RESEARCH PAPER | Computer Science | Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images

KEYWORDS: Steganography, LSB Technique, Cryptography and Encryption

Mamta Juneja
Assistant Professor,
Uiet, Panjab University, Chandigarh, India

Parvinder Singh Sandhu
Professor,
Rbiebt, Sahauran, Punjab, India

ABSTRACT *Communication is the backbone of any enterprise. Communication, without exchange of data, is unimaginable. Security measures must be incorporated into computer systems during transmission of data whenever they are potential targets for malicious or mischievous attacks. This is especially for systems those handle financial transactions or confidential, classified or other information whose secrecy and integrity are critical. This paper proposes an Enhanced form of LSB based Steganography which embeds data in only 2-3-3 LSBs of red, green, blue components respectively of each pixel. This helps to achieve better capacity and immunity to suspicion. In addition, it provides means for secure data transmission using Data Encryption Standard algorithm. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.*

I. INTRODUCTION

A. Cryptography

It often used in situations where the existence of the message is clear, but the meaning of the message is obscured. In particular, the sender transforms (encrypts) the message into a form that only the intended recipient of the message can decrypt and read. Encryption is the process of encoding a message in such a way as to hide its contents. To begin with, encryption may make the existence of the message even more difficult to detect, due to the fact that some encryption techniques cause the patterns of the characters in the encrypted version to be more random than in the original version. In addition, even if the existence of the encrypted message is detected, it is unlikely that an eavesdropper will be able to read the message.

Modern Cryptography includes several secure algorithms for encrypting and decrypting messages. They are all based on the use of secrets called keys. A cryptographic key is a parameter used in an encryption algorithm in such a way that the encryption cannot be reversed without the knowledge of the key.

B. Steganography

Steganography is the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows the existence of the message; this is in contrast to cryptography, where the existence of the message itself is not disguised, but the content is obscured. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves, to messengers, or to recipients.

B1. Image Steganography

Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques some are more complex than others and all of them have respective strong and weak points. As stated earlier, images are the most popular cover objects used for steganography. In the domain of digital images many different image file formats exist. For these different image file formats, different steganography algorithms exist [1-3].Three types of steganography techniques used for image are:

a) LSB techniques
b) Masking and filtering techniques
c) Algorithms and transformation techniques

B1.1 LSB Technique

The most widely used technique to hide data is the usage of the LSB- Least Significant Bit technique. Least Significant Bit insertion method is a simple approach to embed information in a cover file [4]. The LSB is the lowest order bit in a binary value. This is an important concept in computer data storage and programming that applies to the order in which data are organized, stored or transmitted [5]. Usually, three bits from each pixel can be stored to hide an image in the LSBs of each byte of a 24-bit image.

Consequently, LSB requires that only half of the bits in an image be changed when data can be hidden in least and second least significant bits and yet the resulting stegoimage which will be displayed is indistinguishable to the cover image to the human visual system [6]. When using a 24-bit image, a bit of each of the red, green and blue color components can be used, since they are each represented by a byte. In other words, one can store 3 bits in each pixel. An 800 × 600 pixel image, can thus store a total amount of 1,440,000 bits or 180,000 bytes of embedded data [7]. For example a grid for 3 pixels of a 24-bit image can be as follows:

(00101101 00011100 11011100)
(10100110 11000100 00001100)
(11010010 10101101 01100011)

When the number 200, with binary representation 11001000, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:
(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

Although the number was embedded into the first 8 bytes of the grid, only the 3 underlined bits needed to be changed according to the embedded message. On average, only half of the bits in an image will need to be modified to hide a secret message using the maximum cover size [8]. Since there are 256 possible intensities of each primary color, changing the LSB of a pixel results in small changes in the intensity of

Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

the colors. These changes cannot be perceived by the human eye and thus the message is successfully hidden.

With a well-chosen image, one can even hide the message in the least as well as second to least significant bit and still not see the difference. In the above example, consecutive bytes of the image data from the first byte to the end of the message are used to embed the information. This approach is very easy to detect [9]. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed. Should an adversary suspect that LSB steganography has been used, he has no way of knowing which pixels to target without the secret key [10]. In its simplest form, LSB makes use of BMP images, since they use lossless compression. Unfortunately to be able to hide a secret message inside a BMP file, one would require a very large cover image.

B1.2 Implementation of LSB Technique

To illustrate implementation of LSB technique, consider figure 1 of parrots showing true colors Image.

Figure 1: Parrot (True Color Image)

This image is composed of red, green, and blue color channels as shown in figure 2. The pixel at the top-left corner of the picture has the values 122, 119, and 92 for its red, green, and blue color components respectively. In binary, these values may be written as 01111010 01110111 01011100.

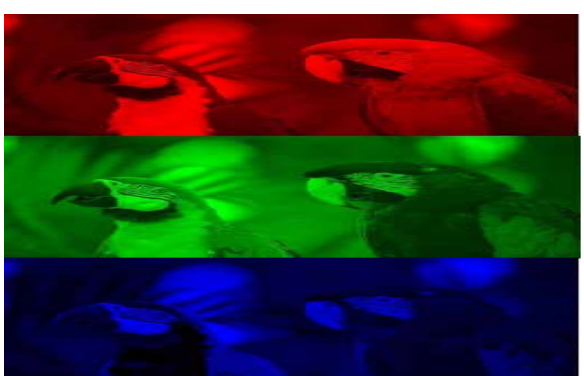

Figure 2: Red, Green and Blue color channels of Parrot Image

To hide the character "a" in the image, the LSB (the rightmost bit) of each of the three 8-bit color values above will be replaced with the bits that form the binary equivalent of the character "a" (i.e., 01100001). This replacement operation is generally called embedding. After embedding, the color value would now change to 01111010 1110111 01011101.

Since there are only three values, only three of the eight bits of the character "a" can fit on this pixel. Therefore the succeeding pixels of this image will also be used. In the three color values shown above, only the last value actually changed as a result of LSB encoding, which means almost nothing has changed in the appearance of the image. Nevertheless, even in case wherein all LSBs are changed; most images would still retain their original appearance because of the fact that the LSBs represent minor portion (roughly 1/255 or 0.39%) of the whole image. The resulting difference between the new from the original color value is called the embedding error. Since there are only three LSBs for each pixel, the total number of bits that can be hidden is only three times the total number of pixels having the dimensions 768x512.

II. THE PROPOSED APPROACH

The proposed approach here uses the following techniques to overcome the difficulties discussed above in existing systems.

A. 2-3-3 LSB substitution based Steganography: It proposes an enhanced form of LSB based Steganography which embeds data in only 2-3-3 LSBs of red, green, blue components respectively of each pixel. This combination has been decided after experimenting with different combinations of the number of bits of red, green and blue components. This ensures better capacity and immunity to get detected across communication media by any intruder.

B. Steganography and Cryptography in combination: Steganography messages are often first encrypted by some traditional means, and then a cover text is modified in some way to contain the encrypted message, resulting in stegotext. So, to take best advantage of their respective features and to provide more robust, secured system, proposed approach combines 2-3-3 LSB substitution based Steganography with DES (Data Encryption Standard) algorithm [13] .The message is encrypted before it is hidden inside a cover message. This provides a double layer of protection. DES is the most widely used encryption algorithm in the world. From many years and For many people, "secret code making" and DES have been used as synonymous. DES works on bits or binary numbers i.e. 0s and 1s common to digital computers. Each group of four bits makes up a hexadecimal, or base 16, number. It works by encrypting groups of 64 message bits, which is the same as 16 hexadecimal numbers. To do the encryption, It uses "keys" which are also apparently 16 hexadecimal numbers long, or apparently 64 bits long. However, every 8th key bit is ignored in the DES algorithm, so that the effective key size is 56 bits. But, in any case, 64 bits (16 hexadecimal digits) is the round number upon which it is organized.

III. DESIGN AND IMPLEMENTATION OF PROPOSED SYSTEM

The Proposed system as shown in figure 3 consists of mainly four modules: Encryption module, Embedding module, Extraction module and Decryption module

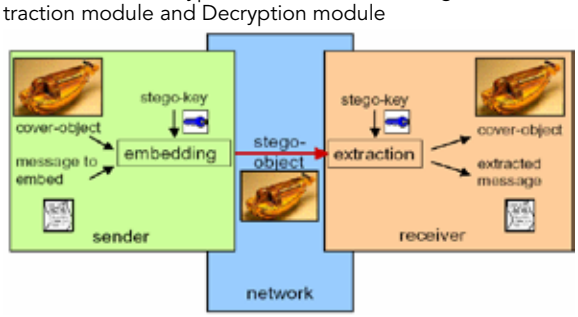

Figure 3: The Proposed system

A. Encryption module: It encrypts the message to be hidden using DES method as mentioned above in Section II .B. It is done by passing a secret key which is used for encryption of the message to be hidden .It provides security by converting it into a cipher text, which will be difficult for hackers to decrypt. Moreover if the message is password protected, then while retrieving message, the retriever has to enter the correct password for viewing the message.

B. Embedding module: It embeds the encrypted message in cover image using 2-3-3 LSB substitution based Steganography as mentioned above in Section II.A. It in-

Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

volves embedding the message into the cover text. Each pixel typically has three numbers associated with it, one each for red, green, and blue intensities, and these values often range from 0-255.In order to hide the message, and data is first converted into byte format and stored in a byte array. The message is then encrypted and then embeds each bit into the LSB position of each pixel position. This program hides the message in the image by doing the following:

a. Reducing the message to the 64-character set beginning with the space character in the ASCII table. Each character can then be represented by eight bits.
b. Decomposing each eight-bit character into three groups of 2-3-3.
c. Replacing the two least-significant bits (LSB) in the red, 3 bits of green, and 3 bits of blue values for a given pixel by the three groups of message bits. Thus, each pixel can carry one character.

C. Extraction module: It extracts the hidden message from cover image. It involves retrieving the embed message from the file independent of the file format. Once the message has been retrieved it has to be converted into original message or file. This can be done by reading the embedded data from the master file. The read data will be in the bytes format. This message has to be converted into the suitable output file format.

D. Decryption module: It decrypts the encrypted message to retrieve the original message. Decryption includes a message or a file decrypting. Decryption involves converting the cipher text into decrypted format. Decryption can be done by passing a secret key. Secret key can be used for decryption of the message that is hidden. It provides security by converting the cipher text, into the original data message or file . Moreover if the message is password protected, then while retrieving message, the retriever has to enter the correct password for viewing the message.

Encryption and Embedding Modules form the modules at the sender side. Extraction and Decryption Modules form the modules at the receiver side.

So, on the whole the steps followed by the proposed system as shown in Figure 4 are:
1. Authenticating the user.
2. Encryption of message or file to be embedded.
3. Embedding of message data/file to cover image.
4. Extraction of message data/file from cover.
5. Decryption of message data.

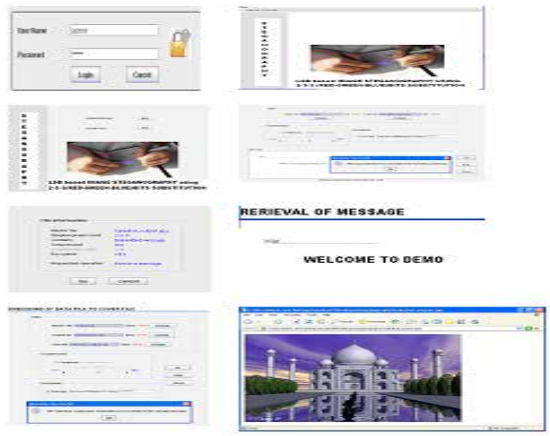

Figure 4. Snapshots of Proposed System

a) Login Form b) Main window c) Decoding Window

d) Embedding message in a master file e) Master File Information f) Retrieved message from master file g) Embedding a file in a master file h) Retrieved file from the master file.

IV CONCLUSION

The proposed approach provides means for secure data transmission and secure data storage network. Hereby, important files carrying confidential information can be stored in the server in an encrypted form. Access to these files is limited to certain authorized people only. Transmission also takes place in an encrypted form so that no intruder can get any useful information from the original file during transit. Further, before trying to access important files, the user has to login to the system using a valid username and password, which is allotted to him by the system administrator.

The proposed approach hides any kind of files including text, picture files, audio files, video files. Cover text can be picture, audio or video files in any format. It provides the option for compressing the contents to be hidden. An encryption password option has been provided, to provide extra security.

REFERENCE [1] B.Schneier, "Terrorists and Steganography", 24 Sep. 2001, available:http://www.zdnet.com/zdnn/stories/comment/0,5859,2814256,00.html. | [2] Y. Linde, A. Buzo, and R. M. Gray, "An Algorithm for Vector Quantizer Design," IEEE Transactions on Communications, pp. 84-95, January 1989. | [3] Andersen, R.J., Petitcolas, F.A.P., On the limits of steganography. IEEE Journal of Selected Areas in Communications, Special Issue on Copyright and Privacy Protection 16 No.4 (1998) 474-481. | [4] Johnson, Neil F. and Jajodia, Sushil. "Steganography: Seeing the Unseen." IEEE Computer, February 1998, pp.26-34. | [5] William Stallings; Cryptography and Network Security: Principals and Practice, Prentice Hall international, Inc.; 2002.[2] | [6] Eric Cole ,"Hiding in Plain Sight: Steganography and the Art of Covert Communication" | [7] Gregory Kipper,"Investigator's Guide to Steganography " | [8] Stefan Katzenbeisser and Fabien, A.P. Petitcolas ," Information Hiding Techniques for Steganography and Digital Watermarking " | [9] Hiding secrets in computer files: steganography is the new invisible ink, as codes stow away on images-An article from: The Futurist by Patrick Tucker | [10] Ismail Avcıbas,, Member, IEEE, Nasir Memon,Member, IEEE, and Bülent Sankur, Member, "Steganalysis Using Image Quality Metrics," IEEE Transactions on Image Processing, Vol 12, No. 2,February 2003.. | [11] Niels Provos and Peter Honeyman, University of Michigan, "Hide and Seek: An Introduction to Steganography" IEEE Computer Society IEEE Security &Privacy. | [12] R. Chandramouli and Nasir Memon, "Analysis of LSB Based Image Steganography Techniques", IEEE 2001. | [13] (FIPS), F. I. P. S. "Data encryption standard (des)" , Federal Information Processing Standards Publication, October 25,1999.