Design of New Secret Key to Increase the Security of LSB Algorithm

Jalal M. Mehalhal[1*], AdemA.bensaid[2] , Mohammed F. Ighbeeshah[1]
[1] Enjjalal@yahoo.com, [2] A.bensaid@uot.edu.ly, [1] abuabdualaziz2240@gmil.com
[1] High Institute-Alkhoms, Dept. of Computer Engineering, Alkhoms–Libya
[2,] Department of Electronics, College of Science, Tripoli University, Libya

ABSTRACT

Nowadays, information security has become a big challenge for the world due to the rapid growth of Internet users day after day. Unauthorized access to confidential data can have serious implications such as financial loss, etc. One of the best techniques for secure communication is secret writing. Hiding data is very important nowadays as data travels over multiple insecure networks. To avoid this problem, encryption is used that hides data, but in some cases encryption cannot provide full security because the message is still available for encryption analysis. Encryption focuses on making the message unreadable to any unauthorized person who might intercept it. On the other hand, hiding information is a means of hiding the existence of a message to allow secure communication in a completely undetectable manner. Hide information and encryption are two different ways to hide data.
In this paper the researcher suggests how to hide the message using the least significant bit algorithm inside an image and encrypt it in a new way, by modifying the DES algorithm, the researcher generated subkeys from the DES algorithm and used them to specify the masking mechanism in the digital image.

Keywords:

cryptography,
LSB,
image,
pixel,
RBG color

1- Introduction

Information security science has become a subject of great interest by researchers and interested people who are trying to obtain new and updated solutions and technologies to ensure the protection of the information that is sent and received over the global network of information without any penetration or disclosure by intruders.

Therefore, it was necessary to keep abreast of the development of information security and the establishment of advanced technologies and means. Hence the science of concealing information and evolved by adopting the technique of concealment .Masking technology is one of the protections that make data sent and received invisible, by hiding specific messages within a specific cover. The goal of the concealment process is to not raise any point of doubt about the existence of hidden data, while the goal of the concealment analyst is to doubt all messages sent, and to check them to ensure that there are hidden data in them. The process in which a party tries to detect, read, change, or delete hidden information is called a decryption process.

Hence the need to find multiple means, for the purpose of communicating information and data in a correct and protected way, from the information of non-authorized parties to access this information, so the science of cryptography appeared as it is the science that is concerned with the methods of data protection and transmission in a wide field, and these methods depend on a secret key used to encrypt the data.

Although encryption is a good way to protect information, it is easy to discover and any intruder can manipulate, so the need for a more sophisticated, more confidential technology and information preservation, especially with the emergence and development of the global network of information.

The coverage system has been resorted to, because seeing the data in its encrypted form is sufficient to cause the intruder or the attacker to believe that there are important or sensitive data that lie in

the randomness or in the encrypted text, so he starts using anti-encryption techniques to try to get its content, and even if he is unable to achieve that, he might tamper with With it, distort it, or use some available means to prevent it reaching its goal.

The major and major challenge that the information security field has faced is the emergence of computer networks and means of communication in order to store, enter and supply information internally within organizations and externally to and from remote host devices. So a new expression has been added to information security which is network security, which is defined as the correct protection of all components related to the computer network, including data, communication tools, and infrastructure.[1]

1.1 Image processing

Color image models With the color format, a digital image can record and provide more information than the gray scale format image does. Digital acquisition devices (such as scanners and digital cameras) can separate beams of light into three primary colors- red, blue, and green, through the assistance of spectroscopes and filters. In order to record the color information, we need at least three parameters (e. g. red, blue, and green) to represent a color. We use the color model to represent the color information of digital images. Since we need three parameters to represent a color, those color models must be with a three dimensional format. The models use some mathematical functions to represent a point position (in the three dimensional space) that is assigned to a color. Some color models (RGB, CMY, YIQ, HSI, l1_l2_l3, and L*a*b)[8].

1.2 Cryptography

Cryptography is synonymous to encryption. Encryption is a process of converting plaintext (data or message) into ciphertext (encrypted text). Since ancient times it has been a practice to try and send a message to your allies without it being picked up an adversary. It is used to provide the strategic leverage needed in order to prevent any unwanted person from gaining any intelligence that might jeopardize the entire mission, for example Julius Caesar used to send messages to his generals in a coded format and the generals would decipher it using a key that only they had access to hence giving birth to "Caesar cipher". This has been an essential element in the art of war and a way of communicating war strategies even during World War I. These "keys" or ciphers usually follow a logical pattern or an algorithm but with the advent of the age of information technology, these methods started becoming obsolete as major algorithms that were earlier known to only an elite group became common knowledge and software's enhanced the process of guessing and cracking the algorithm patterns both previously known or newly created.[6]

Cryptography acts as a shield for the data by keeping it safe form changes and pilferage and as a result has become a prerequisite when data needs to be transmitted via any public medium especially the internet or any other network. Cryptography can also be used as a tool for user verification, but can also be used for user authentication. Encryption is a process of converting plaintext into ciphertext. Decryption is a process where encrypted text or ciphertext is converted back into original message.

The following three cryptographic schemes are very popular typically used with some Cryptographic algorithm [7].

a) Secret key (or symmetric) cryptography
b) public-key (or asymmetric) cryptography and
c) Hash functions.

Secret key cryptography is also known as symmetric key cryptography or private key cryptography. In this scheme both sender and receiver uses the same key to encrypt and decrypt data. The use of a secured channel in order to exchange the key in the process of symmetric encryption lowers its utility usefulness. So the main problem arrives when the keys are to be exchanged. If user wants to communicate with different people with separate confidentiality level he has to use different number of keys for each individual. If there is agroup containing 'N' number of people. Who are using secret-key cryptography scheme, then it is mandatory to administer a number of keys equal to N * (N-1) / 2.

1.3 LSB Hidden algorithm

It is a widely used method, as it uses the field less important than a particular pixel to store information. It is the most used method, and requires that one or more broadcasts of the message to be hidden and replaced by broadcasts of less importance than the pictures be entered. The least important broadcast is the one with the lowest mathematical value (20=1) in that the most important broadcast is the one with the greatest mathematical value (72 = 128).

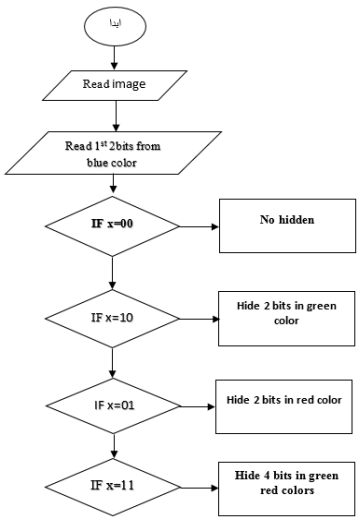


Figure 1: *LSB Algorithm*

2- Related work

In [2], The Sneha Arora suggested a technique to hide the text data into the color images using edge detection method. The alteration in edges cannot be distinguished well so edges can hide more data without losing quality of an image.

in [3] Khan Muhammad presents a novel approach for image steganography using Hue-Saturation-Intensity (HSI) color space based on Least Significant Bit (LSB). The proposed method transforms the image from RGB color space to Hue-Saturation-Intensity (HSI) color space and then embeds secret data inside the Intensity Plane (I-Plane) and transforms it back to RGB color model after embedding.
In [4] Muhammad proposes a way to improve Least Significant Bit (LSB) by randomly inserting message bits into an image to produce a more secure system .

In[5] Manjula K G use DES algorithm is utilized to image file encryption and decryption.

3- The Proposed Algorithm

In this section, the method proposed in this paper will be explained, which includes several operations, which is reading the text, image and secret key and incorporating text into the image based on the secret key, as well as incorporating data in several ways so that we seek to enter the largest amount of data into the image with the least distortions MSE calculation and image resolution evaluation with increased data size.

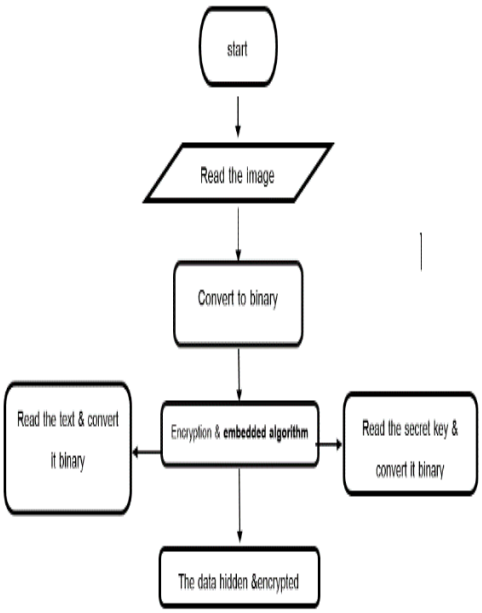


Figure 2: *The Proposed Algorithm*

3.1 The Secret Key Algorithm

In this paper, a secret key was proposed that encrypts the data, as it contributes to the distribution of data within the image in a way that makes it not possible for the third party to extract the text from the image in the event that he obtained the cached image.

Suppose that the value of the main secret key is 1001001101

The following step is to generate the subkeys where:

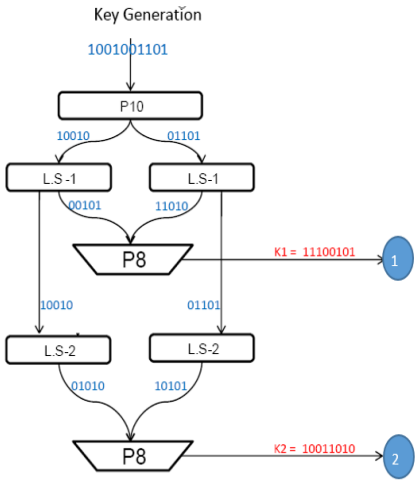


Figure 3: *Generated two sub keys*

p10: represents the demodulator bits from the main key

p8: represent the demodulator bits from the previous ten bits (the permutationoperation) corresponding to the next equation

p8 = [6 3 7 4 8 5 10 9]

LS_1 , LS_2represent the shift to left

Whereon product the two sub keys represent the next

1- The first sub key to determine the value of address of the start pixel
2- The second sub key to determine the value of jump between the pixels

The next table to generate two sub keys

Table 1: *The function of each subkey*

The first sub key	The second sub key
the value of address of the start pixel	the value of jump between the pixels

It represents the address of the first pixel at which the masking process begins Table below The title of the first pixel at which the masking process begins Through the previous table, the subkey of the first pixel, the seventh row and the tenth column, was generated

Table 2: *select the address of the first subkey*

First subkey							
Row Number (for Image Matrix)				Column Number (for Image Matrix)			
1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit
1	1	1	0	0	1	0	1
Convert to decimal				Convert to decimal			
07				10			

The following algorithm explains the process of selecting the first pixel

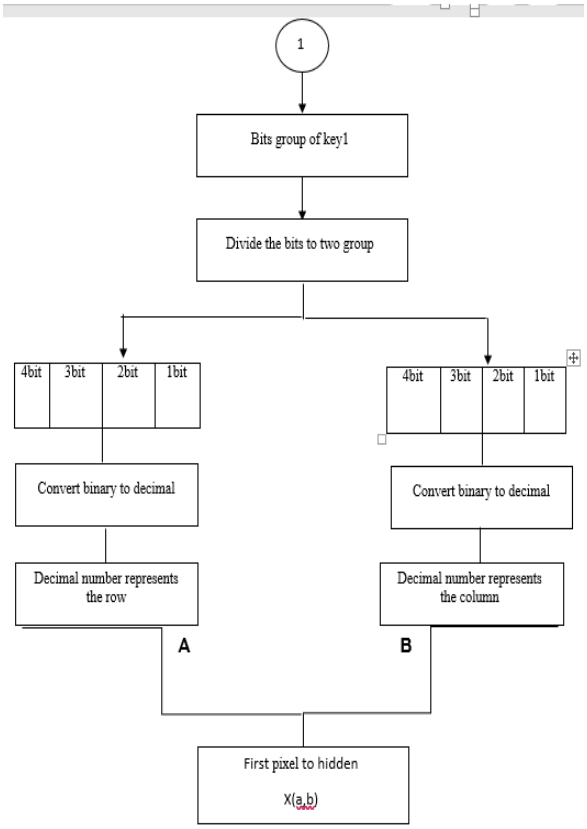


Figure 4: *The algorithm to select the first pixel*

2. Second sub key (jump value between each pixel)

The jumping technique was used and this technique allows to reduce interference in the image file. This technique selects the first two bits in the blue color for each pixel.

Table below The jump value for each pixel

Table 3: *Value of jump*

Value of key(binary)	00	01	10	11
Value of jump (decimal)	0	1	2	3

the table (3) shown the value of jump depending on the second sub key

Table 4: *Select the value of jump of secret subkey*

the second sub key								
00		01		10		11		the value of first two bits from blue color
1bit	2bit	3bit	4bit	5bit	6bit	7bit	8bit	The value of each bits of key
0	0	1	1	1	0	1	0	
0		3		1		1		The value of jump (decimal)

The following algorithm shows determine a jump value between each pixel

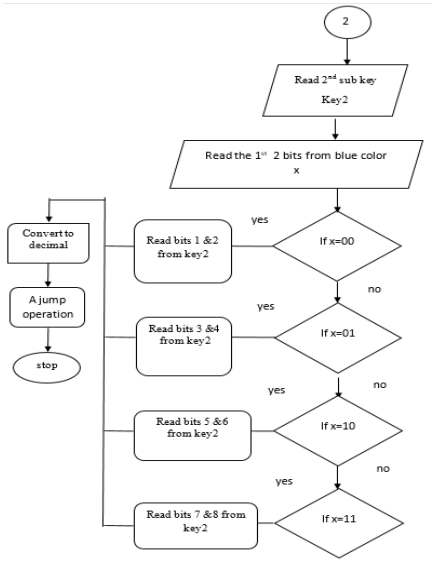


Figure 5: *The algorithm to determine a jump value*

When data is hidden using the key, the data inside the image will be distributed in such a way that the data extracted using the LSB algorithm is encrypted and the locations of the concealment cannot be predicted.

3.2 Evaluate the algorithm's performance after using the encryption key

The image file is subject to many types of distortions during the stages that you may go through, such as storing, processing and compressing. These distortions affect the image quality, and there are several measures used to evaluate the image quality, such as PSNR,

RMSE, MSE, (Histogram) for each image, they are one of the most commonly used standards.

To evaluate the tool of each LSB algorithm and the proposed algorithm and to know which algorithms give better results, this is done by measuring the image quality. Results from each algorithm. MSE, (Histogram) for each imagewere used as measures of image quality.

MSE

It is the average squared difference between the original and the modified image

$$MSE = \frac{1}{M * N} \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]2 \quad (1)$$

Histograms are a very useful tools used to analyze and compare significant changes in the frequency of appearance of the colors of the cover image with steganography images so as to be able to get a quick summary of the tonal range present in any given image.

3.3. Implementation environment

In this study, algorithms have been implemented using the MATLAB program, as the program has multiple uses such as work interferences, curved of direct value, building functions, establishing new functions, and the most important of them is that is easy to use.

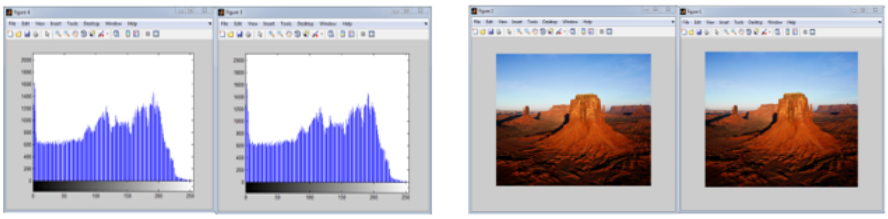
MATLAB programmed for matrix solution , their interactions and their uses in creating programs for large operations. There is a section within the program to build programs for graphics and different types of shapes and results directly on the screen or document them within (M-files) files.

4- Results

In this part, after entered a set of images into the program and using it will be calculated (the Histogram) for each image before and after hiding, calculated text size (TEXT), key size (KEY), calculated the (MSE) standard using a secret key without a secret key, calculated the text and key in each image, and compiling The data is in a table for each image.

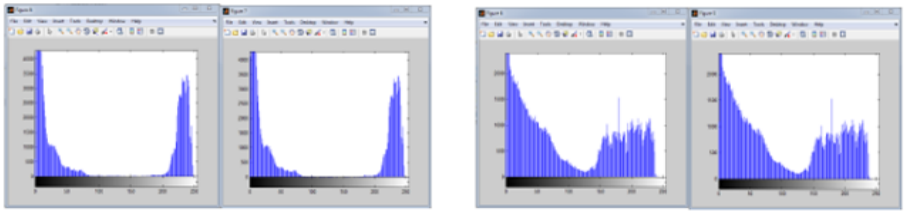
1. Image1:

a



b

Figure 6(a,b) : *The Image & Histogram before & after hide*



c

d

Figure 6(c,d) : *The Image & Histogram before & after hide*

a- The image before& after hiding operation

b- histogram of red color before& after hiding operation

c- histogram of green color before& after hiding operation

d- histogram of blue color before& after hiding operation

The following table calculate the MSE for two text , two keys & without key

Table 5: *Calculate the MSE for Image1*

Text	Size	key	size	Mse	Mse for Lsb without password
Text 1	488 bits	Key 1	248 bits	0.0011	0.000498453776
Text 1	488 bits	Key 2	80 bits	0.000086466	
Text 2	208 bits	Key 1	248 bits	0.0005776	0.0002746582031
Text 2	208 bits	Key 2	72 bits	0.00047302	

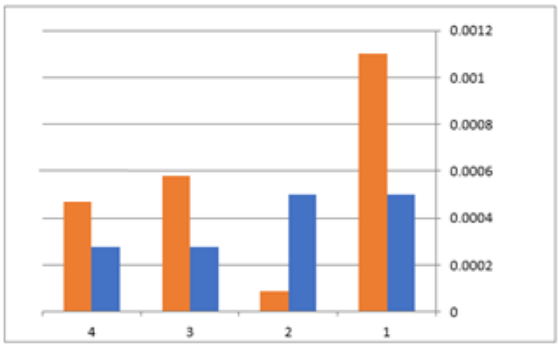
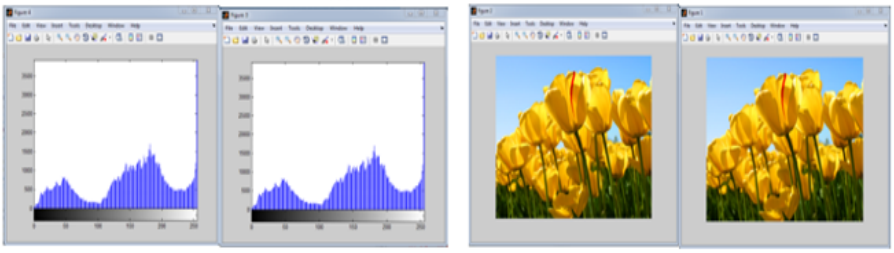
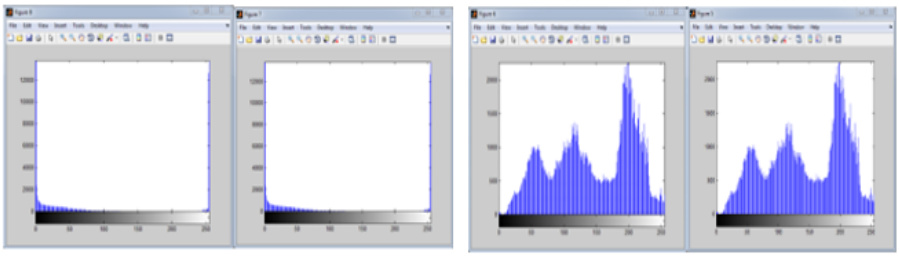


Figure 7 : *the MSE for Image1*

2. Image 2:



a b



c d

Figure 8: *show the image & histogram*

e- The image before& after hiding operation

f- histogram of red color before& after hiding operation

g- histogram of green color before& after hiding operation

h- histogram of blue color before& after hiding operation

The following table calculate the MSE for two text , two keys & without key:

Table 6: *Calculate the MSE for Image2*

Text	Size	key	size	Mse	Mse for Lsb without password
Text 1	488 bits	Key 1	248 bits	0.0015	0.0006256103516
Text 1	488 bits	Key 2	184 bits	0.0014	
Text 2	208 bits	Key 1	248 bits	0.00051371	0.0002136230469
Text 2	208 bits	Key 2	184 bits	0.00056458	

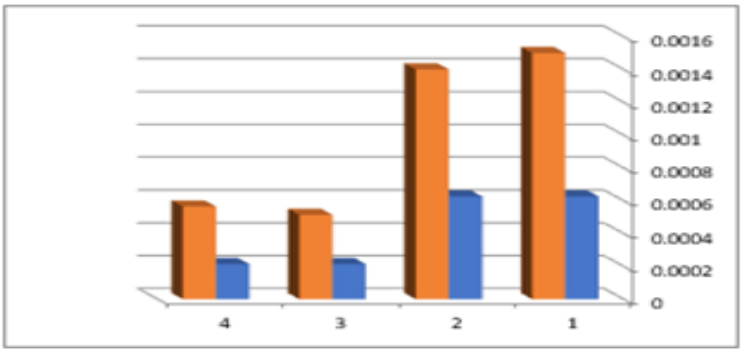


Figure 7 : *the MSE for Image2*

5- conclusion

in this method encrypted data was obtained Without using encryption technology, Using the secret key the data confidentiality service has been increased, No apparent distortions of the digital image, Having more than one jump and starting point depending on the secret key made it more difficult to extract pictures. As a first Recommendations Using the master key for other text hidden techniques such as (FMM) technology, As a second Recommendations This algorithm implements on another data such as video, audio, ..., As a third Recommendations increase the more possibilities for the number of jumps and the starting point by increasing the number of bits selected from the subkey, As a fourth Recommendations Use secret keys designed for encryption algorithms such as (RSA) to distribute data inside the image, and compare it with the proposed algorithm in this paper.

References

[1]. K.Brindha, ," Use of Symmetric Algorithm for Image Encryption", International Journal of Innovative Research in Computer and Commun-ication Engineering, Vol. 2: No. 5, May - 2014.

[2]. Sneha Arora, ," A Proposed Method for Image Steganography using Edge Detection " An International Journal of Engineering Sciences, Vol. 8, June - 2014.

[3]. Khan Muhammad, " A Novel Image Stegano-graphic Approach for Hiding Text in Color Images using HSI Color Model", International Journal of Computational Intelligence and Informatics, Vol. 3: No. 3, October - December 2013.

[4]. Obaida Mohammad, ," Hiding Data in Images Using New Random Technique", International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[5]. Manjula K G," Color Image Encryption and Decryption Using DES Algorithm", International Research Journal of Engineering and Technology, Volume: 03 Issue: 07 | July-2016.

[6]. V.Hemamalini ," A Survey on Elementary, Symmetric and Asymmetric Key Cryptographic Techniques ", International Journal of Computing Academic Research (IJCAR) ISSN 2305-9184, Volume 5, Number 1 (February 2016), pp.11-26.

[7]. Unik Lokhande ," An Effective Way of using LSB Steganography in images along with Crypto-graphy ", International Journal of Computer Appl-ications , Volume 88 – No.12, February 2014

[8]. Muhmed F. Agbisha ," Encrypt The Text and Hide in the RGB Image using three Pointers of color" ,ICTS 2018.