Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An approach for Information Hiding using Inverse Z-Transform and Genetic Algorithm

Aayushi Shukla, Prof. Pradeep Kumar
JSS Academy of Technical Education,
Noida, U.P., India

Abstract - Steganography is an art that involves communication of secret data in an appropriate carrier, e.g., image, audio, video or TCP/IP header file. Steganography's goal is to hide the very existence of embedded data so as not to arouse an eavesdropper's suspicion. For hiding secret data in digital images, large varieties of steganographic techniques are available, some are more complex than others, and all of them have their respective pros and cons. Steganography has various useful applications and the technique employed depends on the requirements of the application to be designed for. This paper intends the encryption of secret message and hiding the data in cover image. Also inverse Z-transform is used to modify the pixel location and then genetic algorithm is used to have more secure message.

Keywords: Steganography, cryptography, Genetic Algorithm, Inverse Z-transform.

I. INTRODUCTION

Network security is typically handled by a network administrator or system administrator who implements the security policy, network software and hardware needed to protect a network and the resources accessed through the network from unauthorized access and also ensure that employees have adequate access to the network and resources to work. Network Security techniques are classified as
secrecy, authentication, non-repudiation and integrity control. The secrecy techniques have two categories: cryptography and steganography. Both cryptography and steganography are very useful technique to achieve secrecy in communication. If both cryptography and steganography are used together then the communication becomes two fold secured.
Steganography is the art of hiding information and an effort to conceal the existence of the embedded information. It is a kind of data hiding technique that provides another way of security protection for digital image data. Steganography and data hiding are not new concepts. It is believed that steganography was first practiced during the Golden Age in Greece.
Steganographic techniques are very important part of the future of Internet security and privacy on open systems such as the Internet because important message can be hidden inside a cover medium which can be image, text, audio and video so that only the user intended to get the message knows that a secret message exists. A cover medium acts as a carrier to embed message. Steganography can be achieved in two ways. One is spatial domain steganography and another is frequency domain steganography . In spatial domain steganography the hidden information is directly embedded into image pixels. In frequency domain steganography the image pixels are first transformed into frequency domain using discrete fourier transformation / discrete cosine transformation/discrete wavelet transformation/inverse z transform.
Cryptography is the art and science of secret writing. Broadly cryptography can be classified into two types: symmetric key cryptography and public key cryptography. Symmetric key cryptography also known as private key cryptography. The sender uses a key and the encryption procedure to encrypt the message (plain text) into cipher text. The receiver uses the decryption procedure and the key to decrypt the cipher text to message. The key at sender is same as the key at the receiver. Public key cryptography uses different keys at the sender and at the receiver end.Cryptographic methods try to protect the content of a message, while Steganography uses methods that would hide both the message as well as the content.

II. RELATED WORK

Cryptography:
Encryption is the process of transforming the information for its security. Security of message is the main concern today. Image encryption techniques try to convert a message to another one that is hard to understand. On the other hand, image decryption retrieves the original message from the encrypted one.
There are various image encryption systems to encrypt and decrypt message.
*DATA ENCRYPTION STANDARD (DES)***:** DES (Data Encryption Standard) was the first encryption algorithm to be recommended by NIST (National Institute of Standards and Technology). It was designed by an IBM in 1977. DES is a 64-bit block cipher under 56-bit key. DES performs 16 processing to convert plain text into cipher text , it is based on substitution and permutation. Information and key bits are shifted, permuted and XORed in each processing round. The main disadvantage of DES is that is can be easily cracked by brute force method.

TRIPLE DES (TDES): TDES is a symmetric key block cipher, which is derived from DES. TDES uses three keys of length 168 bits (3*56 bits) while DES uses a single key of 56 bits. TDES was generally designed to protect cipher text against brute force attack by increasing the key size. TDES uses a block size of 64 bits and performs 48 processing round equivalent to DES. The main disadvantage of TDES is that it is very time-consuming.

*ADVANCED ENCRYPTION STANDARD (AES)***:** It is a symmetric key block cipher established by the U.S. NIST in 2001. AES is based on substitution and permutation network, it is fast in both hardware and software. It has a fixed block size of 128 bits and key size of 128, 192 and 256 bits. If the key size is 128 bits AES perform 10 rounds, if the key size is 192 bits it performs 12 rounds and if the key size is 256 rounds it performs 14 rounds.

***BLOWFISH*:** Blowfish is a symmetric block cipher algorithm. Blowfish is accepted as a fast and strong encryption algorithm because it has not been cracked. Blowfish is fixed 64 bit block cipher and a takes key length from 32-448bits. Total 16 processing rounds of data encryption is performed in Blowfish. The advantages of blowfish algorithm are that it is secure and easy to implement and best for hardware implementation. Blowfish is a 64 bit block cipher and is suggested as a replacement for DES. Blowfish is a fast algorithm and can encrypt data on 32-bit microprocessors.

STEGANOGRAPHY:

SPATIAL DOMAIN-BASED STEGANOGRAPHIC TECHNIQUES:

Spatial domain techniques embed messages in the intensity of the pixels directly.

Least Significant Bit (LSB) Based Steganography: LSB based steganography is one of the conventional techniques capable of hiding large secret message in a cover image.

*Bit Plane Complexity Segmentation Steganography***:** Bit plane complexity segmentation steganography (BPCS) was introduced by Kawaguchi. It is based on the simple idea that the higher bit planes can also be used for embedding information. In BPCS, each block is decomposed into bit-plane.

Information Theory-based Data Hiding: Hadhoud, proposed a technique based on entropy calculation. In this method entropy of the '4' most significant bits (MSBs) are calculated first which contains most detail of each pixel.

FREQUENCY DOMAIN-BASED STEGANOGRAPHIC TECHNIQUES:

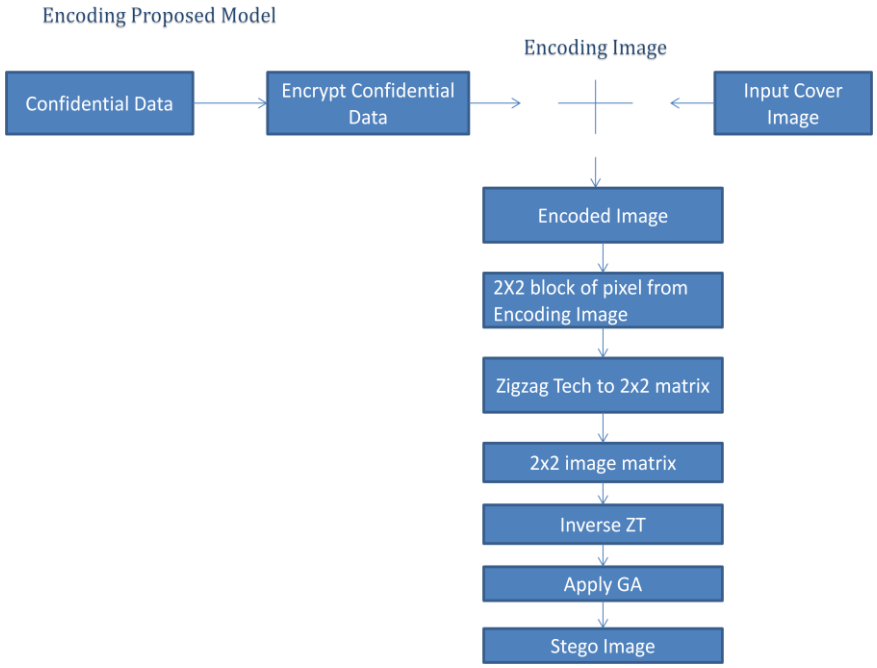
In frequency domain, images are first transformed and then the message is embedded in the image.

Discrete cosine transforms: In this technique the image is divided into 8×8 blocks and DCT transformation on each block is performed. DCT arranged the pixel of image according to their frequency value. The data bits are embedded in the low frequency coefficients of DCT.

Data Hiding Techniques: F3, F4 and F5: F3 decrements the non-zero coefficient's absolute value only if the LSB does not match with the secret bit. Zero coefficients are skipped completely. F5 embeds message bits into randomly-chosen DCT coefficients and employs matrix embedding that minimizes the necessary number of changes to embed a message of certain length.

III. PROPOSED METHOD

To increase the security of message, the combination of cryptography and steganography is used. The process of embedding is divided into following steps, firstly the message is encrypted using the blowfish algorithm then the image behind which the message is to hidden is transformed into frequency domain using the Discrete Cosine transformation (DCT), embedding secret information , re-transformed into spatial domain using inverse z – transform , and applying Genetic Algorithm.



IV. THE TECHNIQUE

In 1993, Bruce Schneier published the Blowfish block cipher. Blowfish is a 64-bit symmetric block cipher that uses a variable-length key from 32 to 448-bits. Blowfish incorporates a 16 round Feistel network for encryption and decryption. But during each round of Blowfish, the left and right 32-bits of data are modified. Blowfish incorporated a bitwise exclusive-or operation to be performed on the left 32-bits before being modified by the F function or propagated to the right 32-bits for the next round. Blowfish also incorporated two exclusive-or operations to be performed after the 16 rounds and a swap operation. Blowfish is a cipher based on Feistel Network. Feistel Network is a general method of transforming any function into a permutation. It was invented by Horst Feistel and used in many block cipher designs. Working of Feitel Network is as:

- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of applying f to the right half and the key.

After encryption of message, the cover image is transformation into frequency domain using Discrete Cosine transformation (DCT). Insertion is made by choosing 2×2 non overlapping sub mask from the source gray scale image in row major order. Discrete cosine transformation is performed on it to generate four frequency components. The most common DCT definition of a 1-D sequence of length N is

$$C(u) = \alpha(u)\sum_{x=0}^{N-1} f(x)\cos\left[\frac{\pi(2x+1)u}{2N}\right], \quad (1)$$

for u = 0,1,2, ..., N − 1. Similarly, the inverse transformation is defined as

$$f(x) = \sum_{u=0}^{N-1} \alpha(u)C(u)\cos\left[\frac{\pi(2x+1)u}{2N}\right], \quad (2)$$

for x = 0,1, 2, ..., N − 1. In both equations (1) and (2) α(u) is defined in equation (3)

$$\alpha(u) = \begin{cases} \sqrt{\frac{1}{N}} & for \quad u = 0 \\ \sqrt{\frac{2}{N}} & for \quad u \neq 0. \end{cases} \quad (3)$$

The 2-D DCT is a direct extension of the 1-D case and is given by

$$C(u,v) = \alpha(u)\alpha(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\cos\left[\frac{\pi(2x+1)u}{2N}\right]\cos\left[\frac{\pi(2y+1)v}{2N}\right],$$

Two bits of the secret information are embedded onto the second and third position of each lower frequency component excluding the highest frequency one.

The resultant image sub mask is converted back to spatial domain by IZT.

The inverse Z-transform is

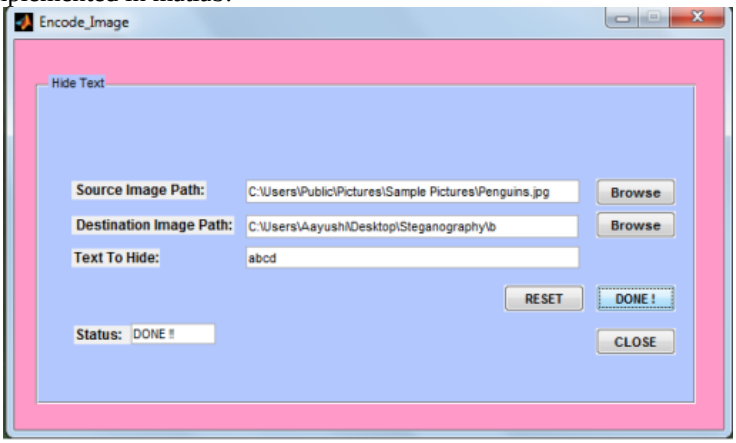
$$x[n] = \mathcal{Z}^{-1}\{X(z)\} = \frac{1}{2\pi j}\oint_C X(z)z^{n-1}dz$$

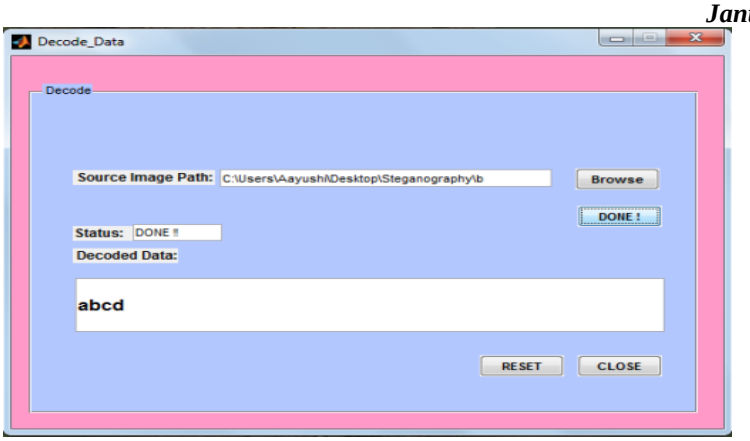
From this image in spatial domain image mask of size 32 bits are taken as initial population. New Generation followed by Crossover is applied on this initial population. New Generation is performed on rightmost three bits of each byte by consecutive bitwise XOR operation on three steps, taking the MSB of the intermediate stream generated in each step. Crossover is applied on the consecutive two pixels in row major order. As a result rightmost two bits of two consecutive pixels are swapped.

Reverse process is followed at time of decoding.

V. IMPLEMENTATION

The proposed method is implemented in matlab:





VI. CONCLUSION

The objective of this paper is to establish a highly secure model with the combination of cryptography and steganography method. For achieving our aim we use best cryptographic technique called Blowfish and for hiding message we use IZT and genetic algorithm. It enables to achieve security and enhance image quality. In this method, the pixel values of the stego image are modified by the IZT and genetic algorithm to retain their statistical characteristics. Thus, it is difficult to detect the existence of the secret message by the attacker or the third person. Further, implementation of this approach enhances the visual quality of the stego image. The probability of detection of secret message by receiver's end is also increases. However, our future work focus upon the improvement in embedding capacity and further improvement in the efficiency of this method.

REFERENCES

[1] Ramlan Mahmod , "Security Analysis of Blowfish algorithm" , Faculty of Computer Science and Information Technology Universiti Putra Malaysia ,Serdang, Malaysia, IEEE , 2013

[2] P.Singh , Prof. Karamjeet Singh , "Image Encryption and Decryption using Blowfish Algorithm in MATLAB", International Journal of Scientific & Engineering Research, July-2013.

[3] Shuchi Sharma and Babloo Saha , "Steganographic Techniques of Data Hiding using Digital Images" , Institute for Systems Studies and Analyses, Delhi, January 2012.

[4] Mohamed Amin , Hatem M.Abdulkader, Hani M.Ibrahem , Ahmed S.Sakr , "A Steganographic Method Based on DCT and new Quantization Technique" , Menofia University, Egypt, Aug 2012.

[5] Christine K. Mulunda, Peter W. Wagacha, Alfayo O. Adede," Genetic Algorithm Based Model in Text Steganography", *University of Nairobi*, Volume 5, Issue 4, October 2013.

[6] Shen Wang, Bian Yang and Xiamu Niu , "A Secure Steganography Method based on Genetic Algorithm " , School of Computer Science and Technology Harbin Institute of Technology , China , 2010

