Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 1, January 2014, pg.300 – 308

RESEARCH ARTICLE

THE IMAGE STEGANOGRAPHY AND STEGANALYSIS BASED ON PEAK-SHAPED TECHNIQUE FOR MP3 AUDIO AND VIDEO

P.Manimegalai[1], K.S.Gomathi[2], D.Ponniselvi[3], M.Santha[4]

[1](M.Phil.) Department of Computer science, Vivekanandha College of Arts and Sciences for Women, Namakkal

[2](M.Phil.) Department of Computer sciences, Vivekanandha College of Arts and Sciences for Women, Namakkal

[3]Assistant professor, Department of Computer science, Vivekanandha College of Arts and Sciences for Women, Namakkal,

[4]Assistant professor, Department of Computer science, Vivekanandha College of Arts and Sciences for Women, Namakkal,

[1] kp.manimegalai@gmail.com; [2] gomathiksraju@gmail.com; [3] gokulponnics@gmail.com; [4] shanthaa30@gmail.com

ABSTRACT: In this paper provides on steganography and steganalysis for digital images, mainly covering the fundamental concepts, the progress of steganographic methods for images in spatial representation and in JPEG format, and the development of the corresponding steganalytic schemes. The steganographic technique for the MP3 audio and video format, which is based on the Peak Shaped Model algorithm used for JPEG images. The proposed method relies on the statistical properties of MP3 samples, which are compressed by a Modified Discrete Cosine Transform (MDCT). After the conversion of MP3, it's possible to hide some secret information by replacing the least significant bit of the MDCT coefficients. The performance analysis has been made by calculating three steganographic parameters: the Embedding Capacity, the Embedding Efficiency and the PSNR. It has been also simulated an attack with the Chi-Square test and the results have been used to plot the ROC curve, in order to calculate the error probability.

Keywords: Information hiding; Steganalysis; MP3 Steganography; Digital Image; Peak-Shaped Technique

I. INTRODUCTION

Cryptography is often used to protect information secrecy through making messages illegible. Steganography refers to the technique of hiding information in digital media in order to conceal the existence of the

information. The media with and without hidden information are called stego media and cover media, respectively. Steganography can meet both legal and illegal interests. For example, civilians may use it for protecting privacy while terrorists may use it for spreading terroristic information. 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. For more details on the difference between steganography and digital watermarking please refer to ref.

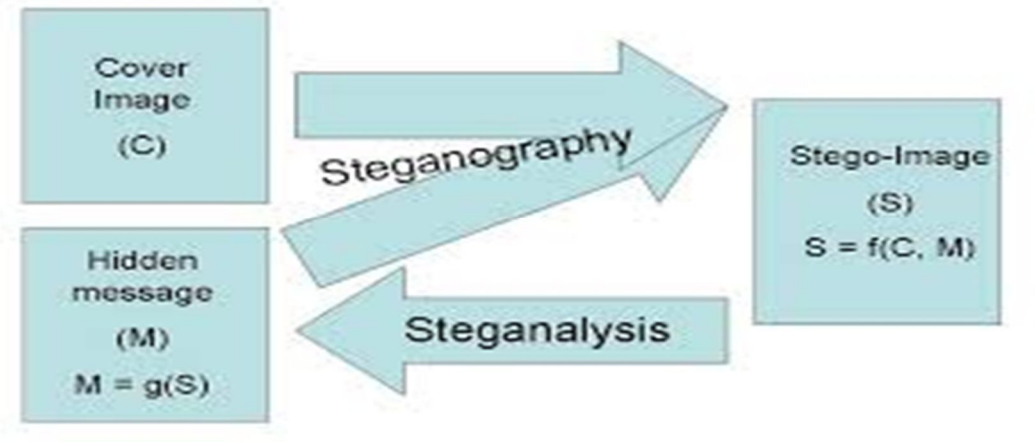

Figure 1: The Model of steganography and steganalysis

Steganography techniques are used to hide secret information in the most common audio/video formats. There are three main different kinds of audio/video steganography

1) Insertion steganography, where the secret message is inserted in the cover object;
2) Substitution steganography, where some bits of the cover object are substituted with the bits of the secret message;
3) Constructing steganography, where an ad hoc cover object is generated to contain the secret message.

The developed technique is based on LSB steganography, a substitution steganography, that replaces the least significant bit of the audio/video file with the secret message bit. This method is very simple to implement and does not allow the human eye/hear to perceive significant changes in the stego object.

However, this technique has lower resistance to the statistical attacks since with a proper steganalysis it is possible to detect the secret information. To solve this problem, Model Based Steganography can be used. The cover object is divided into two parts, and to embed the secret information. The first part is the most relevant, and it will not be modified. The second one is less relevant with respect the other and it will contain the secret message. The division is based on the statistical model of the cover object.

The union between this part and is the stego object. The purpose of this paper is to present a new steganographic algorithm for the MP3 format based on the change, in the Peak Shaped Based for the JPEG, of the discrepancy equation, adapting it to vectors and studying the statistical distribution of the MDCT coefficients. In the following the analysis of the performance of the proposed algorithm is shown and it is demonstrated that this method does not introduce audible distortion when the signal audio is reproduced. Further, it is demonstrated that this method does not create relevant statistical differences in the samples distribution, showing its suitability for steganographic applications and its robustness to steganographic attacks.

II. BASIC MODEL AND CRITERIA CONCEPTS

Three common requirements, security, capacity, and imperceptibility, may be used to rate the performance of steganographic techniques Security. Steganography from many active or passive attacks, correspondingly in the prisoner's problem when Wendy acts as an active or passive warden. If the existence of the secret message can only be estimated with a probability not higher than random guessing in the presence of some steganalytic systems, steganography may be considered secure under such steganalytic systems. Otherwise we may claim it to be insecure. To be useful in conveying secret message, the hiding capacity provided by steganography should be as high as possible, which may be given in absolute measurement (such as the size of secret message), or in relative value (called data embedding rate, such as bits per pixel, bits per non-zero discrete cosine transform coefficient, or the ratio of the secret message to the cover medium, etc.) Imperceptibility. Stego images should not have severe visual artifacts.

Under the same level of security and capacity, the higher the fidelity of the stego image, the better. If the resultant stego image appears innocuous enough, one can believe this requirement to be satisfied well for the warden not having the original cover image to compare.

A. Criteria for Steganalysis

The main goal of steganalysis is to identify whether or not a suspected medium is embedded with secret data, in other words, to determine the testing medium belong to the cover class or the stego class. If a certain steganalytic method is used to steganalyze a suspicious medium, there are four possible resultant situations.

- True positive (TP), meaning that a stego medium is correctly classified as stego.
- False negative (FN), meaning that a stego medium is wrongly classified as cover.
- True negative (TN), meaning that a cover medium is correctly classified as cover.
- False positive (FP), meaning that a cover medium is wrongly classified as stego.

B. Steganographic Security

Security is the most important evaluation criterion in steganography and steganalysis. There are several kinds of definition of steganographic security, each of which are defined from different viewing angles.

1. Information Theoretical Security

From the point of view of information theory,Cachin quantified the security of a steganographic system in terms of the relative entropy between the distribution of X, denoted by PX, and that of Y , denoted by PY ,in face of passive attacks. The relative entropy between PX and PY is defined the security.

2. ROC-based Security

In several shortcomings in the information theoretical definition of steganographic security are discussed and an alternative security measure based on steganalyzer's ROC performance is then proposed. The ROC is a plot of false positive rate versus true positive rate, which represents the achievable performance of a steganalytic system.

C. Image Steganography

Although steganography for binary images and the images have some progresses, researches mainly concentrate on hiding data in gray-scale images and color images. Since the luminance component of a color image is equivalent to a gray-scale image, we focus on the steganography for gray-scale images.

Besides, it is generally considered that gray-scale images are more suitable than color images for hiding data because the disturbance of correlations between color components may easily reveal the trace of embedding. If not specified, the images in this paper are referred to 8-bit gray-scale images. Owing to the fact that bitmap/raw and JPEG images are of great interests in steganography community, we focus on spatial steganography and JPEG steganography.

III. JPEG STEGANOGRAPHY

JPEG is the common format of the images produced by digital cameras, scanners, and other photographic image capture devices. Therefore, hiding secret information into JPEG images may provide better camouage. Most of the steganographic schemes embed data into the non-zero alternate current (AC) discrete cosine transform (DCT) coefficients of JPEG images. As a result, the embedding rate of JPEG steganographic is often evaluated in bit per non-zero AC DCT coefficient (bpac).

The following three major JPEG steganographic methods

A. JSteg/JPHide

Jsteg and JPHide are two classical JPEG steganographic tools utilizing the LSB embedding technique. JSteg embeds secret information into a cover image by successively replacing the LSBs of non-zero quantized DCT coefficients with secret message bits. Unlike JSteg, the quantized DCT coefficients that will be used to hide secret message bits in JPHide are selected at random by a pseudo-random number generator, which may be controlled by a key. Moreover, JPHide modifies not only the LSBs of the selected coefficients; it can also switch to a mode where the bits of the second least significant bit-plane are modified.

B. steganographic algorithm was introduced by Westfeld. Instead of replacing the LSBs of quantized DCT coefficients with the message bits, the absolute value of the coefficient is decreased by one if it is needed to be modified. The author argued that this type of embedding cannot be detected using the chi-square attack. 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. In the embedding process, the message length and the number of non-zero AC coefficients are used to determine the best matrix embedding that minimizes the number of modifications of the cover image.

C. OutGuess

OutGuess is provided by Provos as UNIX source code. There are two famous released versions: OutGuess-0.13b, which is vulnerable to statistical analysis, and OutGuess-0.2, which includes the ability to preserve statistical properties. When we talk about the OutGuess, it is referred to OutGuess-0.2. The embedding process of OutGuess is divided into two stages. Firstly, OutGuess embeds secret message bits along a random walk into the LSBs of the quantized DCT coefficients while skipping 0's and 1's. After embedding, corrections are then made to the coefficients, which are not selected during embedding, to make the global DCT histogram of the stego image match that of the cover image. OutGuess cannot be detected by chi-square attack.

IV. IMAGE STEGANALYSIS

Steganalysis can be regarded as a two-class pattern classification problem which aims to determine whether a testing medium is a cover medium or a stego one. According to its application fields, it can be divided into specification methods and universal methods. A specification steganalytic method fully utilizes the knowledge of a targeted steganographic technique and may only be applicable to such a kind of steganography.

A universal steganalytic method can be used to detect several kinds of steganography. Usually universal methods do not require the knowledge of the details of the embedding operations. Therefore, it is also called blind method. Some methods can be considered as "semi-universal".

A. Improving Steganographic Security

There are some factors that may influence the steganographic security, such as the number of changed pixels/coefficients, the amplitude of the stego-noise signal, the properties of cover images, etc. In the following we discuss some techniques for making the steganography less detectable.

1. Increasing the Embedding Efficiency

If cover images do not need to be modified at all for conveying secret information, certainly the warden cannot differentiate the cover images and stego images. Therefore, if the probability of modification to the images is less, the embedding changes to the image will reduce, and the security of the steganographic method may increase.

Define the embedding efficiency as the number of embedded bits per one embedding change. Hence, increasing the embedding efficiency is a possible way to enhance the steganographic security. One technique, called matrix encoding, can be used to increase the embedding efficiency. The concept was first proposed by Crandall and implemented by Westfeld. The basic idea is to divide coefficients into groups and use Hamming error correction codes to limit the changes in each group. A (d; n; k) code can be used to embed k bits into n coefficients by making at most d coefficients changed.

2. Enhancing Steganalytic Capability

The statistics of stego images may be different from that of cover images. However, the deviated statistics may not obviously fall outside the normal scope where the statistics of cover images belong to. Therefore, some techniques may be needed to magnify the difference between cover and stego image(thereafter cover-and-stego difference) and thus enhancing the capability of a steganalyzer.

V. PEAK-SHAPED TECHNIQUE FOR MP3 AUDIO AND VIDEO

The MP3 format was born to have good audio quality and low file size. An audio file is first converted into a digital format, with a sampling, and then it is processed with the human psychoacoustic model.

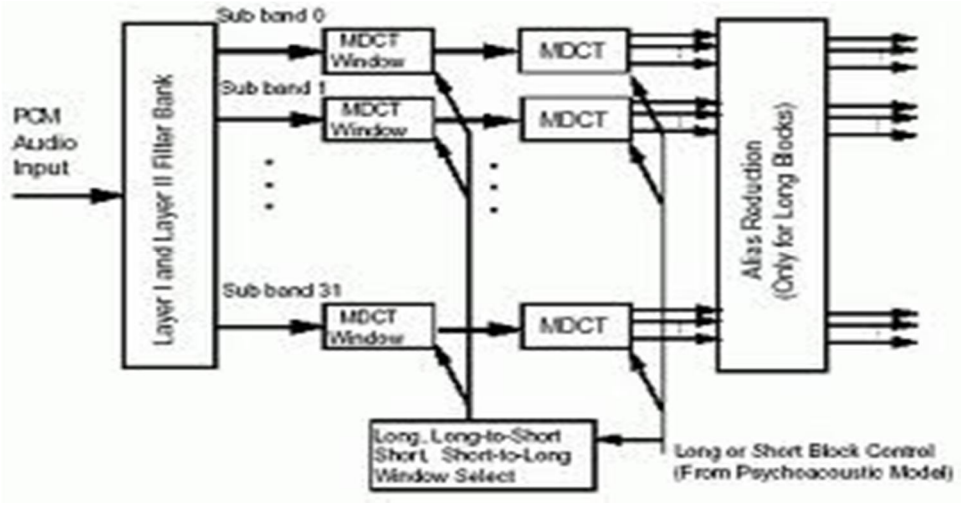

Figure 2: MDCT Filter bank

The Peak Shaped Based (PSB) steganography has been used for the JPEG format. This is a method based on:

- LSB steganography;
- Least significant bit;
- Model Based steganography.

The JPEG coefficient are, for first, divided by group, indicated with $g(b)$

$$g(b)=\text{sign}(b).[b/2] \quad \text{——————} \quad (1)$$

and by offset, indicated with 0(b)

$$0(b)=|b-2.g(b)|+1 \quad \text{——————} \quad (2)$$

The PSB algorithm is based on an assumption, from the properties of the JPEG coefficients statistical distribution processed by the algorithm F5.

$$h(b)>h(b+1) \quad \text{——————} \quad (3)$$

$$h(b)+h(b+1)>h(b+1)-h(b+2) \quad \text{——————} \quad (4)$$

where $h(b)$ indicates the histogram of the coefficient b. With this assumption is possible to calculate a probability, called "offset probability".

A. Differences between JPEG and MP3

To apply the PSB algorithm to the MP3 format it is necessary to study the differences between this format and the JPEG standard, in order to identify possible changes. These differences are:

- The JPEG uses the DCT-II while the MP3 uses the MDCT;

- The JPEG works on blocks; each blocks, or matrix, size is 8*8. Instead, the MP3 works on frame; each frame has dimension equal to 1*1152, that are vectors;
- The PSB is based on an assumption from the F5 algorithm that is used for the JPEG format.

Concerning the first point, it is possible to notice that the PSB works on the coefficients. It is therefore necessary to demonstrate that the DCT-II and the MDCT statistical distributions have the same properties.

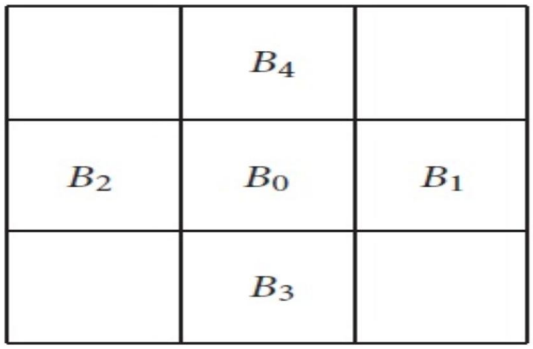

Figure 4: Adjacent blocks to the block B_0

Concerning the second point, it is necessary to detect the operations that in the PSB works on matrix and, to apply it on the MP3 format, transforming them in operations that work on vectors.

Concerning the third point, it should be studied the statistical distribution of the MP3 coefficients after the F5-algorithm in order to identify if this distribution has the same properties than the JPEG distribution processed by F5.

B. The PSB over MP3

Using the previous considerations, it is possible to apply the Peak Shaped Based steganography to the MP3 format. In fact it is possible to utilize the assumption used by this algorithm from the F5 steganography because the MP3 coefficients and the JPEG coefficients have the same statistical distribution. F5 modifies the coefficients, without considering their source. Having both formats, namely both transformed, the same statistical distribution of the coefficients, the use of different transformed becomes irrelevant to the development of the algorithm.

C. The Embedding Process

In the following, the list of steps of the embedding process is reported:

- The first step is represented by the analysis of the MP3 statistical distribution;
- Successively the value of Hg vector that contains the histograms of the MP3 is calculated;
- With the Hg values it is possible to exclude the samples that are statistical most significant;
- The coefficients *b* are divided by group, with the $g(b)$, and by offset, with the $O(b)$;
- The discrepancy is calculated by means of Equation;
- With the discrepancy, the vector ***P*** and a PRNG, according with the secret key, it is possible to determine.

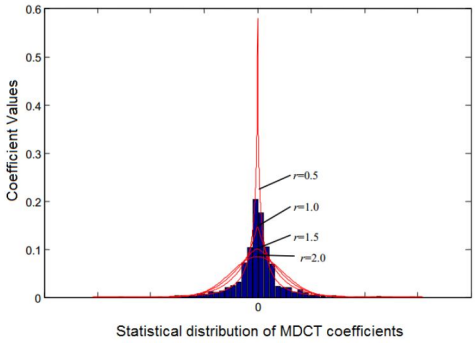

Figure 5: Statistical distribution of the MP3 coefficients approximated with the GG.

D. Chi-Square Test

A steganalytic technique that is possible to use for the PSB-MP3 is the Chi-Square test. Some parameters are calculated with the histograms of the MDCT coefficients probability distribution and the results of the Chi-Square test are compared with the threshold. One method to calculate the chi-square test is the Zhang-Ping attack that evaluates two variables:

$$chi^2 = \frac{(f_0 - f_1)^2}{f_0 + f_1} \qquad (5)$$

C. Roc Curve

This analysis to evaluate the PSB performance is done on a random set of MP3 files. With the comparison with the threshold and the Chi-Square value it is possible to calculate the two probabilities of false alarm and missed detection.

With these two probabilities it is possible to graph the ROC curve. This curve indicates the efficiency of the steganalytic method. If the curve is near the first quad- rant bisector the steganographic algorithm is very strong, otherwise the steganalytic method is efficient.

The ROC curves of the PSB algorithm for the MP3. This curve is very smash on the first quadrant bisector (dashed line). This indicates that the steganographic method is very robust when this steganalytic algorithm is used. When the ROC curve is far from the bisector the steganographic algorithm isn't very robust or else the steganalytic technique is very efficacious. Instead when this curve is very close to the bisector the technique is very secure, since there is perfect security when the ROC curve is exactly equal to the bisector.

VI. CONCLUSION

If the data are embedded in an already generated image, it may be hard to preserve the image statistics. It has been shown that it's possible to improve the steganographic security by embedding data in the creation process of JPEG images. This may be a good solution for steganography. A new steganographic algorithm for the MP3 format has been developed by changing, in the Peak Shaped Based for the JPEG, the discrepancy equation, adapting it to vectors and studying the statistical distribution of the MDCT coefficients. The analysis of the performance of this algorithm showed that this method does not introduce audible distortion when the signal audio is reproduced.

REFERENCES

[1]Huaiqing Wang and Shuozhong Wang, Cyber warfare: Steganography vs. steganalysis, Communications of the ACM, vol. 47, no. 10, pp. 76-82, 2004.

[2] R. Chandramouli, M. Kharrazi, and N. Memon, Image steganography and steganalysis concepts and practice, Proc. of IWDW'03, vol. 2939, pp. 35-49, Springer, 2003.

[3] Eiji Kawaguchi and Richard O. Eason, Principle and applications of bpcs steganography, In Multi-media Systems and Applications, vol. 3528, pp. 464-473, SPIE, 1998.

[4] Andrew Westfeld, F5-a steganographic algorithm: high capacity despite better steganalysis, Proc.of the 4th Information Hiding Workshop, vol. 2137, pp. 289-302, Springer, 2001.

[5] A. D. Ker, Fourth-order structural steganalysis and analysis of cover assumptions, Proc. of IST/SPIE Electronic Imaging: Security, Steganography, and Watermarking of Multimedia Contents VIII, vol.6072, pp. 1-14, 2006.

[6] P. Sallee, "Model-based Steganography ,"Springer Verlang, Berlin, 2004.

[7] L. Rossi, F. Garzia and R. Cusani, "Peak-Shaped Based Steganographic Technique for JPEG Images," *EURASIP Journal on Information Security*, 2009, Article ID: 382310.

[8] R. Bohme, "Advanced Statistical Steganalysis," Springer, Berlin, 2010.

[9] A. Westfeld, "F5-A Steganographic Algorithm," Springer Verlang, Berlin, 2001.

