Imperceptible Stego-Marked Image Manipulation for Encrypted Data Hiding

Ms. Gopika Mane¹, Priti Deshmukh², Sukul Fadnis³
Sheetal Jadhav⁴, Manoj S. Wakchoure⁵

1 Guide and 2,3,4,5 Students of
Marathwada Mitramandal’s Institute of Technology, Lohgaon, Pune

Abstract

In day to day life, people from different sectors need to transfer the digital data for different purposes. But there exist many threats to this type of data transfer. Some important data can be lost during transfer or any intruder can hack the data to gain particular access. To handle these issues, one solution can be the use of a technique which will securely store the data and be sent in a form that no one could get to know that some important data is being transferred.

In this paper, we propose a hidden data transfer system using the Cryptography, Steganography and Watermarking techniques. This system is based on the approach of stream cipher cryptography using RC4 algorithm, steganography by F5 algorithm and watermarking using Quantization Index Modulation algorithm. Our emphasis is to give access to the original data to the authorized party by maintaining the integrity of the encrypted information and the copyright image along with the container image.

Keywords: - Cryptography, Steganography, Watermarking, RC4, F5, QIM.

1. INTRODUCTION

Now-a-days the major threat to the transfer of information is to maintain the security of the information and to be sent without being noticed. Along with that there also exists the risk of piracy of data. So as to know the ownership of the information to which the organization belongs, watermarking comes into picture. The rapidly emerging field of information technology is to embed data in digital form on to a digital media. Covert communication is usually done so as to provide security and to compress the data. Digital Data hiding, along with covert communication and watermarking, is the art of hiding secret message into innocent looking host media by incurring least distortion to both the digital media.

This paper discusses hiding the digital data in encrypted form on the digital media such as images. Further this image is provided with safeguard by embedding the organizations watermark image onto the image.

While handling the digital data and media the key aspects that need to take into consideration are

Stealth: This means that only the legitimate users can gain access to the digital data embedded in the media.

Availability: This means that the data after being processed is same as that before the processing is carried on the information to be stored on the media.

Certainty: This is in which it is ensured that the information is not altered by any non-authorized person.

Hence we need to send the confidential data in such a way that the intruder must not come to know that the information is being sent through the digital medium.

In this paper we are taking a review which explains how we can combine three techniques i.e. Cryptography, Steganography and Watermarking to provide a three way security to the transmission of the information. We are also going to see what the related work was done in this approach before and the study of existing system which includes these techniques.

The rest of this paper is organized as follows. In Section II, we describe the information security concepts-Cryptography, Steganography and watermarking. Before concluding, we analyze the literature and existing system in section IV.

2. BASIC CONCEPTS

To achieve above needs for security of information, we have merged the three data security concepts- Cryptography, Steganography and Watermarking along with the image processing.

2.1 Cryptography:

Cryptography is derived from the German words cryptos meaning hidden and graphein meaning writing. Cryptography is the practice and study of techniques for secure communication in the presence of third parties. It is a process of converting ordinary information or plain text into unintelligible text called as inscribed information. Cryptography includes a pair of algorithms that creates encryption and reversing decryption of the data. Encryption is the process of converting plain text into cipher text by making use of various techniques. Decryption is the reverse process of encryption that is converting cipher text to plain text.
2.2 Steganography:
The word Steganography is a word of Greek origin in which Steganos meaning covered or protected and graphei meaning writing. Steganography is the art and science of writing hidden messages in such a way that no one except the sender and intended receiver suspects the existence of message. Steganography includes the concealment of information within computer files.

2.3. Watermarking:
Watermarking is the process of hiding digits information in copyright image, the hidden information does not need to contain a relation to the copyrights of organization. Digital watermarks are used to verify the authenticity or integrity of the carrier signal or to show the identity of its owner. It is the backbone of authenticity.

3. LITERATURE SURVEY
In this section we will study about the various systems that have been proposed regarding the various techniques implemented for secure digital data transmission by means of covert communication, cryptography and authentication by means of watermarking. We will also review the various disadvantages of the previously proposed systems.

Working of the Various Existing Algorithms:
3.1. Cryptographic Algorithms:

Essentially cryptographic algorithms are of two types:
(a) Block cipher and
(b) Stream cipher.

As the name suggests Block Cipher operates on blocks of data. Meaning the block cipher algorithms breaks the plain text into blocks of length 8 or 16 bytes and operates on each block independently. Security of block cipher algorithms depends
upon the design of encryption function. Errors in transmitting one block generally do not affect other blocks. Software implementation of block ciphers run faster than stream ciphers.

The stream cipher algorithms are designed to accept a crypto key and a stream of plaintext to produce a stream of cipher text. A stream cipher encrypts smaller block of data, typically bits or bytes. Stream Cipher processes the input element continuously producing output one element at a time. It requires less code.

As in the proposed work, we have to embed the encrypted data into an image for steganography; the data should be in small units. Hence we will require the stream cipher algorithm as we want to store the data in pixels of image. Let us see in detail some Stream cipher algorithms:

i) **Trivium Stream Cipher Algorithm:**
It was created in early 2004. Algorithm is having a medium speed of 4 8 cycles per byte. It requires fixed effective key length of 80 bits. It is having computational complexity of 2135 sec. In 2006, the algorithm was successfully cracked by Brute Force Attack.

ii) **PANAMA Stream Cipher Algorithm:**
This algorithm was created in 1998. Its computation speed is 2 cycle per byte. It requires fixed effective key length of 256 bits. It is having computational complexity of 280 sec. The algorithm was cracked in 2001 by hash collision.

iii) **Py Stream Cipher Algorithm:**
This algorithm was created in pre-2004. Its computation speed is 2.6 cycle per byte. It accept key length varying from of 8 to 2048 bits. It is having computational complexity of 275 sec.

iv) **RC4 Stream Cipher Algorithm:**
It is the oldest stream cipher algorithm which is also known as ARC4. It is widely used in WEP to secure wireless networks. In this algorithm the bits/bytes are encrypted using a pseudorandom generated key. The key used in encryption is generated using pseudorandom number generated (PRNG). The stream of plaintext is XORed with the key generated and the information is encrypted to produce the cipher text. Its computation speed is 7 cycles per byte. It accepts key of length varying from 8 to 2074 bits. It is having Computational Complexity of 213 sec. [6]

3.2. Steganographic Algorithms:

Steganography is also known as covert communication. In this process the information in the form of binary bits is stored on the pixels formed by segmentation onto the image. Due to this it is difficult for the intruder to understand that some form of information is being transmitted through the medium.

In ancient times, Steganography was implemented on to the text that was hidden using the Morse code but with the boost in the computer power, the Steganography is carried out using the digital form. Naïve steganographic implementation was that of the use of Windows command prompt. This embeds the message on the image by a simple code as follows:

C:\> Copy Cover.jpg /b + Message.txt /b Stego.jpg

This process is easily noticeable by any user by simply opening the image into word format which displays the information at the end of the file i.e. after the end of the digital symbols of the image, the information is stored as it is in simple form. The main drawback of this process is that the information is easily accessible and it is difficult to retrieve back by other process. Another naïve implementation of steganography is to append hidden data into the image’s Extended File Information, EXIF. EXIF is a standard used by digital camera manufacturers to store information in the image file, such as, the make and model of a camera, the time the picture was taken and digitized, the resolution of the image, exposure time, and the focal length. This is metadata information about the image and its source located at the header of the file.

Now let us see some of the steganographic algorithms in detail:

i) **JSteg Algorithm:**
In this algorithm, least significant bits of frequency coefficients are replaced by the secrete message. The embedding mechanism of the algorithm skips all coefficients with the value 0 or 1. It provide good resistance against visual attacks and offers good embedding capacity of about 12%. It is having moderate computational speed and also the security provided to the message is comparatively less.[10]

ii) **F3 Steganography Algorithm:**
In this algorithm, absolute values of the coefficients are decremented if their LSB i.e. Least Significant Bits does not match. If the coefficients have value 0, it could not be decremented. The LSB of nonzero coefficients matches the secret message after embedding. Unlike JSteg algorithm the LSB is not overwritten as overwritten bits can be detected by statistical methods. The algorithm skips all Zeros which offer necessity of repetitive embedding.[8]

iii) F4 Steganography Algorithm:
This algorithm overcomes all the drawbacks of F3 algorithm. As the previous algorithm was skipping all zeros, this algorithm maps all the negative coefficients to steganographic values. Even negative values represents steganographic ones and odd negative values represent steganographic zeros. F4 algorithm changes more number of bit positions which is not a good feature for attack proof steganographic algorithm. [9]

iv) F5 Steganography Algorithm:
F5 is an advanced version of F4 algorithms. Features are added in F4 algorithm for preventing statistical attacks and improving the embedding capacity of the image.[11] This is done by two steps i.e.
(a) Permutative Straddling
(b) Matrix Encoding

Advantages of F5 Algorithm:
1) F5 has high embedding capacity (>13%) but can be pushed even further.
2) F5 has high embedding efficiency.
3) Resistance against both visual and statistical attacks.
4) Uses a common image format and carrier medium (JPEG).

3.3 Watermarking Algorithms:

The concept of Watermarking is introduced for the preventing the increasing copyrights violation. In this technique copyright of the organization are embedded over the media by means of a logo or some other form. Hence even if the unauthorized party wants to use the data the watermark will restrict assess. There are different algorithms stating various techniques for watermarking the content. Some of these are explained below in detail:

i) Buyer-Seller Watermarking Algorithm:
These algorithms reduce the size of image and perform the processes parallel to perform linear operations on encrypted signals. The algorithm mainly traces the concept of composite signal representation. If the information is accessible only in encrypted form to the watermark embedder, the stated scheme for embedding will not be applicable to it.[4]

ii) Commutative Watermarking Algorithm:
In this algorithm, some sub-bands of lower resolutions are chosen for encryption while watermarking is done on the rest of higher resolution sub-bands. If more sub-bands/bit planes are encrypted and only rest few sub-bands/bit planes are watermarked, it might be possible for an attacker to remove the watermarked sub-bands/bit planes while maintaining the image quality. This will be provide comparatively less security.[5]

iii) A Joint Digital Watermarking and Encryption Algorithm:
In this technique the encryption is performed on most significant bit planes and watermarking is done on least significant bit planes. If the number of sub-bands/bit planes used for encryption is less, an attacker can compute the un-encrypted sub-bands/bit planes and further extract some useful information from the image, even if the image quality may not be good.

iv) QIM Watermarking Algorithm:
It is Quantization Index Modulation (QIM) watermarking algorithm. The QIM depends on the quantizers mentioned in codebook for a particular component of the image in order to insert a digital data. In QIM modulation, the component of an image is substituted to the component nearest to its value so as to allowing us to insert the digital data along with the component from the codebook.[1]

Related Work Done:
In this section we are going to study the existing or already proposed system which uses the same technique. We can say that this system is a motivation for the proposed system. To develop the new system we must study the existing system to understand its drawbacks in order to overcome them.[2]
In this system, the main emphasis is given on image. The proposed algorithm works on compressed code stream of JPEG2000. The compression is done in 5 different steps.
1. Image divided into rectangular tiles and multicomponent transform is performed.
2. Discrete Wavelet Transform
3. Quantization
4. Compressed Byte Stream is generated by optimized truncation
5. The compressed byte stream is arranged into different wavelet packets based on resolution, precincts, components & layers.

In proposed system this newly generated compressed byte stream is encrypted using a symmetric stream cipher algorithm which is further watermarked by combining already proposed three watermarking techniques.[2]

Disadvantages of System:
1. If the watermarking is done on higher resolutions, Image quality will be distorted.
2. Watermark is embedded on different number of bit planes say x. If x≥ 7, the image quality will be affected.
3. Distortion occurs because of the rounding off process.

Expected Future Work:
1. Extending the proposed scheme to different form of images.
2. Work should be done to maintain the file size after encryption and watermarking.
3. Challenges such as lack of error resilience of variable length codes used for encoding.

4. CONCLUSION
To develop a system that gives major emphasis on data security by Cryptography, Steganography and Watermarking techniques of confidential information we can use the algorithms: RC4 Stream Cipher Algorithm for cryptography, F5 Algorithm for Steganography and QIM Algorithm for watermarking.

REFERENCE

AUTHORS

Priti Deshmukh perceiving the BE in Information Technology from Marathwada Mitramandal’s Institute of Technology, Pune affiliated to University of Pune. During Third Year Engineering studied the concepts of “User authentication through mouse dynamics” and given the presentation of the same. Also done a mini Project on “Tourism Management System” using vb.net and Oracle 10g.

Sukul Fadnis pursuing BE in Information Technology from Marathwada Mitra Mandal’s Institute of Technology, Pune affiliated to University of Pune. Individually studied the concept of Touchalytics: On the Applicability of Touchscreen Input as a Behavioral Biometric for Continuous Authentication and given the presentation on the same. Also done a mini Project on “Online Passport Registration.” using vb.net and Oracle 10g.

Sheetal Jadhav BE in Information Technology from Marathwada Mitra Mandal’s Institute of Technology, Pune affiliated to University of Pune. Individually studied the concept of “Multi touch in gesture flow” and given the presentation of the same. Also done a mini Project on “Inventory Management System.” using vb.net and Oracle 10g.

Manoj S.Wakchoure pursuing BE in Information Technology from Marathwada Mitra Mandal’s Institute of Technology, Pune affiliated to University of Pune. Individually studied the concept of “Mobile Biometric combined face and voice verification for a mobile platform” and given the presentation on the same. Also done a mini Project on “RTO Management System” using vb.net and Oracle 10g.