International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

LSB and DCT Steganographic Detection Using Compressive Sensing

Anju.C.K[1], Lekshmy.S[2]

[1]PG Scholar, Department of ECE, Vimal Jyothi Engineering College

[2]Assistant Professor, Department of ECE, Vimal Jyothi Engineering College

Abstract: ***The need for preserving secrecy of sensitive data has been ever-increasing with the new developments in digital communication. During the last years, a large number of information in digital form has been exchanged all over the world. Several techniques have been developed in order to protect the users' privacy of digital content. Steganography is one of them. Its use dates back for many centuries, yet it has been used profoundly in the last decades, as the proper mathematical background has been developed along with the need of the music and film industries. This work presents two new detection methods of steganographic content through the use of compressive sensing. The first method is a probabilistic filter that can increase the probability of detecting steganographic content in images, in case where the LSB method is used. The second one helps identifying the original from stego images when DCT steganography is used, after applying a filter with compressive sensing technique.***

Keywords: Steganography, compressive sensing, steganalysis, DCT, LSB

1. Introduction

Since the mid-90s, the Internet has created a great impact in daily life of people around the world. Using the internet applications like email, the World Wide Web and file sharing, has made the communication between people easier. Nowadays, the Internet has became a source of a large number of digital files containing various forms of data, like text, music, images and videos. A high percentage of these files (e.g. image and video files) bear rights of authors, but due to their digital nature they are easy to steal and make illegal copies. For this reason these kinds of data should be protected in order to be accessible only by legitimate users. This has created the need for for media companies to invest great amounts of their budgets in protecting them and applying the so called DRM, Digital Rights Management. The most widespread method of protection demands the use of steganography in order to store valuable data like user IDs, expiration date, author name etc., in such a way that users other than the authors cannot extract or remove them.

All these have made steganography to receive a lot of attention from corporations and academia, leading to a more solid foundation of steganography and to more sophisticated approaches. The objective of steganography is to hide a secret message within a cover-media in such a way that others cannot discern the presence of the hidden message. Technically in simple words "steganography means hiding one piece of data within another". Steganography and Cryptography proposes popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the contents of message itself. Both the methods can be combined by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego-image can be transmitted without revealing that secret information is being concealed. The two most widely used techniques in images are LSB and frequency domain embedding. The first method is based on embedding the data in the least significant bits of the medium, something that introduces some distortions in the picture. These however may be untraceable, should the pixels used are properly selected. The other methods take the waveform of the image and embed the data in its DCT or DWT form by quantizing the coefficients.

2. Steganography and Steganalysis

Cryptography is one of the oldest methods of data protection and refers to data encryption by using a key and passing the encrypted message to its legal owner. Often, the use of encryption is to define the sender or the receiver as an entity that has something to hide. Apart from that, in cryptography the transmitted data are fully exposed to a third party. For example, there are two entities, "A" and "B", who are the users of the cryptography system. Entity "A" sends an encrypted text message over a public channel to entity "B". The adversary "C", who has perfect read-only access to the public channel, detects the transmission. Even though the transmitted data are encrypted, entity "C" is aware of the fact that the data are in text format. The ability of the exposal of the secret message by entity "C" depends on the strength of the encryption algorithm used by entity "B". Steganography, on the other hand, can be used for the transmission of secret messages, without the danger of exposing the transmitted data. The general model of hiding data in other data can be described as follows: The embedded data is the message that one wishes to send secretly. It is usually hidden in an innocuous message referred to as a cover-text, or cover-image or cover-audio as appropriate, producing the stego-text or other stego-object. A stego-key is used to control the hiding process so as to restrict detection and/or recovery of the embedded data to entities who know it (or who know some derived key value). As the purpose of steganography is having a covert communication between two parties whose existence is unknown to a possible attacker, a successful attack consists in detecting the existence of this communication. If steganography is considered to be the art of hiding information in a medium, then steganalysis is the art of detecting and extracting knowledge about the embedded data in a medium. Depending on the knowledge

that we have about the steganographic system and regardless of the medium that is used as a stego-object, the steganalysis techniques can be categorized to the following main three groups: Blind identification. In this group, we do not have any knowledge of the steganographic system and we try to detect steganographic data based solely on statistical properties of the medium. Parametric statistical steganalysis. In some cases we may know that the used steganographic system changes some properties of the medium with specific patterns on some of its properties. The techniques of this group try to detect the existence of steganographic data by detecting these patterns.

Supervised learning based steganalysis. These techniques use statistical classifiers to see whether the tested image is a stego image. In this group we have a set of known clean set of object and one of stego-object. These sets are used for training our algorithm to detect whether a medium is stego-object or not. Related sample pair analysis is another steganalysis method for detecting LSB data hiding in images. In this approach we take sample pairs of values and we divide them into subsets depending on the relation of the two values to one another. This technique makes the assumption that if it is not a stego image, then the number of pairs in each subset are almost equal and that LSB embedding is quantizing the subsets by changing their numbers, something that can be easily detected.

3. Compressive Sensing

Compressive sensing or sampling is a very recent branch ofsignal processing that originates from Emanuel Candes. He used data of an incomplete medical image and passed them through a sequence of *l*1 transformations, trying to improve their quality. Despite the fact that the original data was inadequate according to the known information theory, he observed that the final images were quite sharp. The results of this procedure, challenged the theorem of H. Nyquist and C. Shannon. The Nyquist-Shanon theorem provides a way to compute the nominal sampling interval required to avoid the aliasing effect. This theorem states that the sampling frequency should be at least twice the highest frequency contained in the signal. In mathematical terms: *fs* _ *fc* where *fs* is the sampling frequency (number of samples taken in time or space), and *fc* is the highest frequency contained in the specific signal. In fact, the process that Candes discovered, recreated an image file very similar to the original, using a reduced amount of image data . This can be consider a form of lossy compression method, as well. This method is called compressive sampling or compressive sensing and has been applied successfully in all forms of digital signal. Compressive sensing, also known as compressed sensing and compressive sampling is a method to reconstruct a signal from a random sparse sample. This method is used by several scientific fields in Information technology, from coding theory and MRIs to music sampling and image compression. Donoho first and then Candes, Romberg and Tao devised a method to reconstruct an image from an amount of data much less from the number of data that would be deemed sufficient by the Nyquist–Shannon sampling theorem . Their approach was that in many cases the signals are sparse, hence using another smaller basis we might be able to recover the most useful part

4. Advantage

In our work we use the compressive sensing method to investigate the existence of steganographic content in Images. We use two very popular methods to embed stego data in images, the LSB and the DCT. The algorithm can detect with high success rate the existence of stego content in LSB pictures and can classify pictures with DCT stego content. The algorithm is very fast and can process a large number of pictures and detect stego content in seconds without any previous training. LSB and DCT Steganographic Detection Using Compressive Sensing, Since the idea is promising and has very good results, there are more things to be studied. For example, whether there are any other image features that can be extracted from compressive sensing, or attacks on watermarking schemes and extensions to sound media. The results of this work show that the use of compressive sensing can find in steganalysis many applications and illustrate that the use of compressive sampling algorithms on steganalysis of other embedding methods can be significantly improved. Our further work will examine the possibilities of the compressive sensing algorithms in others steganograpfhic methods.

5. Literature Survey

Literature survey is done by comparing the papers that I have refered.And I found some disadvantages for those technologies that they are used in their papers and I classified those as follows:

Papers / Characteristics	Neural network based steganalysis in still images	Steganalysis based on Moments of characteristic functions	Texture based steganalysis
Type of steganalysis	Passive	Passive	Passive
Features	Transform domain includes DFT, DCT ,DWT	Moments of characteristic function, Prediction error images	LBP(Local Binary Pattern)
Data hiding technique used	Brain Chen's quantization	Blind SS,Block SS,Generic QIM and a generic LSB	Blind side
Image used	Each image is divided into 8x8 sub blocks	1096 sample images included in the CorelDraw	1000 Clean color JPG images and 1000stego images
Result	Hidden images 85.4% No Hidden images 75.0%	All methods combined 98.7%	Hidden images 68.5% No Hidden imagen99.1%

Many other steganalytic techniques have been proposed in recent years. Some steganalytic methods, for example, the Chi-square attack, are effective to LSB steganography for spatial images as well as JPEG images. The fact that LSB steganography is vulnerable to attack implies that high imperceptivity does not guarantee a high security level. The first ever statistical steganalysis was proposed by West feld and Pfitzmann. There approach is specific to LSB embedding and

is based on powerful first order statistical analysis. It identifies Pairs of Values (POVs) that consist of pixel values, quantized DCT coefficients or palette indices which get mapped to one another on LSB flipping. After the message embedding, the total number of occurrence of two members of certain POV remains the same. This concept of pair wise dependencies is leads to design a statistical Chi-square test to detect the hidden messages . A technique in grayscale images is proposed by Zhang and Ping .This technique uses different image histogram as the statistical analysis tool. Measure of the weak correlation between the LSB plane and the rest of the planes is done by the translation coefficients between different image histograms. This algorithm can identify the existence of secret messages embedded using sequential or random LSB replacement in images and also can estimate the amount of secret messages. This algorithm shows a better performance and computation speed than RS analysis method.

Benton and Chu proposed a soft computing approach to steganalysis specific to LSB. Decision trees and neural networks are used independently for detection purpose. The features are extracted from images which are based on the variables for estimating the embedding probability in the RS method. This approach different from original RS method. The goal of this method is to decide whether the image contains hidden data but not to estimate the embedding probability. Xiang-dong Chen, et al. a proposed a steganalysis technique based on bit plane randomness tests. Two binary sequences are obtained by scanning the 7th and 8th bit planes of the image with Hilbert scan. The randomness of these two sequences is tested individually by 14 kinds of randomness tests. The results of these tests form a vector and are used to construct a SVM classifier to distinguish stego images from the clean ones.

Andrew D. Ker , proposed steganalysis methods for extensions of least-significant bit overwriting to both of the two lowest bit planes in digital images images. There are two distinct embedding paradigms. He investigates how detectors for standard LSB replacement can be tailored to such embedding, and how the methods of "structural steganalysis", that gives the most responsive detectors for standard LSB replacement, He also compares the detectability of standard LSB embedding with the two methods of embedding in the lower two bit planes. In some paper they described a new very accurate and reliable method that can detect LSB embedding in randomly scattered pixels in both 24-bit color images and 8-bit grayscale or color images. Q. Liu et al. proposed a scheme for steganalysis of LSB matching steganography .It is based on feature extraction and pattern recognition techniques. The correlation features are extracted for color images. Statistical pattern recognition algorithms are applied to train and classify the feature sets. This scheme is highly efficient for colour images and reasonably efficient for grayscale images. Fangjun Huang, proposes a new technique for attacking the LSB matching based steganography. The least two or more significant bitplanes of the cover image will be changed during the embedding in LSB matching steganography . So the pairs of values do not exist in stego image

6. Proposed System

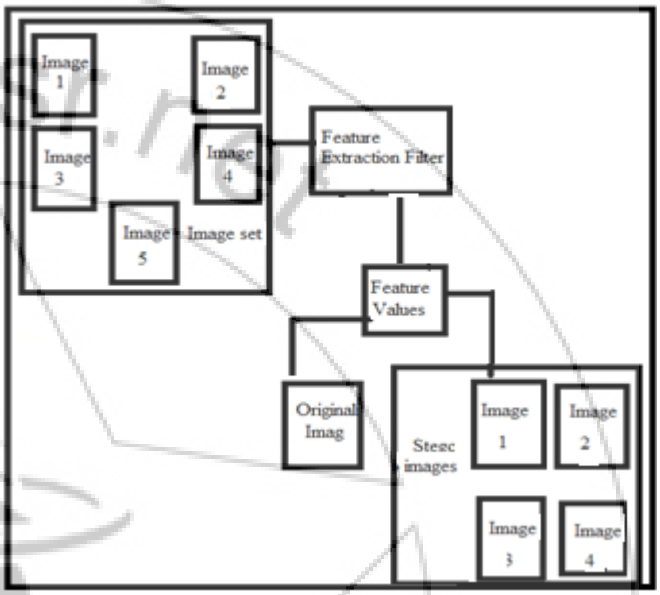

Figure 1: Proposed System

The main idea of our proposal for LSB stego images, is to regard each image to be examined as an image with embedded noise. The more noise our image has, the more the image is probable to have LSB embedded information. The measure of the peak signal-to-noise ratio (PSNR), gives us an idea about the quantity of noise in the under consideration image. The PSNR is the ratio between the maximum possible power of a signal and the power of the under consideration signal. The PSNR is used originally as a measure of quality for the compression codecs in images and videos (e.g., jpeg,mpeg). In our case, the signal is the original data of the picture and the noise is the stego data introduced by the LSB method. The assumption that we make is that if the image has no LSB embedding, then the reconstruction with a compressive sampling will be closer to the original, than to one stego-image..

7. Conclusion

The need for keeping safe secrecy of secret and sensitive data has been ever increasing with the new developments in digital system. With the advancement of technology in this digital age, most of the communication is carried out using some form of digital media. Similarly, steganography is also increasingly being used in the digital format through the use of digital media. Because of the wide spread use of internet for communication, it has become a preferable medium for digital steganography. Compressive sensing method to investigate the existence of steganographic content in Images. Compressive sensing can be potentially used in all

applications where the task is the reconstruction of a signal or an image from linear measurements, while taking many of those measurements in particular, a complete set of measurements is a costly, lengthy, difficult, dangerous, impossible or otherwise undesired procedure. Additionally, there should be reasons to believe that the signal is sparse in a suitable basis (or frame). Empirically, the latter applies to most types of signals.

We use two very popular methods to embed stego data in images, the LSB and the DCT. The algorithm can detect with high success rate the existence of stego content in LSB pictures and can classify pictures with DCT stego content. The algorithm is very fast and can process a large number of pictures and detect stego content in seconds without any previous training. Since the idea is promising and has very good results, there are more things to be studied. For example, whether there are any other image features that can be extracted from compressive sensing, or attacks on watermarking schemes and extensions to sound media. Use of compressive sampling algorithms on steganalysis of other embedding methods can be significantly improved.

Reference

[1] Andrew D. Ker ,” Steganalysis of Embedding in Two Least- Significant Bits , “ Information Forensics and Security, IEEE Transactions on**,** Volume 2 **,** Issue 1, March 2007,pp.46 - 54

[2] A. Westfeld and A. Pfitzmann, "Attacks on Steganographic Systems," Lecture Notes in Computer Science, vol.1768, Springer-Verlag, Berlin, 2000, pp. 61−75

[3] Bin Li, Junhui He, Jiwu Huang, Yun Qing Shi, “A Survey on Image Steganography and Steganalysis,” Journal of Information Hiding and Multimedia Signal Processing,Volume 2, Number 2, April 2011 ,pp.142-172

[4] Fangjun Huang, Bin Li, Jiwu Huang ,”Attack lsb Matching Steganography by Counting alteration rate of the number of neighbourhood gray levels,” ©2007 IEEE I – 401 ICIP 2007

[5] Jessica Fridrich, Miroslav Goljan, Rui Du, “Reliable Detection of LSB Steganography in Color and Grayscale Images”

[6] J. Tian, “Reversible data embedding using a difference expansion.” IEEE *Transactions on Circuits and Systems for Video Technology,* 13, 8, PP 890–896, 2003.

[7] Najeena K.S,B.M Imran,” An Efficient Steganographic Technique Based on Chaotic Maps and Adpative PPM Embedding”, *International Conference on Signal Processing, Image Processing and Pattern Recognition [ICSIPRI*,2013

[8] N.F. Johnson, S. Jajodia, “Steganalys of images created using current steganography software, in: Lecture Notes in Computer Science,” vol. 1525, Springer-Verlag, Berlin, 1998, pp. 273– 289.

[9] N. K.Pareek, Vinod Patidar ,K.K.Sud, (2006),"Image encryption using chaotic logistic map" ,IEEE Transactions on image and vision computing, vol. 24, no. 9, pp. 926-934.

[10] Qingzhong Liu, Andrew H. Sung, Jianyun Xu, Bernardete M. Ribeiro, Image complexity and feature extraction for steganalysis of LSB matching steganography,” in: IEEE Int. Conf. on Pattern Recognition, vol. 2, 2006, pp. 267–270.

[11] Rakesh S, Ajitkumar A, Kallar,Shadakshari B.C Annappa B, (20 12) "Image encryption using block based uniform scrambling and chaotic logistic mapping " International Journal on Cryptography and Information Security (IJCIS),VoI.2, No.1.pp-49-57.

[12] Ryan Benton, Henry Chu, “Soft computing approach to steganalysis of LSB embedding in digital images,” in: 3rd Int. Conf. on Information Technology Research and Education, 27– 30 June 2005, pp. 105–109.

[13] T. Zhang, X. Ping, “Reliable detection of LSB steganography based on difference image histogram,” in: Proc. ICASSP, vol. I, 2003, pp. 545–548

[14] W. Bender, D. Gruhl, N. Morimoto, & A.Lu, “Techniques for data hiding”, *IBM Systems Journal,* 35, PP 210-224, 2002

[15] Xiang-dong Chen, “Detect LSB steganography with bit plane randomness tests,” in: Proc. of 6th World Congress on Intelligent Control and Automation, China, June 21–23, 2006.

[16] Yambem Jina Chanu, Kh. Manglem Singh ,ThemrichonTuithung “Various Steganalytic Techniques Comparison for LSB Embedding*”, Trends in Innovative Computing 2012 - Information Retrieval and Data Mining*,2012