A Survey on Information Hiding Techniques in Digital Media

Snehal Ghormade, Bhagwat Kakade

Abstract— Secure data transmission has been a significant problem throughout human history. It is often thought that communication may be secured by encrypting the traffic, but this has rarely been adequate in practice. From ancient times, the art of hiding is always preferred upon enciphering the secret information because hiding arouses less suspicion as it conceals its very existence. This paper is a brief review of different data hiding techniques within an image which elaborates the suitability of wavelet transform for efficient and robust data hiding. The purpose of this paper is to provide a comprehensive review of the existing literature available on different data embedding algorithms.

Index Terms— Digital image, Discrete Wavelet Transform, Information hiding, JPEG, LSB substitution. Steganography

1 INTRODUCTION

THe digital revolution has resulted in explosion of knowledge in today's technology-driven economy. Digital media offer several distinct advantages over analog media, such as high quality, easy editing, high fidelity copying. Recently, Covert communication is receiving much more attention from the research community after the 9/11 incident. This includes transmitting hidden data which is almost imperceptible to the intruder by using different data embedding schemes. Generally information hiding is used to protect, authenticate data or for secret communication.

Secure data transmission has been a significant problem throughout human history. It is often thought that communication may be secured by encrypting the traffic, but this has rarely been adequate in practice. From ancient times, the art of hiding is always preferred upon enciphering the secret information because hiding arouses less suspicion as it conceals its very existence. This preference persists in many operational contexts to this day. For example, Military and intelligence agencies require inconspicuous communications. Even if the content is encrypted, the detection of a signal on a modern battle field may lead rapidly to an attack on the signaler.

Secure data transmission can be carried out by hiding a message in cover data; the concept which is termed as Steganography. Steganographic techniques allow communication between two authorized parties without an observer being aware that the communication is actually taking place. These techniques have many Army applications in the defensive information warfare arena, such as hidden communication, in-band captioning, and tamper proofing. A useful steganographic system must provide a method to embed data in an imperceptible manner, allow the data to be readily extracted, promote a high information rate or payload capacity, and incorporate a certain amount of robustness to removal [1]. Many interesting steganographic techniques have been created and its continuing evolution is guaranteed by a growing need for information security.

This paper reviews some of the data hiding techniques carried out with their features. Firstly, the desirable characteristics of a data hiding system are briefly discussed. The main categories of information hiding algorithms covered till date are discussed. Lastly, some points are summarized based on the theories given by various researchers.

2 MAJOR CHALLENGES

The significance of embedding in any particular application depends upon the requirements of that specific application [2]. Some of the major challenges of effective steganography are discussed in this section.

2.1 Security of Hidden Communication

In order to avoid raising the suspicions of eavesdroppers, while evading the meticulous screening of algorithmic detection, the hidden contents must be invisible both perceptually and statistically.

2.2 Size of Payload

Unlike watermarking, which needs to embed only a small amount of copyright information, steganography aims at hidden communication and therefore usually requires sufficient embedding capacity. Requirements for higher payload and secure communication are often contradictory. Depending on the specific application scenarios, a tradeoff has to be sought.

2.3 Robustness

Robustness is the ability to detect the embedded watermark after common image processing operations like compression, filtering, geometric distortion etc. Sometimes data hiding systems are developed which have the ability to survive most of the intentional manipulations. Robustness is application dependent and it is not necessary that all the applications require robustness against all the operations.

Steganography and watermarking differ in a number of ways including purpose, specification and detection/extraction methods. The most fundamental difference is that the object of communication in watermarking is the host signal, with the embedded data providing copyright protection. In steganography the object to be transmitted is the embedded message, and the cover signal serves as an innocuous disguise chosen fairly arbitrarily by the user based on its technical suitability. In addition, the existence of the watermark is often declared openly, and any attempt to remove or invali-

date the embedded content renders the host useless. The crucial requirement for steganography is perpetual and algorithmic undetectability. Robustness against malicious attack and signal processing is not the primary concern, as it is for watermarking.

3 EXISTING TECHNIQUES

Image hiding methods can be divided into following two main domains *viz.* Spatial Domain Methods and Transform Domain Methods [3].

3.1 Spatial Domain Methods

Spatial domain watermarking slightly modifies the pixels of one or two randomly selected subsets of an image. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. The different spatial domain methods can be found in literature:

3.1.1 LSB Substitution

The most well-known steganographic technique in the data hiding field is least-significant-bits (LSBs) substitution [4]. This method embeds the fixed-length secret bits in the same fixed length LSBs of pixels. Although this technique is simple, it generally causes noticeable distortion when the number of embedded bits for each pixel exceeds three. Several adaptive methods for steganography have been proposed to reduce the distortion caused by LSBs substitution. For example, adaptive methods vary the number of embedded bits in each pixel, and they possess better image quality than other methods using only simple LSBs substitution. However, this is achieved at the cost of a reduction in the embedding capacity.

3.1.2 Optimum Pixel Adjustment

The proposed [4] Optimal Pixel adjustment Procedure (OPAP) reduces the distortion caused by the LSB substitution method. In OPAP method the pixel value is adjusted after the hiding of the secret data is done to improve the quality of the stego image without disturbing the data hidden.

3.1.3 Inverted Pattern Approach

This inverted pattern (IP) LSB substitution approach uses the idea of processing secret messages prior to embedding [5]. In this method each section of secret images is determined to be inverted or not inverted before it is embedded. In addition, the bits which are used to record the transformation are treated as secret keys or extra data to be re-embedded.

3.1.4 IP Method Using Relative Entropy

Relative entropy measures the information discrepancy between two different sources with an optimal threshold obtained by minimizing relative entropy. In this method instead of finding the mean square error for inverted pattern approach, the relative entropy is calculated to decide whether S or S'suites the pixel. In probability theory and information theory, the Kullback–Leibler divergence (also information divergence, information gain, or relative entropy) is a non-symmetric measure of the difference between two probability distributions *P* and *Q*. It is given by,

$$D(p||q) = \sum_{x \in X} p(x) \log \frac{p(x)}{q(x)} = E_p \log \frac{p(X)}{q(X)}$$

3.2 Frequency Domain Methods

Human visual system (HVS) is having low sensitivity to high and middle frequency information while it's more sensitive to low frequency information. The frequency domain techniques take this advantage of HVS to embed the data. Here, the image is first transformed using any transformation methods such as Fourier transform, discrete cosine transform (DCT) or discrete wavelet transform (DWT) to the frequency domain and the information is added to the values of its transform coefficients. After applying the inverse transform, the marked coefficients form the embedded image.

3.2.1 JPEG Steganography

Hiding secret information into JPEG images may provide better camouage as JPEG is the common format of the images produced by digital cameras, scanners, and other photographic image capture devices. Some of the major JPEG steganographic methods are reviewed in the following:

JSteg and JPHide are the two classical JPEG Steganographic tools which utilizes the LSB embedding technique [6]. In JSteg, the secret information is embedded into the cover image by successively replacing the LSBs of non-zero quantized DCT coefficients with secret message bits. While in JPHide, a key is used to control and to select the quantized DCT coefficients that will be used to hide secret message bits randomly. Westfeld introduced a steganographic algorithm in which the absolute value of the coefficient is decreased by one if it is needed to be modified [7]. The F5 algorithm embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to hide a message of certain length. During the embedding phase, the number of non-zero AC coefficients and the message length are used to find the best matrix embedding that minimizes the number of modifications of the cover image. High embedding efficiency, resistance to visual and statistical attacks was the advantages of this method.

Outguess created by Neils Provos is a steganographic system that improves the encoding step by using a pseudo-random number generator to select the DCT coefficients at random [8]. The least-significant bit of a selected DCT coefficient is replaced with encrypted message data. The main features of Outguess were its ability to preserve the histogram of DCT coefficients exactly and it cannot be detected using the chi-square attack or its generalized versions. Sallee presented a steganography and steganalysis method using a statistical model of cover medium [9]. Model-based steganography adapts the division of the carrier into a deterministic random variable X_{det} and an indeterministic one X_{indet}. In contrast to the previous approaches, model-based steganography does not assume X_{indet} to be independently and uniformly distributed. Therefore the developers propose to find suitable models for

the distribution of X_{indet}, which reflect the dependencies with X_{det}. The general model is parameterized with the actual values of X_{det} of a concrete cover medium, which leads to a cover specific model. The purpose of this model is to determine the conditional distributions. Then, an arithmetic decompression function is used to fit uniformly distributed message bits to the required distribution of X_{indet}, thus replacing X_{indet} by X^{*}_{indet}, which has similar statistic properties and contains the confidential message.

3.2.2 Discrete Wavelet Transform

Wavelets have been effectively utilized as a powerful tool in many diverse fields, including approximation theory; signal processing, physics, astronomy, and image processing. A Wavelet is simply, a small wave which has its energy concentrated in time to give a tool for the analysis of transient, non-stationary or time-varying phenomena. Wavelets are used in the image steganographic model because the wavelet transform clearly partitions the high-frequency and low-frequency information on a pixel by pixel basis.

DWT based techniques are very similar to theoretical model of Human Visual System (HVS). It is more frequently used due to its time/frequency characteristics. Here an image is passed through series of low pass and high pass filters which decompose the image into sub bands of different resolutions [18]. As most of the energy is concentrated in the approximate (LL) sub band having low frequency sub bands, any change in these low frequency sub bands would cause a severe degradation of image. As the human eyes are not sensitive to high frequency sub bands, the secret information is embedded in either vertical, horizontal or diagonal (LH, HL or HH respectively) sub bands. Fig.1 shows a generalized DWT based information hiding scheme.

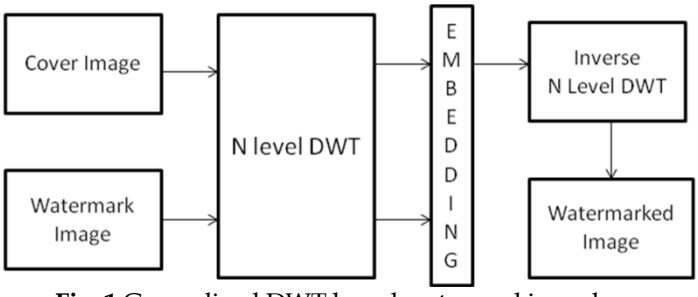

Fig. 1 Generalized DWT based watermarking scheme

The following literature gives a brief description of DWT based different information hiding techniques:

Xia *et al.* added a Gaussian random noise to the large coefficients in the DWT domain [10]. Here the watermark was inserted in the middle and high frequency bands of the image. In the decoding process, the DWT of the marked image was performed and the sections of the watermark were extracted and correlated with sections of the original watermark. A watermark was detected if the cross-correlation was above a threshold. Experimental results showed that the DWT based watermark approach was robust to several kinds of distortion such as additive noise, resolution reduction and compression.

A new approach of information hiding in wavelet domain where human visual system (HVS) characteristics are exploited to hide the watermark was developed by Barni *et al.* [11]. The watermark to be embedded was a pseudo- random sequence which was adaptively added to the DWT coefficients of three largest detail sub-bands. The detection was achieved by measuring the correlation between the watermarked coefficients and the information hiding code. The most important feature of this technique was that the watermark embedding was performed pixel by pixel considering the texture and the luminance content of all the image sub-bands. Experimental results showed that this method performed exceptionally well in case of lossy compression. Also, the information hiding energy can be kept so high that even a small portion of the image is sufficient to correctly guess the embedded code.

Kundur *et al.* proposed the use of gray scale logos as watermark [12]. They addressed a multi-resolution fusion based information hiding method for embedding gray scale logos into wavelet transformed images. The logo undergoes 1-level decomposition for information hiding. Each sub-band of the host image was divided into blocks of size equal to the size of sub-band of the logo. Four sub-bands of the logo corresponding to different orientations were added to the blocks of the same orientation. For fusion, the watermark was scaled by salience factor computed on a block by block basis. Simulation results showed that the proposed technique was highly robust to compression and additive noise. In fact, if the images were almost completely destroyed yet the watermark can be extracted fairly accurately.

Authors had developed a new semi-blind reference information hiding scheme using a combination of DWT and singular value decomposition (SVD) [13]. In this method instead of using a PN sequence, a gray scale logo image was used as watermark. For embedding process the original image was first transformed into wavelet domain and then using directive contrast and wavelet coefficients a reference sub-image was formed. By amending the singular values of the reference image using the singular values of the watermark, the watermark was embedded into the reference image. This technique proved to be very robust and was able to withstand a variety of attacks including ambiguity attack. Also, it was found that after undergoing operations such as filtering, addition of noise, JPEG compression, cropping, resizing, rotation and pixilation, the extracted logo was still recognizable. A blind image information hiding scheme based on wavelet tree quantization was proposed [14]. In this approach a super tree was formed by grouping the wavelet coefficients of the host image. This super tree was quantized in such a way that it exhibits a large enough statistical difference which can be used for embedding and extracting watermark. This technique proved to be robust for both time and frequency domain attacks.

An algorithm was proposed by Ramani *et al.* which was having very high information hiding capacity [15]. It was based on Integer to Integer Wavelet Transform (IWT) with Bit Plane Complexity segmentation (BPCS). IWT was used to decompose the cover image whereas BPCS takes the advantage of HVS which cannot recognize changes in complex positions of the image. The drawback with this method was that it needed separate processing for R, G and B components of the color image. A method based on combination of DWT and a

Generic algorithm which can be used to find the best sub band for watermark embedding was introduced [16]. This technique provided imperceptibility and robustness simultaneously but the process was too lengthy and time consuming.

A 1-level DWT alpha blending technique was proposed which embeds the invisible watermark into the salient features of the original image using Daubechies wavelets [17]. In this approach the decomposed components of both the images were multiplied by a scaling factor and then added. Result shows that the quality of the watermarked image, recovered image and extraction of watermark were dependent only on the values of the scaling factors k and q. Also the process of embedding and extracting was simpler when compared to DCT method. There was a limitation that the size of the watermark must be smaller than the host image and the frame size of both the images should be made equal.

CONCLUSION

Significant number of watermarking techniques can be found in the literature used in the variety of applications because of their advantages over the alternative methods. The overall study in this paper shows that the spatial methods are relatively fast and requires low resources and even they can provide comparable performance over scaling and additive noise attacks. On the other hand, frequency domain methods are computationally complex but performs exceptionally well in terms of robustness, pay load capacity, image operations and imperceptibility. DCT based watermarking systems are highly resistant to JPEG compression and shows high energy compaction property while DWT based watermarking systems are more preferred choice because of the advantages listed out by several authors in their respective research over the years.

REFERENCES

[1] B. Gunjal and R. Manthalkar, " An Overview Of Transform Domain Robust Digital Image Watermarking Algorithms," *J. Emerging Trends in Computing and Inform. Sci.* vol. 2, no. 1, pp.37 42, 2011.

[2] M. Hsieh, D. Tseng and Y. Huang, "Hiding Digital Watermarks Using Multiresolution Wavelet Transform," *IEEE Trans. Industrial Electronics*, vol. 48, no. 5, pp.875-882, Oct. 2001.

[3] C. Lin and Y. Ching, "A Robust Image Hiding Method Using Wavelet Technique," *Journal of Information Science and Engineering*, vol. 22, pp.163-174, 2006.

[4] C.K. Chan and L.M. Chen, "Hiding data in images by simple LSB substitution," Pattern Recognition vol.37, no.3, pp. 469–474, 2004.

[5] C.H. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB substitution," *Pattern Recognition*, vol. 41, pp. 2674–2683, 2008.

[6] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography". *IEEE Security Privacy*, vol.1, issue 3, pp. 32-44, 2003.

[7] A.Westfeld, "High Capacity Despite Better Steganalysis (F5 - A Steganographic Algorithm)", *Proc. 4th Int. Workshop on Information Hiding, Pittsburgh, PA, USA*, pp. 289-302, 25- 27 April 2001.

[8] N. Provos. And P. Honeyman, "Detecting Steganographic Content on The Internet," ISOC Network and Distributed System Security Symposium, San Diego, CA,2002.

[9] P. Sallee, "Model-based steganography," *Proc. of the 2nd Internation Workshop on Digital Watermarking*, vol. 2939, pp. 154-167, Springer, 2003.

[10] X. Xia, C. Boncelet, and G. Arce, "A Multiresolution Watermark For Digital Images," in *Proc. IEEE Int. Conf. Image Processing*, vol. 1, pp. 548–551, Oct. 1997.

[11] M. Barni, F. Bartolini, and A. Piva, "Improved Wavelet-Based Watermarking Through Pixel-Wise Masking," *IEEE Trans. Image processing*, vol. 10, no. 5, pp.783-791, May 2002.

[12] D. Kundur and D. Hatzinakos, "A robust digital image watermarking method using wavelet-based fusion," in *Proc. IEEE Int. Conf. Image Processing*, vol. 1, pp. 544–547 ,Oct. 1997.

[13] G. Bhatnagar and B. Raman, "A New Robust Reference Watermarking Scheme Based on DWT-SVD," Computer Standards and Interfaces, vol.31, no.5, pp. 1002-1013, 2009.

[14] S. Wang and Y. Lin, "Wavelet Tree Quantization for Copyright Protection Watermarking," *IEEE Trans. Image processing*, vol. 13, no. 2, pp.154-165, Feb. 2004.

[15] K. Ramani, E. V. Prasad, Dr. S. Varadarajan, "Steganography Using Bpcs To The Integer Wavelet Transformed Image," *Intl. Journal of Computer Science and Network Security*, vol. 7 no. 7, pp. 293-302, July 2007.

[16] A. Haj and A. Errub, "Performance Optimization of Discrete Wavelets Transform Based Image Watermarking Using Genetic Algorithms," *Journal of Computer Science*, vol. 4 , no. 10, pp. 834-841, 2008

[17] A. Singh and A. Mishra, "Wavelet Based Watermarking On Digital Image," *Indian Journal of Computer Science and Engineering*, vol. 1, no. 2, pp. 86-91,2011.

[18] B. K. Pandhwal and D. S. Chaudhari, "An Overview of Digital Watermarking Techniques ," Intl. Journal of Soft Computing and Engineering, vol.3, no.1, pp. 416-420, 2013.