International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 3, Issue 8, November 2014, pp.355-358, ISSN 2278 -1412

A Review on Comparison between Different Image Steganography Methods

Arun Kumar Sonaniya[1], Rajesh Kumar Rai[2]
[1]M. Tech Scholar, NIIST, RGTU, arun.sonaniya@gmail.com, Bhopal (M.P.) India;
[2] Professor, Electronics Department, NIIST, RGTU,raj.rai1008@gmail.com, Bhopal (M.P) India;

Abstract - *Steganography is the art of hiding the data by hiding the information in the different medium. There are many different carrier files can be used, but digital images are the most popular. There are many different methods are using in the modern era which can help to maintain the securer communication. This paper presents a detailed description of some important steganography methods for secure communication.*

I. Introduction

The word Steganography is derived from the Greek word steganos meaning 'Secret or covered' and grapy meaning writing or drawing. In this way the exact meaning of Steganography is the secret writing or drawing [7]. Basically Steganography is one type of information hiding technique.

Technical Steganography are of many following types:-

1. In digital images 2. In videos
3. In audios. 4. In plain text.

In image steganography, information is hidden in the images. Steganography mainly consist of two process named embedding and extracting process. In embedding process, is to hide the secret message called embedded message, in a given image called cover image. In hidden communication techniques, the cover image is no more than an innocent piece of information that is used to hide that secret information. A secret key called stego key is used in the embedding process such that it makes a embedded message computationally infeasible to extract without possessing this key. The ouput of the embedding process is called stego image which is the orginal image holding the hidden secret message [1]. This output becomes at the order and the input of the extracting process in which the embedding message is extracted from the stego image to complete the hidden communication process. Since the stego key is used in embedding process it need to be used in the extracting process.

Cryptography is also used for hiding the information. But some difference approach for Steganography is that conceals information, making it unseen. Breaking of Steganography is called steganalysis. Whereas the cryptography is encrypt the information, making it unreadable [13]. Crypto+steno= added layer of security (one complement the other). Breaking of cryptography is called cryptanalysis. Watermarking and finger printing related to Steganography are basically used for intellectual property protection. A digital water mark covertly embedded in a noise tolerant signal such as audio or image data.

II. Image Steganography

An image is a picture which has been created or taken from any sources and stored in any type of electronic form. An image can be described in terms of vector graphics or in other form raster graphics. An image which is stored in raster form is occasionally called a bitmap. An image map files containing secret information that associates different locations on the defined image with hypertext links. An image is defined as collection of many numbers that constitute other form of light intensities in different areas of the image. This kind of numeric pixel, grey scale images which use 8 bits for each pixel and which make able to display 256 different colours or shades of grey colour. Digital colour images are typically stored in 24-bit files and use the RGB colour model, also known as true colour. All colour have different variation for the pixels of a given 24 bit images which are derived from the primary colours namely red, green and blue. And each primary colour which is represented by 8 bit. Thus in one given pixel there can be 256 different quantities of the primary colour namely red, green and blue.

III. Image Compression

Image has two types of compression namely lossy compression and lossless compression [8].In lossless compression, every single bit of information which was

originally in the containing file remains after the file will be uncompressed. All other information is completely restored as required. The very most popular image have a formats which was that use lossless compression is in GIF (abbreviation as graphical Interchange Formats) And BMP (abbreviated as bitmap file) Lossy compression reduces a file by eliminating a some information, especially redundant information. When file will be uncompressed, only a some part of original information which is still there. In this case, the obtained resulting image is expected to be similar as original message image. But not the exact same as the original one. An example of an image format which uses this kind compression technique which is JPEG (abbreviated as Joint Photo graphics Experts Group) [9].

III.1 Image Steganography techniques

There are many several Steganography methods for following the given image file format are:-

III.1.1 Spatial or Image Domain

This is one of the types of domain and there are many version of spatial Steganography all which are directly makes changes bit in the image pixel in process of hiding data. Least significant bit (short form is LSB) is one of the simplest Steganography techniques that hide secret information in LSBs of pixel values without any type of distortions. For our human eye, changes in LSB value are imperceptible. Embedding of message can be processed either in simple manner or randomly other manner. Following are the examples spatial domain technique are LSB replacement, Matrix embedding and many more. Special domain or image domain techniques are classified into the following types:

1. Least significant bit (LSB)
2. Pixel value differencing (PVD)
3. Edges based data embedding (EBE)
4. Random pixel embedding method (RPE)
5. Mapping pixel to hidden data method

LSB is very common, easy approach for embedding the information in a cover image. And also in this approach, some of or all the bytes inside a image is changed to a bits of secret image.
For example, when we embedding by using 24-bit image, It can be follow as

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

The above number is 200, which in binary reorientation 11001000 is hide into LSB technique and
The result obtained is

(00101101 00011101 11011100)
(10100110 11000101 00001100)
(11010010 10101100 01100011)

The number was hidden into 1st 8 bytes of the image, only selected 3 bolded bits is needed to change according to desired message.
As there are 256 possible intensities of colures. Each of primary colour, make LSB pixel results in small changes in intensity of colours.All the changes are not be perceived by human eye- In this way, the given message is successfully hide into the image. A very simplest form, LSB makes use of BMP images because they give a lossless compression, but to hide a image in BMP, we have to require a very large cover image. In internet and might arouse suspicion where the images of 800x600 pixels are not used. Due to this reason, LSB have a other option with other image file formats.
In palette based images, where GIF images as example are commonly used on the internet.GIF image have a bit depth less than 8, that make a GIF to store is 256.
And GIF images are those images where the colours are placed in a palette, are also referred as colour lookup table. The palette colours are ordered in a way that colours is to be least for reducing the lookup time.
The final solution to above problem is to use grayscale images, an 8 bit GIF images where 256 different shades of grey. The changes are made is between the colours are very gradual and hard to detect.
Advantages of LSB spatial domain technique are as follows:-

1. Original image is not easily degraded.
2. More information is easily stored in image. I.e. hiding capacity is more.

Disadvantages of LSB spatial domain technique are as follows:-

1. Low robustness.
2. Anyone can destroy the hidden data by simply attack

III.1.2 Masking and Filtering

Both the above are Steganography technique, used on the gray-scale images. Both are similar to placing watermarks on the image which is printed. All these techniques are embedding the message more significant areas than hiding the message into the noise level. Watermarking method for hiding the information is applied without the fear of destruction of image due to lossy compression as all are more integrated into the images.
Advantages of masking and filtering technique - It is very more robust than LSB replacement w.r.t to compression.
Disadvantages of masking and filtering technique -This technique only can be done on gray scale images and also bounded to 24 bits only.

III.1.3 Transform domain Technique

Information is in frequency domain which is inserted into transformed as coefficient of image which giving more

exact information whose hiding capacity and also more robustness provided against all types of attacks.
This domain embedding is termed as a domain embedding technique for which a numbers of algorithms have been suggested [10]. Most of them strong steganography systems, all operate in the transform domain techniques have a advantage over LSB technique, which hiding the information in images areas that are very less exposure for compression, cropping and image processing. Some of this transform domain technique is not seem dependent on image format and all may out run lossless and also lossy format conversions.
Transform domain techniques are of various types are:-

1. Discrete Fourier Transformation technique (DFT).
2. Discrete cosine transformation technique (DCT).
3. Discrete wavelet transformation technique (DWT).

III.1.4 Distortion Techniques

This technique store the information by distortion of signal and also measure the deviation of information from the original cover image during the process of decoding of cover image [11]. The decoder processor is checking the difference between the original cover image and deviated distorted image in order to restore the secret information. In this way, a stego image is created by doing the various sequence of modification to the cover image, which is used to match the secret message required to transmit [12].
The information is encoded at pseudo randomly which had chosen the pixels. If the stego image is differ away from cover image at any given pixels. The message bit is a 1.otherwisw the message bit is a 0.
The encoders modify value 1 in such a way that statistical properties of image are not defected. If an attacker is going to attack with the stego image by various methods like cropping, rotating etc, then the receiver can easily detect the attacks done by attackers.

Characteristic features of data hiding techniques

1. Perceptibility on embedding information distort cover medium to unvisually acceptable levels.
2. Capacity indicating how much the information can be hidden with related to changes in perceptibility.
3. Robustness means the attacks can embedded data exist manipulation of stego medium in efforts for destroying or make changes in the original information's.
4. Tamper resistance which is beyond robustness for destruction. It is difficult to changes a information by attackers after once a embedded in a stego images.

IV. Literature Survey

In [1] author has proposed a method which is special domain Adaptive LSB method. It divides the pixels and generates a key which is known as stego key. This key can divide into 5 gray level ranges each indicate the fixed no. of bits in LSB of image. This method is high capacity and secure for hidden massage.

In [2] author proposed pixel value difference (PVD) in which the size of hidden data is estimate by difference between two consecutive pixels in cover image. This method can hide large data at the edge area of image. This method is more complex than adaptive LSB.

In [3] author proposed a method of multi pixel differencing which is use for more than two pixel for smoothness of each pixel. This method calculate sum of difference value of four pixel block. For small difference it uses LSB and for high difference it uses MPD method. This method having good strength but experimental database is limited.

In [4] author proposed a method which is DCT based data hiding method. It can hide color information in a compress gray level image. This method achieves all the methods in steganography like color quantization, color ordering, and data hiding. This method gives free access to everybody but not for all colors it restricted some color those who have its stego key.

In [5] author proposed a data scheme in which authentication is required to verify the indignity of secret massage from stego image. In this method the hidden massage is transformed from special domain to DWT and then verifies the code and embedded in the special domain of cover image. It also verifies each row of image.

In [6] author proposed a scheme for binary images. This method is not using for gray scale image or color images. In this method compressed data is used and the bit depths of quantized coefficients are also embedded into some code block.

V. Critical Analysis

The following are the parameters which give a very detailed and required analysis of Steganography:-

1. **Capacity-** It needs to embedding only a small part of copyright information, which hidden the messages and also requires sufficient embedding capacity of approach.
2. **Perceptual** - The invisibility of algorithm is first and foremost requirement and strength of technique in its ability to be unnoticed by the human eye. When one can see that an image has been tampered and also the compromised of algorithm.
3. **Robustness-**Statistical steganalysis is the practice of hidden information through the statistical test on the given image data.

Algorithm make a signature when hiding the information easily detected through this kind of analysis. Such as cropping or rotating work to be done on the images before it reaches its destination.

4. **Temper-** it is a process in which message can be retrieve , make changes, or to do any unnecessary inside the image where the information is hidden. For good embedding process of information, this temperness should be very less.

TABLE-I

The following table indicates the analysis of various domain along with their properties.

Lit. Ref.	Domain	Technique	Capacity	Robustness	Temper	Perceptual
1	Special	Adaptive LSB	Y	N	N	N
2	Special	PVD with Adaptive LSB	Y	N	N	Y
3	Special	MPD with LSB	Y	N	N	Y
4	Transform	DCT Coefficient based	N	N	Y	Y
5	Transform	DWT Coefficient permuted and embedding in special domain	N	N	N	N
6	Transform	Secret bits plus bit depth embedded in coded block	N	N	Y	Y

VI. Conclusion

In this paper only some main image steganography techniques were discussed but there exist of large number of methods for the hiding the data into the images. All the methods having different strong and weak points respectively. We have critical analyze the different methods to increase the limit of the different methods.

References

[1] Y. K. Jain and R. R. Ahirwal, "A Novel Image Steganography Method With Adaptive Number of Least Significant Bits Modification Based on Private Stego-Keys", International Journal of Computer Science and Security (IJCSS), vol. 4, **(2010)** March 1.

[2] C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. **(2008)** September 3, pp. 488-497.

[3] K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), **(2008)** August 28-30, pp. 355-358.

[4] M. Chaumont and W. Puech, "DCT-Based Data Hiding Method To Embed the Color Information in a JPEG Grey Level Image", 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, copyright by EURASIP, **(2006)** September 4-8.

[5] K. S. Babu, K. B. Raja, K. Kiran Kumar, T. H. Manjula Devi, K. R. Venugopal and L. M. Pataki, "Authentication of secret information in image steganography", IEEE Region 10 Conference, TENCON-2008, **(2008)** November, pp. 1-6.

[6] S. Ohyama, M. Niimi, K. Yamawaki and H. Noda, "Lossless data hiding using bit depth embedding for JPEG2000 compressed bit-stream", Journal of Communication and Computer, vol. 6, no. 2, **(2009)** February**.**

[7] Pfitzmann, B., Information hiding terminology - results of an informal plenary meeting and additional proposals. In: Proceedings of the First International Workshop on Information Hiding. Springer-Verlag, London, UK, pp. 347–350. **(1996)**.

[8] Moerland, T., "Lossy and lossles", *Leiden Institute of Advanced Computing Science*,
www.liacs.nl/home/ tmoerl/privtech.pdf

[9] Johnson, N.F. & Jajodia, S., "Exploring Steganography: Seeing the Unseen", *Computer Journal*,
February 1998

[10] N. F. Johnson and S. Katzenbeisser, "A Survey of steganographic techniques. in Information Hiding Techniques for Steganography and Digital Watermarking,S.Katzenbeisser and F.Petitcolas, Ed. London: Artech House, **(2000)**, pp. 43-78.

[11] H. S. Majunatha Reddy and K. B. Raja, **(2009)** High capacity and security steganography using discrete wavelet transform. International Journal of Computer Science and Security. pp. 462-472.

[12] S. C. Katzenbeisser. Principles of Steganography. in Information Hiding Techniques for Steganography and Digital Watermarking", S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, **(2000)**, pp. 43-78

[13] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", *Communications of the ACM*,
47:10, October 2004