ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

A Unique Cipher Mechanism Integrating Steganography with Traditional Cryptography

Pankaj Rakheja[1], Sidharth Bhatia[2], Roopakshi Bajalia[3], Pulkit Garg[4]

Assistant professor, Dept. of ECE, ITM University, Gurgaon, Haryana, India [1]

Assistant professor, Dept. of ECE, ITM University, Gurgaon, Haryana, India [2]

B.Tech Student, Dept. of ECE, ITM University, Gurgaon, Haryana, India [3]

B.Tech Student, Dept. of ECE, ITM University, Gurgaon, Haryana, India [4]

ABSTRACT: Now a days most of the information is transmitted over the network whether personnel or professional and concept of electronic money is also in trend, bank transaction or online shopping are more in trend then before so we need to make the network more secure. Traditional cryptographic mechanisms are more vulnerable to attacks now as they are well known to attackers and many new forms of attacks are being developed exploiting their loop holes so we need to design new methods of encrypting or hiding data to make transactions more secure. Here we have developed a cipher mechanism where we can hide a gray scale image in RGB component of a colored image in random manner which adds an element of uncertainty and original and watermarked images are almost similar so it's very difficult to predict any information hidden in the image.

KEYWORDS: Cipher, Public key, RSA,Steganography

I.INTRODUCTION

In Cryptography [7] [9] we use certain algorithms known as ciphers which encrypt the data so as it becomes non readable this is done to enable secure communication over the network. Encryption is the process that is used to carry out this. In an encryption scheme, the message or information, referred to as plaintext, is encrypted using an encryption algorithm, turning it into an unreadable ciphertext. This is done using an encryption key which is the secret key known only to authorized parties. One should not be able to make out anything from ciphertext generated else the very purpose would fail. The strength of the encryption algorithm relies on the randomness of the cipher generated. The desired recipient has the secret key along with decryption algorithm to successfully decode the ciphertext and extract the original message from it. Cipher algorithms need a key generation and sharing mechanism for carrying out the whole process.

Symmetric Key Encryption

Symmetric-key algorithms use the same key or simple transformation of both keys for both encryption and decryption process. The key here represents a secret message shared between two parties for enabling secure communication. Most common examples of symmetric key encryption are AES, DES etc. This requires that both parties have access to the secret key. This is the main flaw of symmetric encryption the whole security of the system rely on the key sharing mechanisms as the algorithms are known to everyone so if somehow attacker gets the key, he has a set of key and ciphertext so would be able to decode the message.

Public-key encryption

In public-key encryption schemes, for encryption public key is used which is known to everyone whereas a private key or secret key is used for the decryption. Public-key encryption is a relatively new as compared to symmetric encryption. It does not rely on the key sharing mechanism like symmetric cryptography. One of the earliest public key encryption

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

applications was called Pretty Good Privacy (PGP). It was written in 1991 by Phil Zimmermann and was purchased by Symantec in 2010.

Visual cryptography

Visual cryptography [2-5] [11-13] is the cryptographic technique which does not require computer for decoding as visual information like text, image etc are hidden in cover image or any other file. It involves creation of multiple shares of the secret data which together will convey any useful information and alone would be of no meaning. Combining these shares would allow decoding the message. Moni Naor and Adi Shamir developed one of the best known visual cryptography techniques in 1994, which involved breaking an image into "n" shares, where any "n-1" shares revealed no information. To reveal original image all " n" shared need to be overlayed. Each share can be printed on a separate transparency, and can be used for one-time pad encryption, where one transparency acts as cipher text and another is a shared random pad. Steganographic techniques can vary a lot one can go for simple LSB insertion [6], use binary encoding techniques [8] or geometry based key sharing approach [13]

II.OVERVIEW

Steganography

Steganography [1] is the art of concealing a message in another message which can be audio in audio or image in image or text in image etc. The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography, which was disguised as a book of magic. Generally, the hidden messages will appear to be or be part of something else. For example, the hidden message may be in invisible ink between the visible lines of a private letter. Some implementations of steganography which lack a shared secret are forms of security through obscurity, whereas key-dependent steganographic schemes adhere to Kerckhoffs's principle.

The advantage of steganography over cryptography alone is that it does not attract attackers as transfer of any secret message is not conveyed as in case of cryptography where the non readable cipher arises curiosity in attacker and may in themselves be incriminating in countries where encryption is illegal. Thus, whereas cryptography is the practice of protecting the secret message from unauthorized access , steganography apart from doing that conceals the fact that any secret information is being sent too. This adds an additional layer of security to the network.

Steganography includes the hiding information within computer files. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are most suitable for steganographic transmission because of their large size. For example, a sender might start with an image and modify 50th pixel or 100th pixel of image for storing an alphanumeric message which wont affect the cover image much its PSNR n histogram remains almost same so would be quite difficult to detect n decode the message..

LSB Encryption

LSB bit encryption method involves the LSB of some or all the bytes inside an image being replaced with bits of the secret message.

For example, a grid of three pixels of a 24- bit image can be as follows:

0101110**1** 0010001**0** 1101010**0**
0110111**1** 0001101**0** 0101000**1**
1001010**1** 0101000**1** 0111010**1**

RSA algorithm[10] is the most popular asymmetric key cryptographic algorithm. It is based on the fact that it is easy to find large prime numbers and multiply them together, but it is extremely difficult to find the factors of their product. In such cryptosystem, encryption key is public and different from the decryption key, which is kept a secret. Process of encryption and decryption is as follows:

- Choose two large prime numbers P and Q.

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

- Calculate N = P*Q.
- Select the public key (encryption key) E such that it is not a factor of (P-1) and (Q-1).
- Select the private key (decryption key) D such that (D*E) mod(P-1)*(Q-1)=1
- For encryption, calculate the cipher text as CT from the plain text PT as $CT=PT^E$ mod N
- Send CT as the cipher text to the receiver.
- For decryption, calculate the PT from CT as $PT=CT^D$ mod N

III.MECHANISM DESIGNED

Here we are hiding a grayscale secret image (120*120) in a colored image (1024*960) using the LSB insertion. Here the secret image, to be hidden is first divided into 9 parts or into 3*3 matrix then those parts are rearrange using basic permutation technique then are hidden in RGB components of the cover image.

Encryption Process

Here at the sender side we hide a grayscale secret image in a color cover image using these steps

Step1: Read cover image

Step2: Divide the cover image into its RGB components

Step3: Further divide the RGB components into 9 parts

Step4: Take the secret image and divide it too into 9 parts

Step5: Generate a random sequence of numbers from 1 to 9

Step6: Hide the first three parts of the secret image as per the sequence in Red component of the cover image using LSB insertion

Step7: Hide the next three parts of the secret image as per the sequence in Green component of the cover image using LSB insertion

Step8: Hide the last three parts of the secret image as per the sequence in Blue component of the cover image using LSB insertion

Step9: Then combining watermarked RGB form a new image which would be sent to recipient

Here we rely on a sequence which decides the order in which the parts of the secret image would be hidden in RGB components of the cover image. That sequence may be used as key and shared using any key sharing mechanism employed in symmetric cryptography. In order to add more security the sequence can be RSA encoded and then shared.

Decryption Process

Here at the receiver side we extract the secret image from the received watermarked image using these steps

Step1: Read watermarked image

Step2: Divide the watermarked image into its RGB components

Step3: Further divide the RGB components into 9 parts

Step4: Using the shared random sequence

Step5: Extract the first three parts of the secret image as per the sequence from the Red component of the watermarked image.

Step6: Extract the next three parts of the secret image as per the sequence from the Green component of the watermarked image.

Step7: Extract the last three parts of the secret image as per the sequence from the Blue component of the watermarked image.

Step8: Then reconstruct the secret image from the parts extracted from RGB components of watermarked image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

IV.RESULT

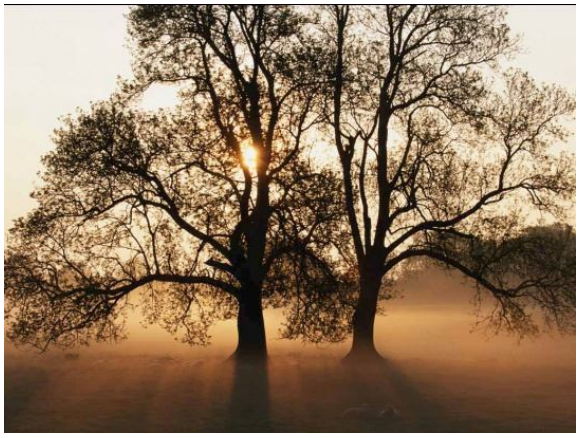

Figure 1: Secret image

The secret image to be hidden is shown in figure 1, which is a colored image which has to be converted to gray scale by using rgb2gray command in Matlab. We are using 8 bit representation so 255 levels in all.

Figure 2: Secret image divided into 9 parts

image to be hidden is further divided into 9 parts as shown in figure 2 which would be hidden in the RGB components of the cover image in a random manner so as it becomes difficult to decode it without prior knowledge of the key.

Figure 3: Permuted image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

The image to be hidden is rearranged as in case of puzzle in accordance with the key to further enhance uncertainty in the process as shown in figure 3.

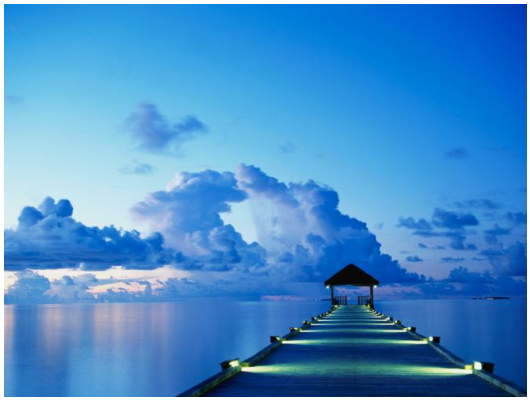

Figure 4: Cover image

Figure 4 shows the cover image used for hiding the secret image. It is decomposed into its RGB components where the the parts of secret image would be hidden .

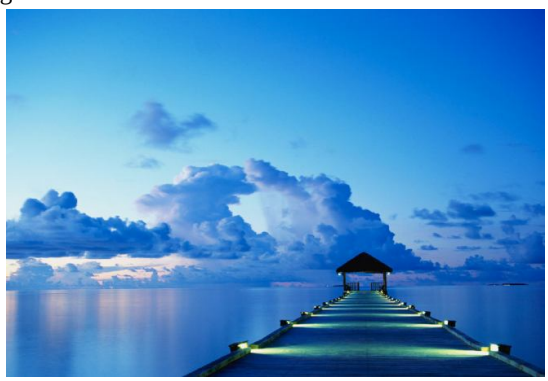

Figure 5: Watermarked image

The watermarked image is shown above in figure 5 , it can be seen that it does not differ from the original image and looks the same so very purpose of steganography gets solved.

Figure 6: Image recovered

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

Then after applying the reverse process and using the key we have successfully recovered the image hidden as shown in figure 6.

V. CONCLUSION AND FUTURE SCOPE

We have developed a cipher mechanism where we can hide a grayscale image in RGB component of a colour image in random manner which adds an element of uncertainty and original and watermarked images are almost similar so it's very difficult to predict any information hidden in the image. Here its strength rely on the randomness of the information hiding algorithm which divides each RGB component into 9 parts, thus in total 27 parts where information is hidden using LSB insertion. Future work may comprise of encoding the secret image using Manchester coding or some other technique

REFERENCES

[1] Sandeep Singh, Aman Singh," A Review on the Various Recent Steganography Techniques" IJCSN International Journal of Computer Science and Network, Volume 2, Issue 6, December 2013
[2] M. Naor and A. Shamir, "Visual cryptography", in EUROCRYPT '94 Proceedings, Lecture Notes in Computer Science, Springer-Verlag, vol. 950, pp. 1-12, 1995
[3] Sarita Poonia, Mamtesh Nokhwal, Ajay Shankar." A Secure Image Based Steganography and Cryptography with Watermarking" International Journal of Emerging Science and Engineering (IJESE) ISSN: 2319–6378, Volume-1, Issue-8, June 2013
[4] Pavithra Vaman, C.R. Manjunath, Sandeep.K," Integration of Steganography and Visual Cryptography for Authenticity "International Journal of Emerging Technology and Advanced Engineering , Volume 3, Issue 6, June 2013
[5] Neha Chhabra," Visual Cryptographic Steganography in Images" IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.4, April 2012
[6] Mr. Vikas Tyagi, Mr. Atul Kumar, Roshan Patel,Sachin Tyagi, Saurabh Singh Gangwar , "Image steganography using least significant bit with cryptography", Journal of Global Research in Computer Science Volume 3, No. 3, March 2012.pp: 53 -55
[7] "Cryptography and network security", Atul Kahate, second edition, Mc Graw hill companies
[8] Kuang Tsan Lin , "Based on Binary Encoding Methods and Visual Cryptography Schemes to Hide Data" , IIH -MSP '12 Proceedings of the 2012 Eighth International Conference on Intelligent Information Hiding and Multimedia Signal Processing pp: 59 -62
[9] B. Schneier, "Applied Crypt ography: Protocols, Algorithms, and SourceCode in C", John Wiley & Sons, Inc, 1996
[10] Rivest, R.; A. Shamir; L. Adleman (1978). "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems". Communications of the ACM 21 (2): 120–126
[11] C.C. Wu and L.H. Chen, "A Study on Visual Cryptography", Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, 1998
[12] F. Liu and C. Wu "Embedded extended visual cryptography schemes", IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp.307 -322 2011
[13] Chien-Chang Chen , Wen-Yin Fu,Chaur-Chin Chen, "A Geometry Based Secret Image Sharing Approach" Proc. IVCNZ (Image and Vision Computing, Newzeland), 28-29 Nov., 2005.