Data Hiding in BMP Images Using Steganography and Cryptography

Khdega A.Yosef Galala
Department of Computer Science
College of Education, Al JufrahUniversity, Waddan, Libya
kdebh@yahoo.com

Abstract—Day after day modern and advanced techniques will be required to secure sensitive information against unauthorized access and attacks. Cryptography and steganography are well known as powerful techniquesused to secure sensitive data transmitted throughunsecured channels.However, the combination of these two methods will enhance the security of datatransmitted. Thus,this work aims to propose anew steganography technique which combining with a new encryption technique to providean extra level of security against attacks. The new technique apply on a BMP file format and itis designed based the Least Significant Bits (LSB) method to embed encrypted data into cover image. The experimental results in this work is executed by VB6 language. The image quality is measured in-terms of Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). Different host images have been tested with different sizes of files to be hidden. The results indicate thatthe new algorithmgives high PSNR and lower MSE values in all tested cases. Hence the proposed algorithm is very efficient to protect the vital information transmitted through unsecured networks.

Keywords - Steganography;Cryptography;LeastSignificant Bit;BMP Images;Network Security; PSNR.

I. INTRODUCTION

Cryptography and Steganography are two popular techniques to protect the transmitted data over unsecured channels.Cryptography scrambles the text information so it cannot be readable or understood. Whilesteganography hides the text information so it cannot be seen. However, the combination of these methods will increases the security of the communication process.Essentially, cryptography technique can be classified assymmetric and asymmetric cryptography.In the symmetric cryptography, both the sender and the target receiver are sharing similar key to encrypt and decrypt the secret data. [1]

Steganography can be performedwith three basic elements which arethe cover media, secret message and steganography algorithm. Besides these, secret key or password also can be used to achieve better security.The cover medium could be an image, text, video or audio file. Butamong of these categories, image steganography is the most popular method and it means the process of hiding the secret data into a cover-image to get stego-image. Steganography by images is quite simple and commonly used for hiding processes. [2]In the domain of digital images many different image file formats exist but using BMP image is most popular choices for steganography processsince they arethe simplicity and wide acceptance of BMP files in Windows programs.[3]The primarily steganography methods can be classified into many categories,some common methods are Least significant bit (LSB), transform techniques and masking and filtering. LSBis one of the most efficient and popular steganography methods. [2][4]

Lately, a large number of steganography algorithm based on least significant bit method have been proposed and discussed. Author in [5] proposed a technique by using RSA and Diffie Hellman algorithm to encrypt the secret information before hiding in the cover image using LSB method. While Jamal N.[6] introduced a new system of LSB steganography which combine with a new a symmetric encryption algorithm called MJEA.It deals with the medical image and patient's information. Experimental results showed that this algorithm has a very good performance under the PSNR and MSE tests.Although there are enormous security techniques have been introduced but the aspect of security still needs to be improved and a new techniques still need to be developed.Thus, this work aims to develop steganography algorithm based on LSB method.

II. THE PROPOSED TECHNIQUE

The proposed technique is based mainly on BMP imagesand it consists of three main algorithms which areencryption, embeddedandextraction and decryption algorithm.The processes of the first algorithm as explained below:

A.Encryption Algorithm

The basic steps of this algorithm are explained as follows:

Step 1: Enter the secret message and get its length.

Step 2: Enter two characters "key1" and "key2",get the ASCII value of each character.

Step 3: Apply XOR operation between key1 and key2 as key3; Key3 = key1 XOR key2.

Step 4: Read a character from the text and get its ASCII value “Ch”.

Step 5: Divide the value obtained in the previous step by 3; Ch1=Int (Ch/3).

Step 6: Subtract thevalue obtained in step 5from the value obtained in step 4;Ch2=Ch1-Ch.

Step 7: Calculate Ch3; whereCh3 = Ch1 + Int(key1/2).

Step 8: Calculate Ch4; whereCh4 = Ch2 + Int(key2 / 3).

Step 9: Apply XOR operation between Ch3 and key3; Ch5 =Ch3XOR key3.

Step 10: Apply XOR operation between Ch4and key3;Ch6 = Ch4 XOR key3.

Step 11:Convert the values of Ch5 and Ch6 into binary.

Step 12: Repeat steps 4 to step 11 for each character in the massage.

B. EmbeddedAlgorithm

In this stage, an encryption data, the secret key (key1 and key2)and the massage length are hiding in cover image in deferent location using LSB method. Just Red“R” and Green “G” planes will be used toembedthe encryption text in the cover image.The mainsteps of this algorithm are described as follows:

Step 1: Load cover image and get its size.

Step 2: Check the cover image size with the size of secret message.

Step 3: Hiding the secret key “key1 andkey2” into cover image by applying the following:

1. Get the binary sequence of key1and key2.
2. Starting from pixel at column 13, row 2, pick up the pixel and divide it into R, G and B components.
3. Hide the least bit of “key1” in the least of byte “R”.
4. Hide the least bit of “key2” in the least of byte “G”.
5. Pick up the previous pixel and split it into R, G and B components.
6. Repeat step 3 to step 5 till the hiding of all bits.

Step 4: Hiding the length of massageinto cover image by applying the following:

1. divide the massage length “msg_len” into three blocks “B1, B2 and B3“ andget the binary number representation of each value as follows:

   B1=Int ((msg_len/1000)/1000)

   B2= Int (msg_len/ 1000) mod 1000

   B3= msg_lenmod 1000
2. Starting from pixel atcolumn 13, row3,pick up the pixel and divide it into R, G and B components.
3. Hide thebit of “B1”in the least of byte “R”.
4. Hide the bit of “B2” in the least of byte “G”.
5. Hide the bit of “B3” in the least of byte “B”.
6. Pick up the previous pixel and split it into R, G and B components.
7. Repeat step 3to step 6 till the hiding of all bits.

Step 5: Hiding the binarysequence of an encryption text by applying the following:

1. Starting from pixel atrow4, column 1, pick up the pixel and divide it into R, G and B components.
2. Hide the bit of “Ch5”in the least of byte “R”.
3. Hide the bit of “Ch6” in the least of byte “G”.
4. Jump two pixels.
5. Pick up the pixel and split it into R, G and B components.
6. Repeat step 2 to step5till the hiding of all bits.

Step 6: Save the stego-image.

C. Extractionand Decryption Algorithm

The main steps of this algorithm are described as follows:

Step 1: Load thestego-image.

Step 2: Extract the secret key “key1 and key2” by applying the following:

1. Starting from pixel at column 13, row 2, pick up the pixel and divide it into R, G and B components.
2. Pick up the least bit of byte “R” and store inkey1, where key1= 0.

3. Pick up the least bit of byte “G”and store in key2, where key2= 0.
4. Pick up the previous pixel and split it into R, G and B components.
5. Goto step 2 to get next byte.
6. Retrieve bits and convert each 8 bit into decimal valueto get the values of key1 and key2.
7. Calculate key3; wherekey3 = key1 XOR key2.

Step 3:Extract the message length “msg_len” by applying the following:

1. Starting from pixel at column 13, row3,pick up the pixel and divideit into R, G and B components.
2. Pick up the least bit of byte “R” andstore in B1,where B1= 0.
3. Pick up the least bit of byte “G”and store in B2, where B2= 0.
4. Pick up the least bit of byte “B”and store in B3, where B3= 0.
5. Pick up the previous pixel and split it into R, G and B components.
6. Goto step 2 to get next byte.
7. Retrieve bits and convert each 8 bit into decimal value to get the values of B1, B2and B3.
8. Calculate the message length “msg_len”;where msg_len=B1&B2&B3.

Step 4: Extract the text message by applying the following:

1. Starting from pixel atrow4, column 1,pick up the pixel and divideit into R, G and B components.
2. Pick up the least bit of byte “R” and store in Ch5, where Ch5= 0.
3. Pick up the least bit of byte“G” and store in Ch6, where Ch6= 0.
4. Jump two pixels.
5. Pick up the pixel and split it into R, G and B components.
6. Goto step 2 to get next byte.
7. Retrieve bits and convert each 8 bit into decimal value to get the values of Ch1and Ch2.
8. XoredCh5 with key3 as Ch3; Ch3 = Ch5 XOR key3.
9. Xored Ch6 with key3 as Ch4; Ch4 = Ch6 XOR key3.
10. Calculate Ch1; whereCh1 = Ch3-Int (key1/2).
11. Calculate Ch2; whereCh2 = Ch4-Int (key2 / 3).
12. Add the Ch1 to Ch2 as Ch;Ch= Ch1 + Ch2.
13. Convert the ASCII codeinto character.
14. Repeat step4for each character.

Step 5: Save/print the secret messageor save the image.

III. EXPERIMENT RESULTS

In this work, the experimental results has been carried out onVB6language on Intel® Core™i52.30 GHZ. Two 24-bit BMP images are used in this test. The first image is (24 x 300 x 300) and it's called “AhmedAl Bashir”. While the second image is (24 x 348 x 249) and it's called “duck”. Figure 1and figure3 show cover images before hiding process using the proposed algorithm. Whilefigure 2and figure4 show stego-images after hiding process using thisalgorithm.

Figure 1. Ahmed image before embedding

Figure 3. Ahmed image after embedding

Figure 2. Duck image before embedding

Figure 4. Duck image after embedding

The above figures clearly depict that stego-images appear to be the same as cover images and the binary data embedded has been successfully extracted.

This work is also measure steganography quality based on the PSNR (PeakSignal to Noise Ratio) and the MSE (Mean Square Error) to evaluate the distortion in the image.Four different color images were used as cover images in the experiments. Table 1 present the results of theMSE and PSNR for each imageused in this test with different file hiding.

TABLE 1. MSE AND PSNR VALUES FOR THE ORIGINAL AND STEGO IMAGES

Images	Image Dimension	Text length	MSE	PSNR
Image 1	300x300	81.920 bytes	0.0349	62.6975
Image 2	480x350	86.016 bytes	0.0368	62.4754
Image 3	600x442	356.352 bytes	0.0410	62.0033
Image 4	950x700	442.368bytes	0.0229	64.5367

The above results indicate that the newalgorithmachievedhigh PSNR values in all the various images used in the testssince PSNR >62dBin all tested cases and itmeans a high-quality images.

IV. CONCLUSION

In this work, steganography was combination with encryptiontechnique to propose a new security technique which provides an extra level of security against attacks.Experiment results gives a goodPSNR values in all tested cases and hidden text files were extracted successfully without loss any data.This algorithmis very secure andworks efficiently on both Arabic and English texts.A future workis expected to make it has ability tohide another type of multimedia data inside another types of cover images.

REFERENCES

[1] Hayfaa Abdulzahra Atee, Robiah A, hmad and Norliza Mohd Noor,"Cryptography and image steganography using dynamic encryption on LSB and color image based data hiding," Middle-East Journal of Scientific Research,vol. 23,pp.1450–1460, 2015.
[2] K.Hemachandran,"Study of image steganography using LSB, DFT and DWT," International Journal of Computers & Technology, vol.11, pp. 2618–2627,October2013.
[3] 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,vol. 3,pp. 363-372, July 2013.
[4] M. Amiri and M.R. Resketi, "An Edge method in steganography," Proceedings of World Academy of Science Engineering and Technology, vol. 37, pp. 1058-1063, 2009.
[5] Shailender Gupta, Ankur Goyal and Bharat Bhushan, "Information hiding using least significant bit steganography and cryptography," International Journal Modern Education and Computer Science, vol. 6, pp.27–34, 2012.
[6] Jamal N. Bani Salameh,"A Secure transmission approach for medical images and patient's information by using cryptography and steganography," International Journal of Computer Science and Network, vol.7, pp.289 – 303, October 2018.