional neuralnetworks from ultrasound scanning images, International Journal of Computer Vision and Signal Processing 8 (1) (2018) 12–20.