ANALYSIS OF DATA HIDING ALGORITHMS FOR IMAGE SECURITY

Swati B. Singh¹, Ameya K. Naik², Pragati Dwivedi³, Swapna Patil⁴
Department of Electronics and Telecommunication, Shree L.R. Tiwari College of Technology
Mumbai, Maharashtra, India
1singhswati.18.08@gmail.com
2ameyanaik@somaiya.edu
3 Pragatiupadhyay27@gmail.com
4 Swapna80patil@gmail.com

Abstract—The main goal of reversible data hiding algorithms is to embed the secret information in cover image and recover it back successfully. So we have implemented two methods. In first method, cover image is encrypted using stream cipher and pseudo randomly generated key and compressed using haar wavelet compression. The encrypted compressed image acts as a media for hiding secret image. And in second method, secret image is encrypted using randomly generated key and it is hidden in cover image. In both the method data hiding is done using LSB based image steganography. At the receiver, reverse process is done to extract secret image and recover cover image. At the end, we conclude that second method gives better security of image compared to method one.

Index Terms—Image encryption, steganography and reversible data hiding.

I. INTRODUCTION

There are lots of essential and confidential data or information over an internet, security and protection of such contents are of major concern. Digital Watermarking is one technique for overcoming these problems. Data Hiding is a one generalization of watermarking technique [1]. A number of reversible data hiding methods have been proposed in recent years. For example, difference expansion method, histogram shift mechanism and use of redundancy in a cover by performing lossless compression to create a spare space for data embedding [2].

Data hiding techniques helps in protecting the data or information from unwanted hands, by making it difficult to obtain from marked media while keeping it accessible for future use. There are two types of data hiding techniques i.e. lossy and lossless data hiding techniques. In lossy data hiding techniques original image is not retrieved back after extraction of secret information. In lossless data hiding, original image is retrieved after extraction of secret information. It is also known as reversible data the hiding techniques [3]. This paper presents an overview of work using cryptography and steganography which provides information hiding and secrecy. Encryption is applied before transmission of information using encryption key and decryption is applied after extraction of the encrypted data. Whereas information hiding is applied before transmission and extraction process is applied after receiving the information [1][3].

Here encryption is done using stream cipher algorithm. Stream cipher is produced with pseudo randomly generated key values. Original message is ex-ored with the key to produce cipher output. Let us consider the input message bits to be ‘mi’ and the key values ‘ki’ and the generated cipher output to be ‘Ci’. Mathematically Exor operation can be represented as Ci = mi Θ ki.

Key generation for encryption is the major issue. There are various ways of generating key. For example; using linear feedback shift registers (LFSR) and in matlab by using rand command. In our algorithm, we generate key for encryption using pseudorandom key generator (LFRS). Advantages of LFSRs include the ease of implementation, simplicity and speed [1][4]. Least significant bit (LSB) insertion is used as data hiding technique. LSB is simple approach for embedding information in a cover image. MSB bit of image contains maximum data whereas LSB bit contains minimum data of an image. The LSB of an image are changed to a bit of the secret message for data hiding. Cryptography along with steganography makes great partner providing two level of security. The main difference between them is that cryptography focuses on keeping the content of message secret and steganography focuses on keeping the existence of the message secret [3][5].

II. DESIGN AND IMPLEMENTATION OF PROPOSED DATA HIDING ALGORITHMS FOR IMAGE SECURITY

A. Proposed method 1

Figure 1 shows the block diagram of data hiding of encrypted compressed cover image using steganography.
Algorithm
- All the pixels of input cover image are read.
Encryption of original cover image is done using stream cipher process. Key for encryption is produced using pseudo randomly generator.

- Encrypted image is used as a media for hiding secret images.
- Encrypted cover image undergoes compression. Compression reduces redundancy and the amount of data required for representing an image.

**B. Proposed method 2**

Fig.2 shows the block diagram of data hiding of encrypted secret image using steganography.

**Algorithm**

- Firstly, the secret image to be hidden containing the message is encrypted.
- Encryption is done using randomly generated key.
- Basically this key is generated using rand command in matlab.
- Further the encrypted secret image is hidden in cover image using LSB based steganography method to produce stego image.
- At the receiver, apply reverse steganography and then make use of same key to retrieve the hidden image.
- The major advantage of doing this is that we generate the key randomly.
- And it makes it difficult for anyone to find the exact key and in this way that person will not be able to retrieve the hidden information.
IV. CONCLUSION

In the first algorithm recovering cover image is not important. Hence we have compressed it. The size of original image is 67.3Kb and size of compressed image is 39.4Kb which leads to faster transmission due to reduced size. It also results in security of the information. However in second algorithm secret image is encrypted and then hidden in cover image by using steganography.
The key for encryption is generated using random command. And this method makes it difficult for anyone to find the exact key for decryption and making it more difficult to retrieve the hidden information. Hence, cryptography and steganography together offers double protection to the secret data. It provides secure transmission and improved authentication.

V. REFERENCES


