Scientific Journal of Impact Factor(SJIF): 3.134
e-ISSN(O): 2348-4470
p-ISSN(P): 2348-6406

International Journal of Advance Engineering and Research Development

Volume 2,Issue 5, May -2015

A REVIEW PAPER ON STEGANOGRAPHY

VEENU YADAV[1], PRABHAKAR SHARMA[2]

[1]C.S.E, Raipur Institute of Technology
[2] C.S.E, Raipur Institute of Technology

Abstract—*This paper provides a review on steganography techniques, their advantages and disadvantages. Today the tremendous increase in data flow on internet has raised various security concerns. The information being transferred, must be secure from a third party or any unauthorized person. The steganography provides a way to hide a sensitive message within a cover file discreetly. The message can be either text, audio or video.*

Keywords— *Steganography, Stego-Image, Transform domain, Spatial domain, Payload.*

I. INTRODUCTION

Steganography is a special way of hiding data under data, so that it passes unnoticed from an unaware observer, or unauthorized person. This is actually, the very aim of steganography. It consists of two Greek words - steganos and graphia, where steganos means secret/covered and graphia means graphic, i.e. drawing or writing. In steganography, the sender embeds his message in a cover file, which be either text, image or video. The resulting file is called stego. This technique is not very new, but it has been there for ages. The methods used by military included invisible ink and microdots, etc. Some of them etched messages on a wooden table and covered with wax. They also used to tattoo a shaved messenger's head, let the hair re-grow and then the recipient will shave it again to view the message.

Steganography should not be confused with cryptography. The latter one changes the format of data so that it cannot be understood by an eavesdropper, while the former one simply hides the message or data itself so that it becomes invisible which makes it very difficult for an unaware observer to find where the message is.

The performance of a steganographic system is analyzed on three basis: statistical undetectability, i.e. imperceptibility, its capacity, and finally its robustness. The undetectability property shows how difficult it is to find the hidden message, capacity is a measure of how much data can be hidden, and robustness is a criterion of being able to withstand the attacks on the system.

II. STEGANOGRAPHY

There are two types of steganography- fragile, and robust. The fragile steganography loses the hidden message if the stego file is modified in any way. For example, if the stego-image is in .jpg format and we convert it to .bmp or some other format, the message is destroyed. In robust steganography, the secret message is not so easily destroyed. However, it is also difficult to implement[1].

For steganography, we need a secret message, and a cover image(in which the message is to be hidden). Also, a secret key is required that is shared between the sender and receiver, utilised for embedding and extraction of the secret message. After embedding, the cover image plus the secret information become stego-image. This is now sent over a communication channel, and at the receiver side extraction is performed using the same key with which embedding was done.

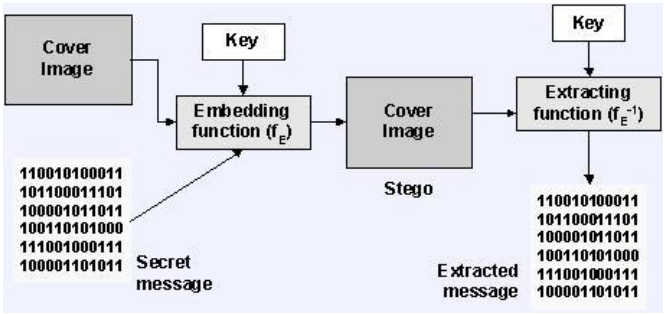

Fig.1 General block diagram of steganography

On the basis of file formats, steganography can be classified as,

- **Text based steganography**- The message to be sent is embedded in a text file using line shift coding, word shifting, feature coding, etc. Reformatting of the text destroys hidden message, hence this method is fragile.
- **Audio steganography**- Alters audio files so that they contain hidden messages. The techniques implemented here are, echo hiding, phase coding, LSB substitution, etc.
- **Image steganography**- Message is hidden in images. This is the most popular steganographic technique because almost full imperception of the secret message. It also provides high capacity i.e, large amount of data

can be hidden in an image. Depending on the procedure of embedment, it can be widely categorised in to spatial domain (image/pixel domain), or transform domain (frequency domain). Most commonly used technique is the LSB substitution, where the LSBs of cover image are modified according to the message to be hidden.

- **Video steganography**- This extends the application of image steganography discussed above. Video steganography hides data in a digital video format like AVI, MPEG, mp4, etc. Video is used as a cover for the payload (or secret info). It processes a video frame by frame, where the data is actually hidden.

III. STEGANOGRAPHY IN SPATIAL DOMAIN

Steganography techniques that modify/alter the pixels directly to hide a message are known as spatial domain methods. The LSB (least significant bit) substitution is the most commonly used approach [2]. The underlying concept here is to hide the payload in the bits of cover image which have least significance/weight, so that original pixel value is not affected much.

A novel method to hide a secret message in a gray-scale cover was developed in [3]. Here, the cover image is partitioned in to non overlapping blocks of two consecutive pixels. Then a difference value is computed from the values of two pixels. This difference value is now replaced to hide the secret message. This technique produces better results in terms of imperceptibility as compared to simple LSB techniques. Lin et.al [4] proposed a technique with distortion tolerance, giving better quality processed image.

The simplicity of LSB substitution technique, while being advantageous also creates a basic disadvantage; the extraction is also simple. Thus an eavesdropper may easily extract the hidden message.

IV. STEGANOGRAPHY IN TRANSFER DOMAIN

In wake of LSB technique's limited resistance to attacks, other techniques for data security were developed, which were less vulnerable to cropping, compression and image processing. The idea of steganography was extended from spatial domain to the transform domain. A reversible and loss-less technique has been developed that uses each quantised block of DCT coefficients in images to hide discrete data [5]. This method gives high image quality, and reversibility too. Another reversible data hiding approach using histogram shifting method based on DCT coefficients was proposed in [6]. Here, cover image is partitioned into blocks of different frequencies. The high frequency blocks are used to embed secret data. The process of histogram shifting implemented here shifts the positive coefficients around zero to the right and negative ones to the left. It elevates both the data hiding capacity and stego image quality. However, this may cause underflow and overflow problems.

The wavelet transform (WT) has also been utilised in steganography, because it separates the high frequency and low frequency information pixel-wise. The use of WT offers numerous advantages, such as increased capacity and robustness. A discrete wavelet transform based reversible steganography model , using Haar wavelet family was proposed in [7]. In this technique, a spatial domain cover image is converted in frequency domain, using HDWT (Haar discrete wavelet transform). As previously, high frequency coefficients are used to hide the secret message.

V. ATTACKS ON STEGANOGRAPHY

The steganography system is not perfect. That is, a third party (attacker) can try and detect/destroy the embedded payload in many ways. If the attacker gets hold of the cover image used, he simply has to do a bit by bit comparison with the stego-image to obtain the hidden message. That's why publicly accessible images (like those on internet) should never be used as cover. The ability of a steganographic system to withstand various attacks determines its robustness. Following are the categories of basic attacks on a steganography system.

- Stego only: The attacker has access to the stego-image and needs to determine the presence of payload. This is the weakest form of attack. It is completely dependent upon statistical analysis to reveal the existence of a secret message.
- Stego and cover: The third party has somehow gotten hold of the stego and cover image. As discussed earlier, the embedded message can be determined by difference in both files. The attacker, in this case can replace the stego file in the channel with original cover image to simply destroy the message.
- Reformatting: The attacker can change the file format (eg., from jpg to bmp, tif, png, etc) . This type of attack is possible since different formats store data in different ways.
- Compressing: Another simple yet effective attacking idea is to compress the stego image. Different compression formats try to remove the extraneous information from the image (like JPEG).
- Visual attack: This is done by stripping away a part of stego image so that a human can perceive visual anomalies and detect the presence of a hidden message. It is only effective when steganography is based on LSB substitution technique. It's slow and costly too. Digital cameras and scanners often leave echoes in the LSBs. These random noises actually reveal the presence of a secret payload in the images.

- Structural attack: The embedment of payload alters the structure of cover image, i.e., the steganography system leaves a characteristic structure in the data. By analyzing the bit statistical profile, the existence of secret message can be determined. A steganography algorithm that leaves such changes in the data file actually falls in the category of easily detectable patterns.
- Statistical attacks: It is a false assumption that the least significant bits are absolutely random and thus replaced by secret data. Statistical attacks compare the frequency distribution of a possible cover image, with the theoretically expected distribution of the cover image. If the obtained image doesn't contain the same expected statistical profile, then it can be said that it contains some secret information.

VI. ATTACKS

The most common measures for performance analysis are peak signal to noise ratio (PSNR) and mean square error (MSE). The expressions for both are as follows

$$PSNR = 10log(\frac{C_{max}^2}{MSE})$$

$$MSE = \frac{1}{MN}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

where x and y are image coordinates, and M and N are the dimensions of the image. S_{xy} is the stego -image and C_{xy} is the cover image and C_{max}^2 is the maximum value of image. The other image quality metrics are normalized cross correlation coefficient (NCC), maximum difference (MD) and average difference (AD) [8].

$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})\frac{1}{\sum_{j=1}^{M}\sum_{k=1}^{N}x_{j,k}^2}$$

$$MD = Max(|x_{j,k-}x'_{j,k}|)$$

$$AD = \sum_{j=1}^{M}\sum_{k=1}^{N}\frac{x_{j,k-}x'_{j,k}}{MN}$$

where $x_{j,k}$ and $x'_{j,k}$ are cover image and stego image pixels corresponding to jth row and kth column, respectively.

Spatial domain techniques have large capacity, but suffer from a major drawback- easy extraction due to alteration of statistical properties of image. It's also not able to withstand lossy compression, image filters, rotation, cropping and translation noise. Whereas DCT based steganography techniques tradeoff robustness with capacity. However it is also prone to rotation, cropping and translation. DWT steganography provides better result [9].

VII. CONCLUSION

Different basic steganography techniques have been discussed in this paper, with their advantages and limitations. All of them focus on three requirements - imperceptibility, robustness and capacity. LSB methods offer higher payload capacity, but fail to be robust against most common of the attacks. The frequency domain techniques (DCT) are successful in hiding small messages. That is, they aren't prone to usual attacks until the message is large. In other words, they suffer from small capacity issue. They often modify high frequency coefficients in transform domain, and thus produce minimal distortion. However, working with the discrete wavelet transform (DWT) technique is better as compared to the LSB and DCT based steganography. Nowadays with the extensive research already going on in this field the steganography at higher levels is based on hybrid domain, or is adaptive. Hybrid domain includes operating on the spatial as well as transform domain of the cover image. Adaptive being in the sense that it is statistics aware version of plain steganography. Statistical characteristics of cover image decide what sort of changes can be made to the pixels. Thus a huge number of data hiding schemes exist, and all of them are analysed in performance according to the three parameters discussed earlier.

REFERENCES

[1] Steganography And Digital Watermarking, Copyright © 2004, Jonathan Cummins, Patrick Diskin, Samuel Lau and Robert Parlett, School of Computer Science, The University of Birmingham.
[2] Chan, C.K., Chang, L.M., "Hiding data in image by simple LSB substitution", Pattern Recognition, vol 37, pp.469-471, 2003.
[3] Da-Chun Wu, Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters 24 (2003) 1613–1626.

[4] I.-C. Lin et al, "Hiding data in spatial domain images with distortion tolerance", Computer Standards & Interfaces 31 (2009) 458–464.
[5] C.-C. Chang et al., "Reversible hiding in DCT-based compressed images", Information Sciences 177 (2007) 2768–2786.
[6] Yih-Kai Lin, "High capacity reversible data hiding scheme based upon discrete cosine Transformation", The Journal of Systems and Software 85 (2010) 2395– 2404.
[7] Y.-K. Chan et al, "A HDWT-based reversible data hiding method", The Journal of Systems and Software 82 (2009) 411–421.
[8] N.Raftari, "Digital Image Steganography Based on Integer Wavelet Transform and Assignment Algorithm", 2011 Sixth Asia Modelling Symposium.
[9] Cheddad, J. Condell, K. Curran and P.M. Kevitt. (2012), "Digital image steganography: survey and analysis of current methods", Signal Processing Journal. [On line]. 90(3), pp.727-752. Available: http://www.abbascheddad.net/Survey.pdf [Aug. 2013].

