Various Techniques of Data Hiding in Image

Mr. Abbas F Tukiwala¹ Mr. Sheshang D. Degadwala²
¹M.E. Student ²Assistant Professor
¹,²Department of Computer Engineering
¹,²Sigma Institute of Engineering, Vadodara

Abstract—Data Hiding in Image is an art to hide the very existence of embedded data in image so as not to arouse an eavesdropper’s suspicion. For hiding secret data in digital images, large varieties of steganography techniques are available, some are more complex than others, and all of them have their respective pros and cons. Applications may require absolute invisibility of the secret data, larger secret data to be hidden or high degree of robustness of the carrier. This paper intends to give thorough understanding and evolution of different existing data hiding techniques in digital image. It covers and integrates research work without going into too much detail.

Key words: image Steganography, Cover writing, Cover Image, Stego Image, Redundant Bits

I. INTRODUCTION

Steganography word is originated from Greek words Steganós (Covered), and Graptos (Writing) which literally means “cover writing” [1]. Generally steganography is known as “invisible” communication. Steganography means to conceal messages existence in another medium (audio, video, image, communication). Today’s steganography systems use multimedia objects like image, audio, video etc. as cover media because people often transmit digital images over email or share them through other internet communication application. It is different from protecting the actual content of a message. In simple words it would be like that, hiding information into other information. The goal of Steganography is to mask the very presence of communication making the true message not discernible to the observer and to hide an information message inside harmless cover medium in such a way that it is not possible even to detect that there is a secret message. Modern steganography goal is to keep its more presence undetectable, but steganography systems, because of their invasive nature, leave behind detectable traces in the cover medium through modifying its statistical properties, so eavesdroppers can detect the distortions in the resulting stego medium statistical properties. The process of finding these distortions is called statistical steganalysis [1].

A. Terminologies in Steganography [1]

1) Payload (Secret Message): The information which is to be concealed.
2) Carrier File (Cover Image): The media where payload has to be hidden.
3) Stego-Medium (Stego Image): The medium in which the information is hidden.
4) Redundant Bits: Pieces of information inside a file or image which can be overwritten or altered without damaging the file.
5) Steganalysis: The process of detecting hidden information inside of a file or image.
6) Stego medium = Payload file + Carrier file.

B. Aspects of Data Hiding [14]

An information-hiding system is characterized by having three different aspects that contend with each other. These are capacity, security, and robustness as shown in Fig 1.

Capacity refers to the amount of information that can be hidden in the cover medium.

Security refers to an eavesdropper’s inability to detect hidden information.

Robustness refers to the amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Fig. 1: Aspects of Data Hiding

C. Types of Steganography [14]

There are basically three Steganography types:
1) Pure Steganography (No Key is used).

Pure Steganography is a Steganography system that doesn't require prior exchange of some secret information before sending message; therefore, no information is required to start the communication process: the security of the system thus depends entirely on its secrecy.

Fig. 2: Pure Steganography

2) Secret key Steganography (Secret Key is used).

A secret key Steganography system is similar to a symmetric cipher, where the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message.

Fig. 3: Secret Key Steganography

3) Public key Steganography (Public Key is used).

Public key Steganography does not depend on the exchange of a secret key. It requires two keys, one of them private (secret) and the other public: the public key is stored in a public database, whereas the public key is used in the
embedding process. The secret key is used to reconstruct the secret message.

Fig. 4: Public Key Steganography

D. Classification of Steganography [1]

Depending on the type of the cover object there are many suitable steganography techniques which are followed in order to obtain security. It can be shown in Figure 5.

1) Image Steganography:
Taking the cover object as image in steganography is known as image steganography. Generally, in this technique pixel intensities are used to hide the information.

2) Network (Protocol) Steganography:
When taking cover object as network protocol, such as TCP, UDP, ICMP, IP etc., where protocol is used as carrier, is known as network protocol steganography.

3) Video Steganography:
Video Steganography is a technique to hide any kind of files or information into digital video format. Video (combination of pictures) is used as carrier for hidden information.

4) Audio Steganography:
When taking audio as a carrier for information hiding it is called audio steganography. It has become very significant medium due to voice over IP (VOIP) popularity. Audio steganography uses digital audio formats such as WAVE, MIDI, AVI MPEG or etc. for steganography.

5) Text Steganography:
General technique in text steganography, such as number of tabs, white spaces, capital letters, just like Morse code is used to achieve information hiding. An obvious method was to hide a secret message in every nth letter of every word of a text message.

Fig. 5: Classification of Steganography

E. Image Steganography Techniques

Image steganography techniques can be classified into two broad categories: Spatial-domain based steganography and Transform domain based Steganography.

1) Spatial Domain (Time Domain) Steganography
In Spatial domain, cover-image is first decomposed into bits planes and then least significant bit (LSB) of the bits planes are replaced with the secret data bits. Advantages are high embedding capacity, ease of implementation and imperceptibility of hidden data. The major drawback is its vulnerability to various simple statistical analysis methods.

The most direct way to represent pixel’s color is by giving an ordered triplet of numbers: red (R), green (G), and blue (B) that comprises particular color. The other way is to use a table known as palette to store the triplet, and put a reference into the table for each pixel. The spatial domain-based steganography techniques use LSB (Least Significant Bit) algorithm for embedding/extraction of data

- LSB (Least Significant Bit)
A simple way of steganography is based on modifying the least significant bit layer of images, known as the LSB technique. The LSB technique directly embeds the secret data within the pixels of the cover image. In some cases LSB of pixels visited in random or in certain areas of image and sometimes increment or decrement the pixel value.

2) Transform Domain (Frequency Domain) Steganography
Frequency domain embedding techniques, which first transforms the cover-image into its frequency domain, secret data is then embedded in frequency coefficients. Advantages include higher level of robustness against simple statistical analysis. Frequency domain methods hide messages in significant areas of the cover-image which makes them more robust to attacks such as compression, cropping or image processing methods than LSB approach and moreover they remain imperceptible to the human sensory system as well. The Transform domain based Steganography techniques can classified as shown in fig.

Fig. 6: Transform Domain Based Techniques

- DCT (Discrete Cosine Transform)
The DCT transforms a cover image from an image representation into a frequency representation, by grouping the pixels into non-overlapping blocks of 8 × 8 pixels and transforming the pixel blocks into 64 DCT coefficients each. A modification of a single DCT coefficient will affect all 64 image pixels in that block. The DCT coefficients of the transformed cover image will be quantized, and then modified according to the secret data.

- DWT (Discrete Wavelet Transform)
Discrete Wavelet Transform (DWT) is a mathematical tool for hierarchically decomposing an image [1]. Non-stationary signals can easily be handled using DWT [1]. The entire transform is based on tiny waves, called wavelets. These wavelets vary with respect to frequency and limited duration. The DWT splits the signal into high and low frequency parts. The high frequency part contains information about the edge components, while the low frequency part is split again into high and low frequency parts. As shown in Fig. 7, initially we have a whole image. After first level of decomposition, the image is decomposed into four sub-bands namely LL1, LH1, HL1, and HH1. To apply second level of decomposition, LL1 is given as the first input and is followed by LH1, HL1, and HH1. At the
end of second level decomposition, LL1 has got 4 sub-bands namely LL2, LH2, HL2, HH2.

Fig. 7: Two Levels DWT

– Discrete Curvelet Transform
Curvelet, proposed by Candes and Donoho in 1999, are invented to overcome some shortcoming of wavelet transform. The curvelet transform is a multiscale directional transform that allows an almost optimal non-adaptive sparse representation of the object with edges.

F. Comparison of Various Image Steganography Techniques

<table>
<thead>
<tr>
<th>Techniques</th>
<th>Advantages</th>
<th>Disadvantages</th>
</tr>
</thead>
<tbody>
<tr>
<td>LSB (Least Significant Bit)</td>
<td>Simple &amp; easiest way of hiding information.</td>
<td>Its vulnerability to various simple statistical analysis methods such as Compression, Rotation and Scaling.</td>
</tr>
<tr>
<td>DCT (Discrete Cosine Transform)</td>
<td>Hidden data can be distributed more evenly over the whole image in such a way as to make it more robust.</td>
<td>It is less robust than DWT and It does not maintain temporal information during transformation.</td>
</tr>
<tr>
<td>DWT (Discrete Wavelet Transform)</td>
<td>Coefficients of the wavelets are altered with the noise within tolerable level. It has high flexibility.</td>
<td>Many No. of Coefficients are needed to account edge.</td>
</tr>
<tr>
<td>Discrete Curvelet Transform</td>
<td>Less Coefficients are needed to account edge.</td>
<td>It requires more time than DWT.</td>
</tr>
</tbody>
</table>

Table. 1: Comparison of Various Image Steganography Techniques

II. LITERATURE REVIEW

This section describes the previous work which had been done for data hiding.

Mehdi Hussain et al., (and other) [1] critically analyzed various steganography techniques and also covered steganography overview, its major types, classification and application.

Firas A. Jassim [2] proposed method to hide the secret message inside the cover image using five modulus method. The main advantage of that novel algorithm is to keep size of cover image constant while secret message increased in size.

Chaitra h et al., [3] developed proposed system is to hide message using FMM along with genetic algorithm and Visual Cryptography to ensure improved security and reliability. The major merit of that system is to increase the embedding capacity and secure the information.

Rahul Joshi et al., [4] introduced the concept of steganography using LSB method. This method is easy to implement but has some disadvantages. One of the major disadvantage is that intruder can change LSB bit of all image pixels. Hidden message will be destroyed by changing the image quality. It is not immune to noise and compression technique.

Shivani kundra and Nishi madaan [5] performed analysis of different image steganography techniques and their comparison is done. They found that performance of the Hash-LSB would be more secure than other techniques and RSA algorithm itself is very secure that no one can break it easily.

Saeed Ahmed et al., [6] proposed method using Dynamic Substitution and Secret Key is more difficult to attack because of message bits are not inserted in to the fixed position. In their method, the message bits are embedded into deeper layer depending on the environment of the host image and a secret key resulting increased robustness. The robustness specially would be increased against those intentional attacks which try to reveal the hidden message.

Barnali Gupta and Prof. Samir [7] discussed image steganography using DWT method. It divides the image in frequency components. The low frequency components are approximate coefficients holding almost the original image and high frequency components are detailed coefficients holding additional information about the image. These detailed coefficients can be used to embed secret image.

Yung kuan chan et al., [8] developed proposed method that transform a spatial domain cover image into a frequency domain image using Haar digital wavelet transform method, compresses coefficients of the high frequency band by the Huffman or arithmetic coding method and then embeds the compression data and secret data in high frequency band. This method utilizes the Huffman coding to recover the cover image without any distortion.

Vikas pratap and Prof. Shrikant [9] proposed a new frequency domain method using Haar Wavelet for image steganography. The merit is to increase image quality by hiding the messages in HL, LH, and HH sub-bands while keeping LL sub-band invariant. The advantage of this is that the original cover image does not have to be present on the receiver side.

Mrs. D. Mathivadhani and Dr .C. Meena [10] developed hybrid method to hide an image and secret message into a cover image using Discrete Wavelet Transformation (DWT), SLSB (Selected Least Significant Bit) and Visual Cryptography (VC) is proposed. This proposed system can resist various attacks while maintaining the visual quality of the cover image and text message.

Md. Palash et al., [11] developed a Cryptographic Algorithm Based on ASCII Conversions and a Cyclic Mathematical Function is to make the encrypted message undoubtedly unprintable using several times of ASCII conversions and a cyclic mathematical function. The final encrypted message received from three times of encryption becomes an unprintable text without increasing the size of data or loosing of any data. But if size of original message is not divisible by Packet size then size of encrypted message
in bits is larger than that of original message. This algorithm which follows a different methodology from the traditional symmetric-key cryptography, asymmetric-key cryptography or hashing function.

S. Shanmuga Priya et al. [12] consider digital images as covers and investigate an adaptive and secure data hiding scheme in the spatial least-significant-bit (LSB) domain. LSB replacement is a well-known steganography method. In that embedding scheme, only the LSB plane of the cover image is overwritten with the secret bit stream according to a pseudo random number generator (PRNG).

Mr. Vikas Tyagi [13] discussed a technique used on the LSB (least significant bit) and a new encryption algorithm. By matching data to an image, there is less chance of an attacker being able to use steganalysis to recover data. Before hiding the data in an image the application first encrypts it.

Ali and Fawzi [14] proposed a modified high-capacity image steganography technique that depends on wavelet transform with acceptable levels of imperceptibility and distortion in the cover image and high level of overall security. The basic decomposition step for images using the 2D Wavelet transforms. Also, different levels of Wavelet transform were tried in that paper (up to 5).

Prabakaran. G and Bhavani R. [15] proposed a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Arnold transformation is performed to scramble the secret image. Discrete Wavelet Transform (DWT) is performed in both images and followed by Alpha blending operation. Then the Inverse Discrete Wavelet Transformation (IDWT) is applied to get the stego image.

G. Prabakaran et al. [16] developed proposed method extracts either Discrete Wavelet Transform (DWT) or Integer Wavelet Transform (IWT) coefficients of both cover image and secret image. After that two extracted coefficient values are embedded by fusion processing technique. Then the stego image is obtained by applying various combinations of DWT and IWT on both images.

Nadiya P and B Mohammed Imran [17] present an advanced method for embedding encrypted secret data in grayscale images to provide high level security of data for communication over unsecured channels. The proposed system combines the features of Cryptography and Steganography. Cryptography involves converting the secret message into a non-recognizable cipher. Steganography is then applied using Double-stegging to embed this encrypted data into a cover media and hides its existence.

Pratibha Sharma and Shanti Swami [18] present a digital image watermarking based on 3 level discrete wavelet transform (DWT) & compare it with 1 & 2 levels DWT. In this technique a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique.

S. Bhargav Kumar and K. Esther Rani [19] propose a new technique of watermarking, combining both Discrete Wavelet Transform (DWT) and Bit-Plane Slicing (BPS) techniques. In the first unit, they decomposed the image to be watermarked in to four dimensional modified DWT coefficients, by adding pseudo-random codes at the high and middle frequency bands of the DWT of an image. In the second unit, a key has been generated from LHLH frequency bands of the 4-Level DWT image and this key is watermarked in to the original gray image. In the third unit, for data compression we used bit plane slicing technique where the original gray image is sliced in to 8 planes and we used bit plane 3 to embed in to the key watermarked image. The embedded key watermarked image is transmitted and the key watermarks are extracted with robustness.

Nikita Kashyap and G.P. Sinha [20] use a multi-bit watermark is embedded into the low frequency sub-band of a cover image by using alpha blending technique. The insertion and extraction of the watermark in the grayscale cover image is found to be simpler than other transform techniques. The proposed method is compared with the 1-level and 2-level DWT based image watermarking methods by using statistical parameters such as peak-signal-to-noise ratio (PSNR) and mean square error (MSE).

Sree Rathna Lakshmi [21] present a steganalytic algorithm based on III Level DWT with Energy as Feature that detects the stego/normal image with 90% accuracy.

III. CONCLUSION

There are a wide variety of different techniques with their own advantages and disadvantages. Many currently used techniques are not robust enough to prevent detection and removal of embedded data. This paper presented the research work in the field of data hiding deployed in different transformation of digital images and present comparison of different techniques with their advantages and disadvantages. From that we conclude that frequency domain techniques are more robust than spatial domain.

REFERENCES


Various Techniques of Data Hiding in Image (IJSRD/Vol. 2/Issue 09/2014/132)


