RESEARCH ARTICLE OPEN ACCESS

A Review: A Digital Image Steganography

Mrs.M.A.Wakure [1], Mrs.S.A.Wakure [2]
Department of Computer Science & Engineering [1]
Dr. BAMU University, Osmanabad
Department of Electronics & Telecommunication Engineering [2]
JSPM'S COE, Pune University
Pune - Maharashtra

ABSTRACT

Now a days, a lot of applications are Internet based and in some cases it is desired that the communication be made secret, digital communication has become an essential part of infrastructure. Information hiding has an important research field to resolve the problems in network security, quality of service control & secure communication through public & private channels. Steganography is the science that involves communicating secret data in an appropriate multimedia carrier, e.g., image, audio, and video file. Steganography has various useful applications. Steganography's ultimate objectives, which are undetectability, robustness (resistance to various image processing methods and compression) and capacity of the hidden data, are the main factors that separate it from related techniques such as watermarking and cryptography. This paper provides a state-of-the-art review of existing methods of steganography in digital images.

Keywords :- Information hiding, Security, Steganography, Staganalysis.

I. INTRODUCTION

Internet has an become essential the most effective and fastest media for communication and transmitting Large amount of data in different part of the world. The safe & secure transmission of long distance communication remains an issue. Hence, the need for secret communication is required. Cryptography [1,2] and Steganography are the two fields for data security.[3,4]. In Cryptography, the data is encrypted so that it cannot understood by any one else. The encrypted data is unreadable but is not hidden from the eavesdroppers. Cryptography has helped in data surety but it has some disadvantages. The encrypted data will arous suspicion to unwanted users and there is possibility of it being decrypted or being suppressed. The Steganography solve this problem by embedding d in the cover object so that it is hard to detect.

There are other two techniques related to steganography are watermarking and fingerprinting. Watermarking is the process that embeds data called watermark tag or label into a multimedia object such that watermark can be detected or extracted to make an assertion about the object. In fingerprinting unique marks are embedded in distinct copies of the carrier object that are supplied to different customers. Steganography is the art and science that hides the information in an appropriate cover carrier like image , text, audio and video media. Following fig.1 shows classification of data hiding techniques [14].

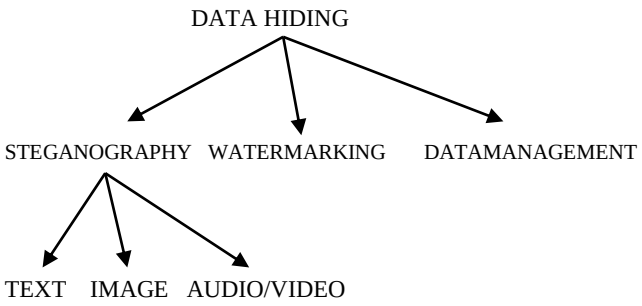

Fig. 1. Classification of Data Hiding

Steganography technique based on the two approaches i.e spatial domain and frequency domain approach. In spatial domain approach secret message are embedded into least significant pixels of cover image. They are fast but sensitive to image processing attacks. In frequency domain transforming the cover image into the frequency domain coefficients before embedding secret messages in it. The transformation can be either Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) . Though these methods are more difficult & slower than spatial domain. They have an advantage of being more secure and noise tolerant[5].

This paper is organized as follows. Section II describe the spatial domain method which involves encoding at the LSB's level. Section III describes the frequency domain methods such as discrete cosine transform (DCT) and discrete wavelet transform (DWT). Section IV describes analysis of

different existing methods of Steganography. Finally section V describes conclusion.

II. STEGANOGRAPHY IN THE SPATIAL DOMAIN

In spatial domain methods a Steganographer modifies the secret data and the cover medium in the spatial domain, which is the encoding at the level of the LSBs.This method has the largest impact compared to the other two methods even though it is known for its simplicity [6, 7]. Embedding in the 4th LSB generates more visual distortion to the cover image as the hidden information is seen as "non-natural". Potdar et al., used this technique in producing fingerprinted secret sharing Steganography for robustness against image cropping attacks[8]. This paper addressed the issue of image cropping effects rather than proposing an embedding technique. The logic behind their proposed work is to divide the cover image into sub-images and compress and encrypt the secret data. The resulting data is then sub-divided and embedded into those images portions. To recover the data a Lagrange Interpolating Polynomial was applied along with an encryption algorithm. The computational load was high, but their algorithm parameters, namely the number of sub-images (n) and the threshold value (k) were not set to optimal values leaving the reader to guess the values. If n is set, for instance, to 32 that means we are in need of 32 public keys, 32 persons and 32 sub-images, which turns out to be unpractical. Moreover, data redundancy that they intended to eliminate does occur in their stego-image. Shirali-Shahreza [9] exploited Arabic and Persian alphabet punctuations to hide messages. While their method is not related to the LSB approach, it falls under the spatial domain. Unlike English which has only two letters with dots in their lower case format, namely 'i' and 'j', Persian language is rich in that 18 out of 32 alphabet letters have points. The secret message is binarized and those 18 letters' points are modified according to the values in the binary file. Colour palette based Steganography exploits the smooth ramp transition in colours as indicated in the colour palette. The LSBs here are modified based on their positions in the said palette index. Johnson and Jajodia were in favour of using BMP (24-bit) instead of JPEG images.

Their next best choice was GIF files (256-color). BMP as well as GIF based Steganography apply LSB techniques, while their resistance to statistical counter attack and compression are reported to be weak . BMP files are bigger in size than other formats which is improper for network transmissions. However, JPEG images were at the beginning avoided because of their compression algorithm which does not support a direct LSB embedding into the spatial domain[10].

Spatial Steganography generates unusual patterns such as sorting of colour palettes, relationships between indexed colours, exaggerated noise , etc, all of which leave traces to be picked up by Steganalysis tools. There is a serious conclusion drawn in the literature- "LSB encoding is extremely sensitive to any type of filtering or manipulation of the stego-image. Scaling, rotation, cropping, addition of noise, or lossy compression to the stego-image is likely destroy the message. Furthermore an attacker can easily remove the message by removing (zeroing) the entire LSB plane with very little change in the perceptual quality of the modified stego-image" [6]. Almost any filtering process will alter the values of many of the LSBs [11]. By inspecting the inner structure of the LSB, Fridrich et al., claimed to be able to extract hidden messages as short as 0.03bpp (bit per pixel) [12]. Xiangwei et al., stated that the LSB methods can result in the 'pair effect' in the image histograms. This 'pair effect phenomenon is observed in Steganography based on the modulus operator. This operator acts as a means to generate random locations to embed data**.** It can be a complicated process or a simple one like testing in a raster scan if a pixel value is even then embed, otherwise do nothing [13]. The least-significant bit (LSB) insertion method is the most common and easiest method for embedding messages in an image. The basic idea of LSB embedding is to embed the message bit at the rightmost bits of pixel value so that the embedding method does not affect the original pixel value greatly. The formula for the embedding is as follows:

$X^2 = X - X \bmod 2k + b$

where k is the number of LSBs to be substituted. The extraction of message from the high frequency coefficients is given as: $b = X \bmod 2k$

There are two types of LSB insertion methods, fixed-sized and variable-sized. The former embeds the same number of message bits in each pixel of the cover-image. On embedding fixed four random bits in the four LSBs of each pixel, some false contours can occur. The unwanted artifacts may arise suspicion and defeat the purpose of steganography. To treat this problem, either fewer bits must be used for message embedding or a variable-sized method needs to be applied. For the variable-sized embedding method, the number of LSBs in each pixel used for message embedding depends on the contrast and luminance characteristics. Thus the most important requirement is maintaining the image fidelity while adapting these local characteristics to estimate the maximum embedding capacity [14]. Direct LSB techniques handles large payload But often offset the statistical properties of the image.

III. STEGANOGRAPHY IN THE FREQUENCY DOMAIN

The need for enhanced security, has led to the development of other algorithms. LSB technique has weak resistance to attacks. So to overcome this shortcoming, researchers found a better way for hiding information in areas of the image that are less exposed to compression, cropping, and image processing. Steganographic methods of the second type employ the transformed domain of a host image to hide secret data[15]. Transformation functions like the discrete cosine transform (DCT) or discrete wavelet transform (DWT) are first exploited to transform the pixel values in the spatial domain to coefficients in the frequency domain. Then the secret data are embedded in the coefficients. A lossless and reversible steganography scheme has been introduced that use each block of quantized discrete cosine transformation (DCT) coefficients in JPEG images for embedding secret data [16]. In this scheme, the two successive zero coefficients of the medium-frequency components in each block are used to hide the secret data. This method results in a high image quality of stego image and successfully achieves reversibility. A reversible data hiding scheme that use the histogram shifting method based on DCT coefficients was proposed [17].

Cover images are partitioned into several different frequencies, and the high-frequency parts are used for embedding the secret data. For hiding secret data, this method of histogram shifting shifts the positive coefficients around zero to the right and the negative coefficients around zero to the left . It improves the hiding capacity and quality of the stego-images. On reversing the frequency domain stego-image back to the spatial domain image may cause underflow and overflow problems. Wavelets transform (WT) converts spatial domain information to the frequency domain information. 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. Many practical tests propose to use the Wavelet transform domain for steganography because of a number of advantages. The use of such transform will mainly address the capacity and robustness of the Information Hiding system features. A Haar discrete wavelet transformation (HDWT)- based reversible data hiding method was proposed in 2009 [19]. In this method a spatial domain image is transformed into a HDWT-based frequency domain image and then the high frequency coefficients are used to embed the secret data. This method provides a high hiding capacity and a good stego-image quality. In the recent year DWT based algorithm for image data hiding has been proposed that uses CH band of cover image for hiding the secret message. Vijay kumar [18] proposed an algorithm in which secret message is embed in different bands of cover image. PSNR has been used to measure the quality of stegano image and it gives better PSNR by replacing error block with diagonal detail coefficients (CD) as compare to other coefficients. A new image steganography technique based on Integer Wavelet Transform (IWT) and Munkres' assignment algorithm was introduced. IWT converts spatial domain information to the frequency domain information. For embedding secret data, assignment algorithm is used for best matching between blocks. Stego image is subjected to various types of image processing attacks and it shows high robustness against these attacks. The experiments on the Discrete Cosine Transform (DCT) coefficients showed promising results and redirected researchers' attention towards this type of image. In fact acting at the level of DCT makes Steganography more robust and not as prone to many statistical attacks.

Prabakaran G. proposed a steganography approach for hiding a large-size secret image into a small-size cover image. Transformation is performed to scrambles the secret image. Both secret and cover images are decomposed using discrete wavelet transform (DWT) and followed by Alpha blending operation [20]. Discrete wavelet coefficients are used for hiding the data in order to maximize the hiding capacity. This DWT based approach provides high security and certain robustness.

IV. ANALYSIS

Three common requirements, security, capacity, and imperceptibility, may be used to rate the performance of steganographic techniques. As a performance measure for image distortion due to embedding, the well-known peak-signal-to noise ratio (PSNR), which is categorized under difference distortion metrics, can be applied to stego images.

$$PSNR = 10\log_{10}\left(\frac{255^2}{RMSE}\right) \quad (1)$$

Where MSE denotes the mean square error, which is given as

$$RMSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j) - F(i,j)]^2}{M * N} \quad (2)$$

Where and are the image coordinates, and are the dimensions of the image, is the generated stego-image and is the cover image. Also represents the maximum value in the image. The original cover image sized and the stego image sized, and the and are pixel located at the row and the column of images and , respectively.

Spatial domain techniques have large payload but often offset the statistical properties of the image. It is not robust against lossy compression, image filters, rotation, cropping and translation noise. As LSB insertion is simpler and good for steganography, we can try to improve one of its major drawbacks: the ease of extraction. We don't want that an eavesdropper be able to read everything we are sending.

DCT based domain techniques are less prone to attacks than the spatial domain methods at the expense of capacity. It is not robust against rotation, cropping and translation. Embedding in the DWT domain gives better result.

V. CONCLUSION

Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. It is therefore a book on magic. It is emerging in its peak because it does not attract anyone by itself. In this paper reviewed stegnographic techniques. In spatial domain LSB technique have high payload but they fail to prevent statistical attacks and thus easily detected. The emerging techniques such as DCT, DWT and Adaptive Steganography are not an easy target for attacks, especially when the hidden message is small. That is because they alter bits in the transform domain, thus image distortion is kept to a minimum. Generally these methods tend to have a lower payload compared to spatial domain algorithms. In short there has always been a trade off between robustness and payload.

REFERENCES

[1] Bruice Schneier, "Applied Cryptography Protocols, Algorithm and Source Code in C", Second edition. Wiley India edition 2007.

[2] W.Diffie and M. E. Hellman, "Exhaustive Cryptanalysis of the NBS Data Encryption Standard,‖ IEEE Computer", Vol. 10, 1977, pp. 74-84.

[3] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods Signal Processing ", (2010) 727–752.

[4] S. Katzenbeisser, F.A.P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, Norwood, MA, 2000.

[5] Ahmed A. Abdelwahab and Lobha A. Hassan, "A discrete Wavelet Transform based technique for image data hiding", 2 nd National Radio science Conference, Egypt,2008.

[6] Lin, E. T. and Delp, E. J., "A Review of Data Hiding in Digital Images. Retrieved on 1.Dec.2006 from Computer Forensics, Cyber crime and Steganography Resources, Digital Watermarking Links and Whitepapers" , Apr 1999.

[7] Kermani, Z. Z. and Jamzad, M., " A Robust Steganography Algorithm Based on Texture Similarity using Gabor Filter. Proceedings of IEEE 5th International Symposium on Signal Processing and Information Technology" , 18-21 Dec. 2005, 578-582.

[8] Potdar, V. M., Han, S. and Chang, E., " Fingerprinted Secret Sharing Steganography for Robustness against Image Cropping Attacks. Proceedings of IEEE's 3rd International Conference on Industrial Informatics (INDIN)", Perth, Australia, 10-12 August 2005.

[9] Shirali-Shahreza, M. H. and Shirali-Shahreza, M., " A New Approach to Persian/Arabic Text Steganography. Proceedings of 5th IEEE/ACIS International Conference on Computer and Information Science (ICIS-COMSAR 2006)" 10-12July 2006, 310- 315.

[10] Johnson, N. F. and Jajodia, S., "Exploring Steganography: Seeing the Unseen" , IEEE Computer, 31 (2): 26-34, Feb 1998.

[11] Anderson, R. J and Petitcolas, F.A.P., "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4): 474-481, May 1998.

[12] Fridrich, J., Goljan, M. and Du, R., "Reliable Detection of LSB Steganography in Grayscale and Color Images. Proceedings of ACM, Special Session on Multimedia Security and Watermarking", Ottawa, Canada, October 5, 2001, pp. 27- 30.

[13] Xiangwei Kong, Ziren Wang and Xingang You., "Steganalysis of Palette Images: Attack Optimal Parity Assignment Algorithm", 860- 864, 06-09 Dec 2005.

[14] S.K.Muttoo,Sushil Kumar**, "**A mulltilayred secure, robust and high capacity image steganographic algorithm*"*, 2011.

[15] A.M. Fard, M. Akbarzadeh-R., and F. Varasteh-A., "A new genetic algorithm approach for secure JPEG steganography", in Proc. of IEEE International Conference on Engineering of Intelligent Systems ICEIS, 2006. pp. 216-219.

[16] C.C. Chang et al., "Reversible hiding in DCT-based compressed images", Information Sciences 177 (2007) 2768–2786.

[17] Yih-Kai Lin, "High capacity reversible data hiding scheme based upon discrete cosine Transformation", The Journal of Systems and Software 85 (2012) 2395– 2404.

[18] Vijay Kumar and Dinesh Kumar, "Performance Evaluation of DWT Based Image Steganography", 2010 IEEE 2nd International Advance Computing Conference.

[19] Y.K. Chan et al, "A HDWT-based reversible data hiding method", The Journal of Systems and Software 82 (2009) 411–421.

[20] Prabakaran. G and Bhavani.R, "A Modified Secure Digital Image Steganography Based on Discrete Wavelet Transform",International Conference on Computing, Electronics and Electrical Technologies [ICCEET], 2012.