Secure Image Transmission Using Stochastic Diffusion

Mr. H.D. Gadade[1]
Dept. of Computer Engineering,
Government College of Engineering,
Jalgaon- Maharashtra India
gadade4u@gmail.com

Pranita Patil[2]
Dept.of Computer Engineering,
Government College of Engineering,
Jalgaon- Maharashtra-India
pranitapatil1812@gmail.com

Priyanka Patil[3]
Dept of Computer Engineering,
Government College of Engineering,Jalgaon- Maharashtra-India
priyanka.patil520@gmail.com

Abstract- Proposed paper is methodical study of a method called Stochastic Diffusion for efficient encrypting digital images and hiding the information in another image or image set. The paper recommends efficient algorithm and mathematical model. This algorithm satisfies imperceptibility and robustness requirements. A secret key is used to securely embed the message text in the image and securely transfer the image over the network and the safely retrieve the original message text. There are two methods to implement the approach are considered. The first method uses binary image watermarking algorithm .This method is used for hiding an image in a single host image in which binarization is used for encrypted data. The second used to solving the problem of 24-bit image hiding in three host image which recovers original data after decryption. Both method are implemented using 'hidden code' technique.

Keywords—*Encryption, Decryption, Stochastic Diffusion*

*****

1. INTRODUCTION

Since the rise of 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.

The term steganography literally means "covered writing". The objective of steganography is to communicate information in an undetectable manner such that when the messages are observed by unintended recipient there will not be enough evidence that the messages conceal additional secret data [2].

The protection of sensitive information against unauthorized access or fraudulent changes has been of prime concern throughout the centuries. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

Steganography is the art of secret communication. Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not possess the right keys [1]. Digital images, videos, sound files, and other computer files that contain Perceptually irrelevant or redundant information can be used as "covers" or carriers to hide secret messages. After embedding a secret message into the cover image a so – called stego-image is obtained. It is important that the Stego-image does not contain any detectable artifacts due to message embedding[3].

The aim of digital watermarking is to hide some secret information or logo into the multimedia content for protecting the content from unauthorized access or illegal use. Digital image watermarking is a promising domain for various applications, for example, ownership identification, copy protection, authentication, broadcast monitoring, tamper detection etc.

II. MODULAR DESCRIPTION

A. Encrypted Information Hiding Modules

With the addition of cryptographic algorithm, encrypted information hiding is also used. Thus, increasing security of data. Data hiding techniques embed information into another medium making it not detectable to others except for those that are intended to receive the hidden information and also the receivers that are aware of it presence[6]. . In these methods, to increase the security of transmitted data, cryptographic algorithms are combined with the information hiding techniques. .In such techniques, the secret data is first encrypted, then embedded into cover data to generate 'stego-data', which is then sent through a network or via the Internet[7][1].

B. Stochastic Diffusion Module

The stochastic diffusion process is used as cryptography method. In terms of plaintexts, diffusion ensures that similar plaintexts should result in completely different ciphertexts even when encrypted with the same key. This requires that any element of the input block influences every element of the output block in an irregular way. In terms of a key, diffusion ensures that similar keys result in completely

different ciphertexts even when used for encrypting the same block of plaintext[1].

C. Hidden Codes Module

A method of randomizing the cipher bits over multiple host image LSBs as well as randomizing the embedding bits order using different noise distribution (models) as hidden codes is used to avoid LSB extraction .This results in increase in security of hidden data and improve the robustness of the binary watermarking algorithms[1]. We consider the Gaussian, Log-normal, and Uniform distributions as hidden codes.

D. Image Decryption Module

It consist of extraction of lowest 1-bit layer from stego-image. Using the same key, regenerate the cipher. A way is determined of extracting the hidden information from host data and then decrypting it to recover the original information. Stochastic fields can be computed using random number generators that depend on a single initial value or seed which can be used as a private key for the encryption/decryption process[1].

III. PRINCIPAL ALGORITHM

The principal algorithms associated with the application of stochastic diffusion for watermarking with ciphers are as follows:

[Algorithm Taken From Reference Number [1]]

Algorithm I: Encryption and Watermarking Algorithm

Step 1: Get the plain text.
Step 2: Get the Image in which text is to be hidden.
Step 3: Calculate Height And width of Image
Step 4: Calculate No Of Pixels as Height * Width.
Step 5: Compute the size of cipher text generated using a private key.
Step 6: place the binary plaintext image along with the cipher and create the output image.
Step7: Binarize the output image generated in Step 6 using Gaussian distributed ciphertext.
Step 8: Embed the binary output obtained in Step 7 into the original image at LSB to generate the image for distribution.

The following points should be noted:

(i) The host image is an 8-bit or higher grey level image which must ideally be the same size as the plaintext image or else resized accordingly using the same proportions.

(ii) Pre-conditioning the cipher and the convolution processes are undertaken using a Discrete Fourier Transform (DFT).

(iii) The output given in Step 3 will include negative floating point numbers upon taking the real component of a complex array. The array must be rectified by adding the largest negative value in the output array to the same array before normalisation.

(iv) For colour host images, the binary ciphertext can be inserted into one or all of the RGB components.

(v) The binary plaintext image should have homogeneous margins to minimize the effects of ringing due to 'edgeeffects' when processing the data using Fourier transform.

Algorithm II: Decryption and Extraction Algorithm

Step 1: Read the stego-image and extract its lowest 1-bit layer.
Step 2: Regenerate the (non-preconditioned) cipher using the same key used in Algorithm I.
Step 3: Correlate the cipher with the input obtained in Step 1 and normalise the result.
Step 4: Quantize and format the output from Step 3 to construct the original image.

The following points should be noted:

(i) The correlation operation should be undertaken using a DFT.

(ii) For colour images, the data is decomposed into each RGB component and each 1-bit layer is extracted and correlated with the appropriate cipher.

(iii) The output obtained in Step 3 has a low dynamic range and therefore requires to be quantized into an 8-bit image based on floating point numbers within the range max(array)-min(array).

Mathematical Model:

In' image space,',the plaintext is considered to be an image p(x,y)of compact support x∈ [-X,X];y∈[-Y,Y].Stochastic Diffusion is that process compounded in the following encryption /decryption algorithm.

For Encryption:

$$C(x,y)=m(x,y)\Theta x\,y p(x,y)$$

Where

$$m(x,y)=F2\text{-}1[M(kx.ky)\text{and } \forall kx.ky$$

$$M(kx.ky)=\begin{cases} N*((kx.ky)/|N(kx.ky)|2, & |N(kx.ky)|\neq 0; \\ N*((kx.ky), & \\ N(kx.ky)|=0. & \end{cases}$$

The symbols Θx and Θy denote convolution in x and y respectively. kx and ky are the spatial frenquencies ,F2-1 denotes two dimensional inverse fourier transform and the function N(kx.ky) is taken to be fourier transform of a cipher n(x,y).

For Decryption:

$p(x, y) = n(x, y)\ \Theta x\ \Theta yc(x, y)$

where Θx and Θy denote correlation in x and y, respectively.

For digital image hiding, we consider a discrete image array pij, i = 1, 2, ..., I; j = 1, 2, ...,J of size I × J and discrete versions of the operators involved, i.e. application of a discrete Fourier transform and discrete convolution and correlation sums[1].

IV. CONCLUSION

The application of stochastic diffusion for transmitting message and digital images through the internet in such a way that encrypted information can be communicated covertly and the information authenticated.Transmission of data over networks and Internet-based dissemination of digital information has brought about several security issues[1]. A binary watermark insert into a host image obtained by binarizing a floating point cipher text provides a cryptographically secure solution. So binarization is an entirely one-way process. Thus, although the watermark may be neglected from the cover text image, it cannot be decrypted without the recipient having access to the correct cryptographically secure algorithm and key.

The method of stochastic diffusion has been extended to hide 24-bit colour images in a set of three 24-bit colour images. This produces a lossless method of encrypting and covertly communicating 24-bit colour images over the Internet as required. The applications to which stochastic diffusion can be applied are numerous and, coupled with appropriate key-exchange protocols, provides a generic method of
encrypting and hiding digital image information[4].

References

[1] Jonathan Blackledge and AbdulRahman Al-Rawi , Image Authentication Using Stochastic Diffusion. 15th Interntional Conference On Computer Modelling And Simulation Year 2013.

[2] Aakanksha Upadhyay, Brajesh Patel, Spatial desynchronization in image steganography, International Journal of Computer Engineering & Science, Jan. 2014.

[3] Rehana Begum R.D, Sharayu Pradeep ,Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks , International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014.

[4] Jonathan Blackledge and Abdul Rahman Islam Al-Rawi, Steganography Using Stochastic Diffusion for the Covert Communication of Digital Images International Journal of Applied Mathematics, 2011, vol. 41, issue 4, pp. 270 - 298.

[5] Anu Bajaj , International Journal of Computer Science & Engineering Technology (IJCSET), Comparative Analysis of Digital Image Watermarking Techniques - SVD based Algorithms in Different Wavelet Domains.

[6] R. Tao, Y. Xin and Y. Wang, Double Image Encryption based on Random Phase Encoding in the Fractional Fourier Domain, Optics Letters, 16067-79, 2000.

[7] W. Na, Z. Chiya, L. Xia and W. Yunjin, Enhancing Iris-Feature Security with Steganography, The fifth IEEE Conference on Industrial Electronics and Applications (ICIEA), 2233- 2237, 2010.