RESEARCH ARTICLE OPEN ACCESS

Suggested Approach to Embedded Playfair Cipher Message in Digital Image

Lecture Hadab Khalid Obayes
College of education for human sciences, Babylon University, Iraq

ABSTRACT
This research presents a technique for protect the data through using cryptography and steganography. The cryptography stage is using Play fair cipher to encrypted the secret message. In steganography stage convert Playfair cipher text to binary and store the first bit in every letter in secret message in the LSB of pixel in the image and then the second bit in every letter embedded in the LSB of pixel and continue so until the last bit in last letter in the secret message. The greater size of the text more difficult to decode See's picture does not know what the image bits and what are bits of text.

Keyword- cryptography, LSB, Playfair cipher, steganography, text embedded.

I. INTRODUCTION

Because of the development in communication devices, information processing and the Internet. Information security and privacy has therefore become a core requirement for data transfer, driven by the need to protect critical assets. Cryptography is popularly known as the study of encoding and decoding private massages. This article use playfair method as a cryptography. In Play fair cipher, the alphabets are arranged in 5X5 diagram based on secret key, it is very difficult to break the cipher text but it can be breakable by few hundreds of letters[1]. Steganography is one of protection ways, which is defined as that is the art of hiding information. The best known steganographic method that works in the spatial domain is the LSB [2] (Least Significant Bit), which replaces the least significant bits of pixels selected to hide the information [3]. LSB steganography is the process of adjusting the least significant bit pixels of a carrier image in order to hide a message. In its simplest form, the bits of the secret message substitute the LSBs of consecutive pixels of an image, one bit in each pixel. For this method to work, the pixels of the image must have fixed length, e.g. 8 bits for grayscale images or 24 bits for color images[4].

II. PLAYFAIR CIPHER

The Playfair cipher is a substitution cipher invented in 1854 by Charles Wheatstone (1802-1875). The name of the cipher as it is known in the cryptology literature comes from the name of the lord Playfair who strongly promoted the cipher[1]. Playfair cipher is Unlike a simple substitution cipher, which takes a message one letter at a time and replaces each letter with another letter, a Play fair cipher takes a message two letters at a time and replaces each pair of letters with another pair of letters. In other words, each diagram is replaced with another digram. (A pair of letters is called a digram.) A given digram is always replaced by the same digram.[5] The enciphering process is based on a table where one letter of the English alphabet is omitted, and the remaining 25letters are arranged in a 5x5 digram. Typically, the letter “J” is removed from the alphabet and an “I” takes its place in the text that is to be enciphered. The digram, with no key, look like the following [6]:

A B C D E
F G H I K
L M N O P
Q R S T U
V W X Y Z

the The alphabet square is a five-by-five digram. The key phrase is first written without repeating any letters. The remaining letters of the alphabet are filled in in order, Using the word “CIPHER” as the key, enciphering digram becomes:

C I P H E
R A B D F
G K L M N
O Q S T U
V W X Y Z

To encrypt a message, the following four rules are applied to each digram in the plaintext:[7]

1. If both letters are the same (or only one letter is left), add an "X" after the first letter. Encrypt the new pair and continue. Some variants of Playfair use "Q" instead of "X", but any infrequent letter could be used. For example, “balloon” would be treated as “ba lx lo on”.
2. Plaintext letters that fall in the same row of the digram are each replaced by the letter to the right, with the first element of the row circularly following the last. For example, HE is replaced with EC.

3. Plaintext letters that fall in the same column are each replaced by the letter beneath, with the top element of the column circularly following the last. For example, VC becomes OV.
4. Otherwise, each plaintext letter is replaced by the letter that lies in its own row and column occupied by the other plaintext letter. Thus, QD becomes TA and GY becomes MV.
5. To decrypt, the inverse operations of the last 3 rules are applied, and also taking into consideration the 1st rule)dropping any extra "X"s or "Q"s) that don't make sense in the final message when finished). All non-letters are ignored and not enciphered. Numbers, spaces, and punctuation are also skipped. Some other customizations are possible, depending on the cipher variant used.

III. STEGANOGRAPHY PRINCIPLES

The word steganography comes from the Greek *Steganos*, which mean covered or secret and –*graphy* mean writing or drawing. Therefore, steganography means, literally, covered writing. Steganography is the art and science of hiding information such that its presence cannot be detected [8]. The strength of steganography resides in how strong the carrier medium is imperceptible and how much the covered message is difficult to be detected and uncovered by unauthorized observers. In critical situations, people known as steganalysts are hired to identify suspicious files and detect whether or not they contain secret information, and if possible, recover this information. Actually, developing a steganography algorithm that firmly conceals data in a hard-to-notice, hard-to-detect, and hard-to-recover way ensures that the secret information being communicated through certain carrier medium would pass undetected by forensics and illicit third parties[9]. The basic model of steganography consists of Carrier, Message and Password. Carrier is also known as cover-object, which the message is embedded and serves to hide the presence of the message[10].

IV. ELEMENTS OF STEGANOGRAPHY

Steganography has two processes, one for covering and one for uncovering secret data. The covering process is about hiding overt data into a cover medium, also known as stego or carrier file. In contrast, the uncovering process is just the reverse; it is about extracting the covert data from the carrier file and returning them back to their original state. Fundamentally, modern digital steganography is governed by five key elements. They are as follows [11]:

1. Covert Data: Often known as the payload and refers to the overt data that need to be covertly communicated or stored. The covert data can be anything convertible to binary format, from simple text messages to executable files.
2. Carrier Medium: It is basically a file into which the covert data are concealed. The carrier medium can be any computer-readable file such as image, audio, video, or text file.
3. Stego File: Sometimes called package, it is the resulting file which has the covert data embedded into it.
4. Carrier Channel: It denotes the file type of the carrier, for instance, BMP, JPG, MP3, PDF, etc.
5. Capacity: It denotes the amount of data the carrier file can hide without being distorted.

V. STEGANOGRAPHIC TECHNIQUES

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed [12]. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible.Common approaches are include [13]:

(i) Least significant bit insertion (LSB)
(ii) Masking and filtering
(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the *cover-image* in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small. The advantages of LSB are its simplicity to embed the bits of the message directly into the LSB plane of cover-image and many techniques use these methods [14]. Modulating the LSB does not result in a human-perceptible difference because the amplitude of the change is small. Therefore, to the human eye, the resulting stego-image will look identical to the cover-image. This allows high perceptual transparency of LSB.

VI. PROPOSED ALGORITHM

Proposed algorithm is using two layers of security to maintain the privacy, confidentiality and accuracy of the data. First layer is cryptography where the message is encode in playfair method and second layer is steganography where the encoded message is embedded in cover image. The algorithm steps are showing in figure(1).

VII. STEPS OF PROPOSED ALGORITHM

1- Enter the secret key for playfair method.
2- Select the cover image.
3- Enter the message.

4- Encode the message in playfair using the entered secret key.
5- Convert the message characters to the ASCII code.
6- Convert the ASCII code to the binary system (series of zeros and ones) and find the row and Column of the binary array.
7- Convert the cover image to binary system.
8- Embedded the encoded message bits in the pixels bits of cover image.
9- Return the cover image to decimal system.
10- Send stego image in unsecure channel.

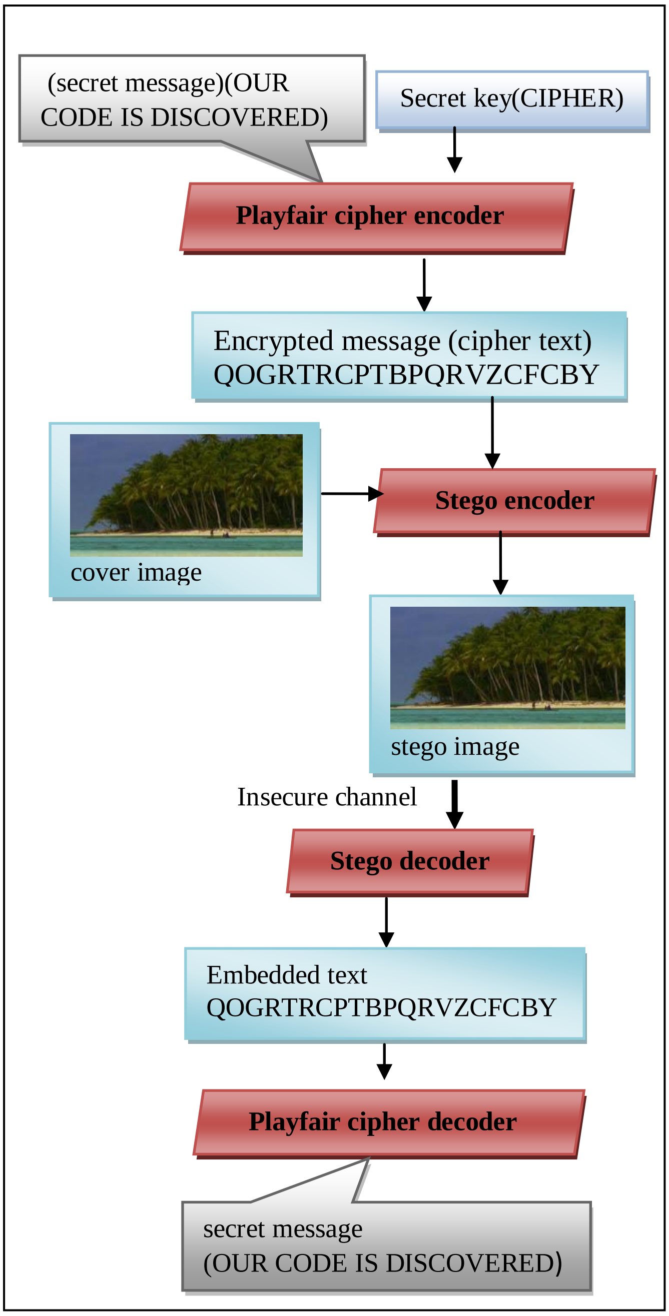

(secret message)(OUR CODE IS DISCOVERED)
Secret key(CIPHER)
Playfair cipher encoder
Encrypted message (cipher text) QOGRTRCPTBPQRVZCFCBY
cover image
Stego encoder
stego image
Insecure channel
Stego decoder
Embedded text QOGRTRCPTBPQRVZCFCBY
Playfair cipher decoder
secret message (OUR CODE IS DISCOVERED)

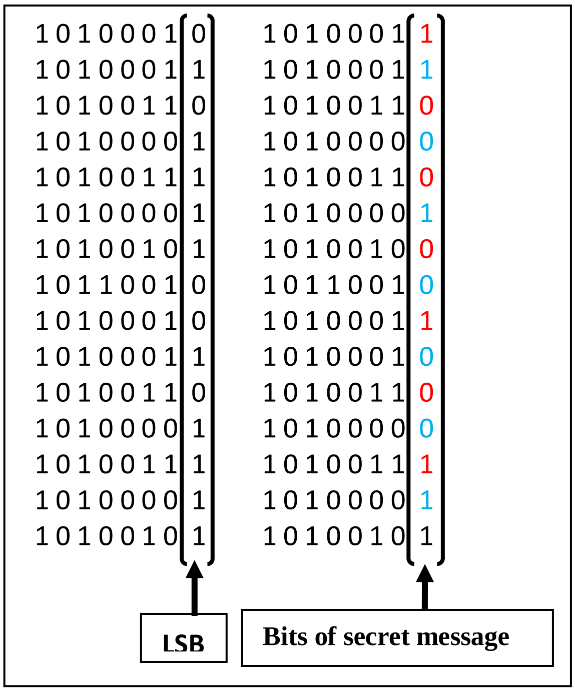
Figure (1) proposed Algorithm

VIII. APPLYING THE ALGORITHM'S STEPS IN MATLAP R2010a

The secret key will be "CIPHER". The enciphering digram becomes

CIPHE
RABDF
GKLMN
OQSTU
VWXYZ

- The cover image will be "img.jpg"
- the secret message will be "HI"
  the PlayFair = EP.
- ASCII code = (69 80)
- Binary system "**1000101** ","**1010000**".
-insert the bits of secret message in the cover image bits as shown in figure (2).



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

Figure (2) insert secret message bits

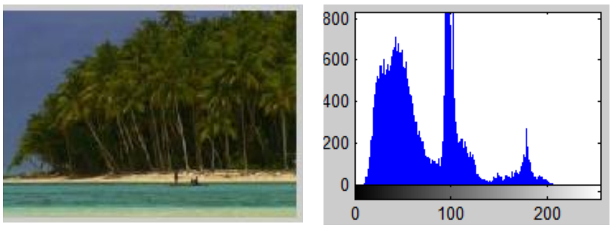
The quality of the stego images have been measured using PSNR (Peak Signal-to-Noise Ratio). PSNR is a standard measurement used in steganography technique in order to test the quality of the stego images. The higher the value of PSNR, the more quality the stego image will have. If the cover image is *C* of size *M* × *M* and the stego image is *S* of size *N* × *N*, then each cover image *C* and stego image *S* will have pixel value *(x, y)* from *0* to *M-1* and *0* to *N-1* respectively. The PSNR is then calculated as follows:

$$PSNR = 10.\log_{10}\left(\frac{MAX^2}{MSE}\right) \qquad (1)$$

where

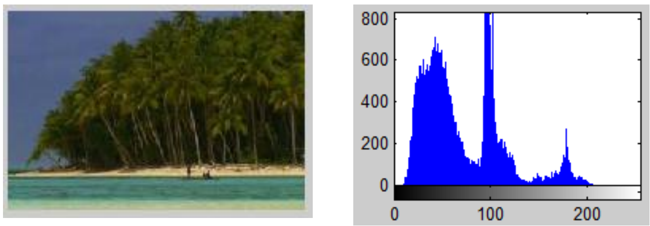
$$MSE = \frac{1}{MN}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y)-S(x,y))^2$$

IX. EXPERIMENTAL RESULTS



(a) (b)

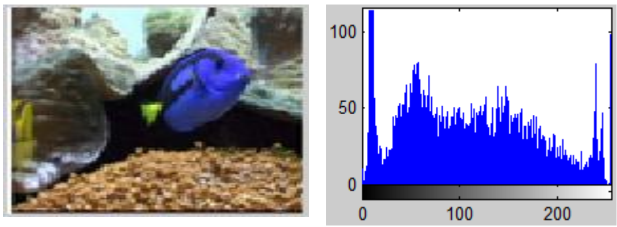
Figure (3-a) original image,(3-b) histogram of original image



(a) (b)

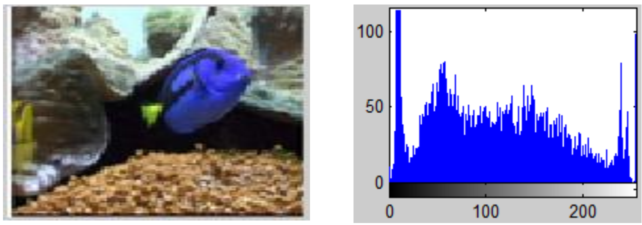
Figure (4-a) stego image,(4-b) histogram of stego image

The experimental results are observed in figure(3-a) the cover image (img1.jpg) and figure (3-b) its histogram and in figure (4-a) the stego image with 11KB file of text and figure (4-b) its histogram the PSNR is (61.9946).



(a) (b)

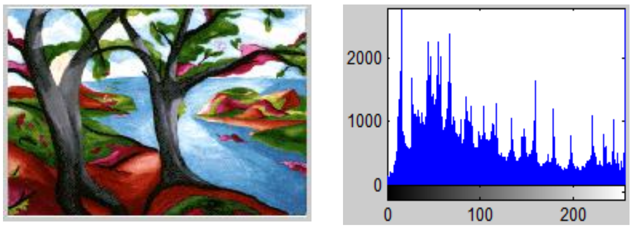
Figure (5-a) original image,(5-b) histogram of original



(a) (b)

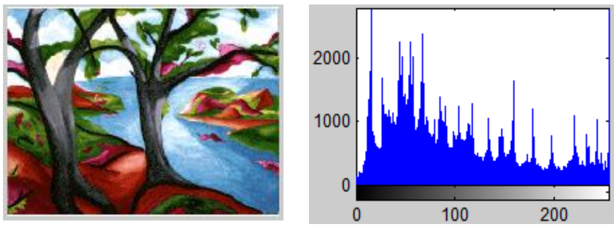
Figure (6-a) stego image,(6-b) histogram of stego image

In figure(5-a) the cover image(img.bmp) and figure (5-b) its histogram observed in figure (6-a) the stego image with 11KB file of text and its histogram, theSNR is (52.6333).



(a) (b)

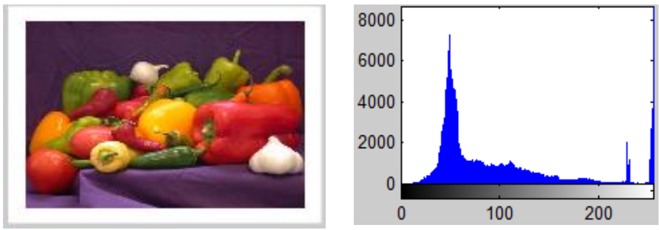
Figure (7-a) original image (tree.png), (5-b) histogram of original image



(a) (b)

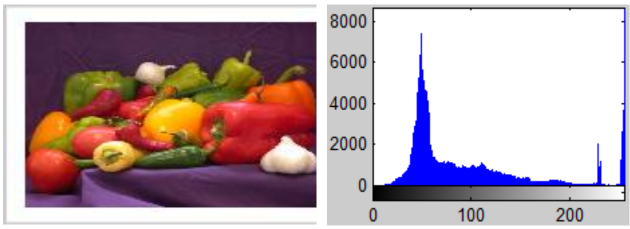
Figure (8-a) stego image (tree.png), (8-b) histogram of original image

The figure (7-a) shown the original image in (png) format file and (7-b) shown its histogram, the PSNR is (65.7825) between the cover image and stego image with 11KB file text where the figure (8-a) shown the stego image and figure (8-b) shown the stego image histogram.



(a) (b)

Figure (9-a) original image,(9-b) histogram of original



(a) (b)

Figure (10-a) stego image,(10-b) histogram of stego

The last experiment in image.png shown in figure (9-a) the cover image and its histogram where the stego image in figure (10-a), the PSNR is 72.5598 between the cover image and the stego image.

X. Conclusion

Two levels of safety have been proposed in this research through the use of two important technologies in information security that mean stronger approach provide. Playfair cipher represent an improvement in security over substitution ciphers, pair of letters and the 5x5 digram are makes a good security, In order to increase the level of security has been hidden encrypted text into a digital image. Different type of image are tested in proposed algorithm and stego images tested by using PSNR value. The PSNR value of each stego image is highe value and this mean stego image does not have a noticeable distortion on it. The amount of message that can be embedded is also very good. The technique is not susceptible to histogram based attacks.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practice. Second edition, Pearson Education. Simon Haykin , Communication Systems. , 4th Edition, Willey.

[2] Kurak, C. and McHugh, J.: A Cautionary Note on Image Downgrading. *Proc. IEEE 8th Annual Computer Security Applications Conference*. San Antonio, USA, Nov./Dec. 1992, pp. 153-155.

[3] Moskowitz, I., Longdon G. and Chang, L.: A New Paradigm Hidden in Steganography. *Proc. 2000 Workshop on new security paradigms, Ballycotton*, Country Cork, Ireland, 2000. ACM Press, New York, pp. 41-50.

[4] Sharp, T.: An implementation of key-based digital signal steganography. *Proc. 4th* International Workshop on Information Hiding, Pittsburgh, USA, April 25, 2001. Springer LNCS, vol. 2137, pp. 13-26.

[5] ttp://jnicholl.org/Cryptanalysis/Ciphers/Playfair

[6] Alex Biryukov, Cryptanalysis of the Classical Ciphers, http://www.wisdom.weizmann.ac.il/~albi/cryptanalysis/lect3.html.

[7] V.U.K. Sastry, N. Ravi Shankar, S.Durga Bhavani, Generalized Playfair Cipher involving Intertwining, Interweaving and Iteration, *International Journal of Network and Mobile Technologies ISSN 1832-6758 Electronic Version VOL 1, ISSUE 2 ,* November

[8] M. Ramkumar & A.N. Akansu. "Some Design Issues For Robust Data hiding Systems", *<http://citeseer.nj.nec.com/404009.html>*

[9] Youssef Bassial, An Image Steganography Scheme using Randomized Algorithm and Context-Free Grammar , (*JACST), ISSN: 2227-4332, Vol. 1, No. 4,* December 2012

[10] Muhalim Mohamed Amin, Subariah Ibrahim, Mazleena Salleh,Mohd Rozi Katmin, *Information Hiding Using Steganography*, Department of Computer System & Communication Faculty of Computer Science and Information system, Universiti Teknologi Malaysia, 2003

[11] Eric Cole, Hiding in Plain Sight: Steganography and the Art of Covert Communication, Wiley Publishing, 2003.

[12] N.F. Johnson & S. Jajodia, "Steganalysis of Images Created Using Current Steganography Software", *in Proceeding for the Second Information Hiding Workshop, Portland Oregon*, USA, April 1998, pp. 273-289.

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

[14] R. Chandramouli, N. Memon, "Analysis of LSB Based Image Steganography Techniques", *IEEE*, pp. 1019-1022, 2001.