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. 4, Issue 5, May 2015

Unique Cipher Mechanism for Ensuring Secure Data Flow over Network

Pankaj Rakheja [1], Renu Saini [2], Nankita Asija [3], Diwakar Kamboj [4]

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

PG Student, Dept. of ECE ITM University, Haryana, India[2]

PG Student, Dept. of ECE ITM University, Haryana, India[3]

PG Student, Dept. of ECE ITM University, Haryana, India[4]

ABSTRACT: Cryptography is the art of making text non readable from human readable to ensure secure communication over the network. It is classified basically into two types one is symmetric cryptography and the other is asymmetric cryptography. In the symmetric cryptography we use single key for encryption and decryption process which creates trouble of key sharing whereas in asymmetric cryptography two different keys are used for one for encryption and other for decryption which solves dependence on key sharing to large extent. But now traditional cryptographic ciphers are more prone to attacks and problem of authentication also exists as users have increased and few of them try to have unauthorized access. In order to solve this issue we have integrated biometric and visual cryptographic modules in the basic RSA module to make it more secure. The RSA encrypted text or message is hidden through LSB insertion in an image which also has shares of the fingerprint of the desired recipient. Along with that we have used the Caesar and mix columnar operation which protects RSA from man in middle attack as to decode the encoded text, attacker needs to know key used in mix columnar operation too. And as the size of text increases mix columnar becomes more effective. Moreover the receiver would be able to get the message only if his fingerprint matches to that of the desired one else he would just be able to see image only that is we have hidden the existence of secret message so as to make it even more secure. Matlab simulation has been carried out to validate the proposed technique

KEYWORDS: Block replacement scheme, Biometrics, Caesar, Quantum cryptography

I.INTRODUCTION

As technologies are increasing the rate of cyber attacks and cyber warfare are threatening network infrastructures from various parts of globe are also increasing. Therefore today more emphasis is required on securing data than ever before. In order to solve the problem of securing data many attempts have been made by researchers. Encoding data before sending it has been the basic method for securing data flow over the network. The term cryptography [2-4] came into picture which deals with encoding and decoding data for an effective and efficient communication. There are two types of cryptographic techniques: symmetric and asymmetric cryptography. The former relies on single key whereas the later relies on two keys one public and one private. Then later on different types of cryptographic techniques came namely elliptical cryptography, DNA cryptography, quantum cryptography, visual cryptography etc.

Along with cryptography another method is also used for ensuring secure communication over the network that is Steganography where data is hidden in some other file which can be image or video etc. Juneja, M.; Sandhu, P.S.[5] had designed a Robust Image Steganography Technique Based on LSB Insertion and Encryption. Visual cryptography inculcates or integrates both. One of the data security methods introduced by researcher is visual cryptography. This technique was first proposed by Naor and Shamir in 1994. M. Naor and A. Shamir [6] had explain Visual cryptography as a secret sharing scheme in which secret image are distributed into two or more shares such that when these shares are superimposed exactly together original secret is revealed. Best example of visual cryptography is biometrics. A. Ross and A. A. Othman [7] had used biometric information in form of fingerprint which is kept secret by dividing

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. 4, Issue 5, May 2015

them into shares, which are then distributed to number of parties for safety purpose. The secret is revealed only when shares from all parties are superimposed.

II.OVERVIEW

A. Basic visual cryptography scheme

A basic (k, n) VC scheme produces n share from original image and distributed among n persons. When any k persons or more of these (where $k \leq n$) superimposed their share, than secret is recovered but if k-1 persons attempt to recovered secret image than it fail.

Now let us consider a (2, 2) VC scheme which produces two shares. Here each pixel of image is divided into smaller blocks of either 1 X 2 or 2 X 2 with same number of black and white block. If pixel is divided into two parts then there will be one white and one black block similarly if pixel is divided into four equal parts, there are two white and two black blocks. So if original pixel (which is divided into four equal parts) is white than six combination of share are possible which are shown in figure 1 and similarly the possible share combination of black pixel are also shown in the figure. The original secret image is reconstructed after stacking the shares.

B. Multiple image VC [8-9]

This is technique is used for hiding two secret image at the same time by applying rotation technique. The first secret image is recovered by stacking the first and second share and second secret image is recovered by stacking third and second share. The third share is rotated version of first share in counterclockwise by θ, where θ is 90°, 180°, or 270°. An example of MIVC is shown in figure 3. This approach has many problems associated with it one is pixel expansion and other is limited in rotation angles and also only two secret images can be hidden by this approach.

C. Extended VC

Extended VC scheme [8-10] is a visual secret sharing scheme in which shares are meaningful and when these shares are superimposed their meaningful information disappear and secret is recovered. In this technique images having some form of meaningful information are used for generation of shares which referred as cover images. An example of EVC is shown in figure 4. This approach also has problem of pixel expansion.

D. Simple block replacement scheme (SBR)

In earlier two approaches there was a problem of pixel expansion in order to fix the problem of pixel expansion simple block replacement scheme was introduced. This is a preprocessing step after creating halftone image before any VC scheme is applied. In this scheme instead of working on individual pixel a group of pixel is considered. A group of four pixels is considered as secret block of 2 x 2 and then shares are generated block by block. Each secret block with four pixels produce two secret share each containing four pixels therefore size of reconstructed image is same as original image. The problem associated with this scheme is that reconstructed image has poor contrast.

E. Balanced block replacement scheme

This approach is improved version of SBR. This approach improves the visual quality of reconstructed image. In this approach halftone image is partitioned into non overlapping blocks of 2 x 2 pixels. Each group of four blocks is referred to as cluster. Then in one cluster number of white and black pixel are calculated if they are unequal than they are made equal by adding or removing black pixel. For example if in a cluster there are 7 white pixel and 9 black pixel then to balance the cluster one black pixel is converted to white pixel. Similarly all clusters are processed. Also the problem of visual quality and pixel expansion are solved.

.

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. 4, Issue 5, May 2015

III.MECHANISM DESIGNED

We have designed a cipher mechanism where we have hidden an encoded text in an image using LSB insertion. The main positive fact what makes it different from others available is that it combines traditional cryptographic techniques with modern techniques. As we all know cryptography relies on substitution and permutation so we have used Caesar and mix columnar cipher which will save the RSA encoded text from man in middle attack which is further armoured by steganographic mechanism which hides that in cover image which hides the existence of any secret communication. In this paper we are describing the algorithm designed by us through flow charts and also have included the results obtained through Matlab implementation.

We are using a (2, 2) VC scheme as shown in figure 1. It may be noted that the resulting share images and recovered secret image contain four times more pixel than original image and also visual quality of recovered image has been degraded.

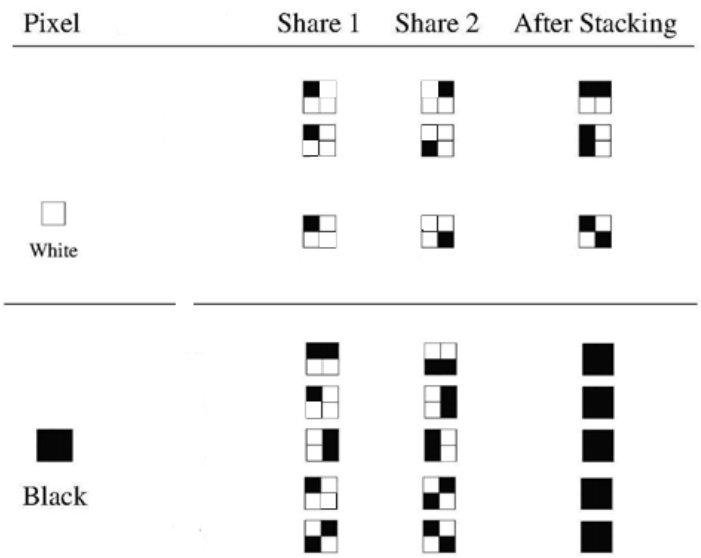


Figure 1: (2, 2) VC scheme

Figure 2 below shows that we have used biometrics that is fingerprints for authentication here two shares are generated using VC scheme shown in figure 1 out of which one share is hidden in the cover image along with the encoded data as shown below in figure 3 below.

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. 4, Issue 5, May 2015

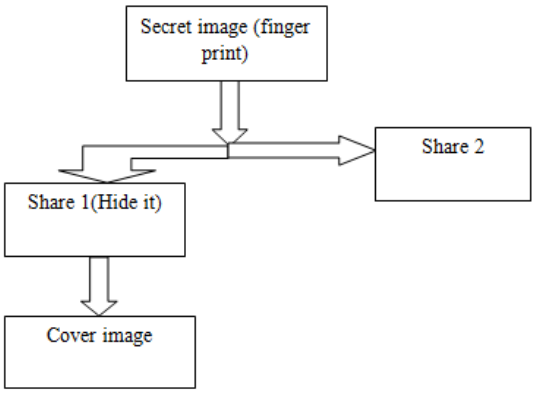


Figure 2: Steganography part

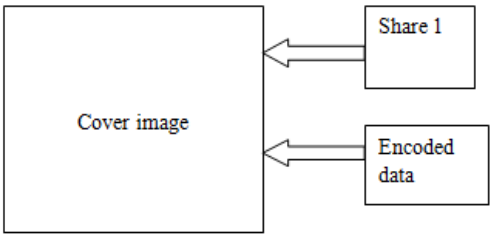


Figure 3: Data and share hidden in cover image

The encryption process employed here encodes the plaintext three times firstly with Caesar then carries out mix columnar operations after that data moves to RSA encoding module which encodes it to obtain the final cipher text as shown in figure 4.

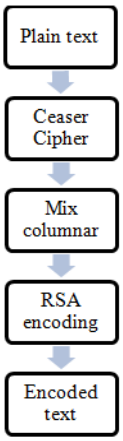


Figure 4: Encryption process

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. 4, Issue 5, May 2015

Here as we said above two shares are generated using VC scheme (figure 1) from the secret image which is a fingerprint image of desired recipient.

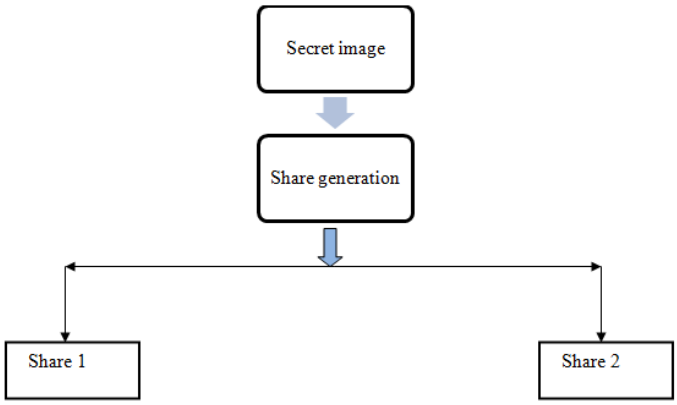


Figure 5: Share generation

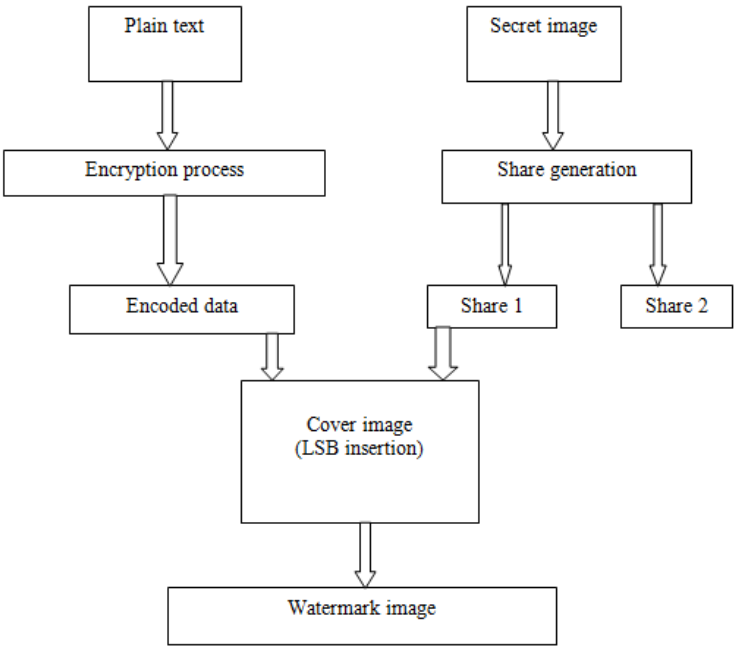


Figure 6: Process at sender side

The overall process at the sender's side is shown in figure 6 above which shows that plaintext is encoded and parallel to that shares are extracted from secret using share generation process and out of two shares one is inserted in the cover image along with encoded text and we obtain a watermarked image at last which will be sent to the receiver over the media

At the receiver side we get watermarked image which would be the one containing the secret message. But before extracting the encoded text from image the algorithm will compare the recipients fingerprint with the fingerprint generated from the share hidden in the cover image. After a good match then only the encoded text would be extracted the undergoes decryption process shown in figure 7 which shows that the encoded text is first decoded by RSA then mix columnar then Caesar cipher to get the original message.

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. 4, Issue 5, May 2015

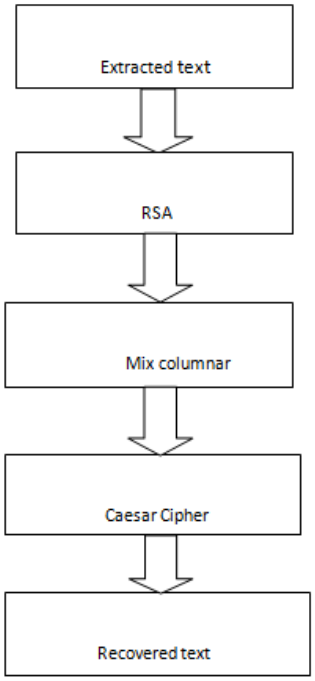
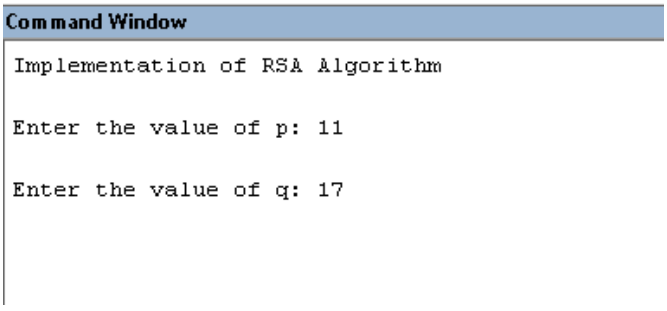


Figure 7: Decoding algorithm

Here we can choose to hide share in Red component of the coloured image and hide encoded value in the blue or green component of the image instead of using a gray scale image.

IV.RESULTS

We have implemented the designed algorithm on Matlab where we take input from user that is the text to be hidden which is encoded by Caesar, Mix columnar and RSA algorithm. Figure 8 below shows the entered plaintext and intermediate and final cipher text obtained.



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. 4, Issue 5, May 2015

```
Command Window
The value of (N) is: 187
The public key (e) is: 3
The value of (Phi) is: 160
The private key (d)is: 107

Enter the message: 'prince'
enter plaintext to be encoded'prince'


sulqfh

remainder =

     0


mod_text =

   115   113
   117   102
   108   104


rearr =

   115   113   117   102   108   104

Cipher Text of the entered Message:
     4     5   145   170    80    59
```

Figure 8: Cipher texts generated in the algorithm

Figure 9: Finger print

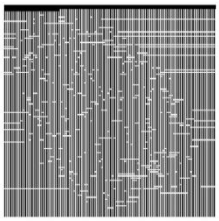
Figure 9 above shows the fingerprint or the secret image of the desired recipient whose shares will be generated using VC scheme shown in figure 1 above. Figure 10 shows the shares generated by the share generation process.

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

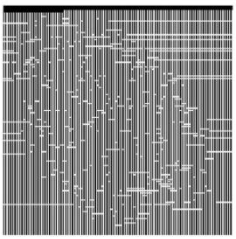
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015



Share1



Share2

Figure 10: Shares generated

The recipient gets the watermarked image from which share hidden would be extracted first the fingerprint matching will take place and after proper match that is above 95% the encoded data will be decoded to get the secret message.

Figure 11: 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. 4, Issue 5, May 2015

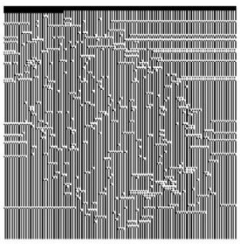


Figure 12: Extracted share

```
message =

prince

Decrypted ASCII of Message:
prince
Decrypted Message is: prince

ans =

prince
```

Figure 13: Recovered text

V.CONCLUSION

Traditional cryptographic methods were actually based on mathematical operations like substitutions and transposition which are now quite pron to attacks but on integrating them with biometric and visual cryptographic modules we can make both of them more efficient and effective if used alone. We have inculcated biometric, cryptographic and steganographic modules together to get a better cipher. We have used Caesar cipher; Mix columnar, block replacement, RSA, LSB insertion etc to get an overall improved cipher. We have used grayscale image but we can also go for RGB or halftone image too. For future work modified Caesar or mix columnar method can be used and along with that we can work with HSI too for data hiding.

REFERENCES

[1] K. 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

[2] "Cryptography and network security", Atul Kahate, second edition, Mc Graw hill companies.

[3] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and SourceCode in C", John Wiley & Sons, Inc, 1996.

[4] Piper," Basic principles of cryptography" , IEEE Colloquium on Public Uses of Cryptography, 1996.Page(s): 2/1 - 2/3

[5] Juneja, M.; Sandhu, P.S.;"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption" ARTCom '09. International Conference on Advances in Recent Technologies in Communication and Computing, 2009. Page(s): 302 - 305.

[6] M. Naor and A. Shamir, "Visual cryptography" in EUROCRYPT'94 (Lecture Notes in Computer Science), vol. 950. Berlin, Germany: Springer-Verlag, 1995, pp. 1–12.

[7] A. Ross and A. A. Othman, "Visual cryptography for biometric privacy," IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81, Mar. 2011.

[8] J. B. Feng, G. C. Wu, C. S. Tsai, Y. F. Chang, and Y. P. Chu, "Visual secret sharing for multiple secrets," Pattern Recognit., vol. 41, no. 12, pp. 3572–3581, 2008.

[9] H. C. Wu and C. C. Chang, "Sharing visual multi-secrets using circle shares," Comput. Standards Inter., vol. 28, no. 1, pp. 123–135, 2005.

[10] N. Askari, C. Moloney, and H. M. Heys, "An extended visual cryptography scheme without pixel expansion for halftone images," in Proc.26th IEEE Canadian Conf. Electrical. Computer Eng. (CCECE), Regina, SK, Canada, May 2013, pp. 1–6.