International Journal of Engineering Research and General Science Volume 4, Issue 6,November-December, 2016
ISSN 2091-2730

Combination between Steganography and Cryptography in Information Hiding by Using Same Key

Orooba Ismaeel Ibraheem Al-Farraji

Lecturer in Al-Nahrain University-College of Medicine

Abstract- Steganography and cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. In my algorithm I try combine between steganography and cryptography and use same key in both ways this mean the key that use in cryptography also use in steganography.

We use transportation cipher to encrypt text by using specific key and same key that using in cryptography, again use in steganography and use LSB method in steganography with key in new technique.

Keywords: Cryptography, Steganography, Information Hiding, LSB, Transposition Cipher

1-Introduction

Cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence respectively. Steganography is the art and science of communicating in a way which hides the existence of the communication (9).

Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. To enhance the embedding capacity of image steganography and provide an imperceptible stegoimage for human vision, we propose a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access (1).

Steganography also can be implemented to cryptographic data so that it increases the security of this data – the propose algorithm is a very secure technique for cryptography and the Steganography methods, which use frequency domain, are highly secured. Even if we combine these techniques straight forwardly, there is a chance that the intruder may detect the original message. Therefore, our idea is to apply both of them together with more security levels and to get a very highly secured system for data hiding.

.As we know that-

• Hiding data is better than moving it shown and encrypted.

• To hide data in a popular object that will not attract any attention.

• In case the data is extracted, it will be encrypted. But still there is a chance that the intruder can break the code (10).

So our final goal of the Algorithm is to develop a new system which is highly secured and even if somebody retrieves the message from stego image it becomes a meaningless for any existing cryptographic techniques (2).

We use transposition cryptography and LSB (least significant bits) method in hide in image in new methods to hide text in image.

In this method we first encrypt a message using transposition cipher method and then embed the encrypted message inside an image using LSB embedding method according specific key. Hiding data using LSB modification alone is not highly secure

2- Transposition Cipher

The proposed method depicts a typical cryptographic system based on classical encryption techniques i.e. substitutions and transpositions and they are regarded as building blocks for encryption (1). Transposition technique changes the order of the letters in a message [9]. Instead of replacing characters with other characters as in the case of substitution technique, this cipher just changes the order of the characters . Transposition does not alter any of the bits in the plaintext, but instant moves the position around within it (1). Letter frequencies are preserved in the cipher text. The cipher text is the disguised form of the information. Such cipher text could be transmitted across a network or stored within a file system with the objective of providing confidentiality [10]. Here the text to be encrypted is arranged in a number of columns. The message is broken in to NXN matrix.

Often the transposition method is of a geometrical nature. In this transposition cipher method, the plaintext is written row wise in a matrix of given size, but is read out column wise in a specific order depending on a key .

Key is something the sender and the recipient agree on beforehand. Key tells the size of the matrix. To encrypt plaintext the transposition cipher writes the message in a rectangle, row by row, and reads the message off, column by column, but permutes the order of the columns based on the key. Both the length of the rows and the subsequent arrangement of the columns are defined by either a keyword or numerical key. In a regular columnar transposition cipher, any extra spaces are filled with nulls and in an irregular columnar transposition cipher, the spaces are left blank.

Write the plaintext in rows of width l and read it off by columns. Take the columns in a order defined by a key. (If you take the columns in their natural order—without using a key—, then the procedure amounts to a path transposition. The Scytale corresponds to such a columnar transposition with a trivial key).

Example: $l = 5$,

Keyword = A P P L E

Key = 1 4 5 3 2

Plaintext = T H I S I

S A C O L

U M N A R

T R A N S

P O S I T

I O N

Ciphertext: TSUTPI ILRST SOANI HAMROO ICNASN.

Written in blocks of five:

TSUTP IILRS TSOAN IHAMR OOICN ASN

The legitimate receiver of the message knows the key, its length l, and the message length r (= 28 in the example). He calculates r/l, rounds this quotient up to the next integer m (28/5 → 6), and then writes down the ciphertext in columns of length m in the order given by the key. He fills the first r mod l (= 3 in the example) columns completely, and leaves blank the last positions of the remaining columns.

3. LSB Based Image Steganography

An image is the most common type of digital media used for steganography [7]. Digital images often have a large amount of redundant data and for this reason it is possible to hide message inside image file [8]. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. These pixels make up the image's raster data. Image steganography is about exploiting the limited power of the human visual system (HVS) [2]. If any specific color is viewed closely it has been observed that single digit modifications to the contribution level are imperceptible to the human eye (i.e. a pixel with a value of (255, 255, 0) is indistinguishable from (254, 255, 0)) in RGB color representation.

3.2 Data Embedding Procedure

The encrypted message to be hidden is converted into its ASCII equivalent character and subsequently into binary digit. For an example if the character "t" is an encrypted character of the message then as ASCII value for "t" is 116 and binary value for it is 1110100.

As image comprises of pixel contribution from red, green and blue components and each pixel has numbers from the color components (for 24-bit bitmap image each of red, green and blue pixel has 8 bit) (3). At 8 bit of the color number, if we change least significant bits, our visual system cannot detect changes in pixel and thus it is possible to replace message bits with image pixel bit. For example if we consider the pixel value 10111011, and we want to store the information in the least significant bit, at the worst situation the pixel changes to 10111010, examinations shows that HVS cannot distinguish this alteration [5]. So we embed the encrypted data into least significant bits of color. If we change the LSB in a byte of an image, we either add or subtract one from the value it represents [6]. In order to hide the encrypted message, data is first converted into byte format and stored in a byte array. The message is embedded into the LSB position of each pixel. Suppose our original pixel has bits:

(r7 r6 r5 r4 r3 r2 r1 r0, g7 g6 g5 g4 g3 g2 g1 g0, b7 b6 b5 b4 b3 b2 b1 b0) In addition, our encrypted character (bytes) has some bits: (c7 c6 c5 c4 c3 c2 c1 c0).

Then we can place the character bits in the least significant of selected pixel, next character bits in the next lowest pixel, and so on. (r7 r6 r5 r4 r3 r2 r1 c2, g7 g6 g5 g4 g3 g2 g1 c1, b7 b6 b5 b4 b3 b2 b1 c0).

4. Proposed Method

To enhance the embedding capacity of image steganography and provide an imperceptible stego-image for human vision, we propose a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access. Steganography also can be implemented to cryptographic data so that it increases the security of this data [4].

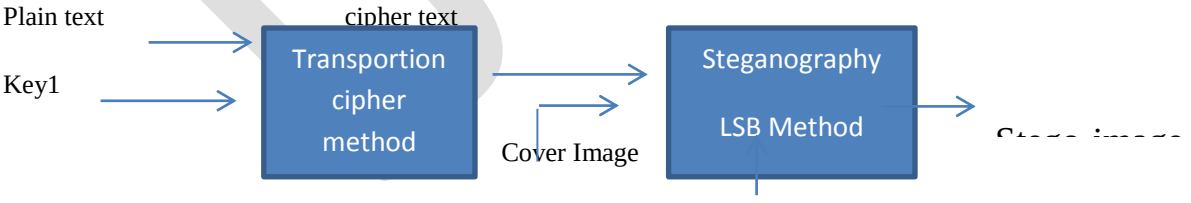

Fig1:Digram of Proposed System

4-1. Operations of Proposed System

1- Chose key to encrypt plain text

2- Encrypt the plain text by using transportation cipher according to chosen key

3- Convert encypt- text to Ascii code and then to binary

4- Chose the properly cover to hide encrypt text .

5- Start hiding crypt text in LSB in image according the key that use in transposition cipher.

6- If the key be for example 4512 that's mean the first bits from first character in crypto text will hide in lsb in pixel four and second bit from first character will hide in Lsb in pixel five and so on.

4-2.The algorithm of the proposed method

The following steps describe the algorithm:

Algorithm 1: Split the cover image

Input : plain text , key

Output : Array of binary code

Step1- input plain text , input key

Step2- Divide the plain text into four characters, four characters

Step3- Order of the letters in the form of a matrix divided every four letters are row

Step 4- Pull the columns matrix in accordance with the key then the encrypted text appears

Step 5- Convert the encrypted text to Ascii code then to binary code

Step6 – Save the binary code of encrypted text in array1

Step7 – Save key in array3

Step7-End

Algorithm 2: Split the cover image

Input : Image

Output : Array of binary code

Step1- Open Image (the bmp-file) Operation

This operation will open the bmp file and save header in a file and save the palette value of body in another file.

Step2- save the value of pixel palette in array2

Step3-End

Algorthim3: Hide encrypted text in the cover image

Input :Array1 , Array2 , key (array3)

Output : array4 (encrypt text binary inside palette of image)

Step1- Input key (array3), array1, array2

Step2- For I =1 to length of array1

Read Array1[I]

For j = 1 to 4

Read key (array3[j])

For m= 1 to length of array2

Read Array2[m]

P= array3[j] * m -2

Array2[p] = Array[I]

Array2[p+1] = Array[I+1]

Next m

Array4[m]= Array2[m]

Next j

Next I

Step3: end

Algorthim4: Extracting the Stego-image

Input :Array4

Output : Stego-image

Step1- Input array4

Step2- back header to palette (array4)

Step3: end

5- Extracting The Plain text

5-1. Operations of Extracting

1- This operation will open the stego-image file and save header in a file and save the palette value of body in another file.
2- Save the palette in array
3- According to key we start extraction the encrypt text
4- According to same key back plain text from encrypt text.

5.2- The Algorithms of Extracting

The following steps describe the algorithm:

Algorthim 1: split stego-Image

Input : Stego-image

Output : Array of binary code

---

step1- Open the stego-image file by reading the header and getting the palette of the file

Step2- Save palette in array5

Step3- end

Algorithm 2: extraction plain text

Input : Array5, key

Output : Plain text

---

step1- For I =1 to length of array4

Read Array5[I]

For j = 1 to 4

Read key (array3[j])

P= array3[j] * i -2

Array6[p] = Array5[I]

Array6[p+1] = Array[I+1]

Next j

Next I

Step 2 – Save array6 to file

Step3 – covert file to Ascii and the to characters

Step 4 – according to key rearrange the characters

Step5- print the plain text

Step6- end

Conclusion

Although its simplicity, but its implementation is not easy, and breaking it is very difficult due to the use of the key in the hiding in LSB.

- In the proposed algorithm, we use the key in cryptography and then use same key in steganography a smart way cannot be expected.

- Combination of cryptography and steganography give great strength to the algorithm against breakage , even if one of them break is difficult to break the other.

- The proposed system proved to be easy to use and efficient in terms security and help to save secret text.

REFERENCES:

[1] Domenico Daniele Bloisi , Luca Iocchi, "Image based Steganography and cryptography", Computer Vision theory and applications volume 1 , pp. 127-134 , 2014.

[2] Kharrazi, M., Sencar, H. T., and Memon, N. , "Image Steganography: Concepts and practice", In WSPC Lecture Notes Series, 2004.

[3] Aaron Miller, "Least Significant Bit Embeddings: Implementation and Detection", http://www.aaronmiller.in/thesis/ May 2012

[4] Westfeld, A., & Pfitzmann, A. (n.d.), "Attacks on Steganographic Systems: Breaking the Steganographic Utilities" EzStego, Jsteg, Steganos , and S-Tools — and Some Lessons Learned, 1-16, 2013.

[5] K.B.Raja, C.R.Chowdary, Venugopal K R, and L.M.Patnaik," A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images" Department of Computer Science Engineering, Bangalore 2005 .

[6] Shilpa Gupta1, Geeta Gujral, Neha Aggarwal, "Enhanced Least Significant Bit algorithm For Image Steganography ", IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012

[7] Anderson , R. J. and Petitcolas, F. A.P. , "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, Vol.16 No.4, pp.474-481, ISSN 0733-8716 ,1998..

[8] R., Chandramouli, and Nasir Memon.(2001), "Analysis of LSB based image steganography techniques." In Image Processing, 2001. Proceedings. International Conference on, IEEE, vol. 3, pp. 1019-1022, 2001.

[9] A. Joseph Raphael , Dr. V. Sundaram, Head & Director, "Cryptography and Steganography – A Survey", J. Comp. Tech. Appl., Vol 2 (3), 626-630 ,2016

[10] Monika1, Sudhir Yadav2, "Data hiding using Cryptography and Steganography " , International Journal of Enhanced Research in Science, Technology & Engineering ISSN: 2319-7463, Vol. 5 Issue 4, April-2016