New Approaches to Encrypt and Decrypt Data in Image using Cryptography and Steganography Algorithm

Ako Muhammad Abdullah
MSc. Computer Science
Faculty of Physical & Basic Education
Computer Science Department
University of Sulaimani
Kurdistan Region-Iraq

Roza Hikmat Hama Aziz
MSc. Computer Science
Faculty of Physical & Basic Education
Computer Science Department
University of Sulaimani
Kurdistan Region-Iraq

ABSTRACT
Nowadays, network has important roles for transferring data accurately and fast from source to a destination. The data is not secure enough to transfer highly confidential. The security of information has become one of the principle challenges of resource sharing with data communication over computer network. Cryptography and Steganography are two methods for protecting data from intruders while transferring over an open channel network. Cryptography is a method to encrypt data and steganography is the art and science of hiding secret message in a cover image. In this paper a Hash Least Significant Bit (H-LSB) with Affine cipher algorithm has been proposed for providing more security to data in a network environment. First we encrypt the data with the new cryptography algorithm and then embed in the image. Eight bits of the secret message are divided into 3, 3, 2 and embedding into the RGB pixels values of the cover image respectively. A hash function is used to select the particular position of insertion in LSB bits. This system allows a message sender to select keys to encrypt the secret message before embedding into the image and a receiver is used the keys to decrypt the message. Receiver can be decrypted the encrypt message with incorrect the keys but to a different form from the original message. This system has the ability to provide better security while transferring the secret message from one end to the other end in network environment.

Keywords
Cryptography, steganography, secret message, Hash based LSB, Affine Cipher, encryption, decryption and embedding process.

1. INTRODUCTION
With the growth different types of network digital images are being exchanged over the networks. The basic need of every growing area today's world is communication. Everyone wants to protect the information of work to be secret and safe. The rise of the internet, the most important factors of information technology and communication has been the security of information [1]. In our day life we have used many insecure pathways for sharing and transferring information using telephonically or internet. However at a certain level it's not safe. Cryptography and steganography are two methods that use information in order to cipher or cover their existence respectively which could be used to share and transfer information in a concealed manner. Cryptography is a technique includes modification of a message for security the secrecy communication [2]. Nowadays, to encrypt and decrypt data in order to protect the message secret many different methods have been developed.

In cryptography it's always clear to intermediate person that the message is encrypted form by an encryption key which is known by sender and receiver only and without using encryption key the message could not be accessed. However, these methods are not enough to protect the contents of a message secret due to another technique is used with cryptography that is called steganography [3]. Steganography is the art and science of invisible communication of message and the secret message is made to hide in cover image and person cannot be seen any message hidden in the image [4]. The cover image containing the secret data is then transferred to the recipient. The receiver is able to extract the message with the retrieving process and secret key provided by the sender.

This paper proposes a new system to embed a secret message in a cover image using Hash based (3, 3, 2) LSB insertion method with Affine cipher algorithm. Our system is designed to encrypt data and hide all the data in patted within the message to keep the privacy of the data. Then, the system has been developed based on the cryptography and steganography algorithm.

The rest of the paper is organized as follows: reviews the related work is discussed in section 2. Section 3 descripting the Cryptography and Steganography. Describe proposed system architecture in section 4. Experimental results and discussion is explained in section 5. Section 6 presents conclusions the reserch.

2. RELATED WORK
Steganography is a method of hiding secret message in a cover image while communication takes place between sender and receiver. Nowadays, communication is one of the most important ways in our daily life for transferring and sharing information by using telephonically or internet. To maintain the information from intruder many in secure path ways have been carried out on the information. Steganography and Cryptography are two methods which could be used to keep the information.

Younes et al. [8] proposed a simple method to hide information in the encrypted image then send the encrypted image to the receiver over the network. This technique that have used by authors can prevent the unauthorized to access the information inside the image. On the other hand, El-Emam [9] to hide a large amount of data with high security, he proposed a steganography algorithm. In this research, the image has been segmented and filtered where bits replacement is used on the appropriate pixels. These pixels have selected randomly rather than sequentially. Author a bitmap (bmp) image has been used to hide the data. Kumar et al. [10] proposed a method in which a message hidden inside an

image by using Hash-LSB with RSA algorithm for providing more security to data inside an image. In this paper, hash function have used to generate a pattern for hiding data bits into LSB of RGB pixel values of the cover image.

Ibrahim et al. [11] proposed a method to hide data inside image by using steganography technique. In this method binary codes and pixels inside an image proposed. The zipped file is used before it is converted to binary codes to maximize the storage of data inside the image. The paper [12], [13], [14], and [15] provides an overview of image steganography, its analysis and uses of various steganography methods to embed data inside an image. Dasgupta et al. [16] proposed a technique for video steganography by using a hash based least significant bit. The authors hash function is used to select the position of insertion in LSB bits where the secret data is embedded in the LSB of the cover frames. Roza [17] proposed a new method to improve courier service online system by using Cryptography and Steganography techniques. The author used these techniques to encrypt detail information about the items, ATM card, collection and destination address. In addition, the administrator on the system can decrypt easily the detail information. In this paper LSB method used to embed data inside image. Yuan et al. [18] proposed a new stenographic technique for data hiding in Microsoft Word documents by a change tracking technique.

3. BACKGROUND

3.1 Cryptography

Cryptography is a mechanism to encode and decode secret messages for protecting message from unauthorized users to access the messages. In a network environment cryptography is playing a main role in data protection in applications running. In Greek, cryptography means "hidden Secret". Moreover, in the past cryptography was used by the political sectors of intelligence and military but presently it is commonly utilized in the ATM cards, e-commerce, e-mail, computer password, and other application. Over the years there are different algorithm have available to modify of a message by an encrypting key which is known by sender and receiver [19]. The message could not be decrypted without using encrypting key. One of the issue is appeared with cryptography is that the message always clear to intermediate person that the message is encrypted form. This means that the sender of the message does not want it to be read by unauthorized person. Today, there are many cryptography techniques which are capable of encrypting data, one of the most widely technique is Affine algorithm. Affine has the ability to convert the information to a form not understandable by the intruder.

3.2 Steganography

Nowadays, various types of networks are used to exchange digital image among users. With the growth of types of computer network a large amount of digital data has been exchanged over the network due to many of data must be confidential, private or both. To protect this data from intruder, the demand for stronger encryption techniques are increased [5]. Steganography is one of the most important techniques are used to embed the secret message within an image [6]. This technique is the perfect supplement for encryption that permits a user to hide information inside an image. As mention at the previous section in cryptography, the problem with cryptography is that the encrypted message is obvious and everyone known that the messages are encrypted. To solve this problem, steganography techniques can be able to provide more additional protection on a secret message with cryptography so that the information is doubly protected [7]. Steganography hiding information within an image so it appears that no information is hiding inside an image. Thus, users can be transmitted the sensitive information over unsecured channel such as the internet. There are various methods of steganography are used. In this paper we have used Least Significant Bit (LSB) method to embed the secret message within an image.

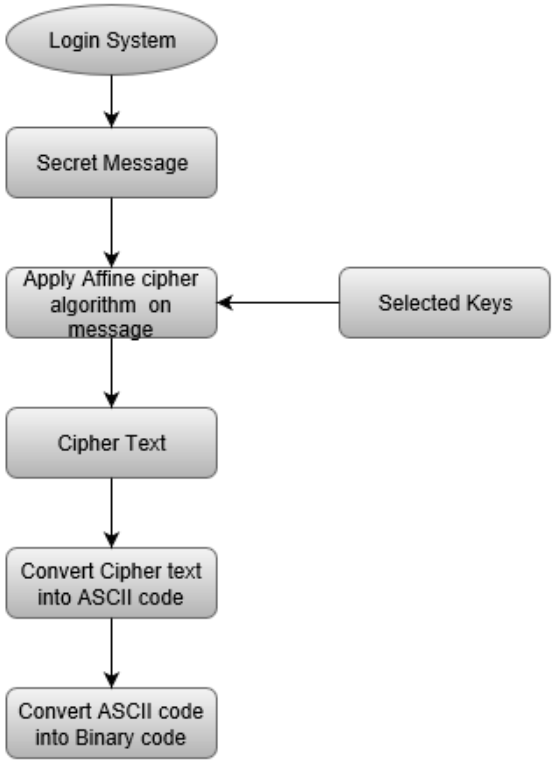
4. PROPOSED SYSTEM ARCHITECTURE

In this paper, we have proposed new security techniques through using cryptography and steganography for providing better security to maintain the privacy, accuracy and confidentiality of the data while transferring from one end to the other end over the network. The main objective of the system is to hide the message or a secret message into an image before transmitting to the destination node on the network without any modification of the data inside an image. The proposed techniques data steganography using Hash based Least Significant Bit (H-LSB) is used to hide secret message in image file (bmp).

The system was run and compiled on windows 10 and tested on University of Sulaimani, Faculty of Physical & Basic Education-Computer Science Department. This system can be used by users without knowledge of programming in C# because the Graphic User Interface (GUI) is designed to be user friendly. This proposed system to input image provides an image platform and different text box to insert data and showing the encrypt data before embedding the image. We have used three phases to apply new proposed techniques:

4.1 Encryption Phase

At the first step to access into the system for hiding the data, the users are needed a user name and password. After login the system, user can write the message to encrypt the data with the secret keys before embedding the data into an image as demonstrate in figure 1. In our system the proposed scheme uses Affine algorithm to encrypt secret information. Affine cipher is one of the algorithms that have used to encrypt data. In this process wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a mathematical function, and converted back to a letter. The formula used means that each letter encrypts to one other letter, and back again, meaning the cipher is essentially a standard substitution cipher with a rule governing which letter goes to which. This technique provides better security to protect the data user from the unauthorized access over a network due to which will not be easy to retrieve the data without the recipient key. After converting the plain text into cipher text by using Affine algorithm we have taken cipher text and converting each letter into ASCII codes then the ASCII codes have converted into a series of binary codes to provide higher security. This proposed technique is used to prevent the intruders to get the real data when they try to retrieve the data. This encrypt data will be embedded inside the image with almost zero distortion of the original image.



Figur 1: A flow chart illustrating the encryption phase

Encryption Process
Step One: Choose the secret message

Step Two: Encrypt the message using Affine Cipher Algorithm

Step Three: Convert the encrypt message into ASCII code

Step Four: Convert ASCII code into binary

For Example:

Input Text: Kurdistan

Encrypt Text: Kofmeilgt

In this process, the alphabet is going to be the letters A through Z.

In this encrypting example, the plaintext to be encrypted is "Kurdistan". For the numeric values of each letter the following function have been used to encrypt each letter:

$$E(x) = (ax + b) \bmod m$$

Where:

x: is the numerical value of the letter in the plaintext.

m: is the number of letters in the plaintext alphabet.

a and **b** are the secret numbers between sender and receiver.

E(x): is the result of transformation.

Table 1 Detect X value

Plaintext	K	u	r	d	i	s	t	a	n
X	10	20	17	3	8	18	19	0	13

Now, take each value of x, and solve the first part of the equation, (3x + 6). After finding the value of (3x + 6) for each character, take the remainder when dividing the result of (3x + 6) by 26. The following table shows the first four steps of the encrypting process:

Table 2 Convert Plain Text into Cipher Text

Plaintext	K	u	r	d	i	s	t	a	n
X	10	20	17	3	8	18	19	0	13
(3x + 6)	36	66	57	12	30	60	63	6	45
(3x+6)mode 26	10	14	5	12	4	8	11	6	19
Cipher Text	K	o	f	m	e	i	l	g	t

Convert Encrypt Text into ASCII Code: 75 111 119 109 101 105 108 103 116

ASCII Code to Binary Conversion: 01001011 01101111 01110111 01101101 01100101 01101001 01101100 01100111 01110100

4.2 Embedding Phase

After encrypting the secret message we have proposed a method to embedding a encrypt message into the image. This process is done by using Hash based Least Significant Bit (H-LSB) which replaces the least significant bit. LSB is the most popular steganography method to embedding data in an image file. This method has applied to hide the encrypt message in the image and then send the image to the intended receiver. In this paper cryptography and steganography methods have been proposed to provide better security to protect data from intruders by using multi-layer of security techniques. The combination of these two methods will enhance the security of data embedding due to some important data that users want to secure from others when data transmission over an open channel. At the start of this process we take encrypt message to be embedded in the cover image, which will be difficult for any intruder to decrypt it without the recipient private key then hash function has used to select the positions and the proposed technique takes eight bits of secret data at a time will be embedded in LSB of RGB (Red, Green and Blue) pixel value in the order of 3, 3, 2 respectively. According to the techniques that we have used to embed the secret data into the image three bits are embedded in Red pixel LSB, three bits are embedded in Green pixels and 2 bits are embedded in blue pixels LSB. These eight bits are inserted in this order because the chromatic influence of blue color to the human eye is more than red and green colors**.** Therefore the distribution pattern chooses the 2 bits to be hidden in blue pixel. Thus, the quality of the image will be not sacrificed. This process is continued till entire message of bits will got embedded into the cover image. To detect the positions to hide data in LSB of each RGB pixels of the cover image the following formula is used:

$$K = p \,\%\, n \quad \ldots\ldots\ldots (1)$$

Where, K is the LSB bit position within the pixel, P represents the position of each hidden image pixels and n is number of bits of LSB which is 4 for the present case.

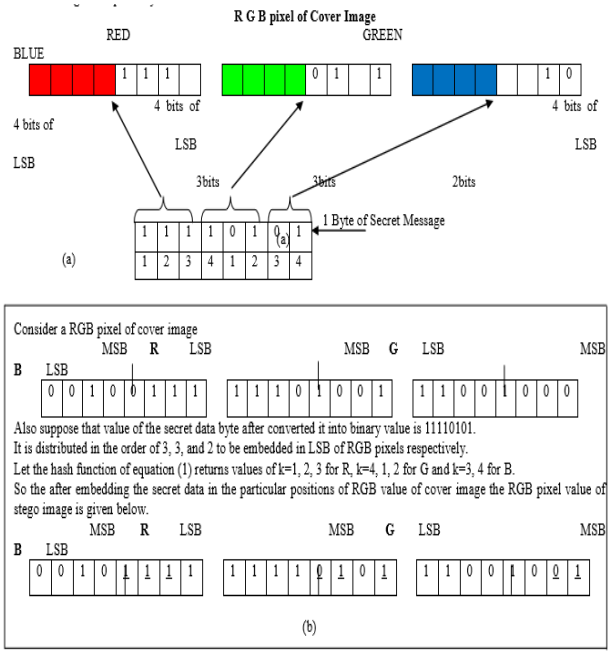


Figure 2 (a) & (b) Hash process to find LSB of RGB pixels value

Embedding proposed algorithm

Step One: Take encrypt the message

Step Two: Choose the cover image "sulaimani university.bmp"

Step Three: Take 4 LSB bits of each RGB pixels (Red, Green, and Blue) of the cover image.

Step Four: Embed 8 bits of the encrypt message into 4 bits of LSB of RGB pixels of cover image in the order of 3, 3, and 2 respectively using the position obtained from hash function in equation 1.

4.3 Decryption Phase

In the decrypt phase to detect the positions of the LSB's where the data bits had been embedded we have again used the hash function. In the same order as they are embedded, the bits are extracted from the position when the position of the bits had been specified. At the end of this phase we will obtain the secret message in binary form which gain converted into ASCII code form then the ASCII code form will be converted into cipher text, finally the receiver will decrypt secret message by using Affine cipher keys.

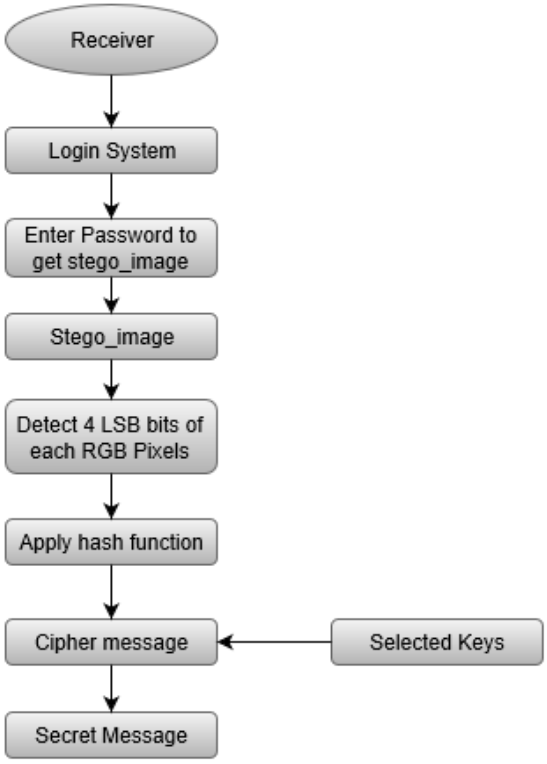


Figure 3: A flow chart illustrating the decryption phase

Decryption Process
Step one: Obtain stego_image

Step Two: Detect 4 LSB bits of each RGB pixels from stego_image.

Step Three: Apply hash function to obtain the position of LSB with hidden data.

Step Four: Retrieve the bits in order of 3, 3, and 2 respectively.

Step Five: Convert the bits into ASCII code

Step Six: Convert ASCII code into letter "Encrypt data".

Step Seven: Apply Affine cipher algorithm to decrypt the retrieve data.

Step Eight: Finally read the secret message.

5. RESULT AND DISCUSSION

Based on the proposed algorithm, we have developed a system, which implements the algorithms. At the first step in our system users must create account to obtain user name and password to login the system as shown in figure 4. Users must fill all field to create account.

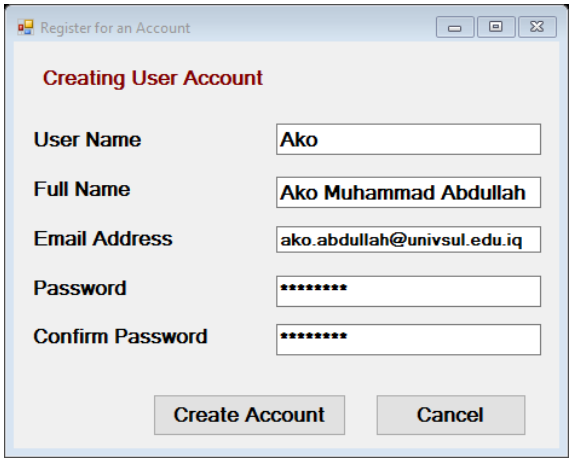


Figure 4 Creating User Account

After creating account on the system users can use the user name and password to login the system as shown in figure 5

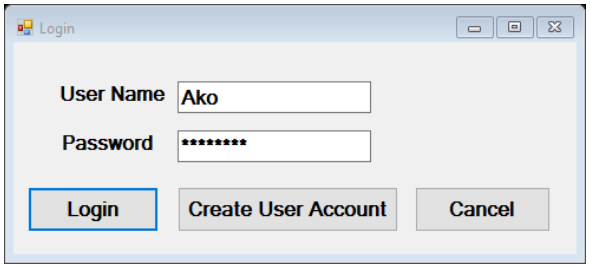


Figure 5 Login System

With login the system users can see two tab options one is Encoding Data for encryption and embedding encryption data into image and another is Decoding Data for retrieving data inside image. The information about the image such as account number of words, maximum size which can be encoding inside the image, size of image, height and width is displays in right top panel. In addition, in top panel in the encoding tab we have one text box and button is used to loading image from any location in computer. The file open dialog box is displays as follows, user should be selected the image file to hide secret image and click on Open button as shown in figure 6.

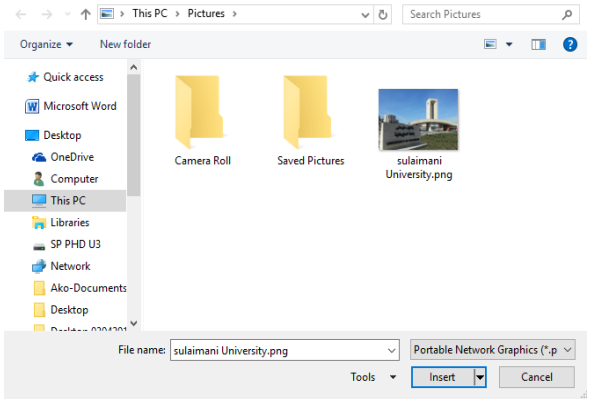


Figure 6 Select Image

Furthermore, in the encoding tab has three text boxes first is Secret Message for writing secret message that users want to be encoded in the image, second text box is Encrypt Message. In this text box user can see directly the encrypt message and third textbox is used to display the convert encrypt message into ASCII code before embedding in the image**.** In addition, to hide the encrypt message inside the image, a password is required for the purpose of security reason. The password is required to enter twice for the verification purposes. For the password, users must be used six characters. This password with data is also embedded inside the image. To encrypt the secret message users must be selected Affine cipher key. Figure 7 shows the main interface for encrypting and embedding secret message inside image.

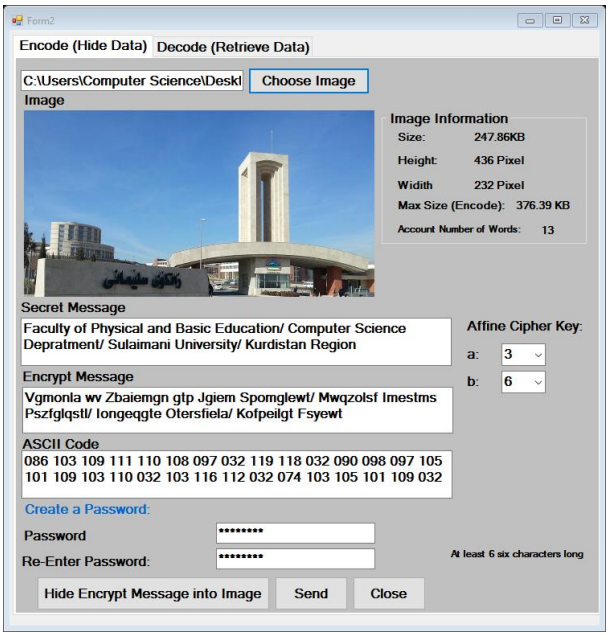


Figure 7 Main Interface for Encoding Data

After embedding the encrypt data users get a message box to verify the encrypt data was embedded successfully as shown in figure 8.

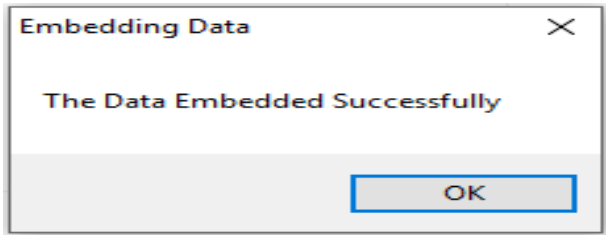


Figure 8 Embedding Data

When the encrypt data embedded successfully, the new stego_image have saved into a database. Moreover, users can send the stego_image directly via internet or email to target users without revealing the secret data inside the image.

In this system a second tab is used to decrypt or retrieve data. The panel for this tab consists of two text boxes, image view, two combo boxes and buttons. The receiver uses the text box one to enter the password to request for the image from the database. After enter the correct password and click on Return Image button the image is directly return to the decrypt panel but receivers cannot retrieve and decrypt the data that have been embedded inside the image until correct selecting affine cipher keys through using two combo boxes for instance a= 3 and b= 6. This is to ensure the integrity and confidentiality of the data as shown in figure 9. For any select of wrong secret key, the receiver will return a meaningless message as shown

in figure 10. This ensures the data is secured against intruders within the network environment.

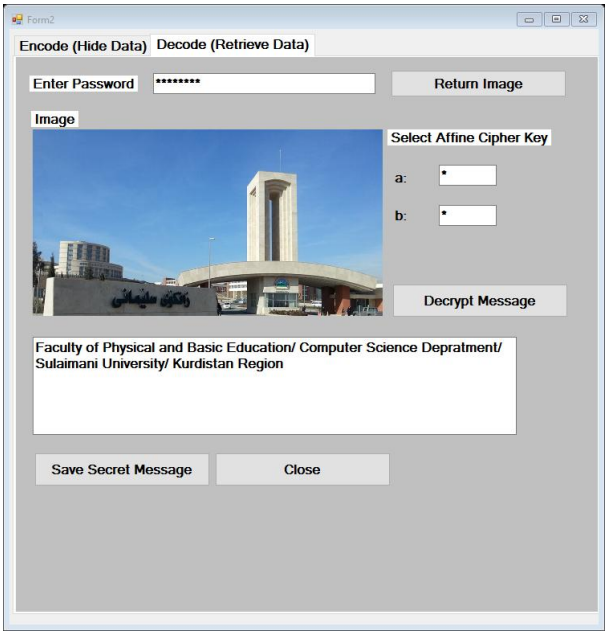


Figure 9 Retrieve Data from Image

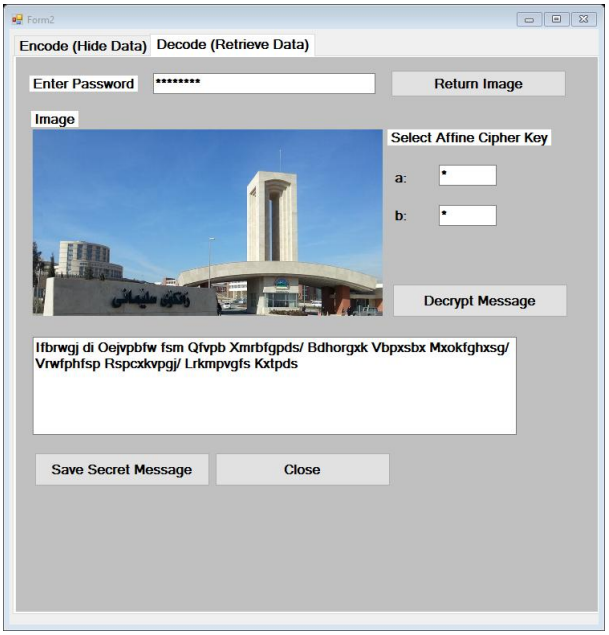


Figure 10 Selected wrong secret key

6. CONCLUSION

In this paper, a cryptography and steganography methods have proposed for providing better security of data in a network environment. With system that we have proposed data can be transferred between sender and receiver via unsecured network environment. Obviously, in a network environment this system is one of the best ways of hiding the secret of message from intruders. The main focus of the paper is to develop a system with extra security features. Cryptography method i.e Affine cipher algorithm has been implemented to encrypt the secret message and converted into ASCII code before embedding it in the image so that it is not easy to intruder to break the encryption without the keys and password. In addition, Hash based Least Significant Bit (H-LSB) technique has been implemented for embedding encrypt message into cover images. To evaluate this system we tested a number of images with various sizes of data to be hidden with the proposed algorithms. According to the tested we found that the system has the ability to provide a better security and easy way to encrypt, embedding and decrypt secret message without the quality of image is decreased as seen by the naked eyes. Hence this system is very efficient to hide the data inside the image.

7. ACKNOWLEDGMENTS

We would like to thank University of Sulaimani for all help and support in the implementation of our research.

8. REFERENCES

[1] R, Poornima and Iswarya R.J. "An Overview of Digital Image Steganography". International Journal of Computer Science & Engineering Survey 4.1 (2013): 23-31.

[2] A, Anagaw and V. Sreenivasarao." A Modified RSA Encryption Technique Based on Multiple public keys". International Journal of Innovative Research in Computer and Communication Engineering, Vol. 1, Issue 4, June (2013):859-864

[3] P, Kumar and V, Sharma." Information Security Based on Steganography & Cryptography Techniques: A Review". International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 10, October (2014):247-250.

[4] O, Mohammad and A, Al-Hazaimeh." Hiding Data in Images Using New Random Technique". IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July (2012):49-53.

[5] C. J, Ezeofor and Ulasi A. G. "Analysis Of Network Data Encryption & Decryption Techniques In Communication Systems". International Journal of Innovative Research in Science, Engineering and Technology 03.12 (2014): 17797-17807.

[6] Rashid, Aqsa, Malik Missen, and Nadeem Salamat. "Analysis Of Steganography Techniques Using Least Significant Bit In Grayscale Images And Its Extension To Colour Images" Journal of Scientific Research & Reports (JSRR) 9.3 (2016): 1-14.

[7] Ahmed Laskar, Shamim. "High Capacity Data Hiding Using LSB Steganography And Encryption", International Journal of Database Management Systems (IJDMS) 4.6 (2012): 57-68.

[8] Mohammad Ali Bani Younes and Aman Jantan." A New Steganography Approach for Image Encryption Exchange by Using the Least Significant Bit Insertion" IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.6, June (2008):247-254.

[9] Nameer N. EL-Emam." Embedding a Large Amount of Information Using High Secure Neural Based Steganography Algorithm". International Journal of Computer, Electrical, Automation, Control and Information Engineering. Vol:2, No:11, (2008):3806-3817.

[10] Anil Kumar and Rohini Sharma." A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique". International Journal of Advanced Research

in Computer Science and Software Engineering. Volume 3, Issue 7, July (2013):363-372.

[11] Rosziati Ibrahim and Teoh Suk Kuan." Steganography Algorithm to Hide Secret Message inside an Image". Computer Technology and Application, Vol. 2 (2011): 102-108.

[12] Neil F. Johnson and Sushil Jajodia." Exploring Steganography: Seeing the Unseen", IEEE Computer, Vol. 31, Issue No. 2, Feb. (1998): 26-34.

[13] K. Thangadurai."An analysis of LSB based image steganography techniques", IEEE Computer, Computer Communication and Informatics (ICCCI), International Conference (2014): 1-4

[14] Ekta Walia , Payal Jain and Navdeep." An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10 Issue 1, April (2010):4-8.

[15] R.Amirtharajan, R. Akila and P.Deepikachowdavarapu." A Comparative Analysis of Image Steganography", International Journal of Computer Applications Vol 2 ,No. 3, May (2010):41-47.

[16] Kousik Dasgupta , J.K. Mandal and Paramartha Dutta." Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April (2012):1-11.

[17] Roza Hikmat Hama Aziz."Improving Courier Service Reservation System: Reliability and Performance", Asia Journal of Natural & Applied Sceinces, Vol. 4 (4), December (2015): 20-36.

[18] Yuan Liu and Wen-Hsiang Tsai." A New Steganographic Method for Data Hiding in Microsoft Word Documents by a Change Tracking Technique", IEEE Transactions on Information Forensics and Security, Vol. 2, No. 1, March (2007): 24-30.

[19] Kavita Kadam, Ashwini Koshti and Priya Dunghav." Steganography Using Least Signicant Bit Algorithm", Engineering Research and Applications (IJERA), Vol. 2, Issue 3, May-Jun (2012): 338-341