Volume 3, Issue 2 (2015) 355-358 ISSN 2347 - 3258
International Journal of Advance Research and Innovation

Blind Extraction of Hidden Data from Digital Media

Radha. A, Kavitha. N
Department of Computer Science Engineering, J. J. College of Engineering and Technology, Tiruchirappalli, India

Article Info
Article history:
Received 21 March 2015
Received in revised form
11 April 2015
Accepted 21 May 2015
Available online 15 June 2015

Keywords
Authentication,
Covert Communication,
Data Hiding,
Steganalysis,
Steganography,
Watermarking

Abstract
Spread-Spectrum (SS) Steganography is attracting increasing interest among researchers and practitioners in the fields of authentication and covert communications. Steganography is the technique for hiding secret information in other data such as still, multimedia images, text, and audio. Whereas Steganalysis is the reverse technique in which detection of the secret information is done in the stego image. Digital data embedding in digital media is an information technology field of rapidly growing commercial as well as national security interest. It considers the problem of extracting blindly data embedded over a wide band in a spectrum domain of a digital medium. To develop a novel embedding and extracting algorithm to demonstrate this problem. Least Significant Bit (LSB) algorithm is used to embed the secret message into the image. Special Cryptography algorithm called triple Data Encryption Standard (DES) is used to encrypt and decrypt the secret message for strengthens the security of this process.

1. Introduction

In the current trends of the world, the technologies have advanced so much that most of the individuals prefer using the internet as the primary medium to transfer data from one end to another across the world. There are many possible ways to transmit data using the internet: via e-mails, chats, etc. The data transition is made very simple, fast and accurate using the internet. However, one of the main problems with sending data over the internet is the "security threat" it poses i.e. the personal or confidential data can be stolen or hacked in many ways. Therefore it becomes very important to take data security into consideration, as it is one of the most essential factors that need attention during the process of data transferring. Data security basically means protection of data from unauthorized users or hackers and providing high security to prevent data modification. This area of data security has gained more attention over the recent period of time due to the massive increase in data transfer rate over the internet. In order to improve the security features in data transfers over and transmitting it to the intended receiver using an unknown key, Steganography provides further security by hiding the cipher text into a seemingly invisible image or other formats. "Steganography is the art of hiding and transmitting data through apparently innocuous carriers to conceal the existence of data".the internet, many techniques have been developed like: Cryptography, Steganography and Digital Watermarking. While Cryptography is a method to conceal information by encrypting it to "cipher texts".

2. Literature Survey

2.1 Information Hiding: A Survey

Cryptography is about protecting the content of messages, the situation is much less clear when it comes to hiding information. For that now look at some of the techniques used to hide information. Many of these go back to antiquity. Steganography and many of the methods depended on novel means of encoding information,

Corresponding Author,
E-mail address: radha.ait22@gmail.com

information hiding schemes that operate in a transform space are increasing in common. Covert communication or steganography, which is literally means "covered writing" in Greek, is the process of hiding data under a cover medium such as image, video, or audio, to establish secret communication between trusting parties and conceal the existence of embedded data.

The original image is needed to check for the presence of a watermark. In the case of grayscale images, a simple example of digital watermarking based on spread spectrum ideas are used. The large bandwidth of the cover medium by matching the narrow bandwidth of the embedded data, another way of getting round this problem is to take advantage of the natural noise of the cover-text. To add or subtracts randomly a Fixed value d to each pixel value. Fragile watermarks are used for the authentication purpose, i.e. to find whether the data has been altered or not.

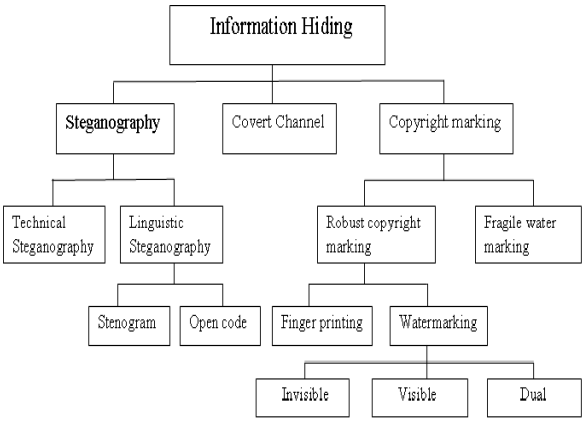

Fig: 1. Information Hiding Techniques

Establishing secrete communication between two trusted parties. Spread spectrum communication is used for security. The information rate can again be improved by placing separate marks in the image. One can split the image into pieces and then apply the embedding to each of them. Data extraction schemes also provide a good recovery of hidden data.

However the information rate is low. General spread spectrum systems encode data in the choice of a binary sequence that appears like noise to an outsider.

2.2 Perfectly Secure Steganography: Capacity, Error Exponents, and Code Constructions

In the analysis of steganographic systems a perfect undetectability condition is considered. Embedding of the message into the covertext, the resulting stegotext is required to have exactly the same probability distribution as the covertext. Then no statistical test can reliably detect the presence of the hidden message. Construct perfectly secure steganographic codes from public watermarking codes using binning methods and randomized permutations of the code. The permutation is a secret key shared between encoder and decoder.

The four basic attributes of a steganographic code are as follows:

1) Detectability: quantifying Willie's ability to detect the presence of hidden information;
2) Transparency (fidelity): closeness of covertext and stegotext under an appropriate distortion (fidelity) metric.
3) Payload: the number of bits embedded in the covertext.
4) Robustness: quantifying decoding reliability in presence of channel noise (i.e., when Willie is an active warden).

The common randomness is provided by a secret key shared between the encoder and decoder.If the covertext distribution is uniform and the distortion metric is cyclically symmetric, the security constraint does not cause any loss of performance.

A randomized code is used to satisfy the perfect-undetectability condition. Without the secret key, a deterministic code generally could not satisfy the perfect-undetectability condition. The security constraint does not cause any loss of performance. Detection of hidden information within a stegotext. Steganographic code is no longer perfectly secure.

2.3 Blind Digital Signal Separation Using

Successive Interference Cancellation Iterative Least Squares

Technique used: SIC-ILS algorithm

Blind separation of instantaneous linear mixtures of digital signals is a basic problem in communications. When little or nothing can be assumed about the mixing matrix, signal separation may be achieved by exploiting structural properties of the transmitted signals.

A monotonically convergent and computationally efficient iterative least squares (ILS) blind separation algorithm is based on an optimal scaling lemma. The signal estimation step of ILS is reminiscent of successive interference cancellation (SIC) ideas. A widely used ILS finite alphabet blind separation algorithm can exhibit limit cycle behavior.

The instantaneous multiple-input multiple-

Output (I-MIMO) observation model is X=AS+V, where

X m × N data matrix;

A m × d mixing matrix;

S d × N signal matrix;

V m × N matrix of i.i.d. Gaussian random variables;

And it is assumed that m ≥ d, N ≥d, and that A and S are full rank (d).

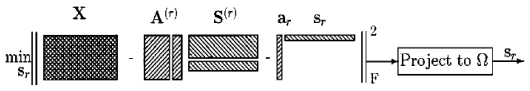

Fig: 2. Key step of SIC-ILS Algorithm

The algorithm features moderate complexity, monotone convergence, and performance. A bonus feature is that the optimal scaling lemma allows easy incorporation of coding constraints. SIC-ILS delivers very good symbol error rate (SER) results even at low SNR. Its complex to identify the information hidden in the least squares.

2.4 Steganalysis using Higher-Order Image Statistics

Technique used: Wavelet Decomposition

A universal approach to steganalysis for detecting the presence of hidden messages embedded within digital images. The goal of steganography is to embed within an innocuous looking cover medium (text, audio, image, video, etc.) a message so that casual inspection of the resulting medium will not reveal the presence of the message. steganalysis is to determine if an image (or other carrier) contains an embedded message. Its a statistical model based on first- and higher-order magnitude statistics extracted from a wavelet decomposition, coupled with a linear discriminant analysis (LDA), could be used to detect steganography in grayscale images.

The decomposition of images using basis functions that are localized in spatial position, orientation and scale (e.g., wavelets) have proven extremely useful in image compression, image coding, noise removal and texture synthesis. One reason is that such decompositions exhibit statistical regularities that can be exploited.

Four different message sizes, and for the following types of SVMs (a) linear, (b) non linear (RBF kernel) and (c) one-class with six hyperspheres (fewer hyperspheres led to poor generalization, and more hyperspheres led to over-fitting.In this approach to compare the effectiveness of our approach to that of Fridrich, as it has clearly emerged has one of the most effective techniques. We expect that as universal steganalysis continues

To improve, steganography tools will simply embed their messages into smaller and smaller portions of the cover image.The detection accuracies are given with respect to the total cover capacity.

Efficiency is high.Presence of hidden datas are undetectable. When the message size becomes smaller, the chance of detection falls-messages utilizing approximately 5% of the cover are unlikely to be detected. The hidden messages will continue to be able to be transmitted undetected, but high-throughput steganography will become increasingly more difficult to conceal.

3. Proposed System

Proposed algorithm used here is to reduce the risk of using cryptographic algorithms alone. Data hiding techniques embed information into another medium making it imperceptible to others, except for those that are meant to receive the hidden information and are aware of it presence. It focuses on methods of hidden data in which cryptographic algorithms are combined with the information hiding techniques to increase the security of transmitted data. Least Significant Bit (LSB) algorithm used to hide the secret message into the image. Triple DES Cryptography algorithm is used here to encrypt and decrypt the secret message which strengthens the security in better way.

In this proposed algorithm, Encryption process of hidden file increases the security while embedding. Decryption process of extracted file increases the security after extraction is done. Computational security is achieved. Focuses on both embedding and extraction process. Embedding and extraction is more effective. Error probability is low.

4. Module Description

1. **Admin Detail:** This module is for user authentication process. Enables the user to register and login. It takes the details like Host name, IP address, User ID and Password as input. Allow them to access the data which is to be embedded or extracted.
2. **Encrypt File:** This module encrypts the loaded file which is to be embedded using Triple DES encryption algorithm. The encryption algorithm encrypts the file using specific key.
3. **Embed Secret Data:** The encrypted file is watermarked or embedded with cover image using the password. LSB algorithm done this embedding process. It replaces the pixel values of the cover image. It reduces the detectability of the stego image.
4. **Host File:** This module enables the user to load the embedded image to the server. Server will receive the stego image and the key file from the sender. Stores it on specific location. Then transmits this stego image over the network to the requested recipient.
5. **Extract Secret Data:** Once the detection is found the recipient with key will extract the embedded stego image. This is achieved by using the extraction technique. Extraction is achieved when the keys are matched otherwise failed extraction. Here the encrypted text file is separated out from the stego image.
6. **Decrypt File:** Triple DES algorithm of decryption method is used here. Decryption algorithm decrypts the separated encrypted file. The key which is used for encryption is used here for decryption. Finally the original secret text file is viewed by the recipient.

5. Conclusion

The problem of blindly extracting unknown messages hidden in image hosts via multicarrier/signature spread-spectrum embedding is considered. The proposed algorithm encrypts the hidden data and embeds with multicarrier for transmission. The embedded file is send to the server for information transaction along with the secure key file. The receiving end will request for the embedded information to server for extraction. The server sends the embedded data along with key file to the requested client only if the end user is an authenticated to receive it. Finally the end user will extracts the embedded file and decrypt it using the key to view the hidden data. In future this work may achieved by using different multicarrier like audio or video stream and different algorithms for better performance.

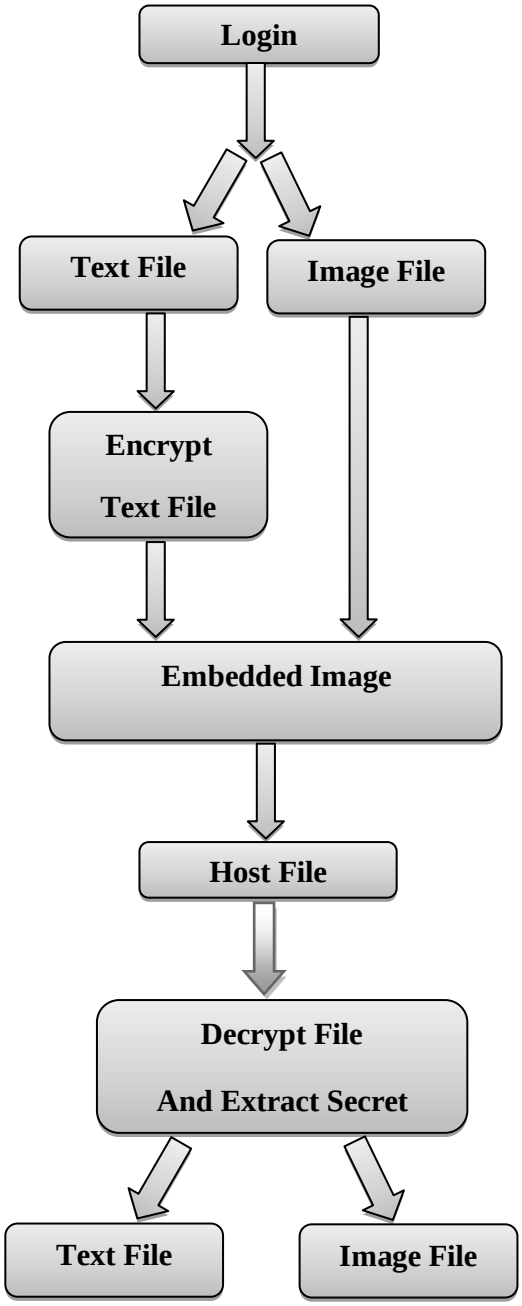

Fig: 3. System Architecture

References

[1] F. A. P. Petitcolas, R. J. Anderson, M. G. Kuhn, Information hiding: A survey, IEEE (Special Issue on Identification and Protection of Multimedia Information), 87, 1999, 1062-1078

[2] Y. Wang, P. Moulin, Perfectly secure steganography: Capacity, error exponents, and code constructions, IEEE Trans. Inform. Theory, 54, 2008, 2706-2722
[3] T. Li, N. D. Sidiropoulos, Blind digital signal separation using successive interference cancellation iterative least squares, IEEE Transaction on Signal Processing., 48, 2000, 3146-3152
[4] S. Lyu, H. Farid, Steganalysis using higher-order image statistics, IEEE Trans. Inform. Forensics and Security, 1, 2006, 111-119
[5] M. Gkizeli, D. A. Pados, S. N. Batalama, M. J. Medley, Blind iterative recovery of spread-spectrum steganographic messages, IEEE Intern. Conf. Image Proc. (ICIP), Genova, Italy, 2, 2005, 11-14.