International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869, Volume-3, Issue-3, March 2015

ONLY-BLUE LSB Steganography- A new proposed approach for improvised quality and distortion free image

Bharat Sinha, Deepali Gupta

***Abstract*— We are living in an era where everyday something new is created. These innovations are making our lives easier in terms of efforts, speed, communication etc. The increasing amount of this ever expanding list of inventions is making the entire population dependent on it for accomplishing its day to day task. This high correlation is good for us but with every good comes a bad. This huge dependency can be used for a wrong purpose by exploiting these huge correlations. Thus, a need of security for this necessity of human race is very important. It is the right of every human to have its fair amount of privacy which is being exploited by various measures. Thus, a huge amount of work is continuously being done for attain privacy specially communication.**

Due to this fact the art of information hiding have captured the spotlight in security. One such technique to provide secure communication is the Steganography which is used to hide messages behind an overlaying object thus, avoiding spoofing by unauthorized entity. Steganography has become the hero in terms of security and privacy of data and communication. A huge array of algorithms has been developed for Steganography. One such algorithm is LSB which is the most easy and popular algorithm in terms of spatial domain of image processing.

This proposed technique is an improvement over the conventional LSB. Only-Blue LSB takes care of the quality aspect of the image after the embedding of message. It targets LSB of blue component only unlike conventional LSB thus, providing lesser distortion from real image and thus, making it impossible to analyze it visually and providing better security and privacy of data.

***Index Terms*— blue, quality, LSB, steganography.**

I. INTRODUCTION

A. Cryptography

Cryptography is a method of storing and transmitting data in particular form so that only those for whose it is intended can read and process it. The term is most often associated with scrambling plain text into cipher text(a process called encryption),and then back again to plain text (called decryption).Encryption is the process of encoding the message to hide its content.[1]

The modern field of cryptography can be divided into several areas of study. The chief ones are the symmetric Key-cryptography and public key-cryptography. It uses several algorithms for encrypting and decrypting the message using the keys. The algorithms cannot be implemented without the keys.

Manuscript received March 23, 2015.

Bharat Sinha, Department of Computer Science and Engineering Galgotias College of Engineering and Technology, Greater Noida, India

Deepali Gupta, Department of Computer Science and Engineering Galgotias College of Engineering and Technology, Greater Noida, India

B. Steganography

Steganography is the art of covered or hidden message such that no one apart from intended recipient knows that the message really exists. This differs from the cryptography, which is makes the message unreadable to the third party, but does not hide the existence of secret communication.[8] The advantage of steganography over cryptography alone is that the intended secret message does not attract attention to itself as an object of scrutiny

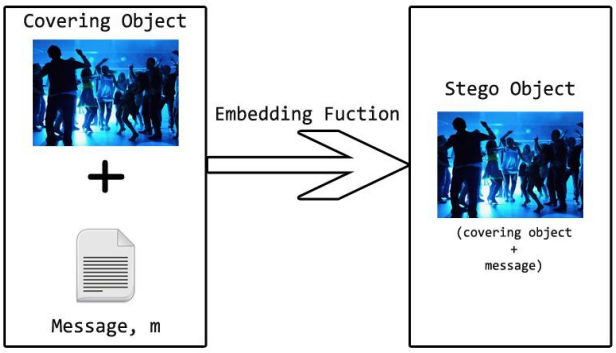

Fig 1.Steganography Process

Steganography differs from cryptography in the sense that where cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret. Steganography and Cryptography is both ways to protect information from unwanted parties but neither technology alone is perfect and can be compromised. [3]

B1.Image Steganography

Image steganography techniques can be divided into two groups: the one in the Image Domain and the other in the Transform Domain. Image – also known as spatial – domain techniques embed messages in the intensity of The pixels directly, while for transform – also known as frequency – domain, images are first transformed and Then the message is embedded in the image [3].Image domain techniques encompass bit-wise methods that apply bit insertion and noise manipulation and are Sometimes characterized as “simple systems”. Image steganography is used for hiding the secret messages under the images.There are large variety of steganography techniques, some of which are more complex than the others. For different image file formats such as JPEG, JPG, PNG, GIF, TIF different steganography techniques are

used. There are three types of steganography techniques .They are-
a) LSB techniques
b) Masking and filtering techniques
c) Algorithms and transformation techniques

B1.1LSB Technique
Least significant bit (LSB) insertion is a common and Simple approach to embed information in an image file.[4].It is lowest order bit in binary value. In this the LSB of a byte is replaced by M's bit. This works best with the image .to the human eye, stegano image looks just like carrier image. When the data is embedded subsequently to the all bytes of cover image, it would be rather easy to detect and extract the message It is important concept in programming and computer data storage. It applies in order in which data is organized, stored or transmitted.

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 [3].

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, which binary representation is 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 an average, only the half of the bits in an image will be needed to be modified to hide a secret message using the maximum cover size. [3] Since there are 256 possible intensities of each of the possible color which are red, green and blue, changing the LSB of the pixel image of each color results in changing the intensity of the color of the image. These Changes cannot be perceived by the human eye - 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.

With a well chosen image, we can hide the secret message in the least as well as in the second least significant bit and even then not see any difference. In the previous example consecutive bytes of image data from the first bit to the end bit are used to embed the information. This approach which is used can be used to easily detect. A slightly more secure system is for the sender and receiver to share a secret key that specifies only certain pixels to be changed.

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.

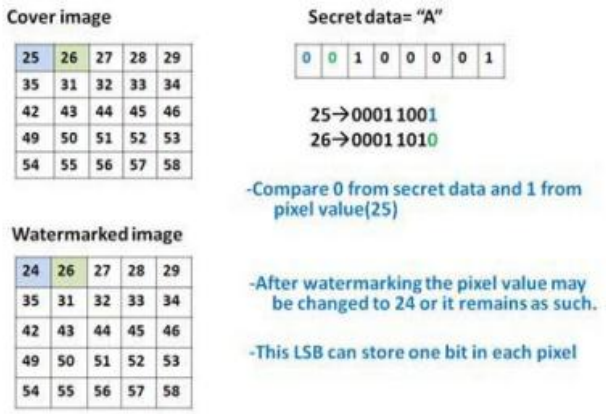

Fig 2 an Example of LSB Technique [8]

B1.2.Implementation of LSB Technique
To illustrate implementation of LSB technique, consider figure 2 of flower showing true colors Image as well as composed of red, green, and blue color channels. 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. 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, red green and blue and 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.
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. [1]

II. THE PROPOSED APPROACH

The proposed technique which promises to improve visual quality of image after Steganography is stated as under:

A. Only-Blue LSB Algorithm is the improvement suggested over regular LSB algorithms where instead of substituting Red, Green and Blue components of a pixel we just target blue components and substitute them to hide our message, m.
B. This approach concentrates on the Visual quality of image after steganography such that it becomes hard

to analyze an image visually and find out the imperfections in image

C. It improves quality and at the same time decreases the size of file which can be hidden in the image as we are just targeting the Blue pixels.

D. As blue component is the last in any pixel belonging to RGB color model, thus, taking its LSB will affect the image the least as compared to substitution made in MSB or LSB of red or green component.

E. It makes a slight compromise on the storing capacity but it gets overshadowed by the quality of stego object obtained.

III. DESIGN AND IMPLEMENTATION OF PROPOSED SYSTEM

The detailed description and the proposed algorithm is stated as under

A. Each Color image consist of tiny pixels having three color components i.e. RGB (Red, Green, Blue) which forms the entire image. Based on quality of image the number of bits per pixel or color depth varies. The higher the number of bits higher will be the quality of image.

Fig 3 Image in Blue Color Channel

Fig 4 Image in Green Color Channel

Fig 5 Image in Red Color Channel

B. The Embedding function, E which gives out stegano object as output on passing covering object and message as a parameter undergoes following steps :

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. The Covering object is scanned each pixel at a time and the last bit of blue component is targeted and substituted with the message bit.

c. The resultant is a stego object which has the message hidden underneath the covering object.

C. The Extraction module working is exactly opposite of the embedding module. The working is explained as under:

a. The stegano object is scanned each pixel at a time and the last bit of the blue component is extracted.

b. Grouping is done with each group consisting of 8 bits and are matched against the ASCII table to extract their real value.

c. The Message is formed by combing all the characters together.

D. The whole process mentioned above provided better quality of Stegano object and thus, preventing visual analysis of message.

E. If image used as a covering object is 640 x 480, 24 bit image then the storing capacity will be 38400 bytes or 37.5Kb which is far less than conventional LSB i.e. 921600 but the level of distortion is marginally less.

Fig 6 Image before Steganography

Fig 7 Image after Steganography

IV.CONCLUSION

This approach is just a small contribution towards the growing popularity of the art of Steganography. This process discussed above is useful in a scenario where quality of final image is more important than the quantity of message to be hidden.

REFERENCES

[1] Parvinder Singh Sandhu "*Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images*" Volume : 3 | Issue : 5 | May 2013 | ISSN - 2249-555X

[2] T. Morkel, J.H.P. Eloff, M.S. Olivier "*An Overview of Image Steganography*" Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.

[3] Shilpa Gupta , Geeta Gujral and Neha Aggarwal "*Enhanced Least Significant Bit algorithm For Image Steganography*" IJCEM International Journal of Computational Engineering & Management, Vol. 15 Issue 4, July 2012 ISSN (Online): 2230-7893 www.IJCEM.org

[4] B.Schneier, "*Terrorists and Steganography*", 24 Sep. 2001, available:http://www.zdnet.com/zdnn/stories/comment/0,5859,2814256,00.html.

[5] Johnson, Neil F. and Jajodia, Sushil. "*Steganography: Seeing the Unseen*." IEEE Computer, February 1998, pp.26-34.

[6] Niels Provos and Peter Honeyman,University of Michigan, "*Hide and Seek: An Introduction to Steganography*" IEEE Computer Society IEEE Security &Privacy

[7] Koyi Lakshmi Prasad "A Novel Secured RGB LSB Steganography with Enhanced Stegano-Image Quality" ISSN:2248-9622,Vol.3,Issue6,Nov-Dec 2013,pp.1299-1303.

[8] Gary C.Kessar "*An Overview of Steganography for the Computer Forensics Examiner"* February 2004 (updated June 2014).