IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-2, Issue-4 E-ISSN: 2347-2693

A New Method of Secure Communication with Crystography

Suganya.A[1*],Sharmila.R[2], Gopinathan.N[3]

[1*,2,3]Department of EEE, Anna University, India

www.ijcseonline.org

Received: 09/03/2014 Revised: 29/03/2014 Accepted: 22/04/2014 Published: 30/04/2014

Abstract— In the development of digital communication the need for security of data is often required. In this paper, a new method is Crystography, a combination of Cryptography and Steganography together through image processing. Cryptography is the process of converting the data into gibberish form whereas; Steganography is to embed secret data in a multimedia file as carriers, so that it will not be able to detect that a secret data existing in the file. This system is able to perform both techniques using keys for Cryptography and image as cover objects for Steganography. So, first the data is converted into cipher text using RSA algorithm of Cryptography. Secondly the encrypted data is to be hidden using LSB algorithm of Steganography. By combining both techniques more security is obtained.

Keywords/Index Term—*Crystography, Cryptography, Steganography*

I.INTRODUCTION

Nowadays, information is rapidly available through the Internet. Many companies are in need to communicate with a worldwide audience through the World Wide Web. Hence so many techniques are introduced for security. These techniques make the attention of corporate people more because where the hacking exists regularly. Many devices present today have the ability to transmit various information between themselves using different ways of communication, like insecure public networks, wireless networks and the most used: the Internet. So we have to protect communication via Internet like e-mail, e-banking, corporate data, etc., mostly used techniques are Cryptography and Steganography.

Cryptography means transforming the information into an unreadable format. It is useful to achieve confidential transmission over a public network. The original text, or plaintext, is converted into a coded equivalent called cipher text via an encryption algorithm with a secret-key. Only those who possess a secret-key on the other side can decipher (decrypt) the cipher text into plaintext. Some of the common goals are:
Confidentiality (or privacy): Only an authorized recipient should be able to extract the contents of the message from its encrypted form. Resulting from steps to hide, stop or delay free access to the encrypted information.
Integrity: The recipient should be able to determine if the message has been altered.
Authentication: The recipient should be able to verify from the message, the identity of the sender, the origin or the path it traveled (or combinations) so to validate claims from emitter or to validated the recipient expectations.
Non-repudiation: The emitter should not be able to deny sending the message.

Cryptography involves all legitimate users of information having the keys required to access that information. Based on the keys the classifications are as follows:

Symmetric Key : If the sender and recipient must have the same key in order to encrypt or decrypt the protected information, then the cipher is a symmetric key cipher since everyone uses the same key for the same message. The main problem is that the secret key must somehow be given to both the sender and recipient privately. For this reason, symmetric key ciphers are also called **private key** (or secret key) ciphers.

Asymmetric Key : If the sender and recipient have different keys respective to the communication roles they play, then the cipher is an asymmetric key cipher as different keys exist for encrypting and decrypting the same message. It is also called **public key** encryption as the user publicly distributes one of the keys without a care for secrecy. In the case of confidential messages to the user, they distribute the encryption key. Asymmetric encryption relies on the fact that possession of the encryption key will not reveal the decryption key.

Hash Function : Hash Functions are **unkeyed** message digests with special properties.

II.SYSTEM ANALYSIS

In previous work the Cryptography and Steganography technique is combined. Here cryptography is implemented by creating one rapidly exchangeable key to that message and trying to secure the message by that key with the procedure of encryption. Automatic key generator device is mainly used to generate a key for every 20mins which believes in security. Those who seek the ultimate in private communication can used this model. Since encrypted data is more difficult to differentiate from naturally occurring phenomena of the plain text, this technique is implemented before hiding. There are several tools by which we can hide message in chosen medium is Steganography. Both methods can be combined to produce better protection of the message. In case, when the steganography fails and the message can be detected but it is still no use as it is encrypted using cryptographic techniques. Though the system is more secure, this model has some failure things. They are: The key will always differ at every 20mins so

Corresponding Author: *Suganya.A*
Department of EEE, Anna University, India

the original key can get collapsed with recent generated key and also the device can get damaged and key distribution server can be a hacker.

III.PROPOSED ARCHITECTURE

The goal of the project is to create a cross-platform tool that can effectively hide an encrypted message (i.e. Word document) inside an image file. It is concerned with embedding information in a secure and robust manner. In our research we proposed a combination of two different methods, RSA for Cryptography and LSB Algorithm of Steganography. This method offers extremely good security with less complexity and less time required for encryption decryption process, compression etc.

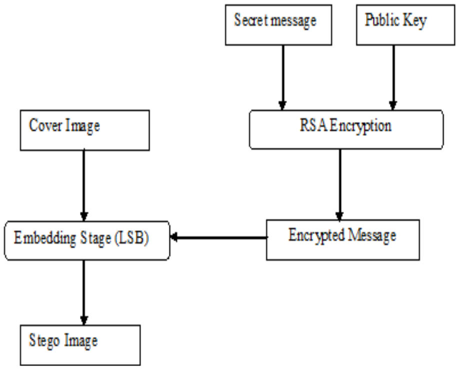

Fig 1 Block Diagram of Sender Side

The architecture model consists of sender and receiver side which is shown in Fig 1. And Fig2. Receiver will perform the reverse operation of Sender. The sender will perform the two operations as Encryption of Cryptography and encoding of Steganography. The term cryptography is to convert the known message into the unknown format of secret message. Here we go to use the Public key cryptography from its three types. In this case we use two keys public key and private keys at sender and receiver respectively. The Steganography processes consist of hiding the secret message behind the carrier file. We taking the carrier file as image, since it is used more frequently by all. Let's see more detail about the two algorithms as follows.

A. *RSA ALGORITHM OF CRYPTOGRAPHY*

Cryptography is the process of converting general data or message into unknown forms of data with the help of key. It is the combination of encryption and decryption. Encryption means converting the plain text into cipher text and Decryption means conversion of cipher text to original plain text. The cryptography has three types based on the keys. We using *public-key* cryptography type which has two keys: public key and private key for encryption and decryption. Ron Rivest, Adi Shamir, and Len Adleman at MIT, was first published the algorithm in 1978.The Rivest-Shamir-Adleman (RSA) scheme is the most widely accepted and implemented general-purpose approach to public-key type. The RSA scheme is a block-cipher (taking input as a blocks of data) in which the plaintext taken as integers between 0 and *n*. A typical size for *n* is 1024 bits, or 309 decimal digits. The three main phases of algorithm are: key generation, encryption and decryption. Now we examine some of the computational and crypt-analytical implications of RSA.

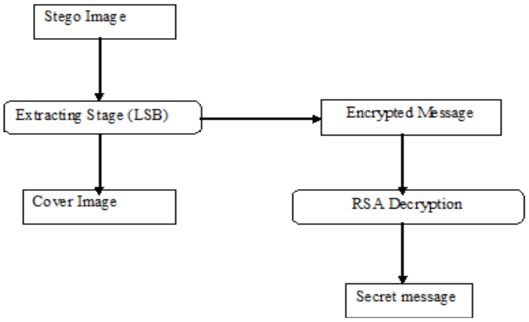

Fig 2 Block diagram Of Receiver Side

Key Generation

Select two prime numbers as p and q. p,q

Calculate the value of n, $n = p * q$

Calculate the value of $\emptyset(n)$, $\emptyset(n) = (p-1) * (q-1)$

Select 'e' such that e is prime, e<=$\emptyset(n)$,

$$\gcd(\emptyset(n), e) = 1$$

Determine 'd' $ed = 1 \, mod \, \phi(n)$

Generate key pair with e,n *Public key={e,n}*

Generate other key pair with d,n *Private key={d,n}*

Encryption

Plain text = M< n ,

$C = M^e mod\, n$

Decryption

Cipher text = C< n,

$M = C^d mod\, n$

B. *LSB ALGORITHM OF STEGANOGRAPHY*

Now we have to embed the encrypted data into an image using LSB algorithm of Steganography. The process of embedding the data in the carrier medium is Steganography. The carrier medium can be: text, image, audio and video. We chosen the medium as image, since itis most suitable for frequency on the internet. We have two types of techniques one is Spatial domain and the other is frequency domain. In spatial domain , we can directly change the pixel value bits intoour message bits. It is very easiest and best method compare to other types of steganography methods.LSB method comes under htis type of domain. LSB type is changing the LSB bits of pixel value into the 8bits of character or text.

If we have to hide word 'AIG' in the image, we take the LSB of every Colour and hide each bit of the word in its RGB Combination. To insert letter "A", we modify three Colour pixels with 3 bits in each Colour pixel. Let us think of our original pixel (a single image pixel) as bits:

(R7 R6 R5 R4 R3 R2 R1 R0, G7 G6 G5 G4 G3 G2 G1 G0, B7 B6 B5 B4 B3 B2 B1 B0)

Our message (single message character) bits look likes *(c7 c6 c5 c4 c3 c2 c1 c0)*

Then we can place three of these character bits in the lowest red pixel, three more in the lowest green pixel, and thelast two in the lowest blue pixel as follows:

(**R7 R6 R5 R4 R3** *c7 c6 c5* **G7 G6 G5 G4 G3** *c4 c3 c2* **B7 B6 B5 B4 B3 B2** *c1 c0*)

IV.IMPLEMENTATION AND RESULTS

The proposed model is implemented using Spartan 3E-XC3S100E family of FPGA in VLSI. The programming code is generated using VHDL language with the help of Xilinx design suite 12.4 as a tool and the results are analyzed with various lengths of bits of text message.. Once the code is dumped in to the kit successfully, the hyper-terminal window has to open. The hyper-terminal window is used for displaying the data. Therefore the system is tested on different size of message and different image format. The analyzed report shown below in Fig.3 with bit size as different.

Sender side
1.Write text input message.(original message).
2.Encrypt message using RSA algorithm.
3.Select cover image.
4.Use DWT algorithm for transforming the image in to coefficients and then hide the encrypt message into an image to get the stego image.

Receiver side
1.Receive the stego image.
2.Use DWT algorithm to extract the message from image.
3.Decrypt message using RSA algorithm.
4.Get the original text message.

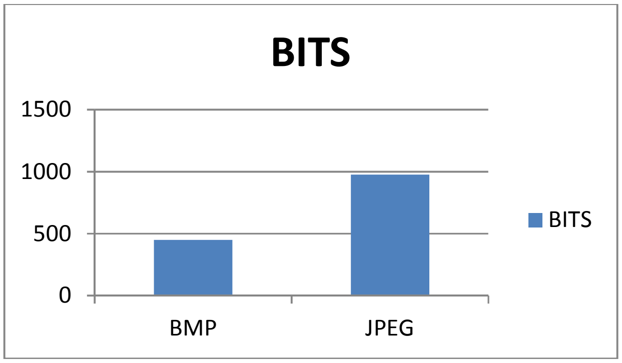

Fig. 3 Bit Analysed Report

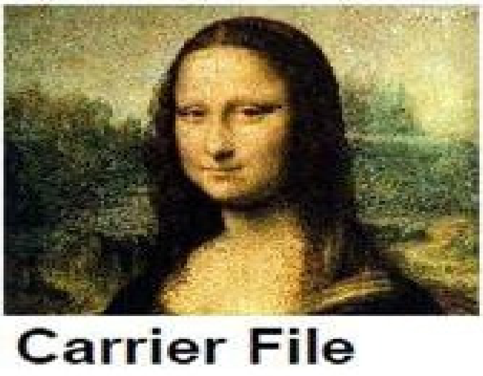

Fig 4.1 File Before Embedding

The implementation is done in JPEG type of image format is shown below in Fig 4.1. The data size of any size is encrypted. Now the encrypted data is to be hidden in the carrier file is shown in the Fig 4.2. from this we notice that the quality of the image is not reduced in both figures.

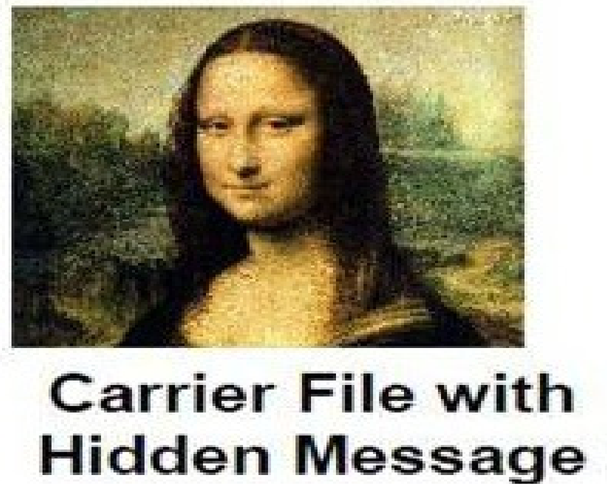

Fig 4.2 File After Embedded

V.CONCLUSION

A new and efficient steganography method for embedding secret messages into images without producing any major changes is proposed . Multilayer security by applying cryptography and steganography together is used. RSA algorithm of public key cryptography is used for encryption and decryption. For embedding LSB algorithm of spatial domain of steganography is used. The concept of embedding capacity of this method is much better than other existing methods in spatial domain. This is a robust method which can avoid various image attacks like visual, statistical and structural.

REFERENCES

[1] Ankit Anand and Pushkar Praveen “Implementation of RSA Algorithm on FPGA” International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 5, July – 2012.

[2] Chandra M. Kota and Cherif Aissi1” Implementation Of The RSA Algorithm And Its Cryptanalysis” ASEE Gulf-Southwest Annual Conference, The University of Louisiana at Lafayette, March 20 – 22, 2002.

[3] Fadhil Salman Abed A Proposed Method Of Information Hiding Based On Hybrid Cryptography And Steganography in International Journal of application in Engineering and Management, Vol 2, Issue 4, 2013

[4] Gurmeet Kaur and Aarti Kochhar,A “Steganography Implementation Based On LSB & DCT “ International Journal for Science and Emerging Technologies with Latest Trends” in vol 4, 2012.

[5] Mihir,H and Rajyaguru “Crystography: combination of cryptography and steganography” in International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 10, October 2012.

[6] Inderjeet Kaur “Digital Stegnaography:hiding data within data” in ITM voyager volume 2, no 1, july-dec 2005.

[7] Padmashree,G and Venugopala,P “Audio Steganography and Cryptography: Using LSB Algorithm at 4th and 5th LSB

layers" in International Journal Of Engineering and innovative Technology volume 2, issue 4, October 2012.

[8] Samidha Diwedi Sharma and Dipesh Agrawal "Analysis of Random Bit Image Steganography Techniques" in International Journal of Computer Applications 2013.

[9] Po-Yueh Chen* and Hung-Ju Lin "A DWT Based Approach for Image Steganography" in International Journal of Applied Science and Engineering 2006. 4, 3: 275-290

[10] K B Shiva Kumar, "Bit Length Replacement Steganography Based On DCT Coefficients", in International Journal of Engineering Science and Technology, Vol. 2(8), Pg: 3561-3570,2010.