ANKARA YILDIRIM BEYAZIT UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

DESIGN AND IMPLEMENTATION OF AN IMAGE BASED STEGANOGRAPHY

M.Sc. Thesis by

Serhat CİHANGİR

Department of Electrical and Electronics Engineering

January, 2020

ANKARA

DESIGN AND IMPLEPENTATION OF AN IMAGE BASED STEGANOGRAPHY

A Thesis Submitted to

The Graduate School of Natural and Applied Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the degree of Master of Science

in Electrical and Electronics Engineering, Department of Electrical and Electronics Engineering

by

Serhat CİHANGİR

January, 2020

ANKARA

M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled "**DESIGN AND IMPLEPENTATION OF AN IMAGE BASED STEGANOGRAPHY**" completed by **Serhat CİHANGİR** under supervision of **Prof. Dr. Hüseyin CANBOLAT** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Prof. Dr. Hüseyin CANBOLAT

(Supervisor)

Assoc. Prof. Dr. Ömer KARAL

(Jury Member)

Prof. Dr. Recep DEMİRCİ

(Jury Member)

Prof. Dr. Ergün ERASLAN

(Director)

Graduate School of Natural and Applied Sciences

ETHICAL DECLARATION

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural and Applied Sciences,

- All data, information and documents are obtained in the framework of academic and ethical rules,
- All information, documents and assessments are presented in accordance with scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of above statements, I accept to renounce all my legal rights.

Date: 2020, 21 Jan **Signature:**

Name & Surname: Serhat CİHANGİR

ACKNOWLEDGMENTS

I would like to express my deep sense of gratitude to my supervisor, Prof. Dr. Hüseyin CANBOLAT, for his skillful guidance, encouragement, patience, support, and great concern, which drove this work to a successful stage.

Special thanks to my parents Turan and Leyla Cihangir, and brother Salih Cihangir for their endless support.

2020, 21 Jan **Serhat CİHANGİR**

DESIGN AND IMPLEMENTATION OF AN IMAGE BASED STEGANOGRAPHY

ABSTRACT

Along with tremendous increase of software based applications, information privacy has become one of the overborne issues today for efficiency of electronic data processing. The main purpose on privacy of communication is to provide secure connection with target while avoiding to be captured by the third person in a way that flowing data should not be construed. In well accepted sense, steganography is the study and practice of concealing information to provide security of communication. Various LSB methods derived from classic LSB (least significant bit) are used as steganography techniques on spatial domains. In case of direct use of the classic LSB technique, security concern becomes an issue because of its simplicity and predictability. Also, traditional applications of classic LSB inevitably causes distortion of image. In this thesis, carried study proposes an improved LSB Steganography technique to enhance security while decreasing the rate of distortion in subject image. Proposed method in this study is based on hiding two bits of secret data in one color (RGB) pixel with only one least significant bit change in one of the layers. LSB value of Red layer is utilized in XOR operation with both Green and Red LSB values respectively. By applying this technique, only with one LSB bit change, two bits of secret data can be hidden as a consequence of XOR bitwise operation nature. XOR based operation provides more secure and unpredictable communication when compared to classic LSB. Aforementioned methods applied on different images, and it was found that improved method studied here revealed favorable results for the concerns of Peak Signal to Noise Ratio (PSNR) and Mean Square Error (MSE) when compared to the classic LSB method.

Keywords: Color Image, LSB (Least Significant Bit), MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), Security, Steganography, XOR Bitwise Operation

GÖRÜNTÜ BAZLI STEGANOGRAFİ TASARIMI VE UYGULAMASI

ÖZ

Yazılım tabanlı uygulamaların muazzam artışıyla birlikte, bilgi gizliliği günümüzde elektronik veri işlemenin verimliliği için en önemli sorunlardan biri haline gelmiştir. İletişim gizliliğinin temel amacı, üçüncü kişi tarafından akan verilerin ele geçirilip yorumlanmasından kaçınılırken, hedefle güvenli bağlantı sağlamaktır. İyi kabul gören anlamda steganografi, iletişim güvenliğini sağlamak için bilgiyi gizlemenin çalışması ve uygulamasıdır. Klasik LSB'den (en az anlamlı bit) türetilen çeşitli LSB yöntemleri, uzaysal alanlarda steganografi teknikleri olarak kullanılır. Klasik LSB tekniğinin doğrudan kullanılması durumunda, güvenlik kaygısı basitliği ve öngörülebilirliği nedeniyle bir sorun haline gelir. Ayrıca, klasik LSB'nin geleneksel uygulamaları kaçınılmaz olarak görüntünün bozulmasına neden olur. Bu tezde yapılan çalışma, denek imajındaki bozulma oranını azaltırken güvenliği artırmak için geliştirilmiş bir LSB Steganografi tekniği önermektedir. Bu çalışmada önerilen yöntem, iki gizli veri bitini tek bir renkli (RGB) pikselde, katmanlardan birinde sadece bir bit değişikliği ile gizlemeye dayanmaktadır. Kırmızı tabakanın en az anlamlı bit değeri, hem Yeşil hem de Mavi tabakanın en az anlamlı bit değerleri ile XOR işleminde kullanılır. Bu tekniği uygulayarak, sadece bir en az anlamlı bit değişikliği ile XOR işleminin çalışma doğasının bir sonucu olarak iki bit gizli veri gizlenebilir. XOR tabanlı işlem, klasik LSB'ye kıyasla daha güvenli ve öngörülemeyen bir iletişim sağlar. Yukarıda belirtilen yöntemler farklı görüntülere uygulanmıştır ve burada incelenen geliştirilmiş yöntemin klasik LSB yöntemine göre Tepe Sinyal Gürültü Oranı (PSNR) ve Ortalama Kare Hatası (MSE) değerlerinin olumlu sonuçlar verdiği gösterilmiştir.

Anahtar kelimeler: Renkli Görüntü, LSB (En Az Önemli Bit), MSE (Ortalama Kare Hatası), PSNR (Tepe Sinyal - Gürültü Oranı), Güvenlik, Steganografi, XOR İşlemi

CONTENTS

NOMENCLATURE

Acronyms

LSB	Least Significant Bit
PSNR	Peak Signal Noise Ratio
MSE	Mean Square Error
ASCII	American Standard Code for Information Interchange
AES	Advanced Encryption Standard
XOR	Exclusive OR

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Importance of Steganography

Information privacy has become the preponderant issue today with the increasing use and efficiency of electronic data processing. The main purpose on privacy of communication is to provide secure connection with target without being captured by the third persons or by bringing them in such a way that they cannot understand. In the most general sense, steganography is the study and practice of concealing information to provide security of communication.

Throughout human history, communication security is very important for countries or communities. People have needed send all secret information, all critical decision and all intel info one point to other point in a secure way for all the time. Thus, steganography is borne by itself. Following of improving and implementation of steganography throughout history gives the very important information about history. Therefore, the importance of steganography comes from history. In the background and literature review part, historical development of steganography will be explained deeply.

1.2 Study Methodology

Indistinguishability and unpredictability of secret data in image is challenging problem of steganography. Classical LSB method is predictable and its causes a distortion of images.

In this thesis, classical LSB steganography method improved with advantages of XOR bitwise operation in order to prevent predictability. Also, image distortion of proposed method less than the classical LSB. Distortion of images decreases because of using natural advantage of XOR operation. This logical operation causes the less bit changing of pixel so its image quality is better. In addition to this, XOR operation procures more secure communication. Because, XOR operation in LSB method unpredictable and its more complex than classical LSB.

Using advantage of XOR operation and adding extra part on implementation to increase security, more secure and unpredictable method of steganography is worked in thesis.

1.3 Study Objectives and Motivations

This study aims to achieve three objectives: Firstly, designing more safety and complexity LSB based steganography method than classical LSB method. Secondly, PSNR and MSE value of proposed method has to be better than classical method. Finally, compare between proposed method and classical method.

The main factor which motivated us to choose steganography as research field is that the design and implementation of new LSB steganography method better than the classical method.

Besides that, XOR bitwise based improved LSB method strengthens with random selection pixel and some cryptographic method. Thus, the newly found and actualized method has been perfected.

1.4 Thesis Outline

This thesis is organized as follows: Following the introduction, Chapter 2 give information about background and literature review of steganography, it gives the idea of historical development about steganography and gives main approaches used for this purpose, then explain well known today methods.

Chapter 3 introduces an overview of the methodology, starting with the classical approach which contains greyscale and color LSB method. Then with the features of XOR operation new proposed method is explained. After that, proposed method is strengthened with random pixel selection and AES encryption.

Chapter 4 begins with experimental result of classical LSB method for the grayscale image, and then same LSB method implements the color images. Finally, proposed method experimental results are given. Last part of chapter, all results is comparing each other.

The thesis is concluded in Chapter 5 which summarizes the whole work, and also offers some ideas about future work.

CHAPTER 2

BACKGROUND AND LITERATURE REVIEW OF STEGANOGRAPHY

Along with increasing use of digital technology and the ease of access to the wide storage options including cloud storages, a new avenue for digital communication, called steganography, was emerged. If the technique term ‘’steganography’’ is not given, it may be confused with cryptography. Although both technique aims to carry information to a specific receiver or group of receivers as camouflaged, the existence of cryptographic communication is mostly evident while transferred information in steganography is concealed. In other words, while both techniques camouflage the chosen content steganography is much more difficult to detect and process depending on the developed steganographic system which supposed to provide some features to embed data imperceptibly such as, promoting high information rate or payload, and impedance for removal [1]. The origin of subjected word ‘’steganography’’ is originally termed from Greek words known as ‘’Covered Writing’’. Steganography has a long history covers thousands of years. In the 5th century BC Histaiacus used slaves with embed messages with tattoo on their skulls, and dispatched them with grown hair. By doing so, message was only visible upon shaving the slave hair by receiver [2-5]. In the same manner, a project carried by King Abdulaziz City of science in Saudi Arabia was applied to translate some Arabic manuscripts into English language by secret writing technique which is believed to have been written 1200 years ago. Italian mathematician Jerome Cardan regenerates a method of ancient secret writing developed originally five hundred years ago in China. This regenerated method was requiring a mask with specific holes, and it is shared among two parties. Firs mask is placed on a blank paper, and sender writes secret message through holes then the mask off and fills the blank regions, and then receiver use the same mask to read actual message upon delivery of letter. In this way, message was appearing to the outside readers who have no mask as innocuous text as shown in Figure 2.1 [5].

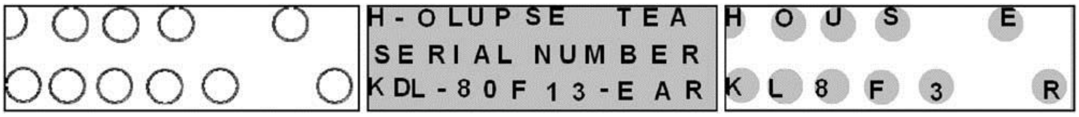


Figure 2.1 An illustration of Cardan Grille technique: mask is left (has no fixed pattern), middle covered text, and the right aimed secret message for the second party or receiver who has mask[6].

World War II was another time that several steganographic techniques were emerged by Nazis, such as Microdots; they are basically microfilm chips requiring high magnification usually over 200x, and it was possible to embed pages of information, drawings to the size of periods, invisible inks and null chippers are another ways of steganographic techniques, and based on taking 2nd letter of each word in a sentence, and one of the most well-known null chipper message was “*Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils.”,* and if the second letter of each word were placed in order, the actual message is revealed as “*Pershing sails from NY June 1*” [3, 7, 8]. Drawing was also applied to hide message in 1945 by concealing Morse code in which hidden message is placed as encoded onto the stretch of grass in Figure 2.2 that long grass indicates a line and the short grass indicates a point. When decoded message read: “Compliments of CPSA MA to our chief Col Harold R. Shaw on his visit to San Antonio May 11th 1945” [9].

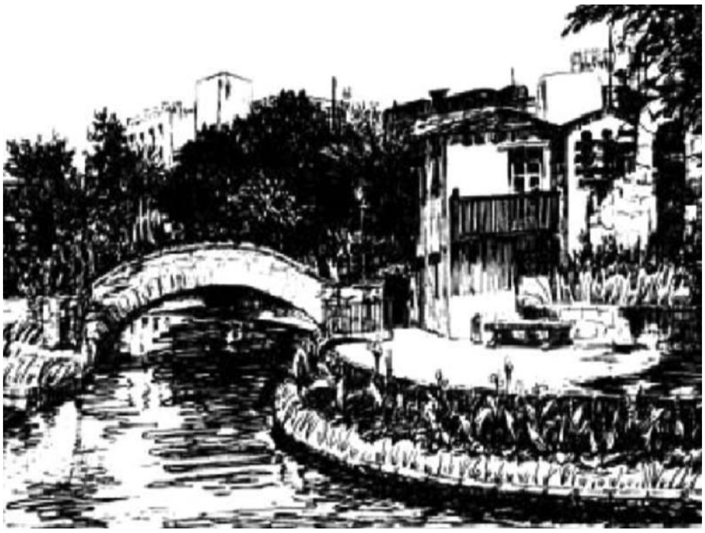


Figure 2.2 Hidden message is concealed with Morse code by encoding onto grass length alongside the river[9].

2.1 Steganography in the Digital Era

Along with widespread use of computer, the internet, and perceiving of its incredible processing power, development of digital signal processing (DSP) carried the concept of steganography in the digital world. Carrying the steganography to the digital world resulted with an environment of corporate vigilance that has spawned varieties of applications which assure its proceeding evolution to be able to hide contemporary information in digital atmosphere. Kurak and McHugh are the holder of one of the earlies methods to argue in which proposed method resembles embedding into the 4 LSBs (least significant bits). Kurak and McHugh studied image downgrading and inquination termed as image-based steganography in today. It is an inevitable fact that cyber-crime benefits from proceedings in digital revolution. Therefore, an immediate concern was emerged to clarify the possible use of steganography in terrorist activities by the released report in USA-TODAY [2]. Lieutenant Colonel Timothy L. Thomas declared that when steganography used in illegal activities by groups or terrorists it is quite difficult to control [10]. Three million images were investigated by Provos and Honeyman from University of Michigan for the existence of any trace of steganography, and no any trace of single message was emerged [4]. If this would be described as failed investigation, Provos and Honeyman claims that steganography does not exist solely in still images, and embedding secret notes in video and audio files are also probable. There are detected examples [11] concealing the data in music files, and even Hyper Text Mark up Language (HTML), executable files (.EXE), and Extensible Markup Language (XML) as much more simpler forms [12]. Therefore, the claims of no trace of hidden steganographic messages by USA-TODAY is not supported anymore and the writer of that article report resigned about two years later due to other editors' consensus on writer deceived researchers during the period of their investigation [6].

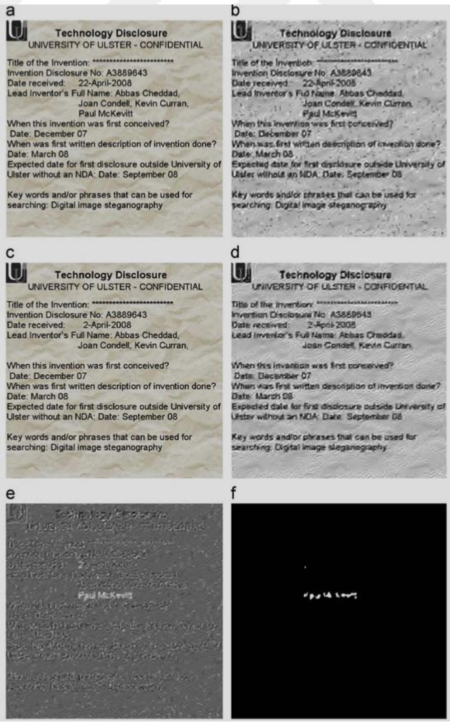
2.2 Use of Steganography in Applications

While steganography takes great attentions of professional illegal organizations to hide and transfer messages as innocuous scenes to the third-party viewers, it has also a great deal of beneficial uses for applications, e.g., controlling the copyright of market products, improving robustness of image search engines and smart identification cards in which photograph of card holder on the smart ID, individual's details as embedded form. Additional applications are synchronization of video-audio files, classified data circulation by companies, TV broadcasting, TCP/IP packet traffic control by embedding unique ID into an image to analyse the network traffic of specific users [2] as well as checksum embedding [13]. The field of application of steganography can be extended through human DNA, Peticolas [14] presented some modern applications as one of them was in Medical Imaging Systems to disunite of confidential information of patients' image data or DNA sequences and their captions, such as patient address and ID details. By doing so, while a link is maintained between patient image, a useful but confidential information is stayed hidden to the third parties. In fact, if one goes back to the old techniques, the main idea left stable in which two coder and decoder is required, and it was a physical mask in the past, and a software in today thanks to the digital signal processing. The answer of the question of that why steganography is in interest and showing an impressive evolution is not difficult as "steganography" presents definite guarantee of authentication that no other tool may ensure of security in that robustness.

LSB embedding technique is also used for patient records by Miaou and co-workers [15] in which electronic patient records depending upon bi-polar multiple-base data concealment is performed by LSB embedding; value difference of a pixel between an original image and its JPEG format is taken to be a number conversion base. For more information, two publications one from Nirinjan and Anald [16] and other from Li et. [17] al can be viewed for patient data hiding in digital images.

The techniques and logarithmic flow of steganography is applied as embedded in the normal printing process by Japanese company Fujitsu. A technology in the process of developing period demonstrates encoding data into a printed picture that is out of sight of human eye vision capability, but can easily be decoded by a camera carrier mobile phone as exemplified in Figure 2.3. This developed process embeds approximately 12 bytes and so takes less than a second. By doing so, users can encode the captured data by their camera carrier mobile phones, and users are charged with a small fee for accessing and processing of the company's server which operates the decoding software. In basic description, colour scheme of an image is transformed during printing to its hue, HSV, saturation and value components, then embed into Hue domain that human eye is not capable to catch, and only camera carrier cellular phones can detect concealed data and retrieve it.

The practical application of the steganographic method can be quite wide including medical prescriptions, business cards, billboards, food wrappers, printed media [18] or even replacing barcodes. It is a fact that evolution of digital signal processing and so the steganography caused a loss of confidence in integrity of visual imagery which resulted with requirement of more effort in research for digital forensics. In light of this, Cheddad and co-workers released a security scheme to protect scanned documents from forgery by applying embedding techniques. This proposed method, as given example in Figure 2.3, not only aims to contend with forgery but also aims manipulating original documents for others to keep visible only for forensics expert to access original data.



Technology Disclosure
UNIVERSITY OF ULSTER - CONFIDENTIAL

Title of the Invention: ************************
Invention Disclosure No: A3889643
Date received: 22-April-2008
Lead Inventor's Full Name: Abbas Cheddad,
Joan Condell, Kevin Curran,
Paul McKevitt
When this invention was first conceived?
Date: December 07
When was first written description of invention done?
Date: March 08
Expected date for first disclosure outside University of Ulster without an NDA: Date: September 08

Key words and/or phrases that can be used for searching: Digital image steganography

Technology Disclosure
UNIVERSITY OF ULSTER - CONFIDENTIAL

Title of the Invention: ************************
Invention Disclosure No: A3889643
Date received: 2-April-2008
Lead Inventor's Full Name: Abbas Cheddad,
Joan Condell, Kevin Curran,

When this invention was first conceived?
Date: December 07
When was first written description of invention done?
Date: March 08
Expected date for first disclosure outside University of Ulster without an NDA: Date: September 08

Key words and/or phrases that can be used for searching: Digital image steganography

Figure 2.3 (a) is the original image, (b) is the stego-image carries self-duplicate, (c) is the human-eve visible form but differ from original image (a) with one of the number in date '*2*', and the 4th name '*Paul McKevitt*' from inventors are deleted (invisible), (e) is the error signal of image (b) and (d), (f) is the image following the thresholding operation perform [19].

2.3 Steganographic Techniques in Digital Images

There are many image formats used on the internet, but the common formats can be given as; graphics interchange format, GIF, Joint Photographic Expert Group, JPEG, and the portable network graphics, PNG. Developed techniques mainly aimed to establish to exploit structure of given formats along with certain exceptions proposed in the literature that use the BMP; bitmap form for its elementary data structure.

Definition of embedding process may differ in different sources with similar schemes. Cheddad and co-workers gives a graphical representation of process of embedding given in Figure 2.4 in which C represents the cover carrier, ie., image A, and C' the stego-image. If K denotes an optional key a seed applied to encrypt the information or to compose a pseudorandom noise (noise can be taken as Ø for ease of understanding) while M represents the actual information to be aimed to transfer, i.e., image B. Em represents the acronym for embedding and Ex for Extraction [19].

One of the most detailed publication is from Johnson et. al. [20], but a significant evolution has been occurring. However, for detailed information one can read the Johnson et. al. article that discusses substation systems, transform domain techniques, spread spectrum techniques, distortion techniques, statistical methods, and cover generation methods. Similarly, if the discussion about frequency domain software/methods and core algorithms are not in interest, detailed research for GIF format supporting spatial domains can be accessed from survey of Bailey and Curran [21].

There is no characterization of steganographic algorithms into a single, commonly accepted category. Therefore, written characterization list here is self-designed with no claims of any standardization.

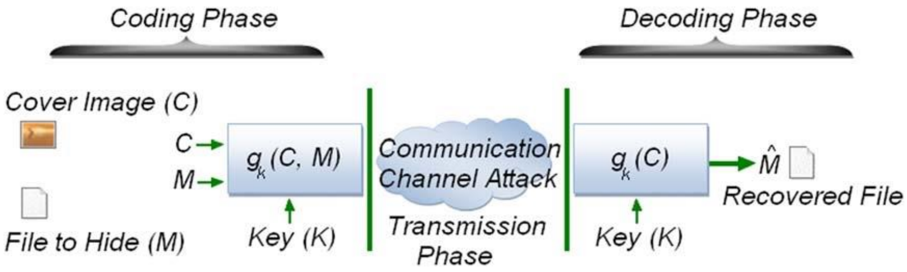
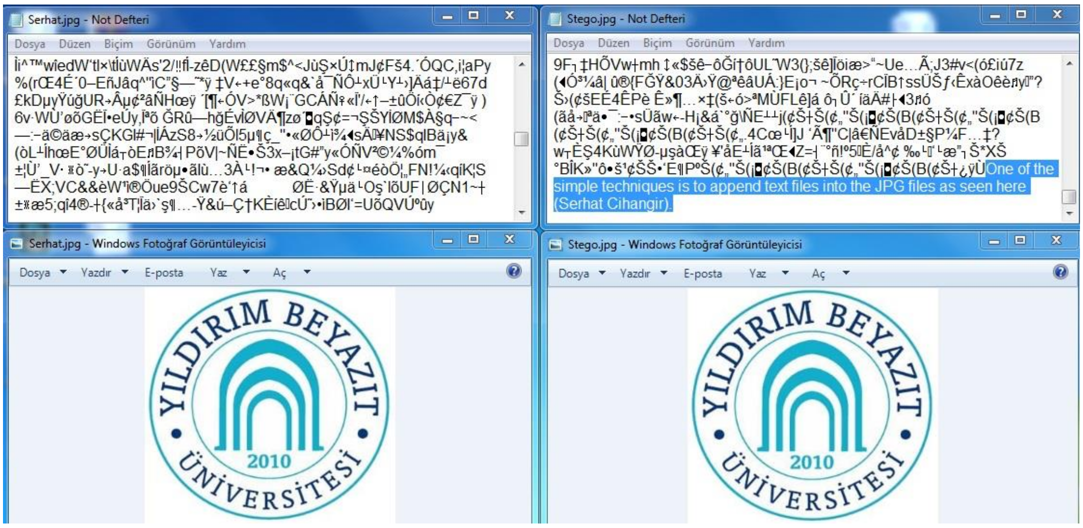


Figure 2.4 Prepared graphical representation for theoretical view of communication process, while C represents cover image, M represents the data to protect from others [19].

2.3.1 Exploiting the Image Format for Steganography

One of the simple methods for performing steganography in Windows OS command windows, e.g., Windows XP, is to feed the following code: C:> Copy Cover.jpg /b + Message. txt /b Stego.jpg

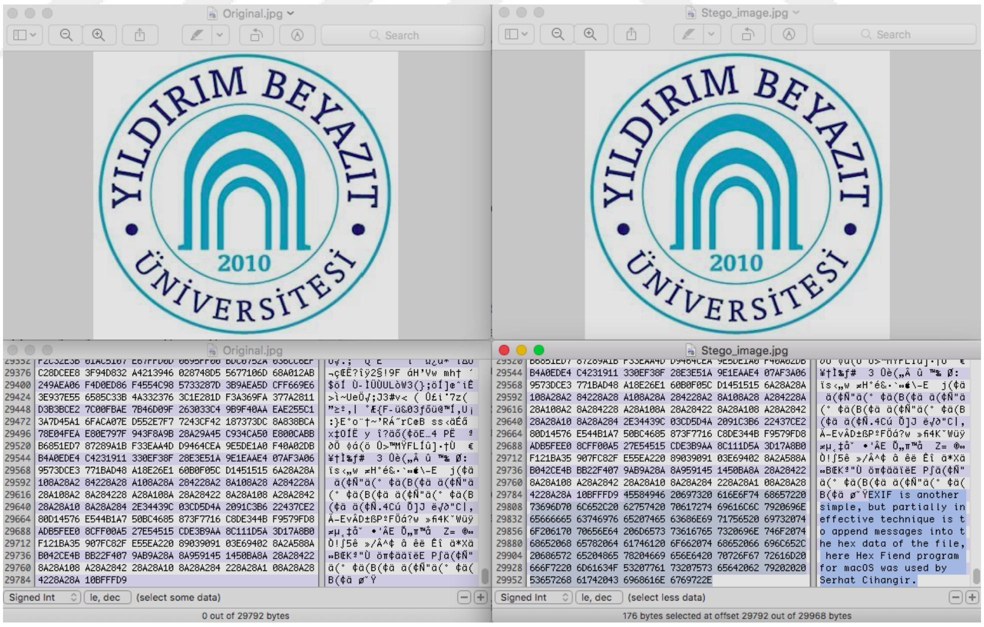
By inputting this code, a secret message in a text file (Message.txt) is appended into the JPEG image file, called Cover.jpg as given in the code, and so; a stego-image is generated. The main idea behind this technique is simply manipulating the recognition of EOF (End of file). By doing so, the message is played a role as package, and inserted following the EOF tag. As a result, when Stego.jpg is desired to be opened by any photo editing program, the image will be shown as it should be. However, when Stego.jpg is opened by a text editor, e.g., notepad, embedded message will be appeared along with some data. It is also impossible to detect any difference between two image files as inserted text file content does not impair the image quality in terms of image histograms or visual perception because of hiding methodology applied here comes after EOF tag as shown in Figure 2.5. Although this method hide itself for a normal user, and has lots of user-ready software, e.g., Camouflage, JpegX, etc., it does easily appear by any kind of stego-image editing program/technique as well as attacks performed by steganalysis experts.


Serhat.jpg - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
Stego.jpg - Not Defteri
Dosya Düzen Biçim Görünüm Yardım
Serhat.jpg - Windows Fotoğraf Görüntüleyicisi
Dosya Yazdır E-posta Yaz Aç
Stego.jpg - Windows Fotoğraf Görüntüleyicisi
Dosya Yazdır E-posta Yaz Aç
YILDIRIM BEYAZIT ÜNİVERSİTESİ 2010
YILDIRIM BEYAZIT ÜNİVERSİTESİ 2010

One of the simple techniques is to append text files into the JPG files as seen here (Serhat Cihangir)

Figure 2.5 No any visual deformation exists, and embedded hidden message is appeared when stego-image is opened by any text editor.

Image’s extended file information (EXIF) is also used as one of elementary implementation method to append a hidden message into its hexadecimal chunk as given example in Figure 2.6.



EXIF is another simple, but partially in effective technique is to append messages into the hex data of the file, here Hex Fiend program for macOS was used by Serhat Cihangir.

0 out of 29792 bytes

176 bytes selected at offset 29792 out of 29968 bytes

Figure 2.6 Left image and hexadecimal data are original files while right image and hexadecimal data are the modified ones by hiding data without corrupting the file.

EXIF is actually used as standard by digital camera manufacturers to keep some data, such as camera model, manufacturer, picture time, resolution, etc. in the image file. It is all the metadata information and located at the header of the file.

In fact, the possibility of using such headers as digital evidence to combat with child pornography is interpreted by Special agent Paul Alvarez [22]. However, this method is also not reliable as it is suffered by parallel drawbacks as that of the EOF method, and it is important to note here that non-encrypting concealing is not efficient.

2.3.2 Using Image Frequency Domain for Steganography Purposes

Due to continuous development of information technology, improved security systems are also emerging as an essential requirement, and thus; novel algorithms have been rapidly releasing. In fact, progress in LSB embedding mechanism is a big milestone as the method works perfectly by keeping data as secretly embedded from Human Visual System (HVS). However, LSB method to keep secret information as embedded is not enough as it shows low resistance to reveal information in case of attacks, and so the scientists have been sustaining the research until obtaining successful application of the method within the frequency domain.

Discrete Cosine Transformation (DCT) is commonly applied for video and image compression e.g. JPEG lossy compression. When two-dimensional DCT applied an image F, the image B is calculated as output:

$$T_{pq} = \propto_p \propto_q \sum_{m=0}^{M-1} \sum_{n=0}^{N-1} F_{mn} \cos\frac{\pi(2m+1)p}{2M} \cos\frac{\pi(2n+1)q}{2N} \quad \begin{matrix} 0 \le p \le M-1 \\ 0 \le q \le N-1 \end{matrix} \qquad \textbf{(2.1)}$$

In Equation 2.1, α_p and α_q is described below;

$$\alpha_p = \begin{cases} \frac{1}{\sqrt{M}} & ,p = 0 \\ \sqrt{\frac{2}{M}}, & 1 \leq p \leq M - 1 \end{cases} \qquad \alpha_q = \begin{cases} \frac{1}{\sqrt{N}}, & q = 0 \\ \sqrt{\frac{2}{N}}, & 1 \leq q \leq N - 1 \end{cases} \tag{2.2}$$

Upper-case letters (*M*, *N*) shows dimensions of the image used as input, and lower-case letters (*m, n*) changes variably between 0 and *M-1* for ***m***, and 0 to *N-1* and for ***n***. Equation 2.1 is used to acquire DCT coefficients for each block, and they are quantized according to the specifically given quantization table (QT). Given matrix in Table 2.1 is suggested in the Annex of the JPEG standard. It is noteworthy to declare here that some of the camera manufacturers use their own quantization table, and so, not every producer has to follow standard JPEG table because the main aim is choosing a suitable QT which balances image compression and quality factors within the limit of HVS.

Table 2.1 JPEG suggested Luminance Quantization Table used in DCT lossy compression, and DC coefficient is represented with bold number **16** while rest is AC coefficients.

16	11	10	16	24	40	51	61
12	12	14	19	26	58	60	55
14	13	16	24	40	57	69	56
14	17	22	29	51	87	80	62
18	22	37	56	68	109	103	77
24	35	55	64	81	104	113	92
49	64	78	87	103	121	120	101
72	92	95	98	112	100	103	99

Basically, quantization step is given in Equation 2.3, and DCT produces tightened precision, however, if QT is applied as given in Table 2.1, precision loosen up while maintaining the valuable information descriptor.

$$f'\left(w_x, w_y\right) = \left[\frac{f\left(w_x, w_y\right)}{\Gamma\left(w_x, w_y\right)} + \frac{1}{2}\right], \qquad w_x, w_y \in \ 0,1,\ldots,7 \tag{2.3}$$

In Equation 2.3, x and y are the image coordinates. $f(\omega_x, \omega_y)$ is an 8 x 8 non-overlapping intensity image block function, $\lfloor . \rfloor$ is a floor rounding operator, and $f'(\omega_x, \omega_y)$ represents the result function. Quantization step is denoted by $\Gamma(\omega_x, \omega_y)$ which is related to image quality as given below;

$$\Gamma\left(w_x, w_y\right) = \begin{cases} \max\left(\left\lfloor\frac{200-2Q}{100} QT\left(w_x, w_y\right) + \frac{1}{2}\right\rfloor, 1\right), 50 \leq Q \leq 100 \\ \left\lfloor\frac{50}{Q} QT\left(w_x, w_y\right) + \frac{1}{2}\right\rfloor, \qquad\qquad 0 \leq Q \leq 50 \end{cases} \tag{2.4}$$

Q is the quality factor while $QT(\omega_x, \omega_y)$ is the quantization table presented in Table 2.1. Performing compress process is occurred by entropy coding such as Huffman algorithm and result in $\Gamma(\omega_x, \omega_y)$. In this stage, majority of the excrescent data and noise are removed, in other words, lost, and hence the name ‘’lossy compression’’ is termed. All this information given here for JEPG compression is much more detailed by Popescu [23]. Rather than using discrete theory independent of steganography, modification of QT was studied by Li and Wang as a steganographic method, and they inspired by Chang and co-workers study [24]. In developed technique, Li and Wang first modified the QT which is then followed by inserting the hidden bits in the middle of the frequency domains, and so created new version of QT, given in Table 2.2, gives 36 coefficients and each carries 8 x 8 block to embed secret information into them with a plausible payload [25].

Table 2.2 The modified Quantization Table by Li and Wang [25].

8	1	1	1	1	1	1	1
1	1	1	1	1	1	1	55
1	1	1	1	1	1	69	56
1	1	1	1	1	87	80	62
1	1	1	1	68	109	103	77
1	1	1	64	81	104	113	92
1	1	78	87	103	121	120	101
1	92	95	98	112	100	103	99

Different paces are applied to perform steganography with DCT JPEG compression as presented in Figure 2.7.

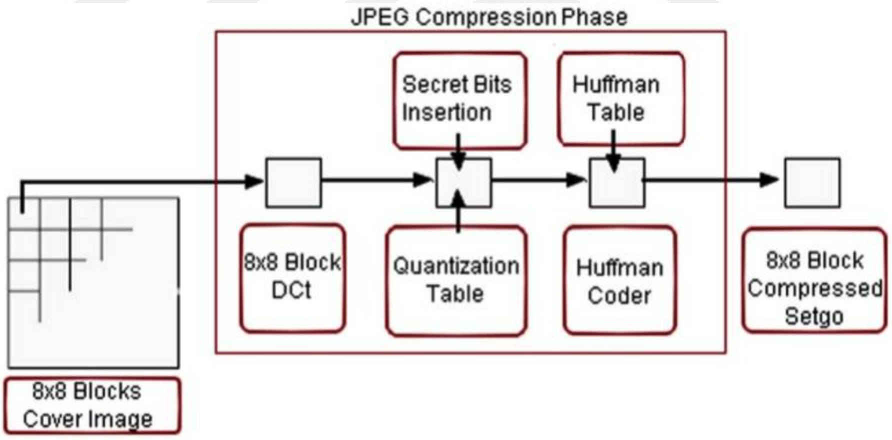


Figure 2.7 Common process of information embedding in frequency domain is shown as data flow diagram [6].

DCT is used for JPEG compression to transform successive sub-image blocks (8 x 8 pixels) into 64 DCT coefficients. Target data aimed to be hidden is inserted into insignificant bits of these coefficients, but changing a single coefficient would potentially influence the whole 65 block pixels [26]. When those coefficients handled with care, cover image will show no sign of change as altering process occurring on the frequency domain rather than spatial domain [27]. Fast Fourier transform (FFT) was also tried to create a method of Fourier based steganography by Raja et al. [28] with unsuccessful results due to round-off errors, but transformations were applied by Johnson and Jajodia [2], and the technique utilised by McKeon with 2D Discrete Fourier transform (DFT) for application of Fourier based steganography in movies [29]. When altering DCT coefficients block, a careful consideration is crucial as it may result with poor implementation as given example in Figure 2.8 in which chosen values in 8 x 8 DCT coefficients-block for alteration process were not a successful choice.

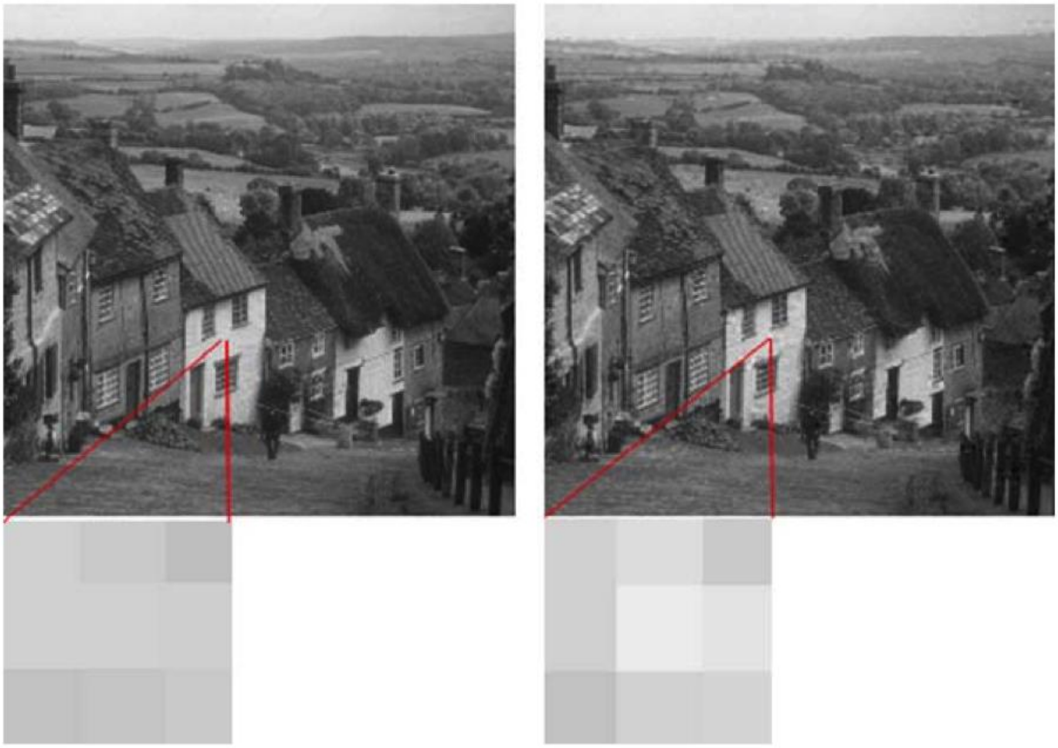


Figure 2.8 Embedding at the DCT level is quite unique and professional method as long as it is managed to be kept the artefacts at the out of the scope with carefully chosen coefficients. Otherwise, artefacts will be unavoidable as shown above.

2.4 Evaluation of Least-Significant Bit Encoding

Matrix of color along with intensity values are constituents of a digital image, and while 24 bits/pixel, as 8 bits allocated to each color, represents a full color image, gray scale image only required 8 bits/pixel. In case of using 24-bit image, batch of all of blue, red, and green are used to embed 3 bits of information for each pixel. In the simplest form of this technique, cover image's least significant bit plane used to embed the bits of message in deterministic sequence, and as amplitude of change is in micro level, modulation of least significant bit does not create human perceptible difference. The main superiorities of LSB embedding are its simplicity, and its modifiable nature with other techniques. By applying LSB technique, embedding the message may allow undiscoverable perceptual transparency. LSB's main disadvantage is its sensitivity of filtering and manipulation, and thus; embedded message may be removed.[30] [31]

2.4.1 Using Image Spatial Domain for Steganographic Purposes

In these techniques, the data desired to be kept secret involves encoding at LSBs level, and medium is covered in the spatial domain by steganographer. In comparison with other two given techniques in section 2.4.1, using spatial domains are still simple but has greater impact [22]. There are various examples in the literature to illustrate main concept of spatial domain technique as similar to one, given in Figure 2.9 along with an applied practical example given in Figure 2.10 by Abbas Cheddad and co-workers [6].

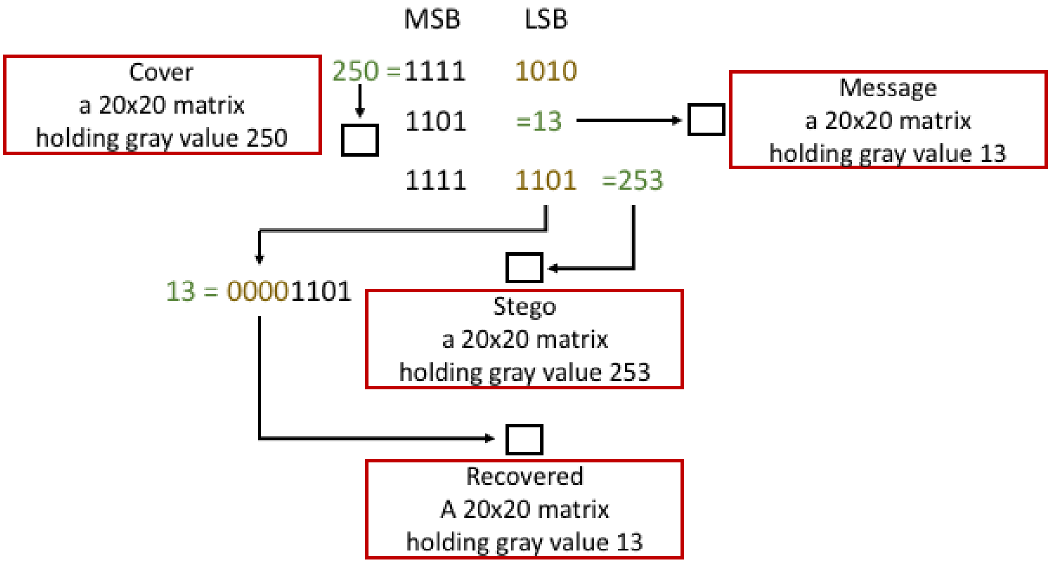


Figure 2.9 Diagram shows the effect of changing the LSBs till to the 4th bit plane (Steganography in a spatial domain).

When Figure 2.10 examined, it can be seen that distortion rate of the cover image is directly proportional with increasing use of LSB from 1st to 4th used to hide information, in other words, naturality of the cover image is significantly protected when just 1st LSB is used to embed information as clearly seen in image j that used to 1st LSB of image a to hide itself in image d with the result of quite minor distortion, and thus; highly protected naturality of image a is the outcome.

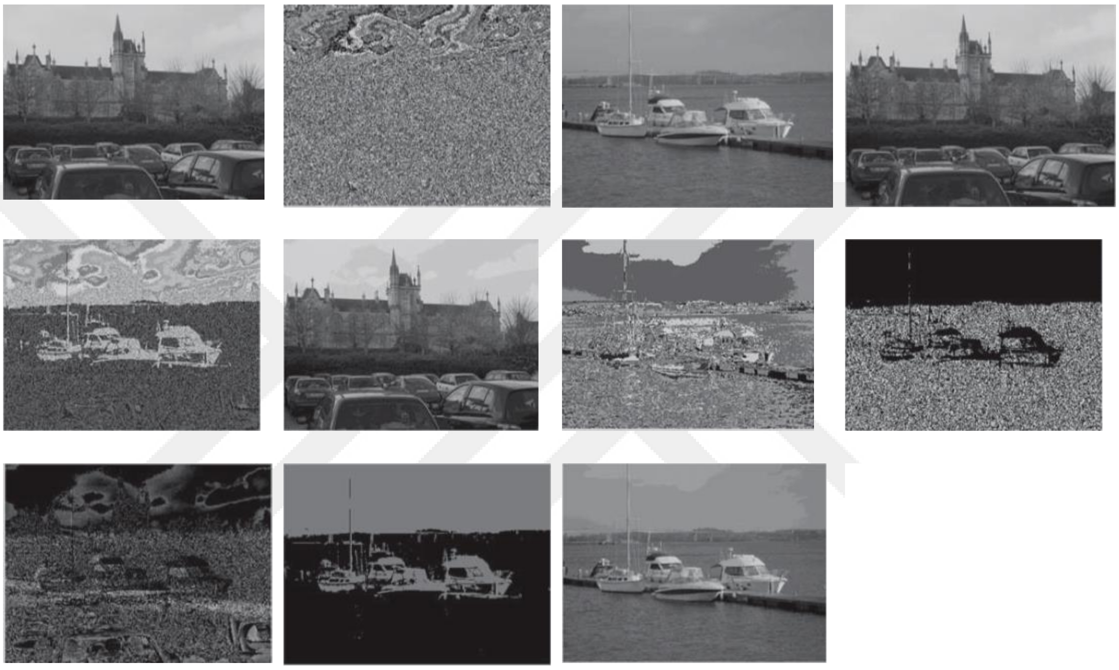


Figure 2.10 All labeled from left to right. Firs row is labeled from ‘’**a**’’ to **d**’’. Second row is labeled from ‘’**e**’’ to ‘’**h**’’. Third row is labeled from ‘’**i**’’ to ‘’**k**’’. ‘’**a**’’ is the university of Ulster picture as cover carrier. ‘’**b**’’ shows 1st ot 4th LSBs of ‘’**a**’’, but contrast was increased to imrove visulization. ‘’c’’ is the Londonderry’s river as target image to conceal. ‘’d’’ is the stego image of ‘’c’’ for the case of replacement of 1st LSBs with 1 MSBs. LSBs of ‘’d’’ is ‘’e’’. ‘’f’’ stego image of ‘’c’’ for the case of replacement of 1st to 4th LSBs with the 1st to 4th MSBs of ‘’c’’. LSBs of ‘’f’’ is ‘’g’’, ‘’h’’ is the difference of ‘’a’’ and ‘’d’’, ‘’i’’ difference of ‘’a’’ and ‘’f’’. ‘’j’’ is extracted secret image from ‘’d’’, and ‘’k’’ extracted hiden image from ‘’f’’.

However, f uses 1st-4th LSB of image a for hiding itself in image with the result of quite distorted image. Therefore, there is a proportional trade-off in terms of noticeability of artefacts between the distortion rate of cover image and payload.

A spatial domain technique based on issue of image cropping effects instead of common embedding techniques were studied by Potdar et. al. [32] which generates a fingerprinted cryptically sharing steganography for increasing its stability to fight against to attacks performed by using image cropping techniques. The main mechanism of exhibited study based on dividing the cover image into sub-images and then these sub-images are compressed and encrypted the concealed data. Outcome data after applying the given process is then sub-divided in turn and embedded into portions of subject image. Recover process of the data is based on application of a Lagrange Interpolating Polynomial with an encryption algorithm. In the proposed technique, although computational load is high, presented algorithm parameters, in other words, amount of used sub-images (n) with threshold value (k) is not set to optimal assets, and thus; values need to be guessed by reader. Moreover, the unpractically of the technique comes from increased number of sub-images with increased n assets, for example, 64 persons and 64 sub-images will be required if the n is set to the 64 which also means 64 public keys will be used. Bear in mind, Potdar et. al. was aimed to eliminate data redundancy, but it unfortunately existed in the created stego-image during the study.

Persian and Arabic alphabet punctuations was studied by Shirali-Shahreza [33] to keep data as secret. This study is not covered under LSB techniques, but related to the spatial domain in the case of evaluating the text as an image. As known, English has two dotted letters as ‘’i’’ and ‘’j’’ in lower case format, but Persian language has 18 out of 32 dotted letters in which these dots are modified depending on the values in binary file.

Exploiting the colour palette is another method of using LSB as steganography technique in which smooth ramp transitions are used to perform LSB by modifying LSBs based on their positions in the palette index [2]. Although some compressions along with weaknesses against statistical counter attacks are reported, BMP (24 bit) and GIF (256-color) files were studied by Johnson and Jajodia while JPEG files was directly kept out of study due to their inherent compression algorithm which does not allow to apply direct embedding with LSB into the spatial domain [4, 34-37]. Fridrich and co-workers declared that quite small notifications in JEPG file as small as flipping one pixel's LSB can be impeccably located [38]. Carried studies on the DCT (discrete cosine transforms) coefficients exhibited reliable outcomes, and thus; researchers started to re-interest with this sort of image. Indeed, application of steganography technique at the level of DCT is resulted in more reliable as well as less vulnerable to the statistical attacks.

Jung and Yoo [39] prepared a sample without changing the dimensions as ready for embedding process by the following process; first taking a down-sampled input image to half of its original size which is followed the application of modified interpolation method, titled as NMI (neighbour mean interpolation) in order to up-sample to turn the original dimensions and then up-sampled image was divided non-overlapping blocks in 2x2 sizes as schematically shown in Figure 2.11.

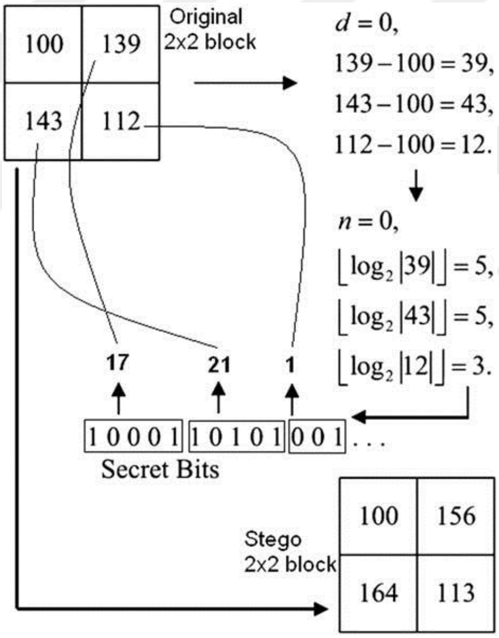


Figure 2.11 Schematic description of Jung and Yoo method [39].

Although method carries originality, use of $\log_2$ in both recovery steps and extraction process causes significant unreliability by causing errors in the recovery, and floating-point values in the extraction, and since in the 222 blocks, the spearheading value, for example block (1,1) is left unchanged, and so; this situation causes to the devastation on the existence of natural strong correlation between adjacent pixels. It is clearly out of favor involvement of a non-natural process [6].

Another scheme of concealing information can be performed by using histogram of images in which Li et al. [40] presented lossless data concealing using adjacent pixels' value difference. The technique is one of the ‘’±1’’ data embedding algorithms, and correlation between the adjacent pixels is the way the technique exploits to perform steganography. Gaussian distribution as show in Figure 2.12 is used to characterize obtained compact histogram.

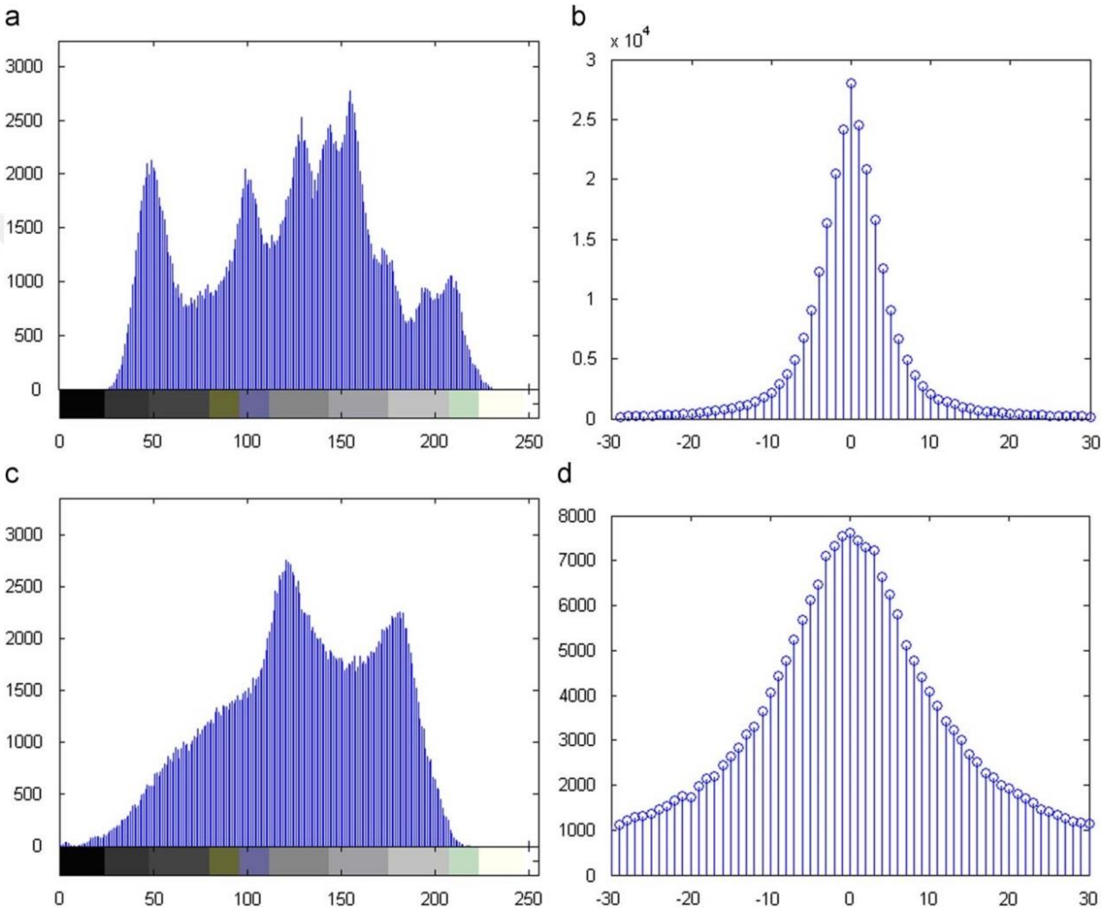


Figure 2.12 Lena and Baboon image histograms are given in (a), difference histogram for Lena is given in (b), histogram of Baboon image is given in image (c), difference histogram for Baboon is given in (d).

As a slightly different way, Pyiu Tsai and co-workers takes the image [41], and then divides into 5x5 blocks which is followed by calculation step of residual image with linear prediction, in another word; adjacent pixels' difference. By doing so; it is possible to embed target data into residual values which is followed by the reconstruction of the blocks.

Software tools proposed by Johnson and Japodia[2], such as White Noise Storm; use encryption with steganography as well integrated in which it is applied PCX files (IBM Paintbrush) by extracting LSBs from cover image to store in the file, and then encryption applied on target message before carrying out these extracted bits to create new LSBs set as ready to be injected into cover image, and S-Tools; takes the original colored cover image then turn into 8-bit cover form while hiding target message, and then spreads the message across the LSBs of the color levels to form final stegoimage.

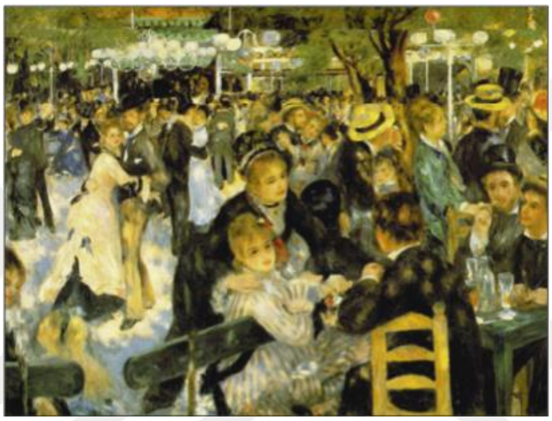


Figure 2.13 Original cover image (access http://www.hs.port.ac.uk/wm/paint/ auth/renoir/moulin-galette).

For testing methods, original cover image is used as given in Figure 2.13, and the resulting images with embedded messages are given in Figure 2.14.

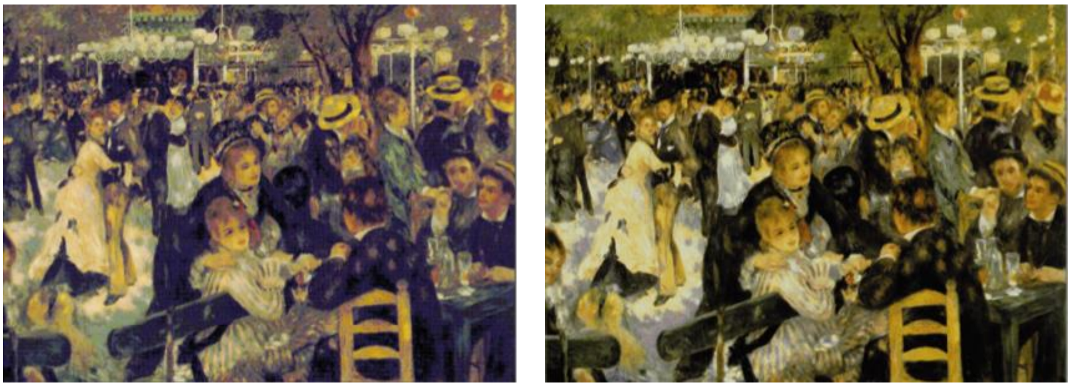


Figure 2.14 Left image is Renoir cover file after the Airfield image was embedded with White Noise Storm with the result of severe shift of palette, and right image is result of embedding by using S-Tools the Airfield image in the Renoir cover with astonishing result.

It is clear that S-Tool exhibited the best results for GIF and BMP images, and S-Tools can even hide the target message in unused fields of floppy diskettes. Another new embedding technique bit to LSB plane applied by Wang as shown in Figure 2.15 with process of pixel adjustment in which a term named by Wang as “Moderately-significant-Bit” is used to describe the process that targets intermediate bit, and thus; secret data can be stay safe in case of any LSB bit damage in the future.[42]

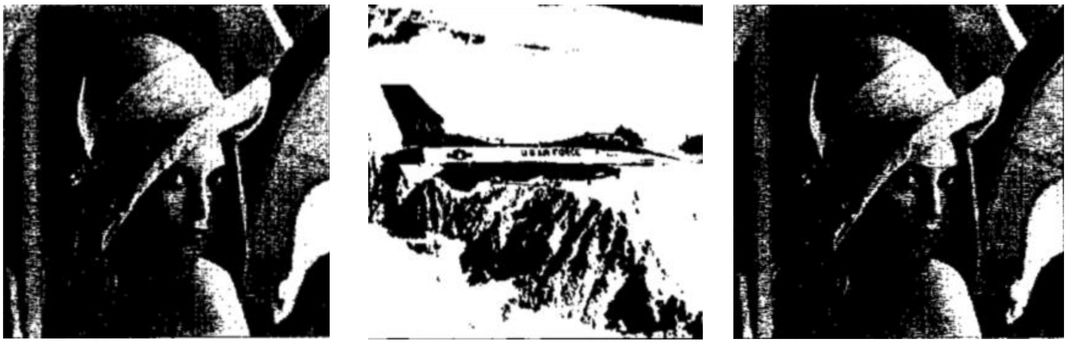


Figure 2.15 Host image Lena, binary important message, and resulting image by MSB substitution are given left to right respectively[42].

Chang also proposed a method to reduce computational time while increasing the capacity of hiding by using dynamic programming termed as “Principle of optimality” to define optimal bit in LSB during substitution in which this technique procure optimal solution for each sub sequence. In the experimental tries, it was proven computational time is less than many other techniques.[43] Another novel approach from Swain and Lenka exhibited a dynamic steganography technique on Leena image as shown Figure 2.16 in which RGB channel used with two levels of security that three LSB bits as 6th, 7th and 8th are applied to embed two bits of text in each pixel of target image.[44]

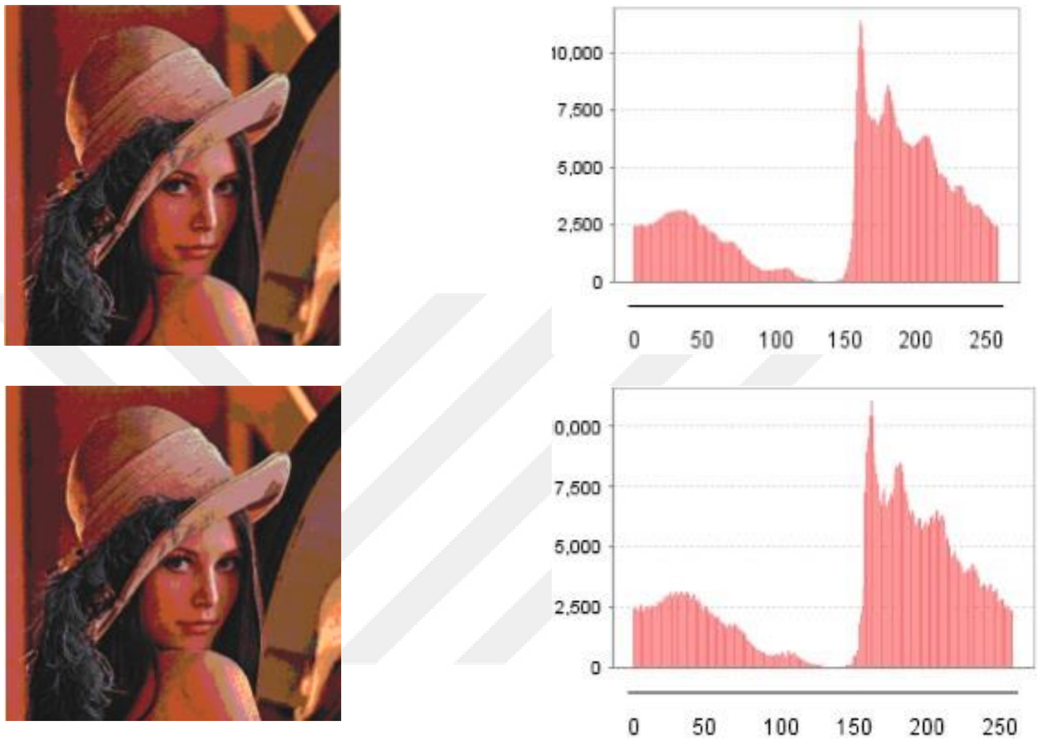
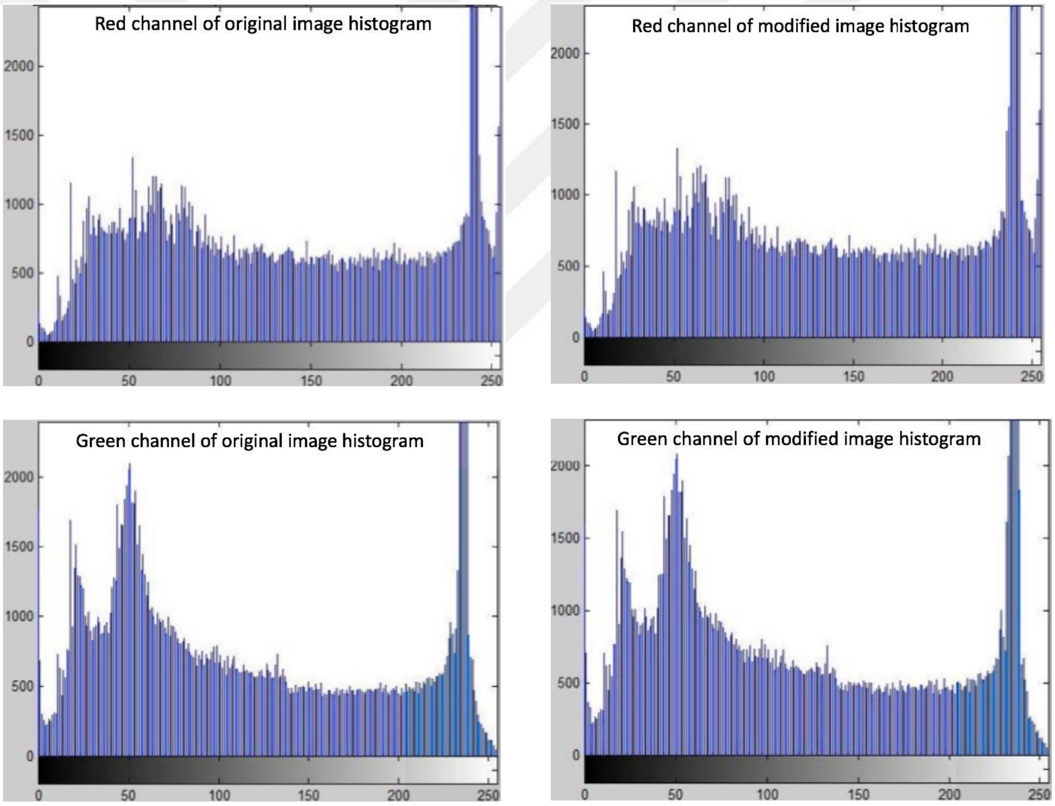


Figure 2.16 Top part show the original Leena image with its histogram, bottom part shows the 40 kilo bytes chipper text embedded Leena image and its histogram[44].

Pixel indicator technique is proposed as novel way of LSB technique by Gutub et al. in which random choice of indicator bit comes from last two bits of any available channel of RGB indicates the presence of target data, and indicator is selected based on RGB channel sequences. By application of this technique, it is not possible to detect any observable differences by human perception as exhibited in Figure 2.17, and also it is pretty stringent to explore the embedded data from histogram comparisons as shown in Figure 2.18.[45]

Figure 2.17 Original BMP cover image is given right, data hidden BMP is given left[45].



Red channel of original image histogram

Red channel of modified image histogram

Green channel of original image histogram

Green channel of modified image histogram

Figure 2.18 Original and modified Red and Green channel histograms of given image in Figure 2.17[45].

2.5 Using LSB with XOR Operation

In order to hide target information in image steganography, Red, Green, Blue main colors into 3 distinct matrices are applied. In a basic schematic given in Figure 2.19, hiding method is exhibited, and Red matrix is induced for giving decision. Then it is switched with matrixes of either green or blue. By doing so, XOR operation is performed to an image's least significant bit. In the application, in case of random key of 8 bit and the pixel 1 from 2nd bit of red matrix is XOR with pixel. Therefore, XOR of taken bit 1 and taken bit 0 is 1, thus; pixel will have to satisfy by sending encrypted message which will be hide the value of 1st LSB bit of pixel. In case of obtained answer 0 while XOR operation is performed then pixel will pass, but in the next step operation will be sustained with same 8-bit random key. This process will continue based on encrypted message length.[46]

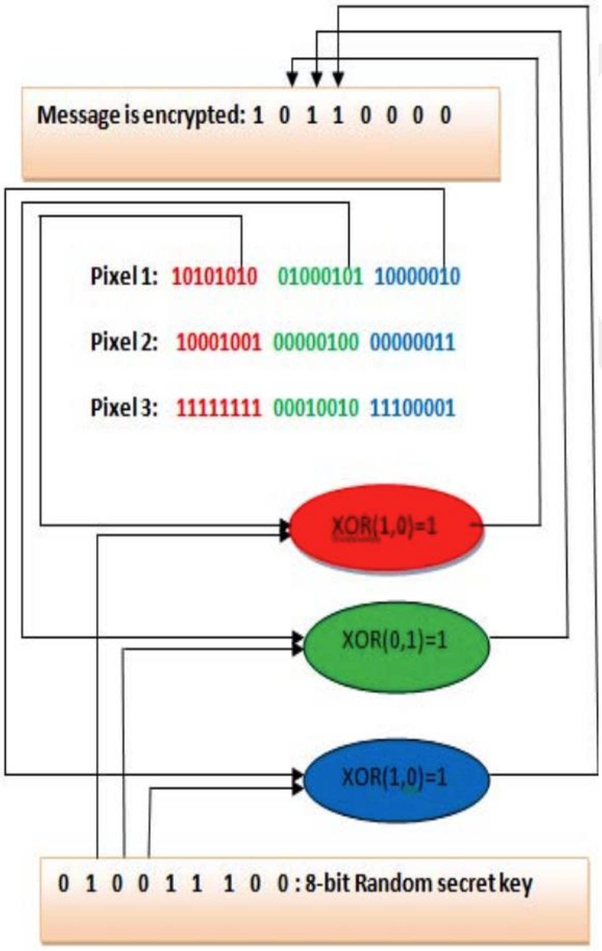

Message is encrypted: 1 0 1 1 0 0 0 0
Pixel 1: 10101010 01000101 10000010
Pixel 2: 10001001 00000100 00000011
Pixel 3: 11111111 00010010 11100001
XOR(1,0)=1
XOR(0,1)=1
XOR(1,0)=1
0 1 0 0 1 1 1 0 0 : 8-bit Random secret key

Figure 2.19 Hiding technique of target message.

In order to recovery of hidden message as shown in matrices from stego image is used, but in the case of recovery process, bits have been taken from pixel and stored in encrypted message. In recovery process, pixel 1 of 2nd bit for red matrix and 8-bit random key are XOR with pixel, and XOR of bit 1 and 0 is resulted as 1, and therefore; pixel must fulfil and send encrypted message that hidden in the value from 1st LSB bit of pixel. In case of given answer is 0 while XOR operation is performed then pixel will pass, but next step in process will be proceeded with same 8-bit random key. These bits are taken into LSB of the same pixel presented in stego image, and following the carrying out this step, decrypted image is taken from stego image. This process will continue based on secret message's length.[46]

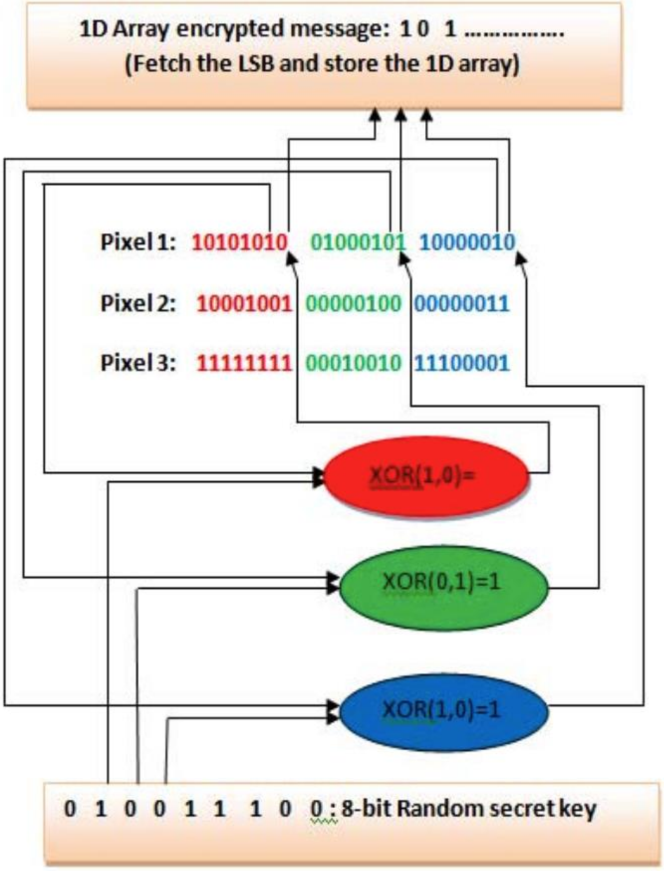

1D Array encrypted message: 1 0 1 ……………
(Fetch the LSB and store the 1D array)
Pixel 1: 10101010 01000101 10000010
Pixel 2: 10001001 00000100 00000011
Pixel 3: 11111111 00010010 11100001
XOR(1,0)=
XOR(0,1)=1
XOR(1,0)=1
0 1 0 0 1 1 1 0 0 : 8-bit Random secret key

Figure 2.20 Recovery technique of hidden message.

As already given, a standard image made up of pixels, and each pixel contains values of Red, Green and Blue ranging from 0 to 255 as 8-bit values (the value of 255 is 11100001) in binary. If one wants to embed "hi" as a message into 4x4 image which has pixel values; [(225, 12, 99), (155, 2, 50), (99, 51, 15), (15, 55, 22), (155, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)], ASCII table can be used to convert this message into decimal values followed by converting into binary values as 0110100 0110101. After iteration over the pixel values one by one, each significant bit with bits of message “hi” sequentially replaced, in other words, last bit replaced with the bit in the right (1) with first data bir (0), and by doing so, pixel values are only modified as +1 or -1. This technique is not noticeable, and 2-LSB can also be used as resulted with by the range -3 to +3. If the message “hi” embed to the 4x4 images that pixel values given above, the result will be [(224, 13, 99), (154, 3, 50), (98, 50, 15), (15, 54, 23), (154, 61, 87), (63, 30, 17), (1, 55, 19), (99, 81, 66), (219, 77, 91), (69, 39, 50), (18, 200, 33), (25, 54, 190)].

After describing the ASCII application, if XOR method is wanted to be probed in much detail in use with ASCII table, another example can be used. Let’s say a secret message “sohel” want to be embedded in a cover image. First secret key is converted into one dimensional circular array as given in Figure 2.21.[47]

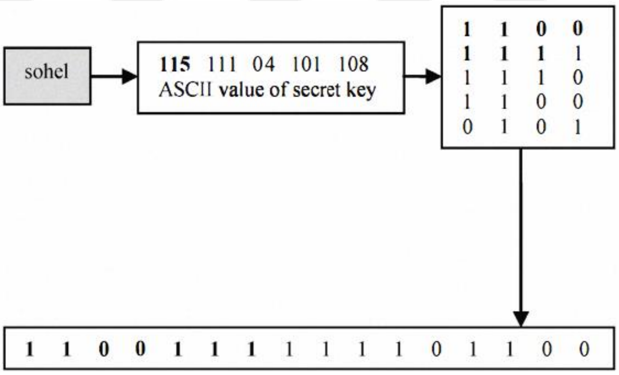
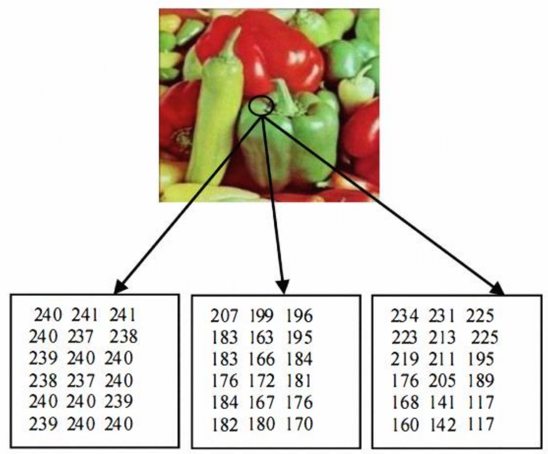


Figure 2.21 Secret key representation with 1d array[47].

A cover image which uses 24-bit color scheme is chosen, and each byte of per pixel in this image represents red, green and blue, known as RGB, primary colors and therefore three different matrices as split is obtained as shown in Figure 2.22. When hidden message is written as binary, each pixel is also converted into 8-bit binary value, and 2D array is arranged as a 1d array which is called bit stream of hidden message as shown in Figure 2.23.[47]



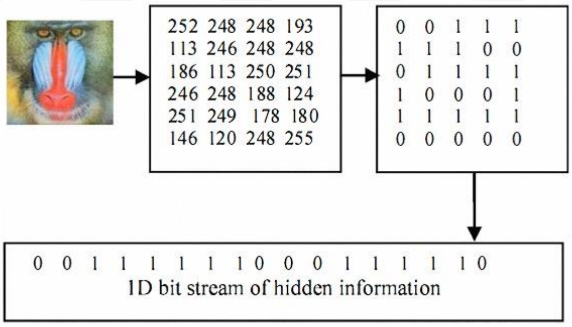
240	241	241
240	237	238
239	240	240
238	237	240
240	240	239
239	240	240

207	199	196
183	163	195
183	166	184
176	172	181
184	167	176
182	180	170

234	231	225
223	213	225
219	211	195
176	205	189
168	141	117
160	142	117

Figure 2.22 RGB matrix representation for a cover image[47].

In here, secret key with Red matrix are applied for decision process to replace hidden message into blue or green matrix. Each bit of hidden message (secret key) is XOR with each LSB of Red matrix.[47]



252	248	248	193
113	246	248	248
186	113	250	251
246	248	188	124
251	249	178	180
146	120	248	255

0	0	1	1	1
1	1	1	0	0
0	1	1	1	1
1	0	0	0	1
1	1	1	1	1
0	0	0	0	0

0 0 1 1 1 1 1 1 0 0 0 1 1 1 1 0
1D bit stream of hidden information

Figure 2.23 Hidden information is represented as 1D array[47].

Thus, obtained XOR makes the decision that 1 bit of hidden message which will be positioned with either blue or green matrix of LSB. This process is sustained until the hidden information is completed as exhibited as flow chart in Figure 2.24.[47]

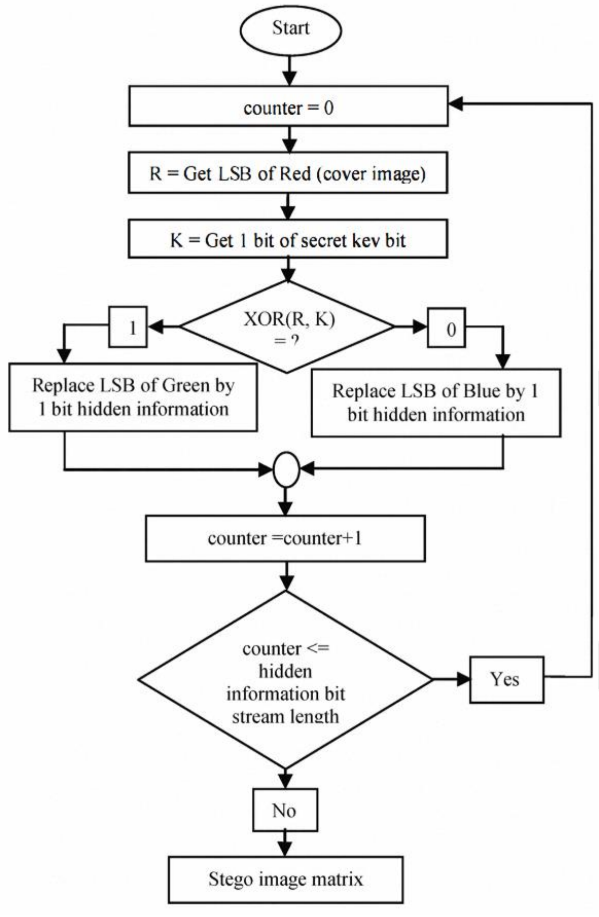

Start
counter = 0
R = Get LSB of Red (cover image)
K = Get 1 bit of secret kev bit
XOR(R, K) = ?
1
0
Replace LSB of Green by 1 bit hidden information
Replace LSB of Blue by 1 bit hidden information
counter =counter+1
counter <= hidden information bit stream length
Yes
No
Stego image matrix

Figure 2.24 Represents the flow chart to hide information into cover image[47].

CHAPTER 3

METHODOLOGY AND IMPLEMENTATION

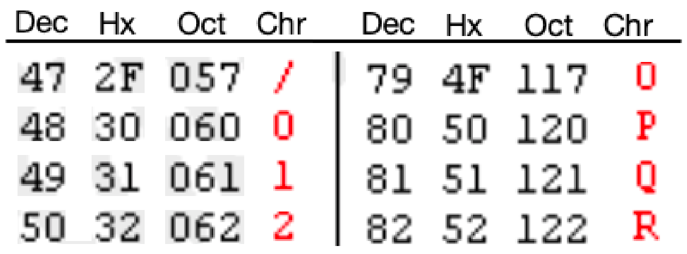
This chapter explains the classical LSB method and improved XOR based LSB method implementation. All steps of implementation will be explained exhaustive. After this chapter, some experimental and comparison results will be shown.

3.1 Classical LSB Method Implementation on MATLAB

In order to implement classical LSB method, the secret message has to convert the binary form. Then, all secret bits are hidden in the picture one by one. In this section, firstly secret message is converted into form of binary. Also, all pixel value of image is converted to binary form. Finally, secret message bits are hidden in each layer of each pixel in picture on MATLAB.

3.1.1 Convert Message to Binary Sequence on MATLAB

As described ASCII number conversion in previous part, ASCII (American Standard Code for Information Interchange) code is the numerical representation of all characters which are used by us for communication in computer. Figure 3.1 shows some part of ASCII table. For example, character “/” equal to 47 in decimal form.



Dec	Hx	Oct	Chr	Dec	Hx	Oct	Chr
47	2F	057	/	79	4F	117	O
48	30	060	0	80	50	120	P
49	31	061	1	81	51	121	Q
50	32	062	2	82	52	122	R

Figure 3.1 Part of ASCII Table.

Also, as you know all process in computer depends on binary numeral base. Decimal to binary conversion is described in below figures.

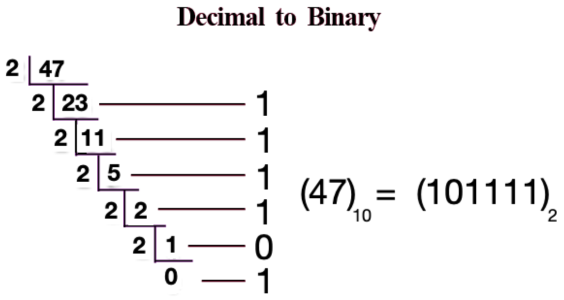


Figure 3.2 Decimal to Binary Conversion.

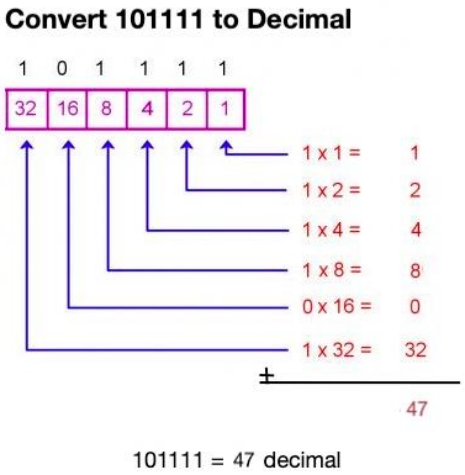


Figure 3.3 Binary to Decimal Conversion.

In the MATLAB operation, all characters of message had to be converted decimal value firstly. Then, all decimal values were converted the binary form.

3.1.2 Classical LSB in Grey Scale Image on MATLAB

As described earlier, LSB is a method in spatial domain. LSB method depends on changing pixel values of picture. Figure 3.4 shows the main idea of the LSB method for one bit changed of greyscale pixel. Firstly, grey image was readed in MATLAB and converted all pixel values to decimal value. One pixel of image was selected then converted binary form in order to synchronize to binary of secret message bits in the location of least significant bit of the pixel in MATLAB. This is literally least significant bit change.

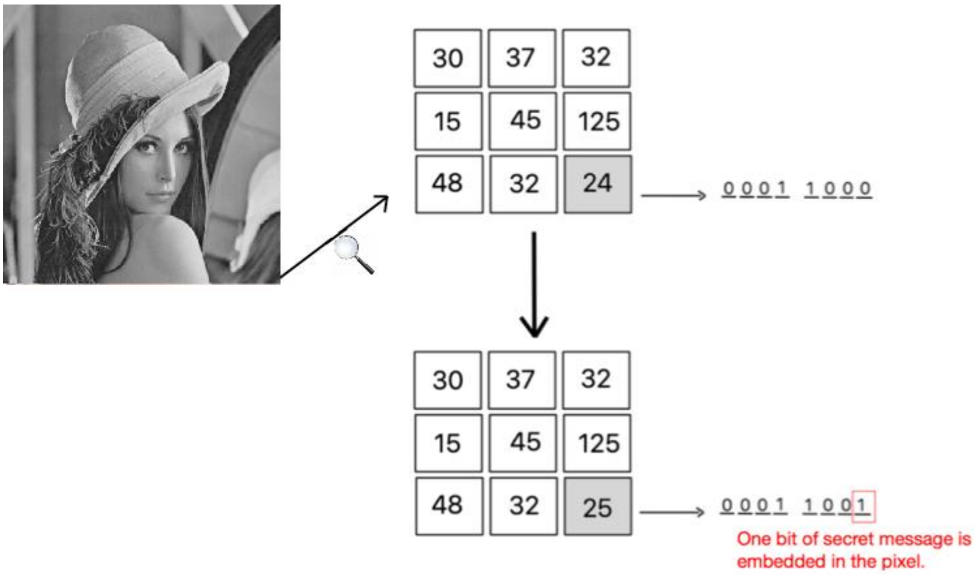


Figure 3.4 One-bit change LSB Method in Greyscale Image.

Also, LSB method includes two or more least significant bit change. Thus, more data capacity can be provided. But, it causes some negative effect like distortion of image. A below figures show the three bits change of one pixel bits.

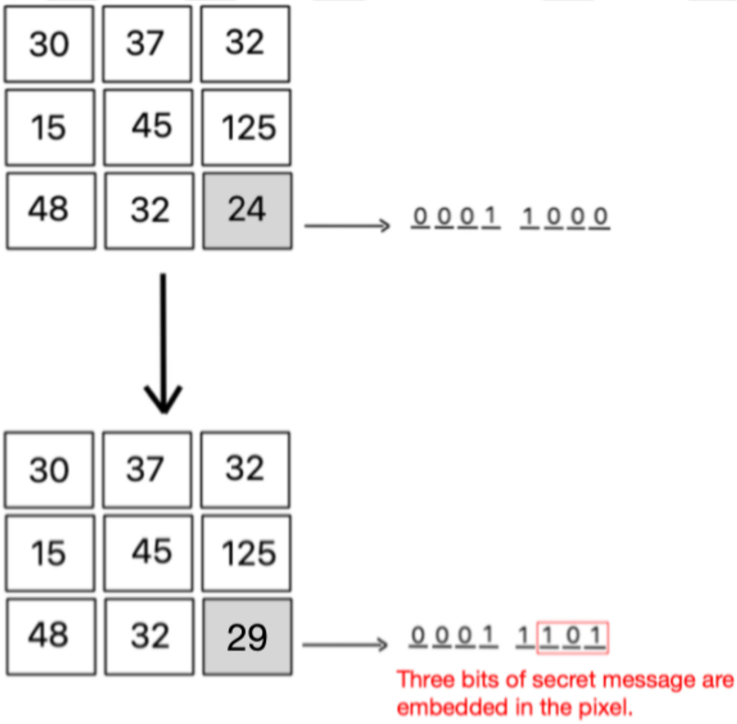
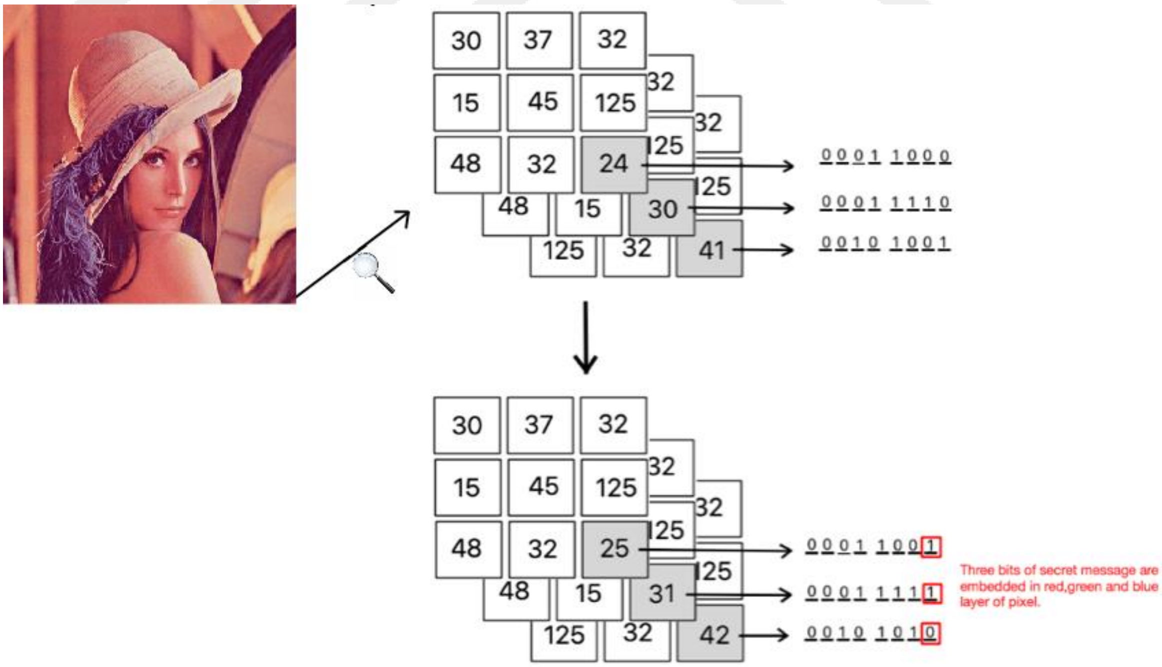


Figure 3.5 Three-bit Change LSB Method in Greyscale Image.

In red square, bits are binary of secret message. Thus, all binary of secret message can be hidden by using LSB method which can be changed one and more bits in pixel.

3.1.3 Classical LSB in Colour Images on MATLAB

Colour images consist of three layers which are red, green and blue. It is called a RGB images. LSB for RGB images is very similar to grey images. LSB method is applied red, green and blue layers separately. There are no any other differences. After a secret message was converted into binary form, images were readed in the MATLAB and converted the all layer of each pixel to the decimal value. One pixel of images was selected then each layers was converted binary form in order to synchronized to some bits of secret message binary data in the location of least significant bit of pixel in MATLAB. Colour images provide the more hidden data capacity and flexibility of different LSB approaches. The improved LSB method is used to advantages of the colour images. Figure 3.6 shows the one-bit change in three layer of pixel.



Three bits of secret message are embedded in red,green and blue layer of pixel.

Figure 3.6 One-bit change LSB Method in Colour Scale Image.

Figure 3.7 shows the three bits change in each layer of pixel.

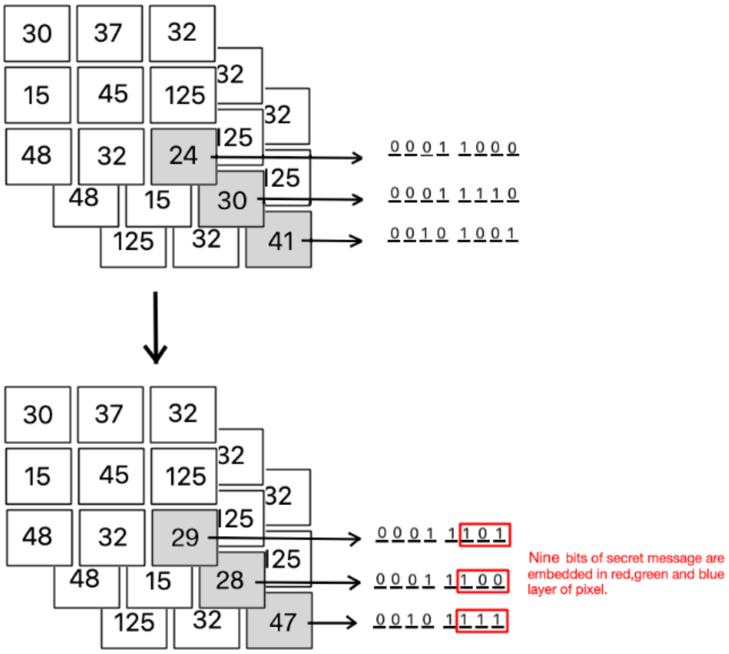


Figure 3.7 Three-bit Change LSB Method in Colour Image.

3.1.4 Retrieval Secret Binary Data from Classical LSB Stego Image with MATLAB

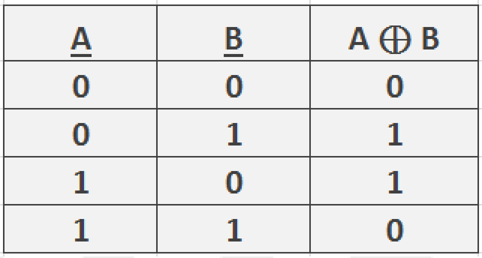
To get secret message from stego-image, classical LSB steganography procedures are applied from end point to start point. All pixels were converted to binary form. Then, starting from last pixel to first pixel was converted binary from and took least significant bits of each pixel. Finally, sequence of secret bit was converted to the decimal value for turning to ASCII character. As a result, getting secret message from stego-image is similar to embedded operation which is LSB based steganography.

3.2 Proposed XOR Operation on LSB Based Steganography

In this part, a new improved LSB technique with XOR operation is explained blow by blow. In this method, two bits of secret messages is hidden one color pixel which is consist of three layers; red, green and blue. This method based on XOR operation advantage. Red layer least significant bit is performed XOR operation respectively green and blue layer least significant bits. In order to equal result of two operations with two bits of secret message only one bit changed. This is the natural advantages of the XOR process.

3.2.1 Natural of XOR Bitwise Operation

XOR (exclusive OR) operation has one output and two inputs. XOR operation produces 0 when both inputs are equal to 0 or 1. It produces 1 for other input combination. Truth table of XOR operation is shown in Figure 3.8.

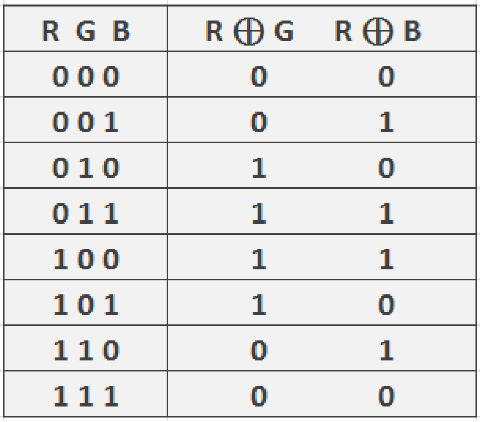


A	B	A ⊕ B
0	0	0
0	1	1
1	0	1
1	1	0

Figure 3.8 Combination of two bits XOR operation result.

3.2.2 Proposed XOR Operation on LSB of Red, Green and Blue Layers

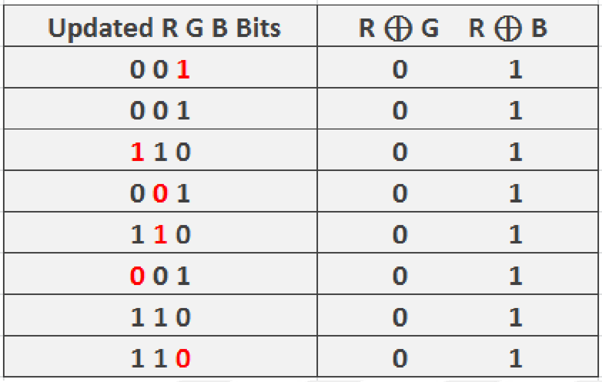
Figure 3.9 shows that that all three-bit combination of least significant bit of red, green and blue layer. In addition to this, table gives the result of XOR operation between red-green and red- blue layers.



R G B	R ⊕ G	R ⊕ B
0 0 0	0	0
0 0 1	0	1
0 1 0	1	0
0 1 1	1	1
1 0 0	1	1
1 0 1	1	0
1 1 0	0	1
1 1 1	0	0

Figure 3.9 XOR operation results for Red-Green and Red-Blue.

For example, two secret bits of message is equal “01”. Only one-bit change, the result of XOR operations can be equal to “01”. Figure 3.10 gives example just one-bit change on all possibilities of three bit, in order to give result of “01”.



Updated R G B Bits	R ⊕ G	R ⊕ B
0 0 1	0	1
0 0 1	0	1
1 1 0	0	1
0 0 1	0	1
1 1 0	0	1
0 0 1	0	1
1 1 0	0	1
1 1 0	0	1

Figure 3.10 One bit changed result for XOR operation.

3.2.3 Improved LSB Based Steganography Technique Using XOR Bitwise Operation in 24 Bit Colour Image on MATLAB

In this part, proposed improved LSB method implemented steps are explained one by one. Then, these steps will be shown with insertion and retrieval algorithm part. Also, these insertion and retrieval operation will be visualized with the flowchart.

Like classical LSB steganography method, secret message was converted to binary form and color image was readed in MATLAB. Then, two bits of secret binary data was used in improved XOR based LSB operation. Red-green and red-blue XOR operation results of pixel had to be equal the selected two bits of secret binary data. To provide this, XOR insertion algorithm which is describe in insertion algorithm part, was used in MATLAB. With using algorithm only one bit was changed in the three layer of pixel. This provides the less image distortion and high security with unpredictability.

3.2.3.1 Insertion Algorithm

- Take the image I.
- Read the all pixels which are consist of red, green and blue layer.
- Get the Pixel P and location (P = I(x,y)).

- Convert the all layer of pixel value into its binary equivalent.
- Get R1, G1, B1, Where;

  R1 is the Least Significant Bit (LSB) of Red Layer in pixel

  G1 is the Least Significant Bit (LSB) of Green Layer in pixel

  B1 is the Least Significant Bit (LSB) of Blue Layer in pixel.
- Two secret bits are represented by S2, S1
- Result of XOR operation respectively X2 and X1, where X2=R1⊕G1 and X1=R1⊕B1.
- To provide equal result of XOR operation and secret bits (S2=X2 and S1=X1), loop is shown below;
  - If R1=0 then
    - If G1=0 and B1=0 then

      If S2=0 and S1=0 then → No Change.

      If S2=0 and S1=1 then → Set B1=1.

      If S2=1 and S1=0 then → Set G1=1.

      If S2=1 and S1=1 then → Set R1=1.
    - If G1=0 and B1=1 then

      If S2=0 and S1=0 then → Set B1=0.

      If S2=0 and S1=1 then → No Change.

      If S2=1 and S1=0 then → Set R1=1.

      If S2=1 and S1=1 then → Set G1=1.
    - If G1=1 and B1=0 then

      If S2=0 and S1=0 then → Set G1=0.

      If S2=0 and S1=1 then → Set R1=1.

      If S2=1 and S1=0 then → No Change.

If S2=1 and S1=1 then → Set B1=1.

- If G1=1 and B1=1 then

  If S2=0 and S1=0 then → Set R1=1.

  If S2=0 and S1=1 then → Set G1=0.

  If S2=1 and S1=0 then → Set B1=0.

  If S2=1 and S1=1 then → No Change.

- If R1=1 then
  - If G1=0 and B1=0 then

    If S2=0 and S1=0 then → Set R1=0.

    If S2=0 and S1=1 then → Set G1=1.

    If S2=1 and S1=0 then → Set B1=1.

    If S2=1 and S1=1 then → No Change.

  - If G1=0 and B1=1 then

    If S2=0 and S1=0 then → Set G1=1.

    If S2=0 and S1=1 then → Set R1=0.

    If S2=1 and S1=0 then → No Change.

    If S2=1 and S1=1 then → Set B1=0.

  - If G1=1 and B1=0 then

    If S2=0 and S1=0 then → Set B1=1.

    If S2=0 and S1=1 then → No Change.

    If S2=1 and S1=0 then → Set R1=0.

    If S2=1 and S1=1 then → Set G1=0.

  - If G1=1 and B1=1 then

    If S2=0 and S1=0 then → No Change.

If S2=0 and S1=1 then → Set B1=0.

If S2=1 and S1=0 then → Set G1=0.

If S2=1 and S1=1 then → Set R1=0.

In this way, two secret bits is hidden into pixel with only one bit change.

3.2.3.2 Retrieval Algorithm

- Obtain the stego image got after the insertion of secret message by insertion algorithm.
- Trace out location.
- Get the R1, G1, B1 bits of selected pixel. (LSB bits of Red, Green and Blue layer)
- Then, calculate XOR operation between R1-G1 and R1-B1.
- Result of XOR operation gives the two secret message bits.
- All secret bits can be calculated with this operation.

3.2.3.3 Flow Chart of Insertion and Retrieval Algorithm

Information about insertion and retrieval method given as flowcharts in Figure 3.11, and Figure 3.12, respectively.

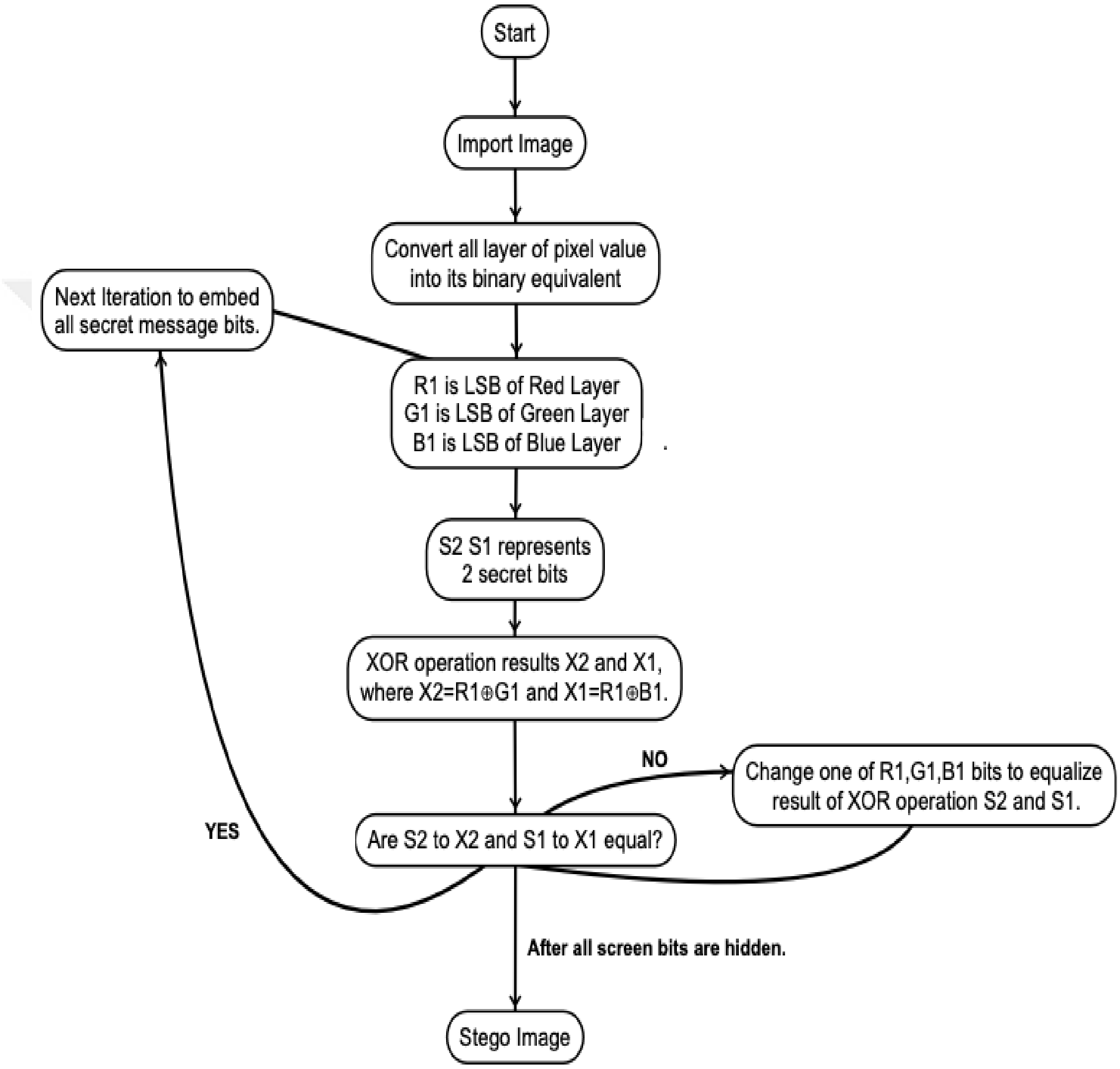

Start
Import Image
Convert all layer of pixel value into its binary equivalent
Next Iteration to embed all secret message bits.
R1 is LSB of Red Layer
G1 is LSB of Green Layer
B1 is LSB of Blue Layer
S2 S1 represents 2 secret bits
XOR operation results X2 and X1, where X2=R1⊕G1 and X1=R1⊕B1.
NO
Change one of R1,G1,B1 bits to equalize result of XOR operation S2 and S1.
YES
Are S2 to X2 and S1 to X1 equal?
After all screen bits are hidden.
Stego Image

Figure 3.11 Flow chart for insertion of message.

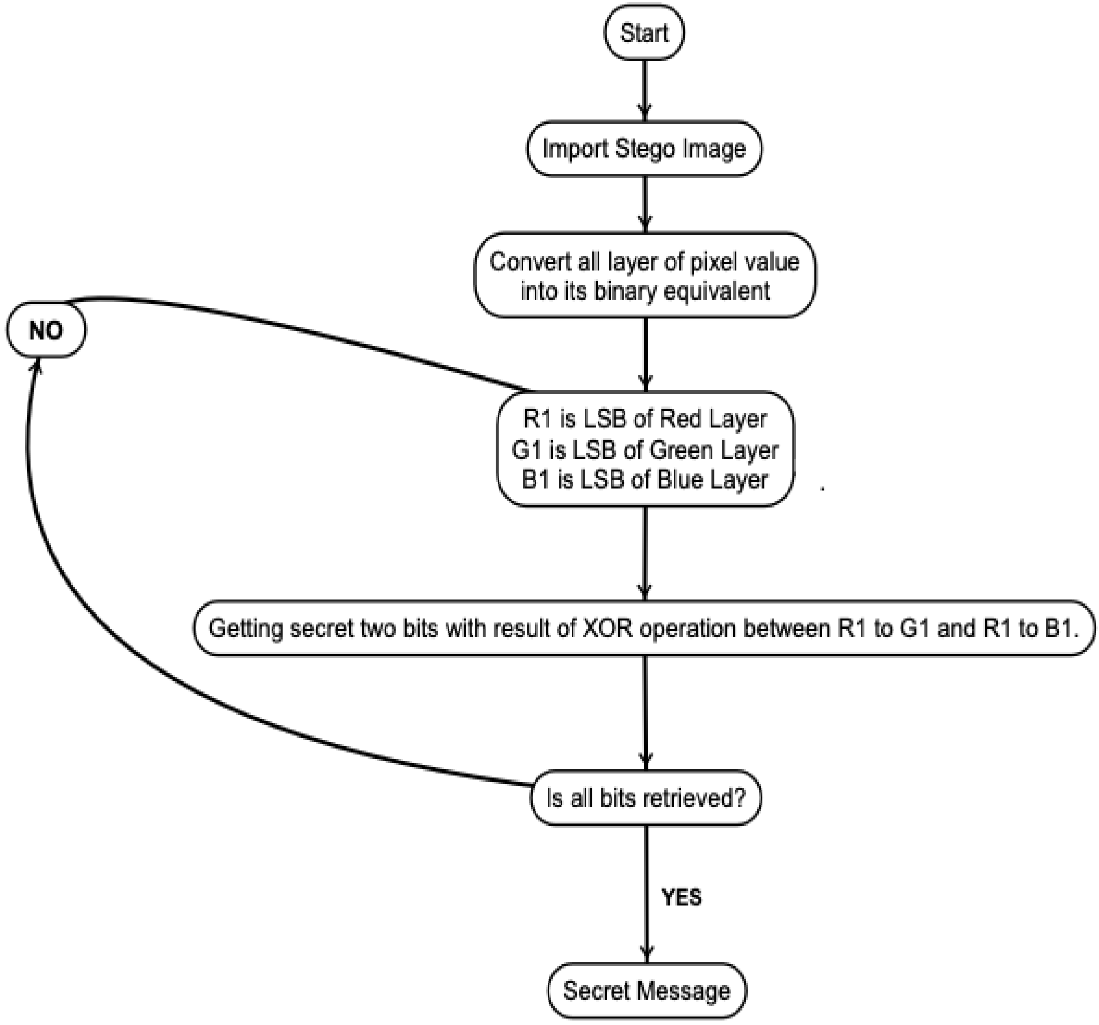

Start
Import Stego Image
Convert all layer of pixel value into its binary equivalent
R1 is LSB of Red Layer
G1 is LSB of Green Layer
B1 is LSB of Blue Layer
Getting secret two bits with result of XOR operation between R1 to G1 and R1 to B1.
Is all bits retrieved?
NO
YES
Secret Message

Figure 3.12 Flow chart for retrieval of message.

3.2.4 Improved Security of New LSB Based Image Steganography

In this part, improved XOR based LSB image steganography can be more secure with extra two security procedures. These are implemented in the MATLAB code.

One of them about how to select pixel. Tiered selection pixel is a predictable. Though, improved XOR based LSB method is safe even if selection method is tiered. Because XOR operation is unpredictable and unforeseen. However, selection pixel can be random in order to increase security. Thus, pixels are selected chaotically for instead of tiered selection.

Second thing is about secret message. Secret message can be encrypted with some cryptographic method. AES encryption can be used as an encryption method. If AES cryptography is used to enhance security level, AES key should be known to receiver side. In the thesis, AES cryptography module is used online module to encrypt the secret message. There are lots of online encrypt decrypt AES website.

XOR bitwise operation based LSB improved steganography method is combined with the random number generator for selection pixel and AES cryptography of secret message. Thus, proposed new improved steganography method is unpredictable and more safety. Because of the AES crypto, even if someone solve the all methodology of proposed method. Very hard to get secret message without key.

3.2.4.1 Pseudo-Random Number Generator(PRNGs)

As the word ‘pseudo’ suggests, pseudo-random numbers are not random. Essentially, PRNGs are algorithms that use mathematical formula or simply precalculated tables to produce sequences of numbers that appear random. A good example of a PRNG is the linear congruential method. A good deal of research has gone into pseudo-random number theory, and modern algorithms for generating pseudo-random numbers are so good that the numbers look exactly like they were really random. The key point of random generator is a deterministic which means a given sequence of numbers can be reproduced at later date if the starting point of sequence is known. MATLAB has own random number generator function to use in proposed high secure LSB method.

3.2.4.2 Advance Encryption Standard (AES)

AES (Advanced Encryption Standard), also known as Rijndael encryption in cryptography, is a block encryption standard adopted by the US federal government. This standard is used to replace the original DES (1977) which could break a DES key in only 22 hours with improvement of technology, and has been widely used around the world, becoming one of the most popular algorithms in symmetric key algorithms.

Before invention of the AES, the most commonly used symmetric key algorithm was the DES encryption algorithm , which was announced in 1977 as the commercial encryption standard of the US government. The problem of DES is key length is short, and it is gradually not suitable for the requirements of data encryption security in distributed open networks. Therefore, in 1998, the US government launched a campaign to solicit candidate algorithms for AES. The basic requirements of the solicitation for AES are: faster than triple DES, at least as secure as triple DES, data packet length of 128 bits, and key length of 128/192/256 bits.

CHAPTER 4

EXPERIMENTAL RESULT

This part of study focuses on improvement XOR based LSB method experimental results. Expression will be started with old LSB based steganography method results. Then, proposed method of experiments will explain and compare with the old method. Also, improvement values are shown in this part.

In this part, experimental results will be compared with some parameters which are histogram of image, PSNR value, MSE value and security improvements.

These experiments were done according to different message size and set of three different images. Then, showing the result of histogram, PSNR and MSE value of classical and proposed method. Thus, all result of proposed and classical method can be compared easily.

4.1 Comparison Parameters

4.1.1 MSE

MSE (Mean Square Error) gives the information about differences between two images. The MSE is equal to cumulative error between original and stego images. The value of MSE should be as possible as low to confirm the quality of the method. The formula is MSE is given in Equation 4.1.

$$\mathrm{MSE} = \frac{1}{\mathrm{R\,x\,C}} \sum_{\mathrm{i=1}}^{\mathrm{R}} \sum_{\mathrm{j=1}}^{\mathrm{C}} (\mathrm{xij} - \mathrm{x'ij})^2 \qquad \textbf{(4.1)}$$

Where x_{ij} and x'_{ij} is the original and stego images respectively.

4.1.2 PSNR

PSNR (Peak Signal to Noise Ratio) gives the information about how two images are similar. It measures peak error between two images. PSNR should be as possible as high for obtaining quality method of steganography. The PSNR of images can be calculated by using Equation 4.2.

$$\mathrm{PSNR} = 10\log_{10}\frac{\mathrm{I}^2}{\mathrm{MSE}} \tag{4.2}$$

Where I is the dynamic range of pixel values, or the maximum value that a pixel can take, for 8-bit images: I=255. MSE is the mean square error.

4.2 Experimental Result of Classical LSB Steganography

4.2.1 Experimental Result of Classical LSB Steganography Method on Greyscale Image

This part gives the basic experimental result of classical LSB method on Greyscale Image.

The purpose of this part, how the effect of changing number of least significant bits on the comparison parameters for same secret message size (80000 bits). Also, picture of Lenna has 200x200 pixel resolution.

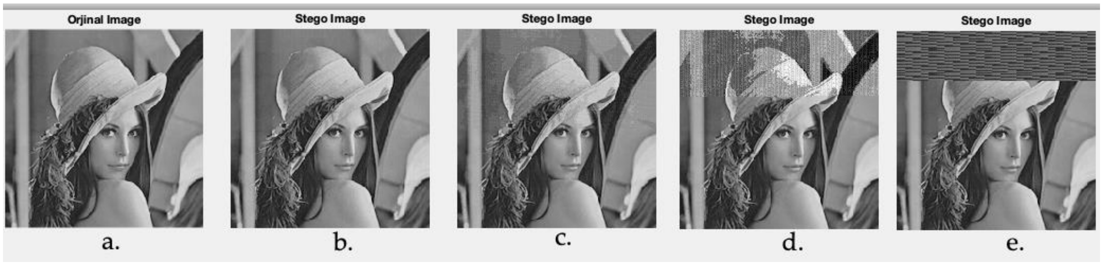


Figure 4.1 a. is original image, b 2 lsb bits changed, c 4 lsb bits changed, d 6 lsb bits changed, e 8 lsb bits changed.

It obviously seen that, image distortion is increased by the increasing number of changing least significant bits of pixel in Figure 4.1. For all images secret bit size equal, when increasing number of changed bit, number of used pixel is decrease.

More number of changing bits cause more pixel value difference and more pixel value difference cause more image distortion. Also, histogram effects of changing bit is shown in Figure 4.2.

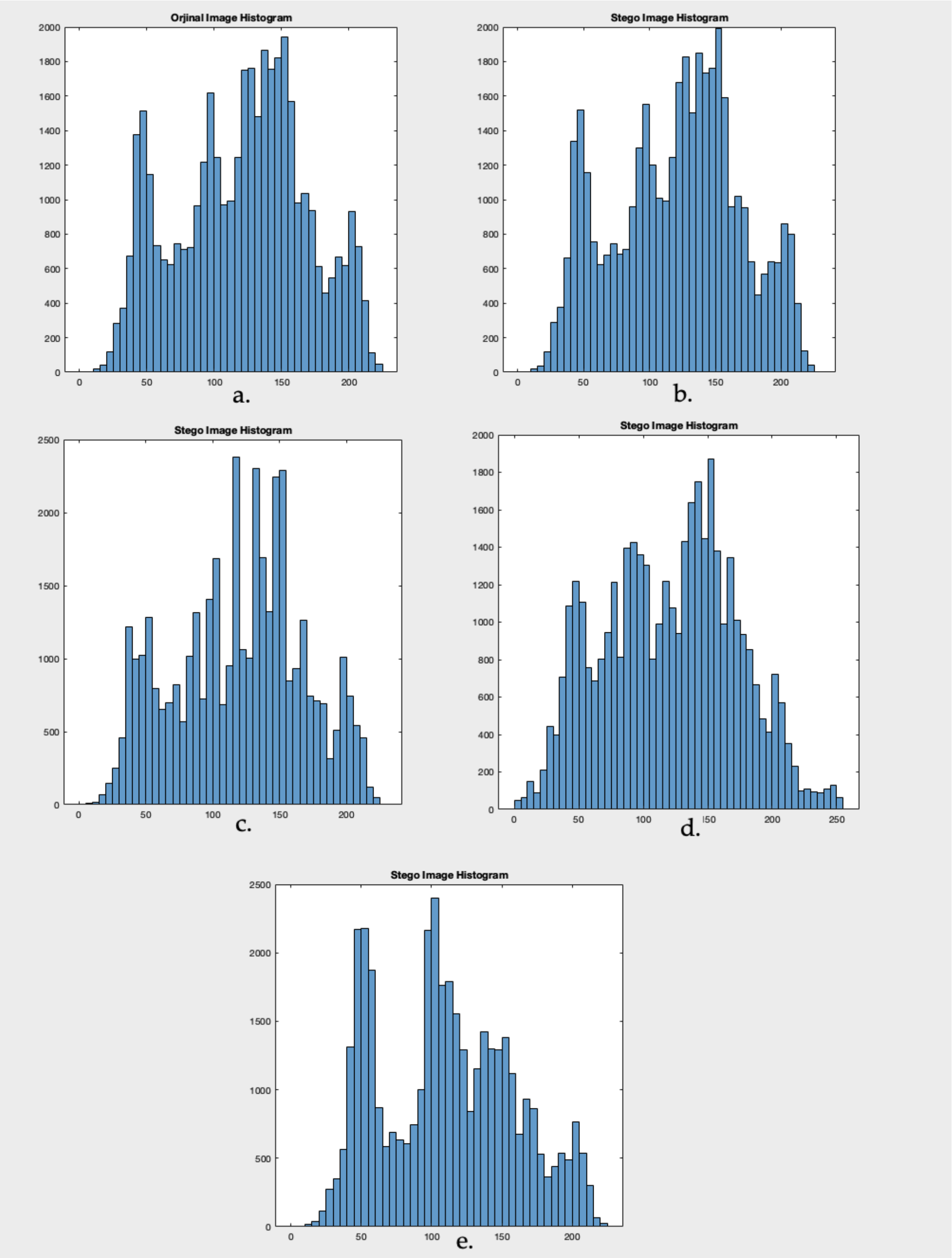


Figure 4.2 a. is original image. b 2 lsb bits changed. c 4 lsb bits changed. d 6 lsb bits changed. e 8 lsb bits changed.

Table 4.1 is proved that if the number of changing LSB bit is increased, MSE values are also increased. Because, mean square error (MSE) formula depend on the square difference of pixels. So, when increasing the changing number of LSB bits, differences of original and stego pixels value increase.

For the view of PSNR values, if the number of changing LSB bits increase, PSNR values are decrease. Because, its formula depends on the MSE value. When MSE increases, PSNR value decreases. As known, PSNR value is peak error between two images. If the increase the number of changing LSB bits of pixel, pixel decimal value change can change in big range. So, difference between original and stego pixel increase. The similarity parameter PSNR decreases.

Table 4.1 Test result parameter values for classical LSB.

Lenna				
PSNR	**44,3063**	**35,4082**	**25,0587**	**18,2524**
MSE	**2,4124**	**18,7179**	**202,8679**	**972,387**
Message Size(bits)	**80000**	**80000**	**80000**	**80000**
Image Size	**200x200**	**200x200**	**200x200**	**200x200**
% of Pixel Used	**100**	**50**	**25**	**12,5**
Number of Changed LSB Bits	**2**	**4**	**6**	**8**

4.2.2 Experimental Result of Classical LSB Steganography Method on RGB Image

In this part, classical LSB based steganography method is implemented in color images. As known, color image pixels consist of three layers which are red, green and blue. One pixel of color image is represented with 24 bits like three times greyscale.

Three images are used; Lenna, Boats and Baboon. Two different of secret message size (40000, 80000 bits) are embedded in image set. The resolutions of all pictures are 200x200 pixels.

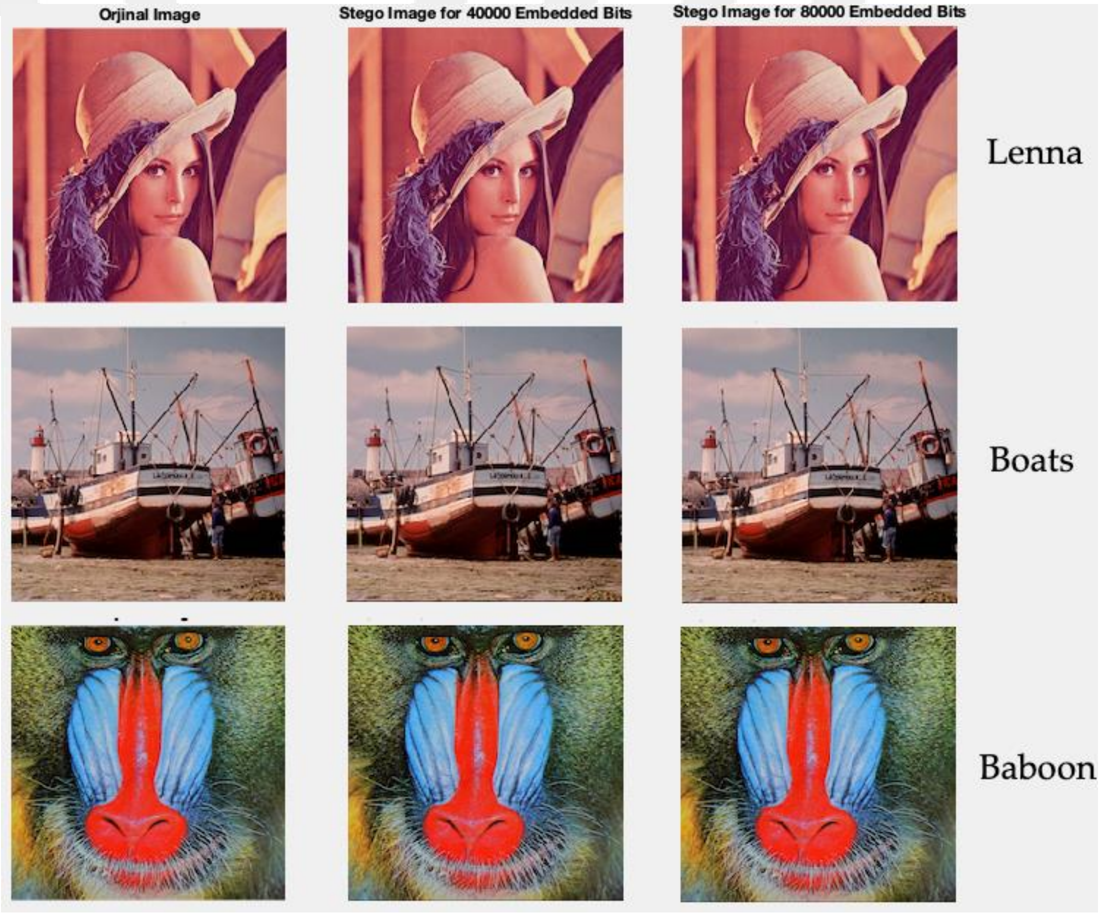

Orjinal Image
Stego Image for 40000 Embedded Bits
Stego Image for 80000 Embedded Bits
Lenna
Boats
Baboon

Figure 4.3 40000 and 80000 bits are embedded in experimental image set for classical LSB.

Figure 4.3 provides information about image distortion. In previous part, when increasing number of changed bit, image distortion is increased too much. So, that is reason why try to embedded data only 1 least significant bit. As seen in the figure, for classic least significant bit change (one bit) does not distort the image so that the human eye can easily see it. But, if you look closely at the picture, you can see difference between the original and stego pixels.

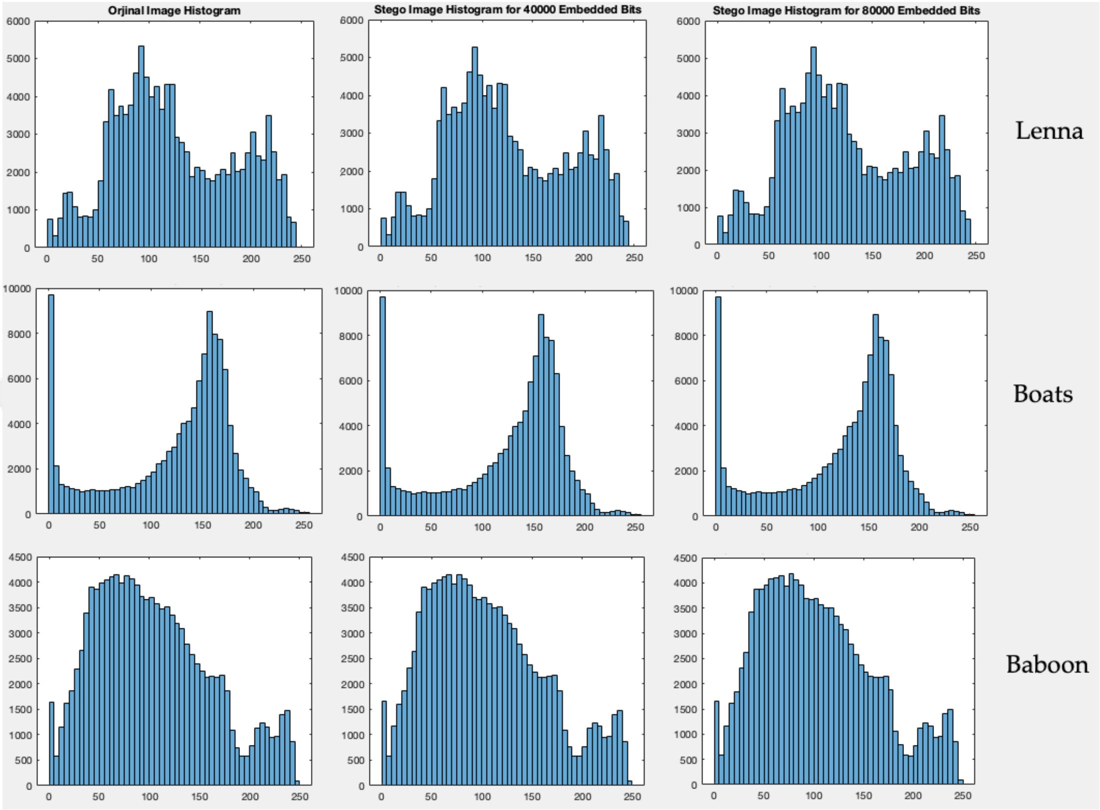


Figure 4.4 Histogram of 40000 and 80000 bits embedded experimental image set for classical LSB.

Histogram figures are changed depending on secret messages size. All histogram graph looks like very similar each other. But if the looking closely enough, some differences can be seen easily.

Table 4.2 Test result parameter values for classical LSB.

Classical LSB Based Steganography Method on RGB Images						
	Lenna		**Boats**		**Baboon**	
PSNR	**55,9199**	**52,9025**	**55,9132**	**52,9144**	**55,9378**	**52,8979**
MSE	**0,1664**	**0,3333**	**0,1666**	**0,3324**	**0,1657**	**0,3397**
Message Size(bits)	**40000**	**80000**	**40000**	**80000**	**40000**	**80000**
Image Size	**200x200**	**200x200**	**200x200**	**200x200**	**200x200**	**200x200**
% of Pixel Used	**33,33**	**66,66**	**33,33**	**66,66**	**33,33**	**66,66**
Num. of Changed LSB Bits	**1**	**1**	**1**	**1**	**1**	**1**

Also Table 4.2 gives the information about how effect the PSNR and MSE value from size of secret message. As show in the table, when secret message size increase, PSNR is decrease and MSE is increase.

4.2.3 Experimental Result of Improved LSB Based Steganography Technique Using XOR Bitwise Operation on RGB Image

In this part, proposed improvement LSB based steganography method is implemented in color images.

Same experimental set is used. Three images are used like previous part. Two different of secret message size (40000, 80000 bits) are embedded in image set. The resolutions of all pictures are 200x200 pixels.

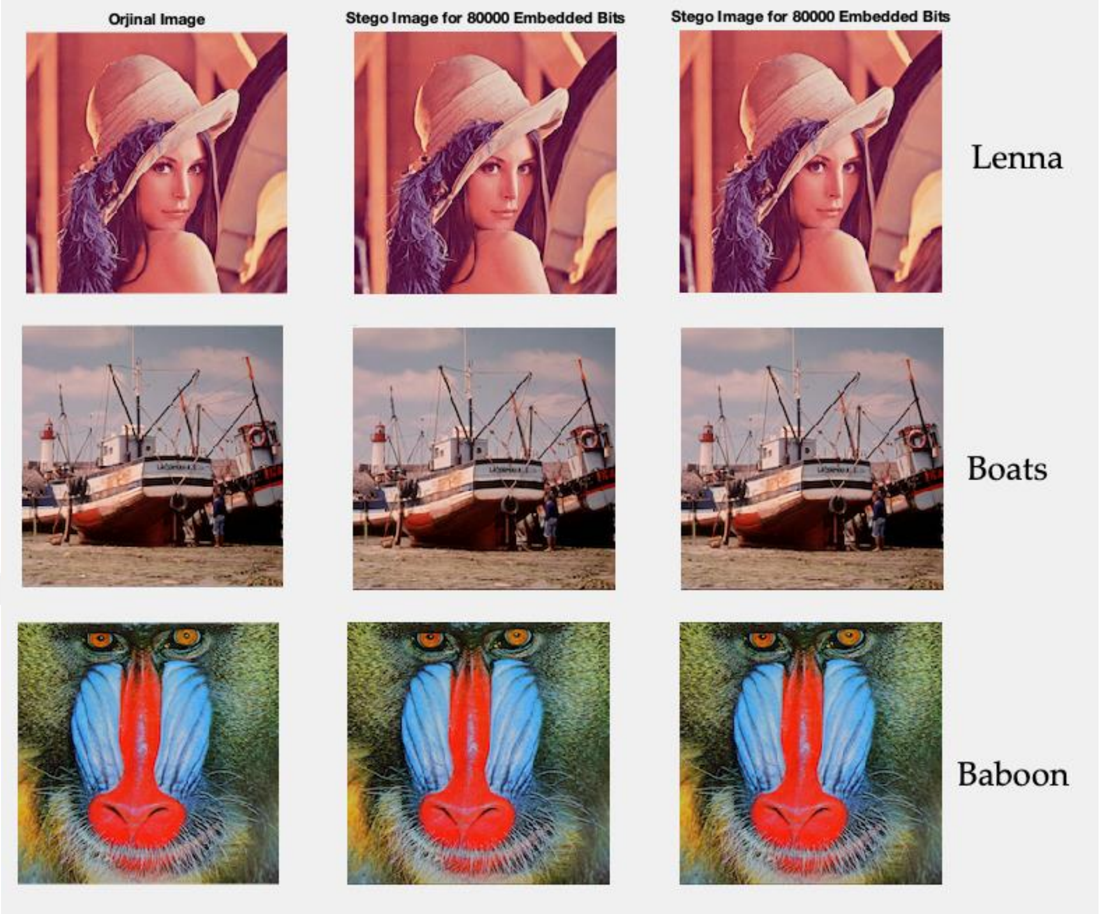

Orjinal Image
Stego Image for 80000 Embedded Bits
Stego Image for 80000 Embedded Bits
Lenna
Boats
Baboon

Figure 4.5 40000 and 80000 bits are embedded in experimental image set for improved LSB.

As shown in the Figure 4.5, the image distortion is not easily visible to the eyes. There is very small change in colour range of pixel. Also, PSNR and MSE value say that image distortion is less than classical LSB method.

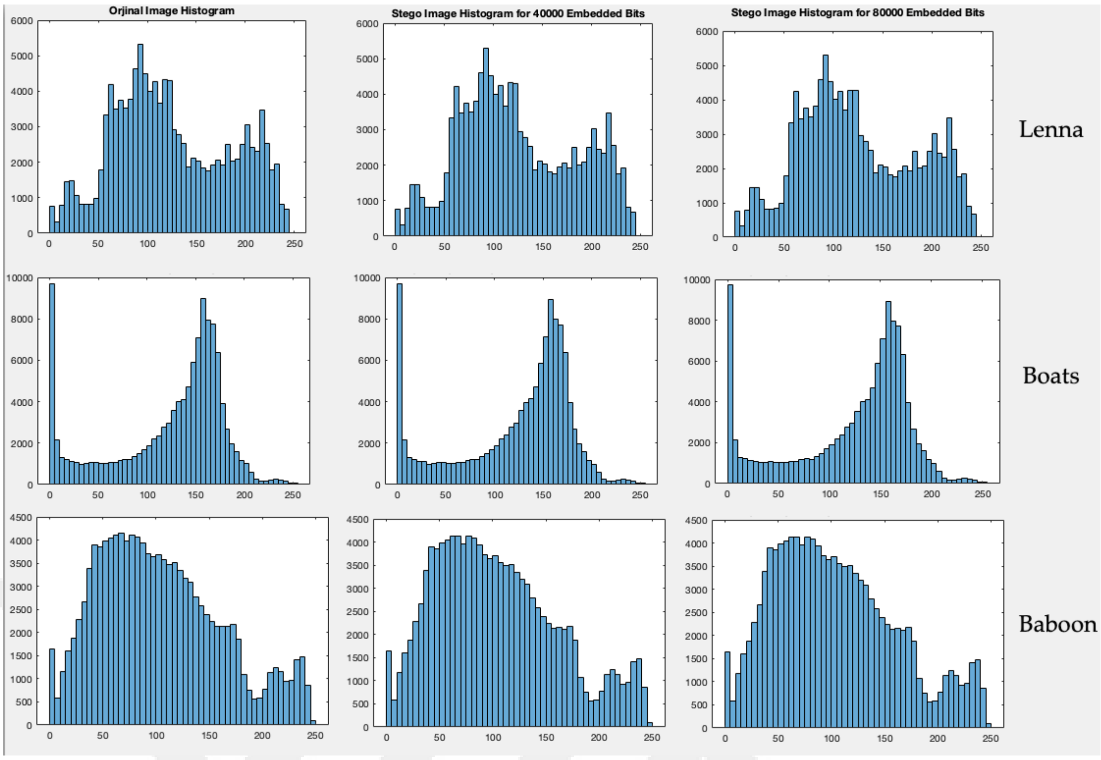


Figure 4.6 Histogram of 40000 and 80000 bits embedded experimental image set for improved LSB.

Table 4.3 Test result parameter values for improved LSB.

Improved XOR Based Steganography Method on RGB Images						
	Lenna		**Boats**		**Baboon**	
PSNR	**57,2039**	**54,1652**	**57,1698**	**54,1542**	**57,1803**	**54,1584**
MSE	**0,1238**	**0,2492**	**0,1248**	**0,2498**	**0,1245**	**0,2496**
Message Size(bits)	**40000**	**80000**	**40000**	**80000**	**40000**	**80000**
Image Size	**200x200**	**200x200**	**200x200**	**200x200**	**200x200**	**200x200**
% of Pixel Used	**50**	**100**	**50**	**100**	**50**	**100**
Num. of Changed LSB Bits	**1**	**1**	**1**	**1**	**1**	**1**

Like previous part, secret message size effect histogram graph, PSNR value and MSE value.

4.3 Comparison between Proposed Improvement Method and Classical Method

Below table is summary of all operations. As you seen in figure, proposed improved method has better PSNR value and MSE value. For all images, PSNR value of proposed method higher than classical method. Also, MSE values of proposed method smaller than classic method which means that confirmed the reliability of improved method. Besides, these PSNR and MSE values proved better image quality for proposed method.

Table 4.4 Improved and Classical experiment parameter results for comparison.

Lenna	**Classical Method**		**Improved Method**	
PSNR	**55,9199**	**52,9025**	**57,2039**	**54,1652**
MSE	**0,1664**	**0,3333**	**0,1238**	**0,2492**
Message Size(bits)	**40000**	**80000**	**40000**	**80000**
Image Size	**200x200**	**200x200**	**200x200**	**200x200**
% of Pixel Used	**33,33**	**66,66**	**50**	**100**
Changed LSB Number	**1**	**1**	**1**	**1**
Boats				
PSNR	**55,9132**	**52,9144**	**57,1698**	**54,1542**
MSE	**0,1666**	**0,3324**	**0,1248**	**0,2498**
Message Size(bits)	**40000**	**80000**	**40000**	**80000**
Image Size	**200x200**	**200x200**	**200x200**	**200x200**
% of Pixel Used	**33,33**	**66,66**	**50**	**100**
Changed LSB Number	**1**	**1**	**1**	**1**
Baboon				
PSNR	**55,9378**	**52,8979**	**57,1803**	**54,1584**
MSE	**0,1657**	**0,3337**	**0,1245**	**0,2496**
Message Size(bits)	**40000**	**80000**	**40000**	**80000**
Image Size	**200x200**	**200x200**	**200x200**	**200x200**
% of Pixel Used	**33,33**	**66,66**	**50**	**100**
Changed LSB Number	**1**	**1**	**1**	**1**

In addition, the security of the confidential message is enhanced by using the XOR bitwise operation. Because the XOR process between the layers is more complex and unpredictable than the classical LSB.

4.4 Improvement Security of New LSB Based Image Steganography

In order to have maximum security, the improved XOR-based LSB method is made more secure with random pixel selection and AES encryption of secret message on MATLAB. Also, in this methodology key is used for decryption of secret message.

The proposed high-security method is to mix two parts that are a random number generator initial value and AES key. Randomization of selecting pixel provides more complex approach and unpredictability. Also, if the recommended method is broken, AES encryption provides the extra security. Key should be known the receiver side.

Figure 4.7 is shown the how look like the random selection pixels on the image.

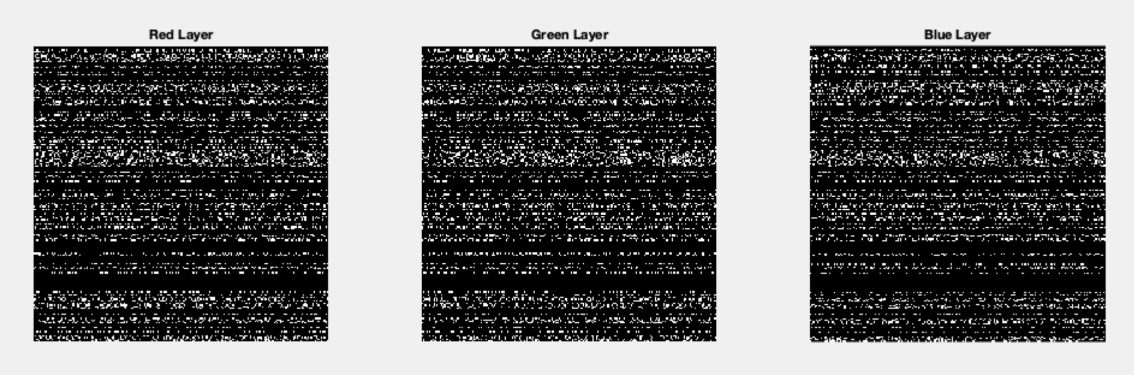


Figure 4.7 Differences between Random pixel selected Stego image and Original image.

CHAPTER 5

CONCLUSION

In this thesis, improved XOR based LSB steganography has been designed and implemented. As aforementioned, purpose of image steganography is embedding secret message in image while managing to be stayed as unnoticeable in a safe way. Whether it is low or high a distortion of subject image which carries the hidden data is inevitable. However, subject image should be distorted as little as possible while staying unpredictable or complex for ordinary security control protocols to be ensure to have decreased external noticeability to the low levels. In order to design a method with less image distortion while having favorable PSNR and MSE values, natural advantages of XOR operation was utilized. XOR operation in three bits provide to embedded two secret bit with just one bit changed, and resulting less bit change for PSNR and MSE values in all three images are exhibited better results than traditional LSB method. Experimental results demonstrate that proposed XOR based LSB method here provides low image distortion and high communication security by keeping the value of PSNR as high, and the value of MSE as low. Moreover, XOR operation provides greatly improved security as well as complexity than classical method while sustaining the less distortion ratio on subject image. Extreme intangibility is not the case here, but it is aimed to provide an alternative method which may be applied to integrated software or even it can be developed to the more complex stages.

In future study, focusing on alternation of selection methodology for red, green and blue layer can be an important point to research as it is highly believed that changing the selection methodology to the more novel way can improve the all process. Additionally, studying for distinct approaches of XOR based method on bits of pixel can be another target subject for providing lesser image distortion along with improved data capacity.

REFERENCES

[1] Marvel L.M, Boncelet C.G., Retter C.T., "*Spread spectrum image steganography*", IEEE Transactions on Image Processing, 8(8):1075-83, 1999.

[2] Johnson N.F., Jajodia S., *"Exploring steganography: Seeing the unseen"*, IEEE Computer Society, 1998.

[3] James C. J., *"Steganography: Past, Present, Future"*, United States, 2001.

[4] Provos N., Honeyman P., *"Hide and seek: an introduction to steganography"*, IEEE Security and Privacy, 1(3):32 - 44, 2003.

[5] Moulin P., Koetter R., *"Data-Hiding Codes"*, Proceedings of the IEEE, 2005.

[6] Cheddad A.,Condell J.,Curran K.,Kevitt P., *"Digital image steganography: Survey and analysis of current methods"*, Signal Processing 90(3):727-752, 2010.

[7] Lyu S., Farid H., *"Steganalysis using higher-order image statistics"*, IEEE Transactions on Information Forensics and Security 1 (1), 111-119, 2006.

[8] Kahn D., The *"Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet"*, United States, 1996.

[9] Delahaye J.P., *"Information noyée, information cache"*, French, Pour la Science, www.apprendre-en-ligne.net/crypto/stegano/229_142_146.pdf, 1996.

[10] Thomas T.L., *"Al Qaeda and the Internet: Tthe Danger of 'Cyberplaning'"*, NCJRS, 2003.

[11] Hosmer C., *"Discovering hidden evidence"*, Journal of Digital Forensic Practice, 1(1):47-56, 2006.

[12] Hernandez-Castro J. C., Blasco-Lopez I., Estevez-Tapiador J. M., and Ribagorda-Garnacho A., *"Steganography in Games: A General Methodology and its Application to the Game of Go"*, Computers and Security, 25(1):64-71, 2006.

[13] Bender W., Gruhl D., Hwang R., Paiz F.J., Pogreb S.,*"Applications for data hiding"* ,IBM System Journal, 0018-8670, 2000.

[14] Stefan Katzenbeisser, *"Information Hiding Techniques for Steganography and Digital Watermarking"*, Artech House, United States, 2000.

[15] Miaou S. G., Tsai Y., Chao, H.,*"A secure data hiding technique with heterogeneous data-combining capability for electronic patient records"*, IEEE 22nd Annual EMBS International Conference, USA, 2000.

[16] Anand D., Nirinjan U.C., *"Watermarking medical images with patient information"*, 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, China, 1998.

[17] Li C.T., Li Y., Wei C., *"Protection of mammograms using blind steganography and watermarking"*, IEEE International Symposium on Information Assurance and Security, 2007.

[18] Frith D., *"Steganography approaches, options, and implications"*, Network Security, 2007.

[19] Cheddad A.,Condell J.,Curran K.,Kevitt P., *"A secure and improved self-embedding algorithm to combat digital document forgery"*, Signal Processing, 2009.

[20] Johnson N., Stefan K., *"A survey of steganographic techniques"*, Artech House, 2000.

[21] Bailey K., Curran K., *"An evaluation of image based steganography methods"*, Multimedia Tools and Applications. Multimedia Tools and Applications 30(1):55-88 , 2006.

[22] Alvarez P., *"Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis"*, IJDE, Computer Science, 2004.

[23] Popescu A.C., *"Statistical tools for digital image forensics"*, Lecture Notes in Computer Science 3200, 2004.

[24] Chang C-C., Chen T.-S., Chung L.-Z., *"A steganographic method based upon JPEG and quantization table modification"*, Information Sciences 141(1-2):123-138, 2002.

[25] Li X., Wang J., *"A steganographic method based upon JPEG and particle swarm optimization algorithm"*, Mathematics, Computer Science Published in Inf. Sci., 2007.

[26] Fard A.M., Akbarzadeh-T M.-R., Varasteh-A F., *"A new genetic algorithm approach for secure JPEG steganography"*, 2006 IEEE International Conference on Engineering of Intelligent Systems, IEEE, 2006.

[27] Hashad A.I., Madani A.S., Wahdan A., *"A robust steganography technique using discrete cosine transform insertion"*, 2005 International Conference on Information and Communication Technology, IEEE, 2005.

[28] Raja K., Chowdary C., Venugopal K., Patnaik L., *"A secure image steganography using LSB, DCT and compression techniques on raw images"*, 2005 3rd international conference on intelligent sensing and information processing, IEEE, 2005.

[29] McKeon R.T., *"Strange Fourier steganography in movies"*, IEEE International Conference on Electro/Information Technology, 2007.

[30] Morkel T., Eloff J.H., Olivier M.S., *"An overview of image steganography"*, ISSA, 2005.

[31] Johnson N.F., Jajodia S., *"Steganalysis of images created using current steganography software"*, International Workshop on Information Hiding, 1998.

[32] Potdar V.M., Han S., Chang E., *"Fingerprinted secret sharing steganography for robustness against image cropping attacks"*, INDIN '05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005.

[33] Shirali-Shahreza M.H., *"A New Approach to Persian/Arabic Text Steganography"*, IEEE/ACIS International Conference on Computer and Information Science and 1st IEEE/ACIS International Workshop on Component-Based Software Engineering,Software Architecture and Reuse (ICIS-COMSAR'06), 2006.

[34] Lin E.T., Delp E.J., *" A review of data hiding in digital images"*, PICS, 1999.

[35] Chang C.-C., Lin C.-Y., Wang Y.-Z., *"New image steganographic methods using run-length approach"*, Information Sciences 176(22):3393-3408, 2006.

[36] Hwang R.-J., Shih T.K., Kao C.-H., Chang T.-M., *"Lossy Compression Tolerant Steganography"*, The Human Society and the Internet Internet-Related Socio-Economic Issues, Berlin Heidelberg, 2001.

[37] Xiangwei K., Ziren W., Xingang Y., *"Steganalysis of Palette Images: Attack Optimal Parity Assignment Algorithm"*, 2005 5th International Conference on Information Communications and Signal Processing, 2005.

[38] Fridrich J., Goljan M., Hogea D., *"Steganalysis of JPEG Images: Breaking the F5 Algorithm"*, F.A.P. Petitcolas (Ed.) Information Hiding, Springer Berlin Heidelberg, 2003.

[39] Jung K.-H., Yoo K.-Y., *"Data hiding method using image interpolation"*, Computer Standards & Interfaces 31(2):465-470, 2009.

[40] Li Z., Chen X., Pan X., Zeng., *"Lossless Data Hiding Scheme Based on Adjacent Pixel Difference"*, 2009 International Conference on Computer Engineering and Technology, 2009.

[41] Tsai P., Hu Y.-C., Yeh H.-L., *"Reversible image hiding scheme using predictive coding and histogram shifting"*, Elsevier, Signal Processing, 2009.

[42] Wang R.-Z., Lin C.-F., Lin J.-C., *"Hiding data in images by optimal moderately-significant-bit replacement"*, IET, Electronics Letters, 2000.

[43] Chan C.-K., Cheng L.M., *"Hiding data in images by simple LSB substitution"*, DBLP, Pattern Recognition 37(3):469-474, 2004.

[44] Swain G., Lenka S.K., *"A technique for secret communication using a new block cipher with dynamic steganography"*, International Journal of Security and its Applications 6(2), 2012.

[45] Gutub A., Ankeer M., Abu-Ghalioun M., Shaheen A., Alvi A., *"Pixel indicator high capacity technique for RGB image based Steganography"*, WoSPA2008, 2010.

[46] Arun C., Murugan S., *"Design of image steganography using LSB XOR substitution method"*, 2017 International Conference on Communication and Signal Processing (ICCSP), 2017.

[47] Karim S.M.M., Rahman M.S., Hossain M.I., *"A new approach for LSB based image steganography using secret key"*,14th ICCIT, 2011.

[48] Cihangir S., Canbolat H., *"An Improved Quality and Security of LSB Based Steganography Technique Using XOR Bitwise Operation in 24 Bit Color Image"*, JPSAT, 2020.

CURRICULUM VITAE

Personal Information

Surname, Name	CIHANGIR Serhat
Date of Birth	10/05/1992
Place of Birth	Malatya/TURKEY
Nationality	Turkish(T.C.)
Phone	0262 675 25 43
E-mail	serhatcihangir@gmail.com

Education

2017 - 2020	**M.Sc** Yildirim Beyazit University, Electrical and Electronics Engineering, Ankara/TURKEY (GPA: 3.69 / 4)
2011 - 2016	**B.Sc** Yildirim Beyazit University, Electrical and Electronics Engineering, Ankara/TURKEY (GPA: 3.04 / 4)

Work Experience

Nov 2017 -	Researcher, TUBITAK - BİLGEM Gebze/KOCAELİ
Summer 2015	Intern, TUBITAK - UZAY. Ankara/TURKEY
Summer 2014	Intern, NETWORK COMPANY Ankara/TURKEY