Public Key Steganography

Nesir Rasool Mahmood
Kufa University
Education College

Ali Abdul Azeez Mohammad
Kufa University
Education College

Zahraa Nesir Rasool
Kufa University
Sciences College

ABSTRACT
In this paper, a new method will be introduced for hiding information in images by using a public key method for ciphering the text before hiding information as well as this public key will be used in determining the position where the information will be hidden by using the last position in finding the new position, symmetric key also will be used in hiding process for deciding the number of bits that will be used from each pixel in the image, the combination of steganography and cryptography provide much strong method for keeping information secured and undiscovered from unwanted persons.

Keywords
Steganography, public key, cipher, hiding, cryptography

1. INTRODUCTION
Steganography is the art and science of hiding information in deterministic sequence that understandable for valid persons to prevent the detection of hiding information [2], there exist two types of materials in steganography: message and carrier [3]. Message is the secret data that should be hidden and carrier is the material that takes the message in it. While cryptography is the science of hiding information meaning, the goal of cryptography is to make data unreadable by unwanted persons [3]. Cryptography algorithms are divided into two types according to the key used in ciphering algorithm, secret- key (symmetric) and public-key (asymmetric) algorithms [5]. Symmetric algorithms are used to encrypt and decrypt plaintext by using the same key in both algorithms. While Public-key encryption algorithms used a pair of keys, one key is used to encrypt information that will be sent to a receiver (public) who owns the corresponding private key which is used to decrypt the information [4].

Steganography and cryptography are closely related. Cryptography scrambles messages so they cannot be understood [4]. Steganography on the other hand, will hide the message so there is no knowledge of the existence of the message in the file [1]. Both sciences can be combined to produce better protection of the message. In this case, when the steganography fails and the message can be detected, it is still unreadable because, it is encrypted by using cryptography Techniques.

2. THE PROPOSED SYSTEM
The proposed system consists of two stages, the first stage for ciphering the message (plaintext) and hiding cipher text in the (image) as illustrated in figure (1) and following steps

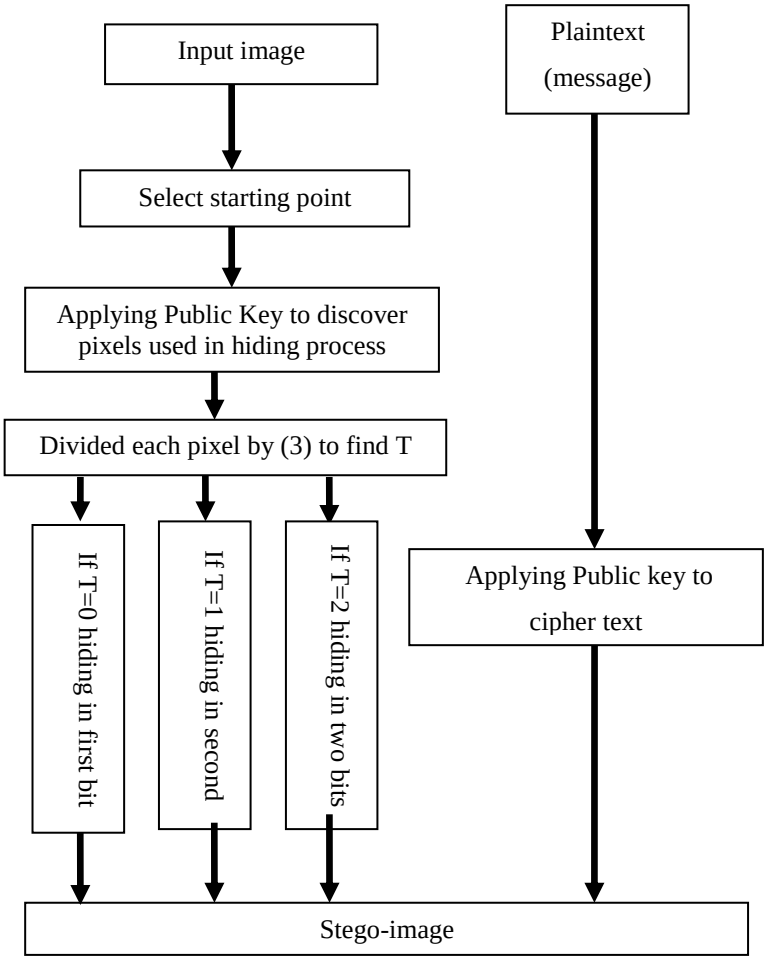


Figure (1): Block diagram of the first stage of the proposed system

1- Encryption plaintext by using the public key of the receiver.
2- Select starting (s) point to hide information.
3- Applying the same public key on the start point to discover pixels that will be used in hiding process.
4- Deciding the number of bits that will be used in hiding information for each pixel from step (3).
5- Hiding cipher text in the image and send modified image (stego-image) to the receiver.
6- Saving the last hiding position (f) and message length (L) in suitable fixed pixels.

While the second stage for extracting the message (Cipher text) from the stego-image and deciphering the message to discover plaintext as illustrated in figure (2) and following steps

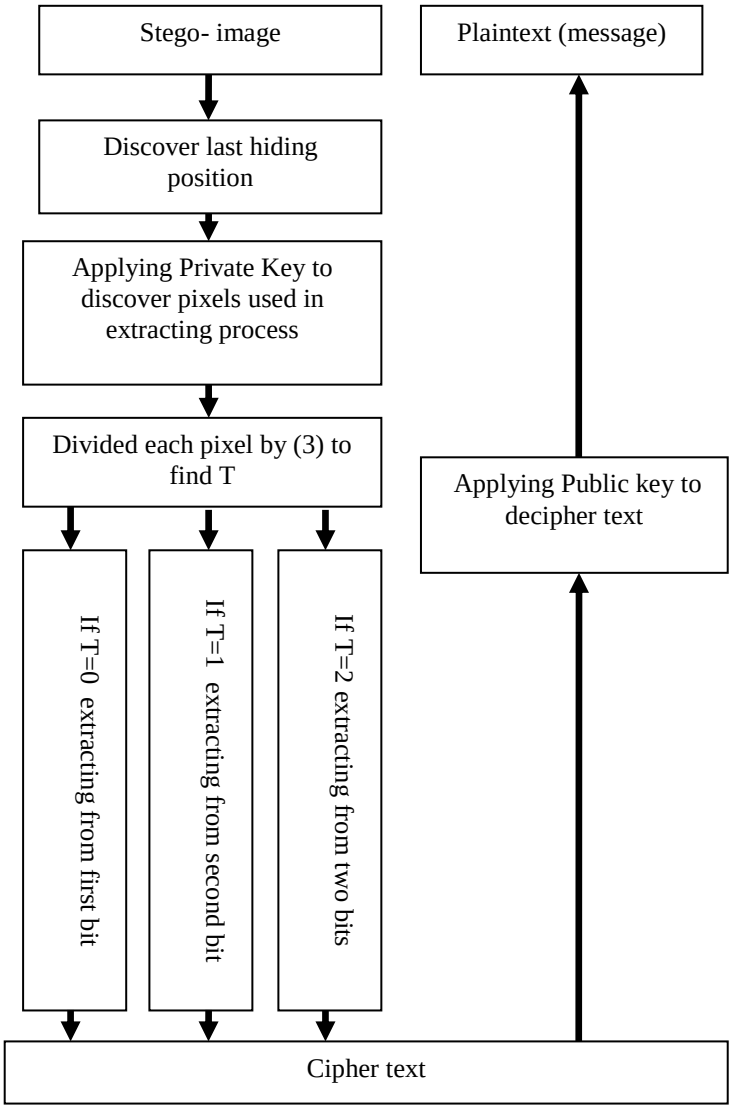


Figure (2): Block diagram of the second stage of the proposed system

1- Starting from last hiding position and fixed pixels.
2- Extracting bits from them.
3- Applying private key on this point to discover the pixels that will be used to extract information.
4- Deciding the number of bits that will be used to extract information from each pixel from step (3).
5- Extracting information from stego-image and constructing cipher text.
6- Applying private key on cipher text to discover plaintext.

Each step in the proposed system will be illustrated in details in the following

2.1. Hiding step

1- Ciphering text: - each person has two related keys one public and the other private, so if person 1 wants to send secret message (HI) to person 2, he used public key of person 2 to encryption text.

$P_2 (e_2, n_2) = (3, 187)$, $(d_2, n_2) = (107,187)$
C (H) = $(72)^3$ mod (187) = 183 (10111011)
C (I) = $(73)^3$ mod (187) = 57 (00111001)

2- Selecting start point:- the first row and column used for hiding last hiding position (LH) and text length(TL), so any position will be selected as a starting point(SP) except them, and for example let the position (5,2) with value 121 as a starting point, where the value of four MSBs is 112 mod 3 is 1, so information will be hidden in second bit as follows

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

3- Discover others pixels that will be used in hiding information:- the same public key will be applied to find the second position from the first position

New (i) = old $(i)^3$ mod (187)
New (j) =old $(j)^3$ mod (187)
New (i) = 5^3 mod (187) = 125
New (j) = 2^3 mod (187) = 8

Information will be hidden in position (125, 8), if the value of this pixel is (217) where the value of four MSBs is 198 then 198 mod 3 is 0, so information will be hidden in first bit as follows

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

New (i) = 125^3 mod (187) = 97
New (j) = 8^3 mod 187 = 138

information will be hidden in position (97, 138), if the value of this pixel is (85) where the value of four MSBs is 80, then 80 mod 3 is 2; information will be hidden in first two bits as follows

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

4- These operations will be continued until last bit of the message.
5- Saving the last hiding position (F) and message length (L) in first row and column by using one least significant bit.

2.2. Extracting stage

All operations applied in hiding stage will be applied in opposite sequence as follows

1- Deciphering text by using receiver private key and finding position that will be used in hiding stage.
2- extracting the last hiding positions(LH) and text length(TL), as example let LH is (97,138) and its value is 87 (as in hiding stage) where the value of four MSBs is 80 then 80 mod 3 is 2; information will be extracted from first two bits as follows

0	1	0	1	0	1	1	1

3- The previous position can be calculated as follows

Old (j) = new $(j)^{107}$ mod 187
Old (i) = Old $(i)^{107}$ mod 187
Old (j) = 138^{107} mod 187 = 8
Old (i) = 97^{107} mod 187 =125

the old position is (125, 8) and its value is 216 (as in hiding stage) where the value of four MSBs is 198 then 198 mod 3 is 0, so information will be extracted from first bit as follows

0	1	0	1	1	0	0	0

Old (j) =125^{107} mod 187 = 5
Old (i) = 8^{107} mod 187 =2

the old position is (2, 5) and its value is 123 (as in hiding stage) where the value of four MSBs is 112,

then 112 mod 3 is 1, so information will be extracted from second bit as follows

0	1	1	1	1	0	1	1

And so on, therefore the first four bits from the message are

1	0	1	1

As illustrated in hiding stage.

4- If the number of bits that will be extracted equals to the length of the message (L) then the operation will be stopped.

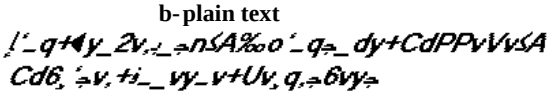
3. RESULTS

After applying the proposed system the results of two examples illustrated below

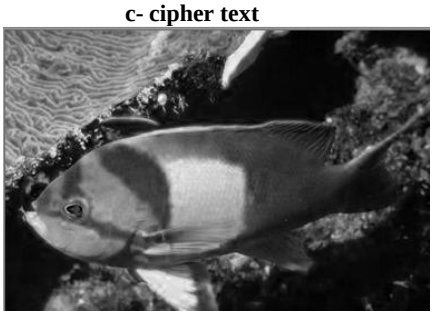
Example (1):-

a- cover

b- plain text



c- cipher text



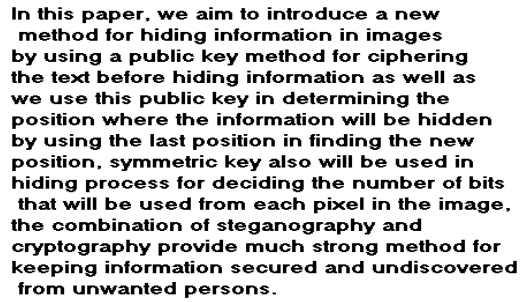
d- stego – object

Figure (3): results (1)

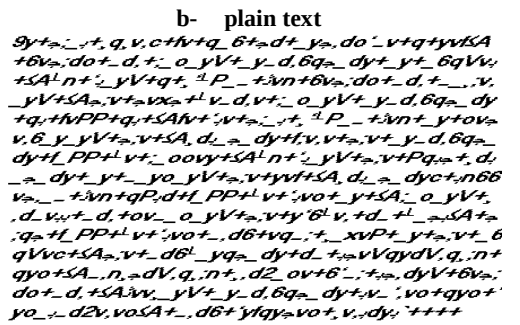
in this example the message length is 504 bits and cover dimensions are 384×256 pixels then the peak signal noise ratio become 64.14.

Example (2):-

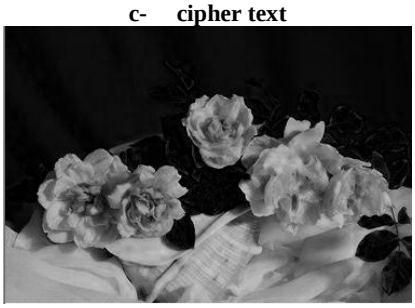
a- cover



b- plain text



c- cipher text



d- stego – image

Figure (4): results (2)

in this example the message length is 4744 bits and cover dimensions are 384×256 pixels then the peak signal noise ratio become 54.76.

$$SNR_{peak} = 10 \log_{10} \frac{(l-1)^2}{\frac{1}{n \times m} \sum_{r=0}^{n-1} \sum_{c=0}^{m-1} [g(r,c) - I(r,c)]^2}$$

Where,

l is the number of gray levels in the image.

I(r,c) are the pixels before hiding process in the image.

g(r,c) are the pixels after hiding process in the image.

n,m are the width and height of the image respectively.

The peak signal noise ratio is an index for stego- image quality with compare to original image , this ratio becomes infinity if stego and original images are identical (no changes) and this ratio becomes small number if stego and original images are so different.

4. CONCLUSIONS

1- The combination of cryptography and steganography is a powerful toll for keeping information secure and undiscovered.

2- Hiding in second (or third) bit makes the difference between cover and stego object greater but useful in keeping stego object more secure against attack(changing LSB).

3- using big image allow for using bigger keys numbers.

4- A special mechanism must be available for avoiding the repeated hiding over the same pixels like shifting by fixed space to right or left depending on pixel position (after or before the middle pixel of the image) , this process is useful in avoiding the loss of information because of the public key cycle.

5. REFERENCES

[1] Michael Backes, and Christian Cachin " Public-Key Steganography with Active Attacks ", Switzerland, 2004.

[2] F´abio Borges, Renato Portugal, and Jauvane Oliveira " Steganography with Public-Key Cryptography for Videoconference ", National Laboratory of Scientific Computing, 2007.

[3] Samir K Bandyopadhyay, Debnath Bhattacharyya, Debashis Ganguly, Swarnendu Mukherjee and Poulami Das "A Tutorial Review on Steganography", University of Calcutta, 2008.

[4] Shahana T "A Secure DCT Image Steganography based on Public-Key Cryptography ", India, 2013.

[5] Ms. Priyanka P. Palsaniya, and Mr. Pravin D. Soni " CryptoSteganography:Security Enhancement by using Efficient Data Hiding Techniques", India, 2014.