ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 7, January 2014

A Review on Different Image Steganography Techniques

Anjali Tiwari, Seema Rani Yadav, N.K. Mittal

Abstract- Digital steganography is considered as method hiding information on another data structure such that the observer cannot suspect hidden information the virtual absence of the hidden data is achieved by stenographic technique. Although the steganography covers many combinations of covering data and hidden data like text to text, image to text, image to image etc. in this paper we are presenting some recent development in the field of image to image steganography the particular field is selected because of its large data hiding capability and difficulties in identification. It also provides greater scope because of its large sharing over social networks.

Keywords: **Steganography, data hiding, Information hiding, spatial domain and transform domain steganography, Cover writing.**

I. INTRODUCTION

Steganography aims to hiding information in a cover data in such a way that non-participating persons are not able to detect the presence of this information by analyzing the information detection. Unlike watermarking, steganography does not intended to prevent the hidden information by opponents of removing or changing the hidden message, which is embedded in the cover data but it emphasizes on remains it undetectable. Steganography is particularly interesting for applications in which the encryption can not used to protect the communication of confidential information.

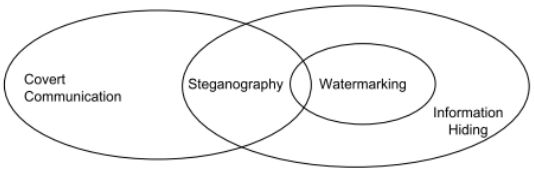

Fig 1: Relationship of steganography to related fields

Largest amount of information that can be embedded in a coverage data without producing either statistical or visual distortion up to a certain degree is called the steganographic capacity. Generally the steganographic techniques are developed such that it will be able to maximally utilize the hiding capacity of the, cover image. Compared to digital watermarking, another branch of information hiding, steganography stresses more on preserving the secrecy of the information instead of making the hidden information robust to attacks. The digital images appealing for steganographic applications because they have a high degree of redundancy in the presentation and pervasive applications in daily life. This results a growing interest in research on image steganography. This paper aims to provide a comprehensive overview of different types of steganography methods for digital images. The rest of the paper is organized as that the second section presents the basic structure of the steganography process followed by the third and fourth section which explains the domains and methods of steganography. The tabular analysis is presented in fifth section and at last the conclusion is drawn on sixth chapter.

II. BASIC STRUCTURE OF STEGANOGRAPHY

The "carrier", the “message” and the “key”, the basic structure of steganography consists of these three fundamental components. The carrier may be, an image, a digital picture, an MP3, even a TCP / IP packet. It is the cover of the “hidden message”. A key is used to decrypt / discover the hidden message. This can be anything from a password, a pattern or a video.

Steganography Concept: let“A” and “B” are two users who wish to secretly communicate. However, all communication between them is examined by the “C” through the ISP a local server or router etc. Specifically, in the general model for steganography, shown in Fig. 2, we have “A” wishing to send a secret message “m” to “B”. In order to do so, “A”, “embeds” it into a cover object “c”, and obtains a stego-object “s”. The stego-object “s” is then sent through the public channel. According to above explanation the main term used in the process can be defined as-

Cover-object: refers to the object used as the carrier to embed messages into. Many different objects have been employed to embed messages into for example images, audio, and video as well as file structures, and html pages to name a few.

Stego-object: refers to the object which is carrying a hidden message. So given a cover object, and a messages the goal of the steganographer is to produce a stego object which would carry the message.

In a standard steganography definition, the technique for embedding the message is unknown to “C” and shared as a secret between “A” and “B”. However, it is generally considered that the algorithm in use is not secret but only the key used by the algorithm is kept as a secret between the two parties, this assumption is also known as Kerchoff’s principle in the field of cryptography. The secret key, for example, can be a password used to map the secret message in to cover image.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 7, January 2014

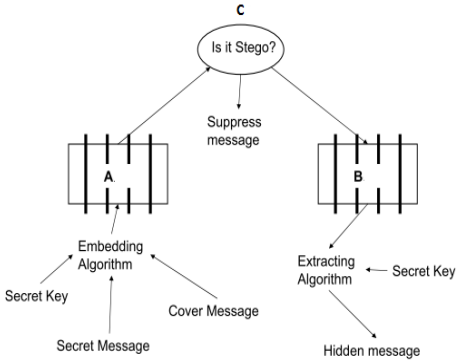

Fig 2: General model for steganography.

III. SPATIAL DOMAIN IMAGE STEGANOGRAPHY

The spatial domain steganography technique refers to the methods in which the data hiding is performed directly on the pixel values of the cover image in such a way that the effect of the message is not visible (at least for the human vision perception) on the cover image. To perform such an embedding many techniques are used but common amongst all is they all utilize the direct pixel embedding although the pixel selection criterion varies. The common methods used in this domain are:

A. Least significant bit (LSB)
B. Pixel value differencing (PVD)
C. Edges based data embedding method (EBE)
D. Random pixel embedding method (RPE)
E. Mapping pixel to hidden data method (PMM)
F. Labeling or connectivity method
G. Pixel intensity or gray level value (GLV) based method
H. Texture based method
I. Histogram based methods
J. Spread Spectrum based methods
K. Color Palette based methods

A. LSB Technique: It is one of the most common and easiest methods for message hiding. In this method, message is hidden in the least significant bits of image pixels. Changing the LSB of the pixels does not introduce much difference in the image and thus the stego image looks similar to the original image. In case of 24-bit images three bits of pixel can be used for LSB substitution as each pixel has separate components for red, green and blue.

B. PVD Technique: Based on the fact that our human vision is sensitive to slight changes in the smooth regions, while can tolerate more severe changes in the edge regions, the PVD-based methods have been proposed to enhance the embedding capacity without introducing obvious visual artifacts into stego images. In PVD-based schemes, the number of embedded bits is determined by the difference between the pixel and its neighbor. The larger the difference amount is, the more secret bits can be embedded. Usually, PVD based approaches can achieve more imperceptible results compared with those typical LSB-based approaches with the same embedding capacity. However, based on extensive experiments and analysis, we find that most existing PVD based algorithms perform bad to resist some statistical analysis even with a low embedding capacity, e.g. 10% bpp (bit per pixel).

C. EDGE BASED: Edge Detection algorithm hides secret data into the pixels that make up the extracted edges of the carrier image. The secret data can be of any type, not necessarily text, and they are actually concealed into the three LSBs (Least Significant Bits) of the pixels of the carrier image, but not in every pixel, only in the ones that are part of the edges detected by the edge detection algorithm.

D. RANDOM PIXEL SELECTION: In this algorithm data is hidden randomly i.e., data is hidden in some randomly selected pixel. Random pixel is generated by using Fibonacci algorithm.

E. PIXEL MAPPING METHOD (MPP):The method for information hiding within the spatial domain of an image. Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbors lies at the boundary of the image or not. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel.

F. PIXEL CONNECTIVITY: A morphological processing starts at the peaks in the marker image and spreads throughout the rest of the image based on the connectivity of the pixels. Connectivity defines which pixels are connected to other pixels. A group of pixels that connected based on Connectivity types called an Object.

G. PIXEL INTENSITY OR GLV: Technique which is used to map data by modifying the gray level of the image pixels. Modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. This technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

H. TEXTURE BASED: In this technique the secret and host images are divided into blocks of specific size and each block in secret image is taken as a texture pattern for which the most similar block is found among the blocks of the host image. The embedding procedure is carried on by replacing these small blocks of the secret image with blocks in host image in such a way that least distortion would be imposed on it.

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 7, January 2014

I. HISTOGRAM BASED: In histogram based data hiding technique the crucial information is embedded into the image histogram. Pairs of peak points and zero points are used to achieve low embedding distortion with respect to providing low data hiding capacity.

J. SPREAD SPECTRUM: The core of spread spectrum image steganography (SSIS) is a spread spectrum encoder. These devices work by modulating a narrow band signal over a carrier. The carrier's frequency is continually shifted using a pseudorandom noise generator feeded with a secret key. In this way the spectral energy of the signal is spread over a wide band, thus decreasing its density, usually under the noise level. To extract the embedded message, the receiver must use the same key and noise generator to tune on the right frequencies and demodulate the original signal. A casual observer won't be able even to detect the hidden communication, since it is under the noise level.

K. PALETTE BASED: The palette based image steganography is similar to the commonly used LSB method for 24 bit color images (or 8 bit grayscale images). After the palette colors are sorted by luminance, it embeds the message into the LSB of indices pointing to the palette colors. Message recovery is simply achieved by selecting the same pixels and collecting the LSBs of all indices to the ordered palette.
General advantages of spatial domain technique are:

1. There is less chance for degradation of the original image.
2. More information can be stored in an image.
3. Low Mathematical Complexity.

Disadvantages of LSB technique are:

1. Less robust, the hidden data can be lost with image manipulation.
2. Hidden data can be easily destroyed by simple attacks.
3. The information may be segmented on a particular part of image.
4. Typically depend on the image format.

IV. TRANSFORM DOMAIN TECHNIQUES

The transform based techniques utilizes the domain specific characteristics of image to embed data on it and for performing it the image firstly transformed to that domain like frequency domain (DCT, DFT), wavelet domain (DWT), curvelet domain etc. in these techniques the data is embedded on the transformed image instead of direct pixels (as in spatial domain) and then the image is retransformed to spatial domain the advantage of the algorithm is that the information can be embedded in are as of the image that are less exposed to compression, cropping, and image processing also the information in one component of transformed domain spreads over larger number of pixels or even in whole image. This reduces the possibility of removal of information by any attack or operation. Although this is a more complex way of hiding information in an image. Transform domain techniques are broadly classified into:

A. Discrete Cosine transform (DCT) based technique
B. Discrete Fourier transform (DFT) based technique.
C. Discrete Wavelet transform (DWT) based technique.
D. Integer Wavelet Transform (IWT) based techniques.
E. Discrete Curvelet Transform (DCVT) Based techniques.

A. DISCRETE COSINE TRANSFORM (DCT) BASED TECHNIQUE:DCT is a general orthogonal transform for digital image processing and signal processing with advantages such as high compression ratio, small bit error rate, good information integration ability and good synthetic effect of calculation complexity. DCT allows an image to be broken up into different frequency bands namely the high, middle and low frequency bands thus making it easier to choose the band in which the watermark is to be inserted [3]. The literature survey reveals that mostly the middle frequency bands are chosen because embedding the information in a middle frequency band does not scatter the watermark information to most visual important parts of the image i.e. the low frequencies and also it do not overexpose them to removal through compression and noise attacks where high frequency components are targeted. Numerous watermarking techniques based on DCT are proposed. Although some of the watermarking techniques embed the watermark in the DC component, most techniques utilize the comparison of middle band DCT coefficients to embed a single bit of information into a DCT block.

B. DISCRETE FOURIER TRANSFORM (DFT) BASED TECHNIQUE: The DFT based technique is similar to the DCT based technique but it utilizes the Fourier transform instead of cosine which makes it lack resistance to strong geometric distortions. Although it increases the overall complexity of the process.

C. DWT BASED: A wavelet is a small wave which oscillates and decays in the time domain. The Discrete Wavelet Transform (DWT) is a relatively recent and computationally efficient technique in computer science. Wavelet analysis is advantageous as it performs local analysis and multi-resolution analysis. To analyze a signal at different frequencies with different resolutions is called multi-resolution analysis (MRA). This method transforms the object in wavelet domain, processes the coefficients and then performs inverse wavelet transform to represent the original format of the stego object.

D. IWT BASED: Since the discrete wavelet transform allows independent processing of the resulting components without significant perceptible interaction between them, hence it is expected to make the process of imperceptible embedding more effective. However, the used wavelet filters (and also the other filters like DCT, FFT) have floating point coefficients. Thus, when the input data consist of sequences of integers (as in the case for images), the resulting filtered outputs no longer consist of integers, which doesn't allow perfect reconstruction of the original image. However, with

ISSN: 2277-3754
ISO 9001:2008 Certified
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 3, Issue 7, January 2014

the introduction of Wavelet transforms that map integers to integers the output can be completely characterized with integers [8].

E. DCVT BASED: Curvelet transform is the new member of the evolving family of multiscale geometric transforms [11]. Since it represents edges better than Wavelet, Curvelet transform offers an effective solution to the problems associated with image steganography using Wavelets and DCT (Discrete Cosine Transform).

General advantages of transform domain technique are:

1. There is less chance for removal or loss of the hidden data.
2. Information is distributed over all whole image.
3. Provides much higher flexibility for hiding data.
4. Typically independent of the image format.

Disadvantages of transform technique are:

1. Greater understanding of the embedding domain required.
2. Careful selection of embedding coefficients required otherwise it can cause degradation of image.
3. Higher Mathematical Complexity.
4. Relatively Low embedding capacity.

V. COMPARATIVE ANALYSIS

Table 1: Performance Comparison

Technique	Domain	Capasity	Viability	Detectability	Robustness	Complexity	Comments
LSB	Spatial	H	L	H	L	L	Independent of image format and texture
PVD	Spatial	M	L	M	L	L	Suitable for high contrast images
EBE	Spatial	L	L	M	L	L	Preferred for images with objects
RPE	Spatial	H	M	L	L	L	Provides better security of information leakage
PMM	Spatial	M	L	L	M	M	N/A
Connect	Spatial	M	L	L	M	M	Preferred for Mosaic Images
PI (GLV)	Spatial	M	L	L	L	L	Robust hiding for noisy images
Texture	Spatial	M	L	M	M	M	Preferred for Patterned
Histogram	Spatial	L	L	M	M	M	Limited Capacity and Hard to detect
SSIS	Spatial	L	L	L	M	M	Dissolves the information over whole image
CPB	Spatial	L	L	L	M	L	Works with specific image formats only
DCT	Transform	M	L	L	M	M	Simplest in the transform domain
DFT	Transform	M	L	L	M	M	Involves the complex calculations
DWT	Transform	M	L	L	H	H	Closely matches with human visual perception
IWT	Transform	M	L	L	H	H	Overcomes the rounding off losses
DCVT	Transform	M	L	L	H	H	Improves the degradations at edge areas

VI. CONCLUSION

This paper presented an overview of different steganographic techniques from the basic systems to the recent approaches it also analyze them. The paper shows the generalized comparison of different technique into tabular form on the basis of visual perception, attack resilient, embedding capacity, detectability and computational complexity. The analysis shows that the transform domain techniques are best for the attack resilient system with relatively lower data capacity and higher complexity while the spatial domain is best for limited complexity systems and also provides greater options for techniques selection for the systems with limited computational power.

REFERENCES

[1] Dulce R. Herrera-Moro, Raúl Rodríguez-Colín, Claudia Feregrino-Uribe "Adaptive Steganography based on textures",17th International Conference on Electronics, Communications and Computers (CONIELECOMP'07).

[2] YildirayYalman 1 , FeyziAkar 2 and Ismail Erturk "Contemporary Approaches to the Histogram Modification

[3] Blossom Kaur, Amandeep Kaur, Jasdeep Singh "STEGANOGRAPHIC APPROACH FOR HIDING IMAGE IN DCT DOMAIN", International Journal of Advances in Engineering & Technology, July 2011.

[4] Xuefeng Wang Zhen Yao Chang-Tsun Li "A PALETTE-BASED IMAGE STEGANOGRAPHIC METHOD USING COLOURQUANTISATION", Image Processing, 2005. ICIP 2005. IEEE International Conference on 11-14 Sept. 2005

[5] Souvik Bhattacharyya, Gautam Sanyal "Study and analysis of quality of service in different image based steganography using Pixel Mapping Method (PMM)", International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 2– No.7, May 2012 – www.ijais.org

[6] M.Shobana, R.Manikandan "EFFICIENT METHOD FOR HIDING DATA BY PIXEL INTENSITY", M.Shobana et al. / International Journal of Engineering and Technology (IJET), Vol 5 No 1 Feb-Mar 2013

[7] K. Naveen BrahmaTeja, Dr. G. L. Madhumati, K. Rama Koteswara Rao"Data Hiding Using EDGE Based Steganography", International Journal of Emerging Technology and Advanced Engineering (ISSN 2250-2459, Volume 2, Issue 11, November 2012).

[8] Hemalatha S., U Dinesh Acharya, Renuka A. and Priya R. Kamath"An Integer Wavelet Transform Based Steganography Technique for Color Images", International Journal of Information & Computation Technology. ISSN 0974-2239 Volume 3, Number 1 (2013), pp. 13-24.

[9] Vijay Kumar and Dinesh Kumar "Performance evaluation of DWT based image steganography", Advance computing conference (IACC), 2010 IEEE 2nd International.

[10] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami "Labeling Method in Steganography", World Academy of Science, Engineering and Technology International Journal of Computer, Information Science and Engineering Vol:1 No:6, 2007.

[11] W. Zhang, S. Wang, and X. Zhang, "Improving embedding efficiency of covering codes for applications in steganography," IEEE Communications Letters, vol. 11, pp. 680–682, August 2007.

[12] AHMED FREIDOON FADHIL"IMAGE STEGANOGRAPHY BASED CURVELET TRANSFORM", Al-Rafidain Engineering Vol.18 No.5 October 2010.

AUTHOR'S PROFILE

I am Anjali Tiwari, currently I am Mtech Scholar in OIST Bhopal, which is affiliated to RGPV University Bhopal, I have completed my Btech from NIIST Bhopal, with electronics and communication branch.

Seema Rani Yadav is a professor in OIST Bhopal which is affiliated to RGPV University.

N.K. Mittal is a professor in OIST Bhopal which is affiliated to RGPV University Bhopal.