IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

EXTRACTING SPREAD SPECTRUM HIDDEN DATA FROM IMAGE

Ashwini P. Bhuse
ComuterEngineering
Babugenu Road,Bhagwat Lane,Deolaligaon,Nashik
bhuseashwini28@gmail.com

Ashvini D. Tile
Comuter Engineering
At. Mohogaon Post-Jakhori Tal-Dist Nashik
tileashvini@gmail.com

Ashwini T. Malode
Comuter Engineering
Chehadi pumping Nashik Road, Nashik
ashwini.malode22@gmail.com

ABSTRACT

we need an efficient and robust data hiding schemes to protect from data tracking and tempering attacks. So the Data hiding and extraction schemes are used in todays communication world . In this project we consider the blindly extraction technique. Blindly extraction means neither the original host nor the embedding carriers are assumed available. We develop a novel multicarrier/ signature iterative generalized least-squares (M-IGLS) to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. M-IGLS algorithm is used to extract the hidden data from digital media.This is a low complexity algorithm. It's peak signal to noise ratio value is high.

This project proposes a information-hiding method to hide more information into image. In the experimental results, we hide more characters into images and extract them correctly & also show that algorithm can achieve recovery probability of error close to what may be attained with known embedding carriers. The cover data should not be significantly degraded by the embedded data and the embedded data should be as imperceptible as possible.Thus it is necessary to encrypt the hidden message.

Keywords

steganography, Blindly extraction, Spread spectrum embedding,M-IGLS Data hiding.

1. INTRODUCTION

In today's world the data tracking and tampering are rapidly increasing everywhere like online tracking, mobile tracking etc.So for that purpose we need safe or secured communication scheme for transmitting the data and for that, we are having many data hiding and extraction schemes.Intially in military communication the data hiding schemes are used like encrypted message for finding the sender and receiver . For the copywrite purpose we used the data hiding schemes. For authentication purpose the fragile watermarks are used in [1] ,i.e to find that whether the data has been altered or not. The good recovery of hidden data is also provided by the data extraction schemes and this is the main goal of the secured or safe communication. For hiding and extracting data steganalysis is the art and science that a communication is taken place. It can embeds the secret file such as image,audio or text into other carrier file. Due to rapid increment of data tracking and data interfere attacks, in communication worldwide Data hiding and extraction schemes are increasing.

Information hiding has attracted more attentions . So to protect from these attacks we need an efficient and robust data hiding schemes. The blindly extraction technique is considered by the proposed paper. The blindly extraction means the original host and the embedding carriers are not require to be available or not require to be known. Using multicarrier spread spectrum embedding the hidden data embedded to the host digital signal. Hence due to the advantages of good robustness and immunity to noise attack it has developed rapidly in this area. Spread spectrum techniques really of digital communications systems. The hidden data is extracted from the digital media(audio, video or image). The extraction algorithm is Multicarrier Iterative Generalized Least Squares (M-IGLS) which is used to extract the hidden data from digital media.M-IGLS is a low complexity algorithm which attains the probability of error recovery equals to known host and embedding carriers.Its peak signal to noise ratio value get is high. Implementation of steganography in digital data using spread spectrum extraction algorithm has been presented in this . To embed the messages in digital data this algorithm can be applied. In this Spread Spectrum method a key is needed to embed messages into noise.This method is secured communication for transmitting the data and hence, we are having many data hiding schemes and extraction schemes.The main purpose of steganograpy is to establish covert communication between parties.

The general objective of steganographic applications is a satisfactory trade off between hidden data resistance to noise/disturbance (robustness), information delivery rate (payload), and low host distortion for hiding purposes. The counter measure technology to data hiding is referred to as steganalysis. Steganalysis has two categories, *passive* and *active*. In this work, we mainly focus on active spread spectrum (SS) steganalysis. In extracting, the aim to recover blindly data hidden in hosts via (multi-signature) direct sequence spread spectrum embedding in which neither

IJETIE
International Journal of Emerging Technology and Innovative Engineering
Volume I, Issue 3, March 2015
ISSN: 2394 - 6598
www.ijetie.org

the original host nor the embedding signatures (spreading sequences) are known (fully blind SS steganalysis).In this scheme, we developed an iterative generalized least squares (IGLS) procedure or method to blindly recover unknown messages hidden in image via Spread Spectrum embedding. The M-IGLS has low complexity and high recovery performance. However, this method is designed solely for *single signature* spread spectrum embedding where messages are hidden with one signature only and is not generalizable to the *multi signature* .In this paper, we implement a new *multi-signature* iterative generalized least squares (M-IGLS) SS steganalysis algorithm for hidden data extraction.

2. RELATIVE TECHNIQUES

2.1 Steganalysis

Steganography is the old technique known as the "Cryptography". This technique provides security to the contents of the message.Convert communication or steganography, which literally means "covered writing". It is the process of hiding data under a cover medium also referred to as host, like as audio, image, and video to establish secret communication between trusting parties and conceal the existence of embedded data. The steganography is a technique to send information by writing on the cover object invisibly. Steganography means covered writing . The stego equals to cover and graphy nothing but the writing and it comes from the Greek word. And it The existence of the hidden message is only aware by the authorized party. The steganographic technique conceals large amount of information ensuring that the modified object is not visually or audibly different from the original object.

The steganography method needs cover object and message that is to be transported .The important requirement for efficient steganographic techniques is that, the cover object is modified in a way that after embedding the message the quality of object is not lost.In blind extraction of Spread Spectrum embedded data, the unknown host acts as a source of intervention /disturbance to the data to be recovered and by the way, the problem parallels blind signal separation applications as they arise in the fields of code-division multiple-access (CDMA) communication systems, biomedical signal processing and array processing.The assumption that the embedded secret messages are independent similarly distributed random sequences and independent to the cover host, independent component analysis (ICA) may be utilized to pursue hidden data extraction. An iterative generalized least squares (IGLS) procedure was developed to blindly recover unknown messages hidden in image via Spread Spectrum embedding. The M-IGLS algorithm has low complexity and strong recovery performance.

2.2 Spread Spectrum Technique

The proposed spread spectrum method uses blind recovery of data and it uses the DCT transform as a carrier for embedding the data in digital media(image ,audio,video). Embedding is done by using multicarrier spread spectrum embedding method.For the extraction of the hidden data this technique uses M-IGLS algorithm. This algorithm is a low complexity algorithm and provides high recovery performance. It provides equal probability of error recovery to known host and embedding carriers .The proposed scheme is used as a performance analysis tool for the data hiding schemes.

3. MODULE DISCRIPTION

3.1 Steganography

Steganography includes the hiding of information within computer files. In digital steganography, E-communications may involve steganographic coding inside of a transport layer, such as a document, image file. Digital steganography can hide confidential data (i.e. secret files) very securely by embedding them into some media data called "vessel data." The vessel data is also called as "carrier, cover, or dummy data". In steganography method the images used for vessel data. The embedding operation in practice is to exchange the "complex areas" on the bit planes of the vessel image with the secret data. The important aspect of Steganography is that the embedding capacity is very large. For a 'normal' image, roughly fifty percent of the data might be replaceable with secret data before image degradation becomes apparent.

3.2 Multi-Carrier Spread Spectrum

The method of spread spectrum may allow partly to fulfill the above requirements. The main benefits of spread spectrum method are widely known: variable data rate transmission, Immunity against multi-path distortion , high flexibility and no need for frequency planning. The capability of minimising multiple access interference in direct-sequence CDMA system is given by the cross-correlation characteritics of spreading codes. In the case of multi-path propagation the capability of difference one component from thers in the composite received signal is offered by the auto-correlation properties of the spreading codes.

3.3 Image Encryption And Watermarking

The host image is an eight bit or higher grey level image .It must ideally be the same size as the plaintext image or else resized accordingly using the same proportions.

Using a Discrete Fourier Transform (DFT) Pre-conditioning the cipher and the convolution processes are undertaken.

The output will involve negative floating point numbers upon taking the real component of a complex array. The array must be resolve by adding the highest

negative value in the output array to the similar array before normalization.

The binary cipher text can be put into one or all of the RGB components for color host images.

When processing the data using FT, the binary plaintext image should have homogeneous margins to minimize the effects of ringing due to 'edge effects'.

3.4 Image Decryption And Extraction

(i) The correlation operation should be assume using a Discrete Fourier Transform.
(ii) The data is decomposed into each RGB component and each one bit layer is extracted and correlated with the appropriate cipher for color images,.
(iii) The output acquire in Step 3 has a low dynamic range and therefore requires to be quantized into an eight bit image based on floating point numbers within the range max (array)-min (array).

4. PROBLEM FORMULATION

Due to the high resolution of digital images as carrier, detecting hidden messages is also considerably difficult. The hidden image often a binary sequence in embedded by put a host signal component with a quantized value. Due to data embedding the quantization error will produce. During the detection, the original image is not available we must treat it as additive noise. Due to the original host image and due to the embedding and compression process the process of distortion can be occurring. Feature vector extraction is used to achieve the detection. It has high overhead for hiding a few bits of information. This drawback can be overcome easily. Another problem is that a steganographic system is rendered useless once it has been discovered. This also can be overcome by utilizing a key for the insertion and extraction of the hidden data , more over Spread Spectrum techniqueis known to be very robust, except the consequence the cost is very high, the implementation is relatively complex, less secure and the information capacity is very limited. Current spread spectrum steganographic applications with audio media are primarily limited to providing proof of copyright and assurance of content integrity. There is the potential to expand the applications to include the embedding of covert communications. By using proposed methodology the mentioned problems related to spread spectrum can be overcome.

CONCLUSION

In this project we consider the blindly extraction technique . Blindly extraction means neither the original host nor the embedding carriers are assumed available. We develop a novel multicarrier/ signature iterative generalized least-squares (M-IGLS) to seek unknown data hidden in hosts via multicarrier spread-spectrum embedding. In the experimental results, we hide more characters into images and extract them correctly.The M-IGLS has low complexity and high recovery performance.In this paper, we implement a new *multi-signature* iterative generalized least squares (M-IGLS) SS steganalysis algorithm for hidden data extraction.

5. ACKNOWLEDGMENTS

The authors would like to thank the anonymous reviewers for a wealth of comments and suggestions that helped improve
significantly the presentation and content of this manuscript.

REFERENCES

[1] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding: A survey," *Proc. IEEE (Special Issue on Identification and Protection*

of Multimedia Information), vol. 87, pp. 1062-1078, July 1999.

[2] I. J. Cox, M. L. Miller, and J. A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan-Kaufmann, 2002.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques," *Proc. IEEE (Special Issue on Identification and Protection of Multimedia*

Information), vol. 87, pp. 1079-1107, July 1999.

[4] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking digital image and video data: A state-of-the-art overview," *IEEE Signal Processing Magazine*, vol. 17, pp. 20-46, Sept. 2000.

[5] N. F. Johnson and S. Katzenbeisser, "A survey of steganographic techniques," in *Information Hiding*, S. Katzenbeisser and F. Petitcolas Eds. Norwood, MA: Artech House, 2000, pp. 43-78.

[6] S. Wang and H. Wang, "Cyber warfare: Steganography vs. steganalysis," *Communications of the ACM*, vol. 47, pp. 76-82, Oct. 2004.

[7] C. Cachin, "An information-theoretic model for steganography," in *Proc. 2nd Intern. Workshop on Information Hiding*, Portland, OR, Apr. 1998,

pp. 306-318.

[8] G. J. Simmons, "The prisoner's problem and the subliminal channel," in *Advances in Cryptology: Proc. CRYPTO'83*. New York, NY: Plenum, 1984, pp. 51-67.

[9] J. Fridrich, *Steganography in Digital Media, Principles, Algorithms, and Applications*. Combridge, UK: Combridge Univeristy Press, 2010.

[10] Y. Wang and P. Moulin, "Perfectly secure steganography: Capacity, error exponents, and code constructions," *IEEE Trans. Inform. Theory*, vol.54, pp. 2706-2722, June 2008.