HIDING THE DATA USING STEGANOGRAPHY WITH DIGITAL WATERMARKING

[1]G.Thirumani Aatthi, [2]A.Komathi

[1]Research Scholar, Department of Computer Science & Information Technology,
Nadar Saraswathi College of Arts & Science, Theni,Tamil Nadu,(India)
[2]Department of Computer Science & Information Technology;
Nadar Saraswathi College of Arts & Science, Theni, Tamil Nadu,(India)

ABSTRACT

Data Security is the method of shielding Information. It protects its accessibility, privacy and Integrity. Access to Stored data on computer data base has improved greatly. More Companies store business and individual information on computer than ever before. Much of the data stored is highly confidential and not for public viewing. Cryptography and steganography are well known and widely used techniques that manipulate information in order to cipher or hide their existence. These two techniques share the common goals and services of protecting the confidentiality, integrity and availability of information from unauthorized access. In Existing research, data hiding system that is based on image steganography and cryptography is proposed to secure data transfer between the source and destination. In this the main drawback was that, the hackers may also get the opportunity to send some information to destination and it may lead confusion to receiver.

In my research I proposed LSB(Leased Significant Bit) Technique used for finding the image pixel position and pseudorandom permutation method used for store the data in random order. Moreover I have proposed digital watermark technique to avoid the unauthorized receiving information from hackers. In this proposed system, the above three technique will be combined for secure data transfer. Experimental results will prove the efficiently and security of my Proposed work.

Key Word: Cryptography, Steganography, Data Security, Key Generation

I. INTRODUCTION

In the Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography.

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. All digital file formats can be used for steganography, the four main categories of file formats that can be used for steganography.

Figure 1: Categories of Steganography

Over the past few years, numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that the alterations made to the image are perceptually indiscernible. Common approaches are include:

(i) Least significant bit insertion (LSB)

(ii) Masking and filtering

(iii) Transform techniques

Least significant bits (LSB) insertion is a simple approach to embedding information in image file. The simplest steganographic techniques embed the bits of the message directly into least significant bit plane of the cover-image in a deterministic sequence. Modulating the least significant bit does not result in human-perceptible difference because the amplitude of the change is small.

Masking and filtering techniques performs analysis of the image, thus embed the information in significant areas so that the hidden message is more integral to the cover image than just hiding it in the noise level.

Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression, Discrete Fourier Transform, or Wavelet Transform. These methods hide messages in significant areas of the cover-image, which make them more robust to attack. Transformations can be applied over the entire image, to block through out the image, or other variants.

II. LITERATURE REVIEW

Here, Ms.Dipti and Ms.Neha, developed a technique named, "Hiding Using Cryptography and Steganography"[01]is discussed. In that, Steganography and Cryptography are two popular ways of sending vital information in a secret way. One hides the existence of the message and the other distorts the message itself. There are many cryptography techniques available; among them AES is one of the most powerful techniques. In Steganography we have various techniques in different domains like spatial domain, frequency domain etc. to hide the message. It is very difficult to detect hidden message in frequency domain and for this domain we use various transformations like DCT, FFT and Wavelets etc. They are developing a system where we develop a new technique in which Cryptography and Steganography are used as integrated part along with newly developed enhanced security module. In Cryptography we are using AES algorithm to encrypt a message and a part of the message is hidden in DCT of an image; remaining part of the message is used to generate two secret keys which make this system highly secured.

Another newly developed Method named,"Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. Signal & Image Processing" [02] is discussed. Mr. Sujay, N. and Gaurav, P,introduces two new methods wherein cryptography and steganography are combined to encrypt the data as well as to hide the encrypted data in another medium so the fact that a message being sent is concealed. One of the methods shows how to secure the image by converting it into cipher text by S-DES

algorithm using a secret key and conceal this text in another image by steganographic method. Another method shows a new way of hiding an image in another image by encrypting the image directly by S-DES algorithm using a key image and the data obtained is concealed in another image.

Another newly developed Method named, " Image Based Steganography and Cryptography "[06] is discussed. In that Mr. Domenico, B. and Luca, L. year.. describe a method for integrating together cryptography and steganography through image processing. In particular, they present a system able to perform steganography and cryptography at the same time using images as cover objects for steganography and as keys for cryptography. They will show such system is an effective steganographic one (making a comparison with the well known F5 algorithm) and is also a theoretically unbreakable cryptographic one (demonstrating its equivalence to the Vernam Cipher)

III. PROPOSED WORK

In this paper I proposed, Data hiding in media, including images, video, and audio, as well as in data files is currently of great interest both commercially, mainly for the protection of copyrighted digital media, and to the government and law enforcement in the context of information systems security and covert communications. So I present a technique for inserting and recovering "hidden" data in image files as well as gif files. Each Color pixel is a combination of RGB Values wherein each RGB components consists of 8 bits. If the letters in ASCII are to be represented within the color pixels, the rightmost digit, called the Least Significant Bit (LSB) can be altered to hide the images.

3.1 Key Stream Generation

In order to encrypt the message, we choose a randomly generated key-stream. Then the encryption is done byte by byte to get the ciphered text. The key stream is generated at the encryption and decryption site.

For encryption, a secret seed is applied to the content which in turn generates the key stream. In order to generate the same key at the decryption site, the seed must be delivered to the decryption site through a secret channel.Once the seed is received, it can be applied to the cipher text to generate the key stream which is further used for decryption

$C = E(M,K) = (M_i+K_i) \bmod 255$ where i=0 to L-1

Where M is Message

K is randomly generated key-stream.

3.2 Watermarking Algorithm

3.2.1 SS (Spread Spectrum)

We proposed a spread spectrum watermarking scheme. The embedding process is carried out by first generating the watermark signal by using watermark information bits, chip rate and PN sequence.The watermark information bits $b = \{b_i\}$, where $b_i = \{1, -1\}$, are spread by, which gives $a_j=b_i$

The watermark signal $W = \{w_j\}$, where

$w_j = a_jP_j$ where $P_j= \{1, -1\}$

The watermark signal generated is added to the encrypted signal, to give the watermarked signal

$C_W= C + W = C_{wi}= c_i + w_i.$

IV. SAMPLE SCREEN SHOTS

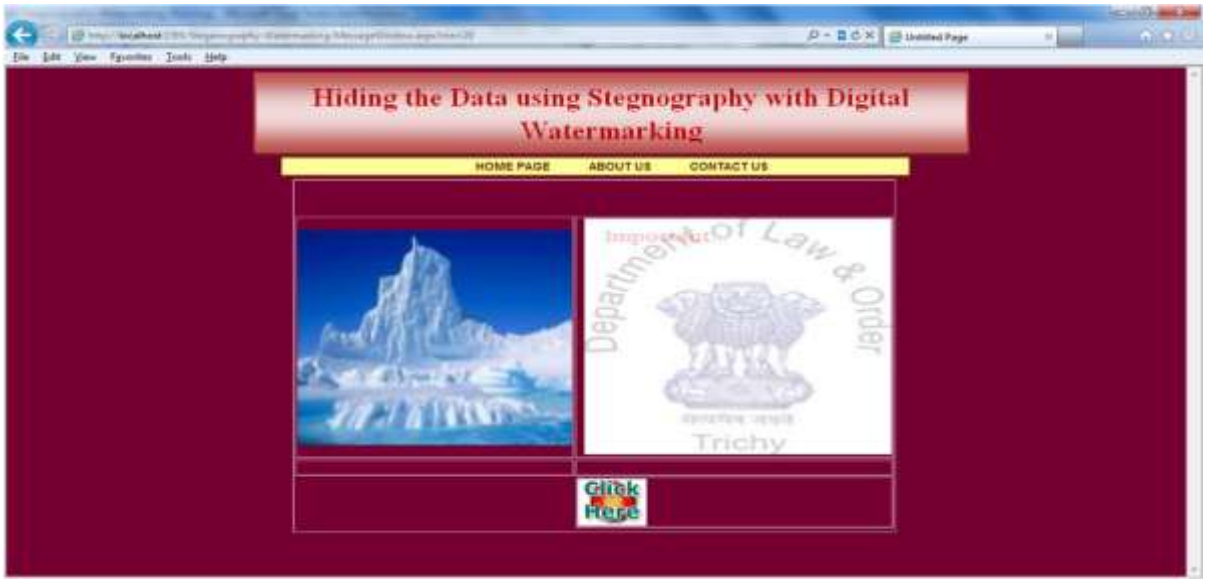
Send the Message

Encrypt & Validation Code

Receive the Message

Verification Encryption Key & Validation Code

Decrypt: (Water Marking With Text)



V. CONCLUSION

I propose a novel technique to embed a robust watermark in the JPEG2000 compressed encrypted images using three different existing watermarking schemes. The algorithm is simple to implement as it is directly performed in the compressed-encrypted domain, i.e., it does not require decrypting or partial decompression of the content.

The scheme also preserves the confidentiality of content as the embedding is done on encrypted data. The homomorphic property of the cryptosystem are exploited, which allows us to detect the watermark after decryption and control the image quality as well. The detection is carried out in compressed or decompressed domain. In case of decompressed domain, the non-blind detection is used. I analyze the relation between payload capacity and quality of the image (in terms of PSNR and SSIM) for different resolutions. Experimental results show that the higher resolutions carry higher payload capacity without affecting the quality much, whereas the middle resolutions carry lesser capacity and the degradation in quality is more than caused by watermarking higher resolutions.

REFERENCES

[1]. Dipti, K. S. and Neha, B. 2010. Proposed System for Data Hiding Using Cryptography and Steganography. International Journal of Computer Applications. 8(9), pp. 7-10. Retrieved 14th August, 2012

[2]. Sujay, N. and Gaurav, P. 2010. Two New Approaches for Secured Image Steganography Using Cryptographic Techniques and Type Conversions. Signal & Image Processing: An International Journal (SIPIJ), 1(2), pp 60-73.

[3]. Domenico, B. and Luca, L. year. Image Based Steganography and Cryptography.

[4]. Jonathan Cummins, Patrick Diskin, Samuel and Robert Par-lett,"Steganography and Digital Watermarking", 2004.

[5]. Clara Cruz Ramos, Rogelio Reyes Reyes, Mariko Nakano Miyata-keandHéctor Manuel Pérez Meana, "Watermarking-Based Image Authentication System in the Discrete Wavelet Transform Do-main".intechopen.

[6]. Domenico, B. and Luca, L. year. Image Based Steganography and Cryptography.

[7]. Niels, P. and Peter, H 2003. Hide and Seek: An Introduction to Steganography. IEEE Computer Society. IEEE Security and Privacy, pp. 32-44.