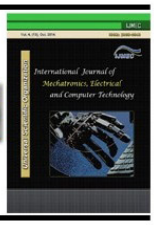
Vol. 8(30), Oct. 2018, PP. 3988-4001

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543



Data Hiding Using Steganography and Cryptography Techniques

WeaamTalaat Ali [1,*] and Abbas Salman Hameed [2]

[1, 2] *College of Engineering, University of Diyala, Diyala, Iraq*

***Corresponding Author's E-mail:** wface2010@yahoo.com*

Abstract

Steganography is the art of communicating a message by embedding it into multimedia data (cover data), where the existence of the embedded message should not be noticeable by unauthorized parties. It conceals the message being communicated in another message or digital media. One of the main problems in steganographic systems is how decide to hide the information while ensuring that the secret information can be correctly retrieved at the detecting stage, even after various image manipulation including attacks.

In this paper, a system which uses Least Significant Bit Steganography (LSB) and ciphering (RSA algorithm and XOR ciphering) for embedding data into image is proposed. This collection between steganography and cryptography is to increase the system security.

The implementation results show that the stego-image is closed related to the cover image, because the correlation is very close to one and Peak Signal to Noise Ratio (PSNR) is good value.The perfect extraction of the secret data satisfied because the Bit Error Rate (BER) equal to zero. Satisfactory results are achieved for the system. The stego-image is visually similar to the original and does not draw any suspension about embedded image. Hence, the steganographic goals are achieved in these systems in the best case.

Keywords: *Rivest-Shamir-Adleman (RSA) Algorithm, correlation Function (COR), Bit Error Rate (BER)), Peak Signal to Noise Ratio (PSNR).*

1. Introduction

The demands of privacy in digital communication is desired when confidential information is being shared between two entities using computer communication. To provide secrecy in communication we use various techniques. One such technique is Steganography [1]. Steganography is the art and science of hiding communication, a steganographic system thus embeds hidden content in unremarkable cover media so as not to arouse an eavesdropper suspicion. And other technique is cryptography. Cryptography protects information by transforming it into an unreadable format. It is useful to achieve confidential transmission over a public network. - Essentially, the information hiding process in a steganographic system starts by identifying a cover medium's redundant bit (those that can be modified without destroying that medium's integrity) [2]. One of the most common steganographic techniques is to embed a text file into an image file. Anyone viewing the image file would see no difference between the original file and the file with the message embedded into it. This is accomplished by storing the message using least significant bits (as one of the steganography techniques) in the data file [3]. The least-significant bits are those that at the far right of a binary

Article History:
Received Date: Jul. 14, 2018
Accepted Date: Sep. 16, 2018
Available Online: Oct. 01, 2018

number. For instance, the decimal number 255 is represented in binary code as 11111111. The least significant bit is the last "1" at the far right of the number. If we change the "1" to a "0" we would get 11111110, which represents 254. The hidden file can be stored using these bits throughout the file. These minor changes cannot be perceived by viewing the image file [4].

2. RSA Algorithm (Rivest-Shamir-Adleman)

The RSA Algorithm is the most popular asymmetric key cryptographic algorithm. The RSA Algorithm is based on the mathematical functions that are easy to find and multiply the large numbers together, but it is extremely difficult to factor their product [5]. The public and private keys in RSA are based on very large numbers. The public key can be shared with everyone, whereas the private key must be kept secret. In RSA cryptography, both the public and the private keys can encrypt a message; the opposite key from the one used to encrypt a message is used to decrypt it. This feature is one reason why RSA has become the most widely used asymmetric algorithm: It provides a method of assuring the confidentiality, integrity, authenticity and non-reputability of electronic communications and data storage. It is also used in software programs browsers are an obvious example, which need to establish a secure connection over an insecure network like the Internet or validate a digital signature. RSA signature verification is one of the most commonly performed operations in IT [6].

3. The General Model of the Proposed System

The general model of the proposed system consists of two parts: sender part and recipient part. In the ***sender part*** many stages are proposed in the sending process to achieve in velvet in the information hiding goal. Fig. (1) shows the general stages

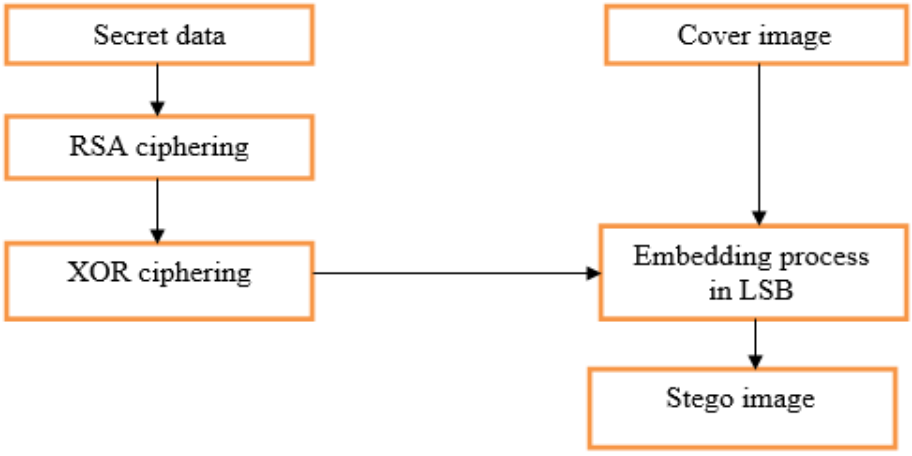
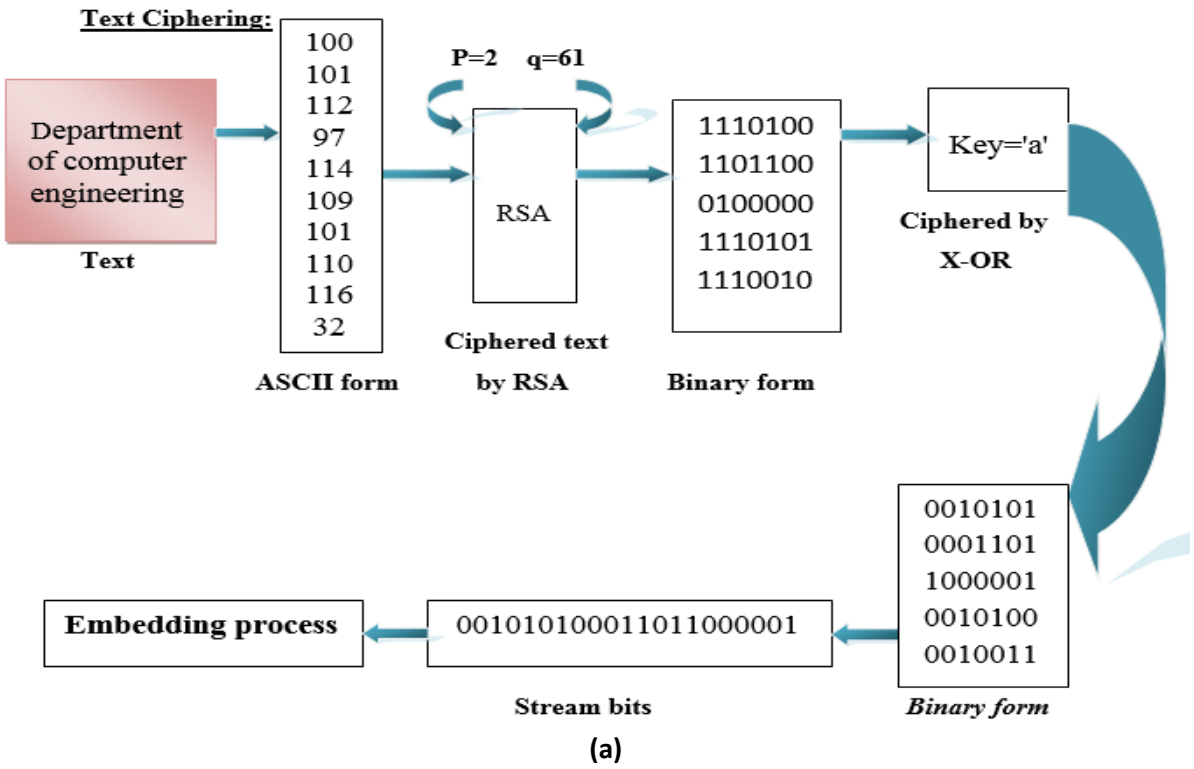


Figure (1): sender part of proposed system

Data Ciphering: Data preprocessing or data ciphering is proposed to increase the security (which mean increase robustness) of the overall steganographic system. The RSA algorithm is used as first cipher steps. A second step achieves by applying an XOR operator to data with secret code. The whole ciphering process of data (text or image) can be briefly described as Figure (2).



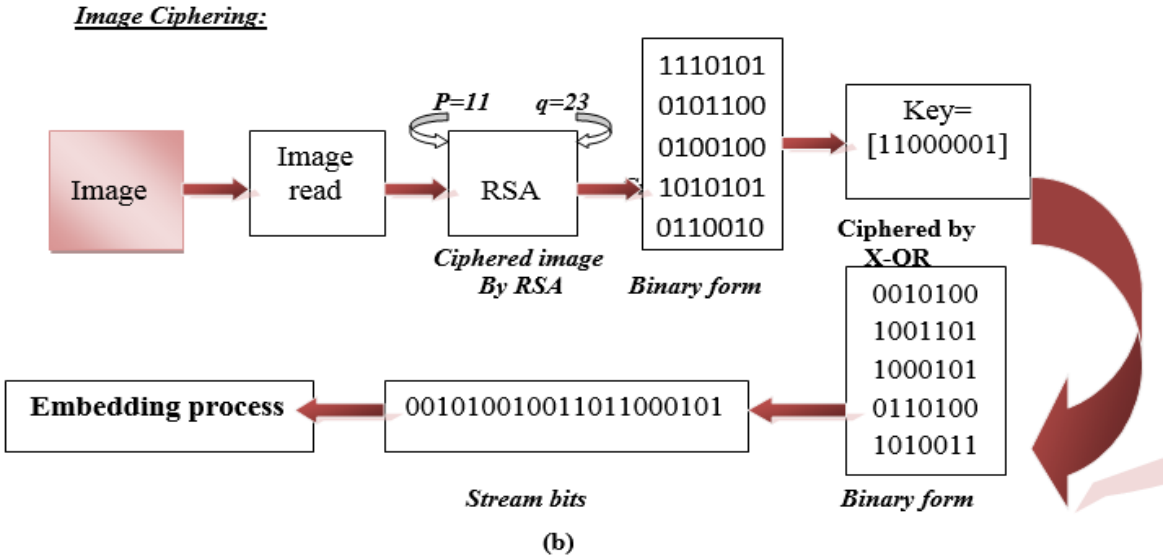


Figure (2): preparing the data for embedding process
(a)Text ciphering (b)Image ciphering

The embedding process has been achieved by embedding the ciphered data bits into the LSB's pixels of the cover image. For 1LSB hiding algorithm, each ciphered data bit is embedded in one pixel of the cover image. For 2LSB hiding algorithm, each two ciphered data bits are embedded in one pixel of the cover image, and so on. This process is repeated until all the bits of ciphered data are completely embedded in the pixel cover image. While in *Recipient Part*, the recipient will certainly get the stego-image, but he could not extract the secret information out of the cover without the knowledge of algorithm of the embedding process. The block diagram of this part is shown in Fig. (3).

At the extracting process, the pixels of stego-image are rearranged in a manner similar to that in the sender. The secret bits will be extracted by using the same algorithm used in the sender and the deciphering process will be done to get the secret data.

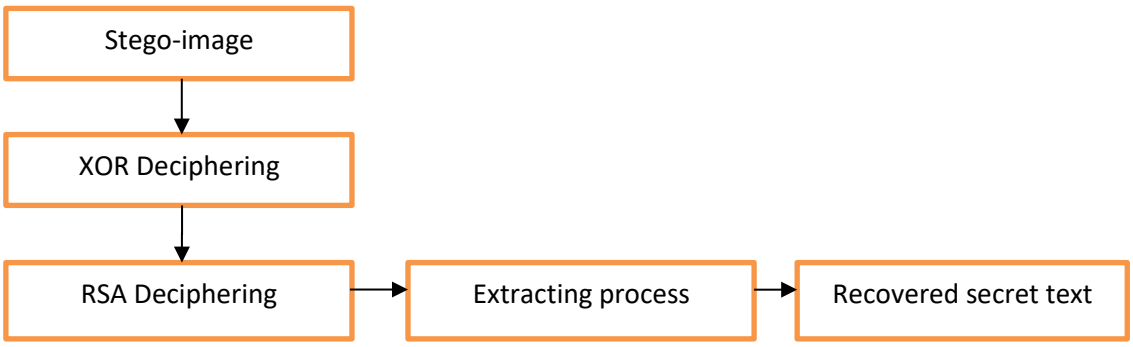


Figure (3): The extraction process.

3.1. The Similarity Test

Similarity test is the correlation between the cover-image and stego image. When the stego-image is perceptually similar to the original cover-image, then the correlation equals one. The correlation can be calculated as shown below [7]:

$$cor = \frac{\sum_{r=1}^{M}\sum_{c=1}^{N}(C(r,c)-\bar{C})(S(r,c)-\bar{S})}{\sqrt{[\sum_{r=1}^{M}\sum_{c=1}^{N}(C(r,c)-\bar{C})^2][\sum_{r=1}^{M}\sum_{c=1}^{N}(S(r,c)-\bar{S})^2]}}$$

Where:

r: row number

c: column number

M: height of cover image(or stego-image)

N: width of cover image(or stego-image)

C(r,c) : cover-image

S(r,c) : stego-image

C : mean of cover image

S : mean of stego-image

$\bar{C}$:The mean of C(r,c),that:

$$\bar{C} = \frac{1}{M \times N}\sum_{r=1}^{M}\sum_{c=1}^{N} C(r,c)$$

$\bar{S}$:The mean of S(r,c),that:

$$\bar{S} = \frac{1}{M \times N}\sum_{r=1}^{M}\sum_{c=1}^{N} S(r,c)$$

3.2. Peak signal to Noise Ratio (PSNR) Test.

According to the human visual system, some amount of distortion between the original image and the modified one is allowed [8], an expression for the ratio between the maximum possible value (power) of a signal and the power of distortion noise that affects the quality of its representation. Because many signals have a very wide dynamic range, (ratio between the largest and smallest possible values of a changeable quantity) the PSNR is usually expressed in terms of the logarithmic decibel scale,To compute the peak signal to noise ratio, one starts by defining the error (between the stego-image and the cover-image) [7,8].

$$\boldsymbol{e} = \sum_{\boldsymbol{r=1}}^{\boldsymbol{M}} \sum_{\boldsymbol{c=1}}^{\boldsymbol{N}} [\boldsymbol{S}(\boldsymbol{r},\boldsymbol{c}) - \boldsymbol{C}(\boldsymbol{r},\boldsymbol{c})]$$

Then the noise power (N) is defined as;

$$N = \sum_{r=1}^{M} \sum_{c=1}^{N} [\boldsymbol{S}(\boldsymbol{r},\boldsymbol{c}) - \boldsymbol{C}(\boldsymbol{r},\boldsymbol{c})]^2$$

Signal power (S) is given by:

$$S = \sum_{r=1}^{M} \sum_{c=1}^{N} [\boldsymbol{S}(\boldsymbol{r},\boldsymbol{c})]^2$$

and PSNR requires finding maximum signal power $\boldsymbol{S_{max}}$,

$$\boldsymbol{S_{max}} = \boldsymbol{M} \times \boldsymbol{N} \times (\boldsymbol{L} - \boldsymbol{1})^{\boldsymbol{2}}$$

where:

L: is the number of gray scales in the stego-image (it is the same as the number of gray scales in the cover-image), in the present case L=256 and the gray scale extends from 0-255.

L – 1: max. gray level.

Then;

$$\boldsymbol{PSNR} = \boldsymbol{10log_{10}} \frac{\boldsymbol{M}\times\boldsymbol{N}\times(\boldsymbol{L}-\boldsymbol{1})^{\boldsymbol{2}}}{\sum\sum[\boldsymbol{S}(\boldsymbol{r},\boldsymbol{c})-\boldsymbol{C}(\boldsymbol{r},\boldsymbol{c})]^{\boldsymbol{2}}}$$

3.3. Bit Error Rate (BER)

The Bit Error Rate Calculation compares input data from a transmitter with recovered data from a receiver. So, A bit error rate (BER) is defined as the ratio of the number of errors to the total number of bits sent [9]:

$$BER = \frac{Error\_bits}{Total\_Secret\_bits}$$

The BER is of great significance to system design, since it is strongly related to practical system requirements such as robustness.

4. Simulation and Results

In this section, we evaluate the proposed system from different points of view using various common images. For evaluating results images of size (1024X768) pixels are used with different secret bits size.

we recovered the data with a different size on the stego image in 1st,2nd ,3rd, and 4th LSB of the cover image hence the secret message can be retrieved without loss at the receiver

4. 1. Embedded text in gray Cover image

In figure (4) illustrates the secret text has a size 86KB to be embedded in gray cover image.

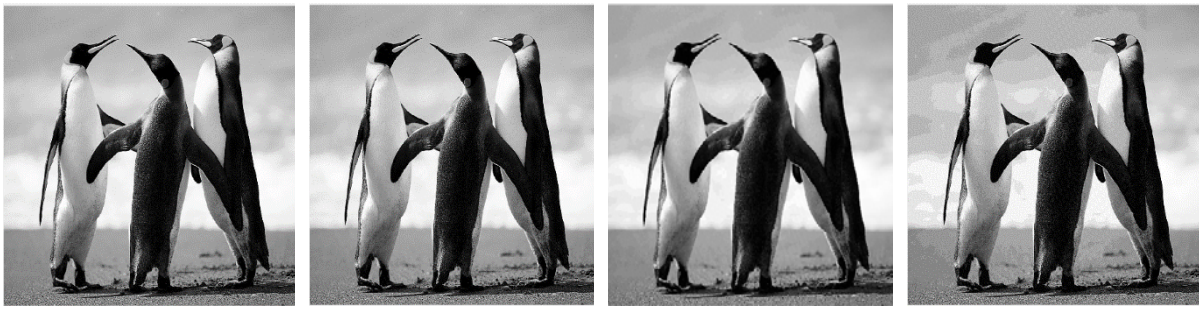
A

Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering

b

Figure (4) a: Penguins (Gray cover image)
b: text:(86KB)

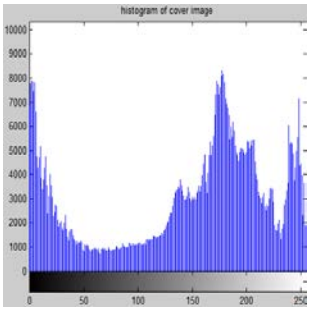
After encrypting text that want to be embedded by using RSA algorithm and XOR ciphering, the figure (5) represents the embedded text in 1LSB, 2LSB , 3LSB and 4LSB, Where we note there is no change in the cover image for the human eye for levels 1LSB , 2LSB, 3LSB and there is very little change in the level 4LSB.



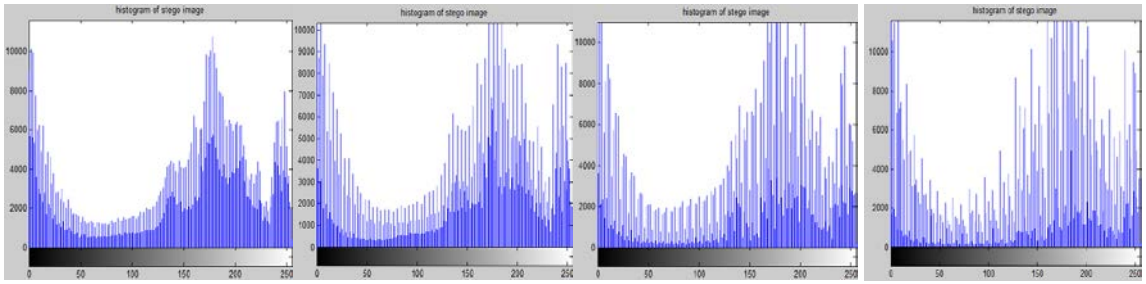
1LSB 2LSB 3LSB 4LSB

Figure (5): Results of embedding text into Penguins (Gray cover image).

In figure (6) illustrates histogram for cover image and stego-image for levels 1LSB, 2LSB, 3LSB and 4LSB after comparing histogram of cover image with the stego image it is quite clear that histogram of stego image is almost similar to cover image, as there is change of only last bit of pixels.so, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye and can't be detect by histogram analysis method



Cover image



1LSB 2LSB 3LSB 4LSB

Figure (6): Results of histogram after embedding text into Penguins (gray image).

Table (1): Show results after embedding text in gray cover image

Gray scale Image	1LSB (86KB)	2LSB (173KB)	3LSB (259KB)	4LSB (346KB)
PSNR	**52.1742**	**45.1719**	**38.9474**	**32.6396**
Cor.	**0.9999**	**1.0001**	**0.9988**	**0.9918**
Cover-BER	**0.0493**	**0.0986**	**0.1478**	**0.1966**
Data-BER True key	**0**	**0**	**0**	**0**
Data-BER False key	**0.3428**	**0.3429**	**0.3429**	**0.3429**

In the table (1) illustrates embedded the ciphertext (86KB) in first LSB of cover image using(Least significant bit) techniques ,then we embedded the ciphertext (173KB) in second LSB of cover image, embedded the ciphertext (259KB) in third LSB of cover image, embedded the ciphertext (346KB) in fourth LSB of cover image, compare the resulting stego-image with the original image we found The value of PSNR and Cor decreases gradually when we insert more bits in cover image ,this shows the efficiency of steganography and properly sample standard rate of change. The value of BER for cover image increases when the embedded bits increases, and the value of BER for stego-image zero because all steganography bits extraction from the cover image without any loss or distortion, but if there is a defect in the key, extraction data will have some error ratio and does not represent the same data that are embedded at the first.

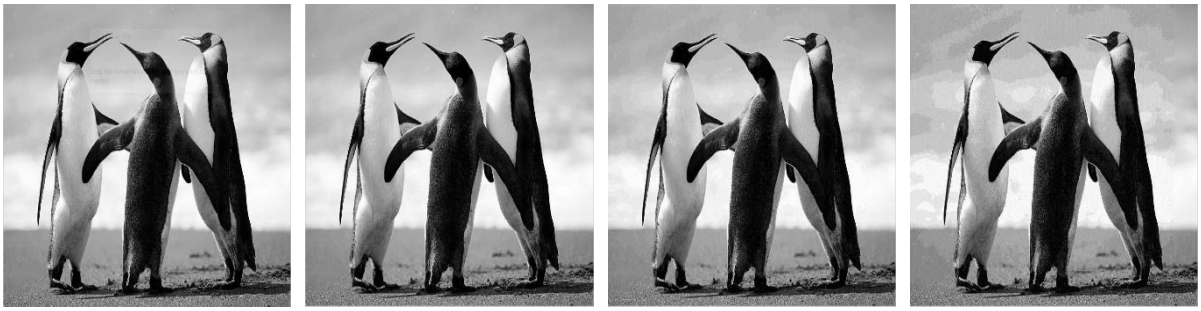
4.2. Embedded gray image in gray cover image

In figure (7) illustrates the gray secret image to be embedded in gray cover image.

a b

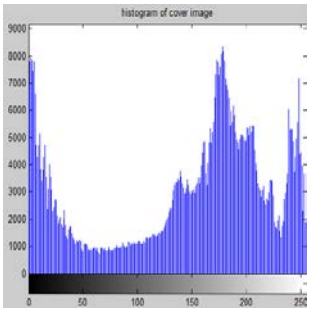
Figure (7) a :- Penguins (Gray cover image)
b :- Tulips (Gray secret image)

After encrypting data of secret image that want to be embedded by using RSA algorithm and XOR ciphering, the figure (8) represents the embedded data in 1LSB, 2LSB, 3LSB and 4LSB, where we note there is no change in the cover image for the human eye for levels 1LSB, 2LSB, 3LSB and there is very little change in the level 4LSB.

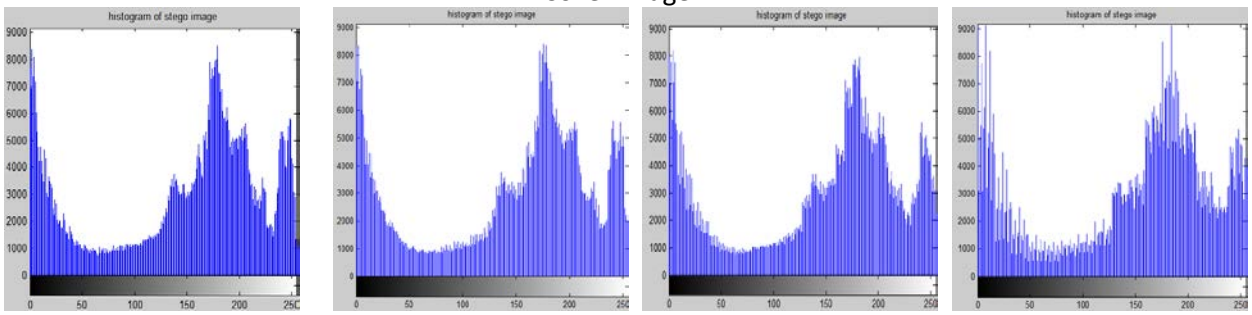


1LSB 2LSB 3LSB 4LSB

Figure (8): Results of embedding Tulips (gray image) into Penguins (gray cover image).



Cover image



1LSB 2LSB 3LSB 4LSB

Figure (9): Results of histogram after embedding Tulips (gray image) into Penguins (gray cover image).

In figure (9) illustrates histogram for cover image and stego-image for levels 1LSB, 2LSB, 3LSB and 4LSB after comparing histogram of cover image with the stego image it is quite clear that histogram of stego image is almost similar to cover image, as there is change of only last bit of pixels. so, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye and can't be detect by histogram analysis method.

Table (2): Show results after embedding gray image in gray cover image

Gray scale image	1LSB (300*300)	2LSB (420*420)	3LSB (515*515)	4LSB (600*600)
PSNR	**51.5277**	**44.6258**	**38.3839**	**32.2100**
Cor	**0.9999**	**1.0001**	**0.9988**	**0.9921**
Cover_BER	**0.0572**	**0.1121**	**0.1686**	**0.2280**
Data_BER True key	**0**	**0**	**0**	**0**
Data_BER False key	**0.1250**	**0.1250**	**0.1250**	**0.1250**

In the table (2) illustrates embedded the data of secret image (300*300) in first LSB of cover image using(Least significant bit) techniques ,then we embedded the data of secret image (420*420) in second LSB of cover image, embedded the data of secret image (515*515) in third LSB of cover image, embedded the data of secret image (600*600) in fourth LSB of cover image, Compare the resulting stego-image with the original image we found The value of PSNR and Cor decreases gradually when we insert more bits in cover image ,this shows the efficiency of steganography and properly sample standard rate of change .

The value of BER for cover image increases when the embedded bits increases, and the value of BER for stego-image zero because all steganography bits extraction from the cover image without any loss or distortion, but if there is a defect in the key, extraction data will have some error ratio and does not represent the same data that are embedded at the first.

4.3. Embedded text in color cover image

In figure (10) illustrates the secret has a size 86KB text to be embedded in color cover image.

a

Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering
Department of computer engineering

b

Figure (10) a: Penguins (Color cover image)
b:text:(86KB)

After encrypting text that want to be embedded by using RSA algorithm and XOR ciphering, the figure (11) represents the embedded text in 1LSB, 2LSB, 3LSB and 4LSB, where we note there is no change in the cover image for the human eye for levels 1LSB, 2LSB, 3LSB and there is very little change in the level 4LSB.

1LSB 2LSB 3LSB 4LSB

Figure (11): Results of embedding text into Penguins (color cover image).

In figure (12) illustrates histogram for cover image and stego-image for levels 1LSB, 2LSB, 3LSB and 4LSB after comparing histogram of cover image with the stego image it is quite clear that histogram of stego image is almost similar to cover image, as there is change of only last bit of pixels. so, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye and can't be detect by histogram analysis method

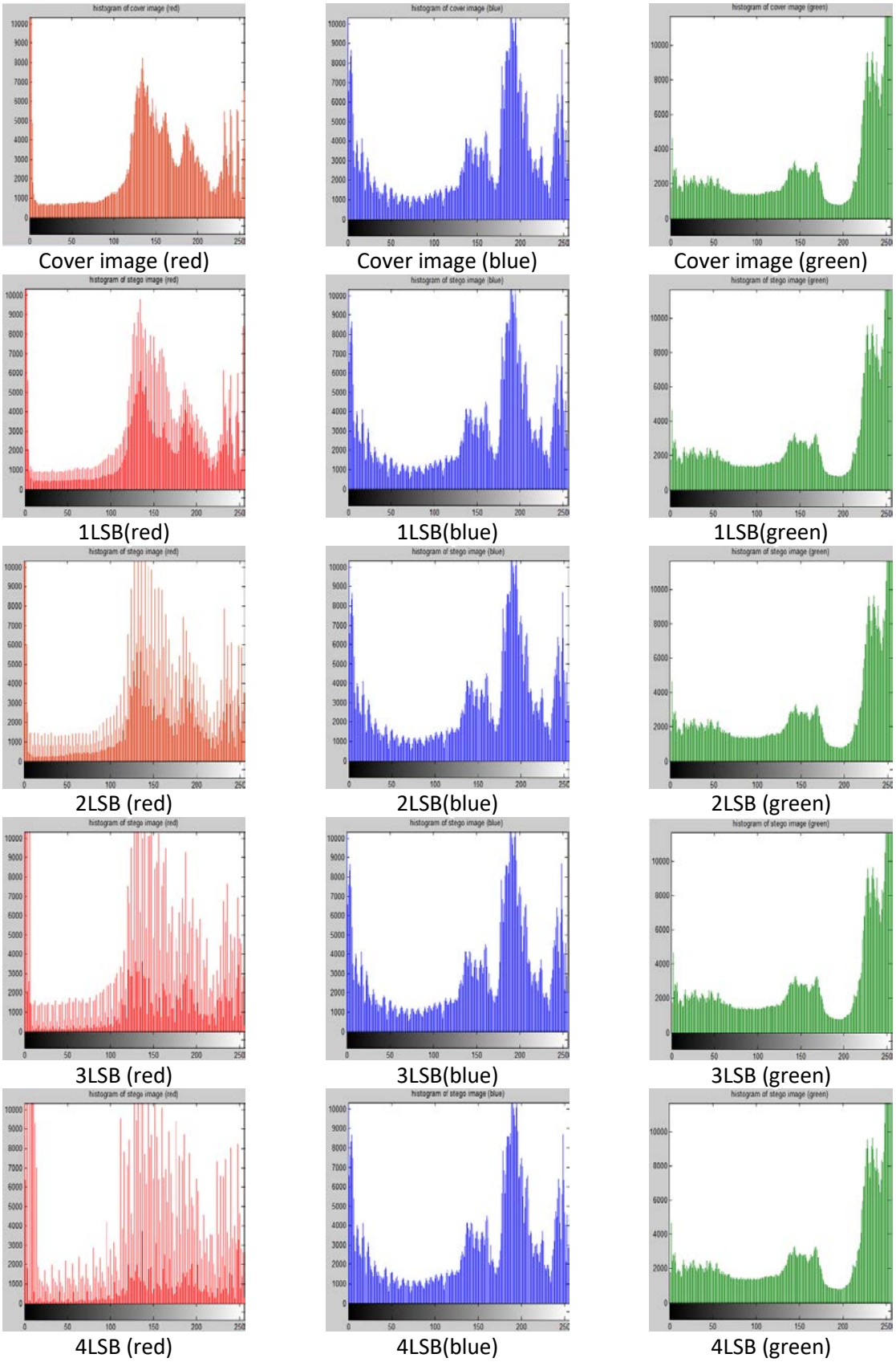


Figure (12): Results of histogram after embedding text in Penguins (color image).

Table (3): Show results after embedding text in color image

Color scale image	1LSB (86 KB)	2LSB (173 KB)	3LSB (259 KB)	4LSB (346 KB)
PSNR	**56.9353**	**49.8062**	**43.9691**	**37.6175**
Cor	**1.0000**	**0.9999**	**0.9994**	**0.9994**
Cover_BER	**0.0165**	**0.0331**	**0.0482**	**0.1924**
Data_BER True key	**0**	**0**	**0**	**0**
Data_BER False key	**0.3428**	**0.3429**	**0.3429**	**0.3429**

In the table (3) illustrates embedded the ciphertext (86KB) in first LSB of cover image using(Least significant bit) techniques ,then we embedded the ciphertext (173KB) in second LSB of cover image, embedded the ciphertext (259KB) in third LSB of cover image, embedded the ciphertext (346KB) in fourth LSB of cover image, Compare the resulting stego-image with the original image we found The value of PSNR and Cor decreases gradually when we insert more bits in cover image ,this shows the efficiency of steganography and properly sample standard rate of change .

The value of BER for cover image increases when the embedded bits increases, and the value of BER for stego-image zero because all steganography bits extraction from the cover image without any loss or distortion, but if there is a defect in the key, extraction data will have some error ratio and does not represent the same data that are embedded at the first.

4 4. Embedded color image in color cover image

In figure (13) illustrates the secret color image to be embedded in cover color image.

a

b

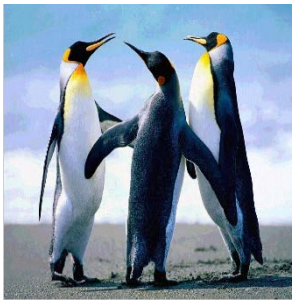
Figure (13) a: Penguins (Color cover image)
b: Tulips (Color secret image)

After encrypting data of secret image that want to be embedded by using RSA algorithm and XOR ciphering, the figure (14) represents the embedded data in 1LSB, Where we note there is no change in the cover image for the human eye for levels 1LSB , 2LSB, 3LSB and there is very little change in the level 4LSB.

1LSB

2LSB

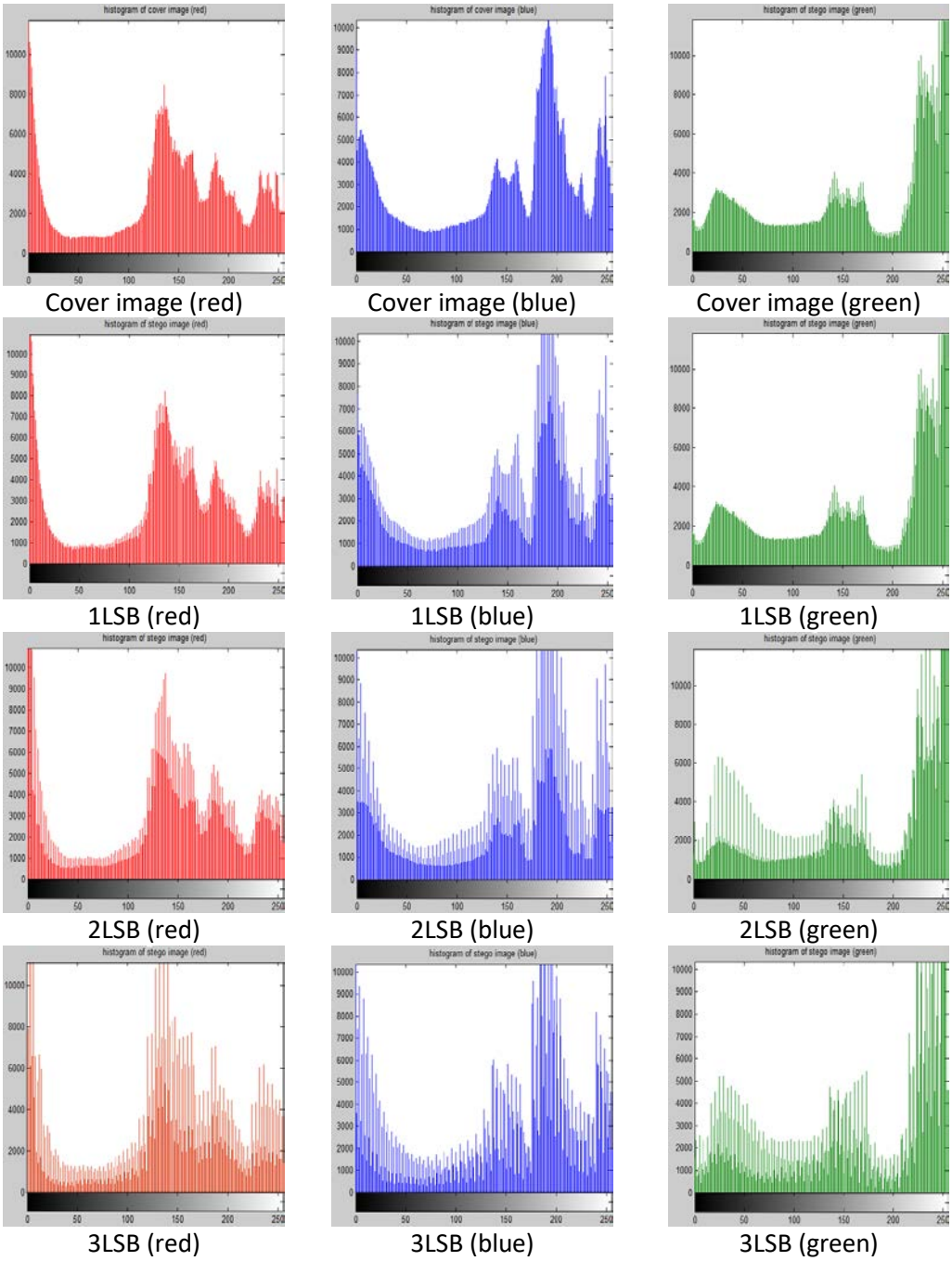
3LSB

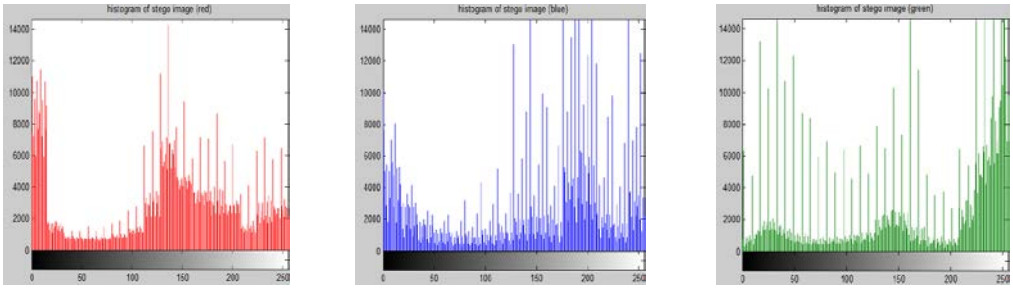


4LSB

Figure (14): Results of embedding Tulips (color image) in Penguins (color image).

In figure (15) illustrates histogram for cover image and stego-image for levels 1LSB, 2LSB , 3LSB and 4LSB after comparing histogram of cover image with the stego image it is quite clear that histogram of stego image is almost similar to cover image, as there is change of only last bit of pixels. so, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye and can't be detect by histogram analysis method





4LSB (red) 4LSB (blue) 4LSB (green)

Figure (15): Results of histogram after embedding Tulips (color image) into Penguins (color image).

Table (4): Show results after embedding color image into color image

Color scale image	1LSB (300*300*3)	2LSB (420*420*3)	3LSB (515*515*3)	4LSB (600*600*3)
PSNR	**51.5120**	**44.4454**	**38.1459**	**31.8326**
Cor	**0.9999**	**0.9999**	**0.9996**	**0.9975**
Cover_BER	**0.0574**	**0.1125**	**0.1693**	**0.2287**
Data_BER True key	**0**	**0**	**0**	**0**
Data_BER False key	**1250**	**1250**	**1250**	**1250**

In the table (4) illustrates embedded the data of secret image (300*300*3) in first LSB of cover image using(Least significant bit) techniques ,then we embedded the data of secret image (420*420*3) in second LSB of cover image, embedded the data of secret image (515*515*3) in third LSB of cover image, embedded the data of secret image (600*600*3) in fourth LSB of cover image, Compare the resulting stego-image with the original image we found The value of PSNR and Cor decreases gradually when we insert more bits in cover image ,this shows the efficiency of steganography and properly sample standard rate of change .

The value of BER for cover image increases when the embedded bits increases, and the value of BER for stego-image zero because all steganography bits extraction from the cover image without any loss or distortion, but if there is a defect in the key, extraction data will have some error ratio and does not represent the same data that are embedded at the first.

Conclusion

After studying the proposed stego-system, one can conclude the following:

1. Human vision scale (Avoid visual attack): Steganography message can be embedded into digital images in ways that are imperceptible to the human eye. In other words, a stego-image which is generated by the present algorithm has to be normal for human vision and cannot be detected.
2. Encryption data sent by using (RSA algorithm & XOR operator) gives more security for storage data.
3. Extracting all secret data that are embedded in cover image and this is evident from the results of BER.
4. Whenever increased amount of data stored, the level of LSB Increase, the result of PSNR and Cor decreased gradually and this mean cover image quality decrease (small increasing in distortion).
5. After comparing histogram of cover image with the stego image it is quite clear that histogram of stego image is almost similar to cover image, as there is change of only last bit of pixels. so, this method is capable of producing a secret-embedded image that is totally indistinguishable from the original image by the human eye and can't be detect by histogram analysis method

References

[1] Muhalim Mohamed Amin. Subariah Ibrahim. Mazleena Salleh. Mohd Rozi Katmin,"Information Hiding Using Steganography", 2003.

[2] Provos,N.and Honeyman,p. " Hide and seek : An introduction to steganography " . IEEE SECURITY & PRIVACY,2003.

[3] S. Adee, “Spy vs. spy," IEEE Spectrum magazine, August 2008.

[4] N.F. Johnson and S. Jajodia, "Exploring Steganography: Seeing the Unseen", IEEE, pp. 26-34, 1998.

[5] S.Asha Latha, A.Sivabalan “Improved Mask Protected DES using RSA Algorithm” MATEC Web of Conferences,2016.

[6] Bhaskar, Ganapathi Hegde, P.R.Vaya,“Anefficient hardware model for RSA Encryption system using Vedic mathematics”, International Conference on Communication Technology and SystemDesign2011

[7] L. W. Abdul-Allah, "Two-Dimensional Image Encryption", M.Sc. thesis, University of Technology, Electrical and Electronic Engineering Dept.2002.

[8] W. Chen and C. Chen, Multi "Resolution Structure Color Image Compression Using DWT and VQ", Dept. of Electrical Engineering, National Cheng Kung University Tainan, 70101, Taiwan, R.O.C.

[9] Suby Maria Sojan, Chinchu S Ragamalika” BIT Error Rate Tester for Wireless Communication Systems”, International journal of Science Technology & Engineering | Volume 2 | Issue 10 | April 2016.