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 6, June 2015

A Novel Cipher Mechanism for Securing Data Flow over the Network

Pankaj Rakheja[1], Ruchika Bhatia[2], Renu Saini[3], Nankita Asija[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: Most of the data flowing over network is prone to attacks .Many cryptographic algorithms are used to secure the data for effective and efficient communication. The cryptographic mechanisms are classified broadly in to two types symmetric and asymmetric. The designed cipher combines both symmetric and asymmetric cryptography which makes it more efficient and effective. Here data is hidden using symmetric key and encoded by well known RSA algorithm. Along with that we have used steganography too where data is hidden in YCbCr components of a colored image. So cipher designed here inculcates the various mechanisms to secure data communication over the network.

KEYWORDS: Symmetric key Cryptography, RSA, YCbCr

I.INTRODUCTION

In today's world everyone wants their data to be secure and protected from cyber attackers which are threading the network. To ensure security of data many methods have been developed. One of the methods is cryptography. The word has been derived from the Greek *kryptos*, means hidden. Cryptography [3-4] is the art of encoding messages into non readable form called cipher which cannot be easily understood by human in order to achieve secure communication over a network. The origin of cryptography came from 2000 BC, with the Egyptian practice of hieroglyphics which consist of complex pictograms. The first use of a modern cipher was done by Julius Caesar (100 BC to 44 BC), who did not trust his messengers when communicating with his governors and officers that is why, he created a system in which each character in his messages was replaced by a character three positions ahead of it in the Roman alphabet. There are two cryptographic mechanisms based on keys used. One is symmetric cryptography and another is asymmetric cryptography. In symmetric cryptography same key is used for encryption and decryption whereas in asymmetric cryptography different keys are used for encryption and decryption. There is various ways of encrypting data such as RSA algorithm, AES algorithm etc. But most popular and common method is RSA algorithm. The RSA algorithm was first publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman at MIT. RSA algorithm is based on fact that it is easy to find and multiply large prime numbers together but extremely difficult to factor their product. Here public and private key are based on large prime number. So only those people who has required secret key can decrypt or decode the message into readable form.

Another method for secure communication over network is steganography where data to be hidden is kept inside other message, image, video etc. Visual cryptography inculcates or integrates both. This technique was first proposed by Naor and Shamir in 1994. M. Naor and A. Shamir [8] 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 [9] had used biometric information in form of fingerprint which is kept secret by dividing 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 superimposedVisual cryptography is 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.

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 6, June 2015

In this paper we have hide data using symmetric key which is encoded by using RSA algorithm. Along with that we have used steganography too where data is hidden in YCbCr components of a colored image for securing our data over network. A colored image consists of three components that is red, green, blue component.

II.OVERVIEW

Cryptography is a technique of transmitting data in non-readable form. Readable data which is known as plain text is converted into non-readable format known as cipher data. The process of conversion of plain text into cipher text is known as Encryption. The data is converted back into plain text by the process of Decryption. Cryptography makes the data flowing on the network secure. Unauthorized users can not access the data due to its non readable form. Cryptography includes various aspects like authentication, non-repudiation, integrity and confidentiality. Various protocols are there to maintain these various aspects. The originator of encrypted message shares the decoding algorithm with the sender. Hence only desired recipient can access the message. Cryptography [3-4] can be symmetric or asymmetric. In asymmetric cryptography, key used for encryption and decryption is different. One key is used for encryption and other is used for decryption. Basically public and private keys are the two different keys used for encryption and decryption process. Public key is known to everyone but private key is kept secret. Only the user knows the private key. Basic example is email id and its password. Email id is public key and password is private key. Sender encrypts the message using algorithm and private key. It sends the encrypted message and its public key to recipient. Recipient then decrypts the message using public key of sender in the decryption algorithm. Asymmetric cryptography is very efficient technique. It requires less number of lock and key pairs. For example if n user communication combinations are there, then only 'n' lock and key pairs would be required. Hence it decreases the complexity. But it is a slow process if cipher text size is large. Whereas in symmetric cryptography, same key is used for encryption and decryption. Only one is required for encryption and same key is required for decryption. Sender encrypts the message using a key and sends the encrypted message along with algorithm used and same key that was used for encryption. If 'n' users want to communicate with each other, then a new key has to be generated for every new combination. For n combinations lock and key pairs are required. Hence complexity increases with increase in lock and key pairs.

Steganography is an art of hiding data into another data [1-2] [5-6]e.g image, audio etc. Secret data is inserted into the image or audio. It is very efficient method of hiding the data. Media files are used for steganography because they are large in size. For example, sender can insert its secret message into least significant bits of the image file. Steganography is one step ahead from cryptography because it encrypts the message and hide it. No one can suspect that the message exists. Anyone scanning user's data will fail to know it contains secret message. Hiding of data into the image or audio does not change the image or audio. No change in terms of pixels or contrast is observed in image containing hidden data. In case of hiding data in audio, audio samples are converted into decimals and then binary .The binary bits of audio message are then modified to embed the hidden message into it. The stego message is then converted into analog form again.

III.MECHANISM DESIGNED

The encryption has the following steps

Step1: Data is entered by the user
Step2: It is then encrypted to cipher text by RSA algorithm
Step 3: Then the cipher text obtained above is hidden in the cover image

RSA algorithm steps

Step1: Generate two large prime numbers A and B.
Step2: Calculate N = A*B
Step3: Choose the public key (encryption key) E such that it is not a factor of (A-1) and (B-1).
Step4: Choose the private key (decryption key) D such that (D*E) mod(A-1)*(B-1)=1
Step5: For carrying out , calculate the cipher text as CT from the plain text PT as CT=PT^E mod N
Step6: Send CT as the cipher text to the receiver.

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 6, June 2015

Step7: For decryption, calculate the PT from CT as PT=CT^D mod N

The steganography part has the following steps

Step1: Take a cover image
Step 2: Extract RGB components from that image
Step 3: Take transpose of the extracted RGB component
Step 4: Then compute YCbCr of the image formed in step 3

```
y(i,j)=0.299*a(i,j,1)+0.597*a(i,j,2)+0.114*a(i,j,3);
Cb(i,j)=128-0.16873*a(i,j,1)-0.331264*a(i,j,2)+0.5*a(i,j,3);
Cr(i,j)=128+0.5*a(i,j,1)-0.418688*a(i,j,2)-0.081312*a(i,j,3);
```

Step 5: Hide the cipher text obtained through encryption mechanism in Y, Cb or Cr based on the random number generated which will work as a key too.
Step 6: Combine the Y,Cb and Cr components to form an image
Step 7: Store that image as watermarked image
Step 8: Send the watermarked image to desired recipient
Step 9: Share the key through any key sharing algorithm

Decryption has the following steps

Step1: Get the watermarked image
Step 2: Extract Y, Cb and Cr components from the image
Step3: Take transpose of the extracted components
Step 4: Extract the hidden text from the Y, Cb or Cr component of the image depending on the key
Step 5: Decode the extracted text using RSA algorithm

If random number generated is

a) prime data is hidden in Y component
b) Even data is generated in Cb component
c) Odd data is generated in Cr component

IV.RESULTS

We have implemented the designed algorithm on Matlab. The figure 1 below shows the cover image chosen for hiding encrypted data. Figure 2, 3 and 4 show the Y,Cb and Cr components extracted from th RGB components of the image. Figure 5 shows the chrominance image formed by combining Y,Cb and Cr components[7] . The figure 6 is the final watermarked image which will be sent to the receiver.

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 6, June 2015

Figure 1: Colored image

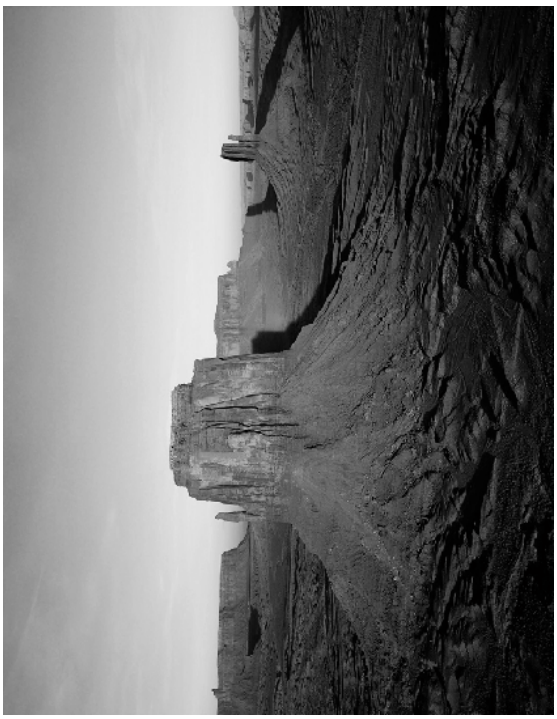

Figure 2 : Y component of original image

Figure 3:Cb component of original 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 6, June 2015

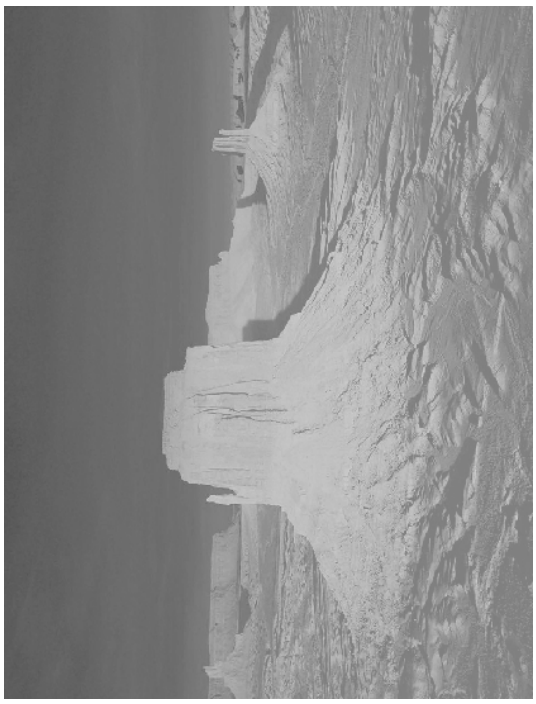

Figure 4: Cr component of original image

Figure 5: Chrominance 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 6, June 2015

```
enter plaintext to be encoded'prince'

me =

     6


ne =

     7

     random number generated is

     randnum =

           606843

The value of (N) is: 143
The public key (e) is: 7
The value of (Phi) is: 120
The private key (d)is: 103

ASCII Code of the entered Message:
    39   112   114   105   110    99   101    39

Cipher Text of the entered Message:
    52    18    49   118    33    44    62    52
```

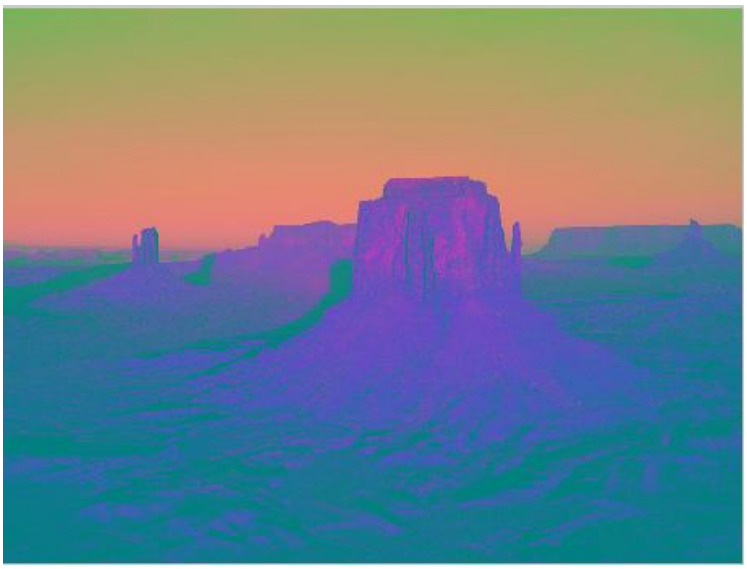

Figure 6: Watermarked image

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 6, June 2015

```
extracted text from the image
     52     18     49    118     33     44     62     52


plain =

   112
   114
   105
   110
    99
   101

plaintext recovered

ans =

prince
```

V. CONCLUSION

We have encrypted the message and hidden it in the chrominance image. The data is encrypted using RSA algorithm. The message is hidden into Y, Cb and Cr components of the image. A random number is generated and by using that random number data is hidden in Y,Cb and Cr components. This adds randomness in the mechanism which makes it more effective. So we have combined symmetric, asymmetric cryptography and steganography in one cipher which combines positive aspects of all. We have implemented the cipher on Matlab successfully.

REFERENCES

[1] Mohammad Tanvir Parvez and Adnan Abdul-Aziz Gutub ,“ RGB Intensity Based Variable-Bits Image Steganography” Asia-Pacific Services Computing Conference 2008 IEEE

[2] 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

[3] “Cryptography and network security”, Atul Kahate, second edition, Mc Graw hill companies.

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

[5] Ching-Sheng Hsu and Shu-Fen Tu,” Digital Watermarking Scheme with Visual Cryptography” Proceedings of the International MultiConference of Engineers and Computer Scientists 2008 Vol I IMECS 2008, 19-21 March, 2008, Hong Kong

[6] Gokul.M, Umeshbabu R, Umeshbabu R, Deepak Karthik, “ Hybrid Steganography using Visual Cryptography and LSB Encryption Method” International Journal of Computer Applications (0975 – 8887) Volume 59– No.14, December 2012

[7] Adel Almohammad ,Gheorghita Ghinea, “Image Steganography and Chrominance Components” 10th IEEE International Conference on Computer and Information Technology, CIT 2010, Bradford, West Yorkshire, UK, June 29-July 1, 2010

[8] 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.

[9] 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