An Enhanced Text to Image Encryption Technique using RGB Substitution and AES

Sourabh Singh[1], Anurag Jain[2]

[1]*Research Scholar Department of Computer Science and Engineering*
Radharaman Institute of Technology and Science Bhopal (M.P) India
[2]*Head , Department of Computer Science and Engineering*
Radharaman Institute of Technology and Science Bhopal (M.P) India

***Abstract* - In network security applications, before transmitting data to a remote machine it is encrypted at the sender side using any standard encryption algorithm. Most of the encryption algorithms make use of secret key without which it becomes very difficult to retrieve the actual data In this paper we propose a method which at first transforms the text into an image using an RGB substitution, and then encrypts the resulting image using AES Algorithm, under this approach, the secret key is smartly sent along with the cipher text in a single transmission, thus it also solves the key exchange problem that generally arises in most of the encryption models. The encryption and decryption process make the use of a combination database for text to image transformation. This paper is divided into following four sections; in section- I, we presented basic introduction of Network Security, in section-II, a survey on related algorithms has been presented, section-III discusses the proposed model and section IV concludes the paper.**

***Key Words* - Symmetric key, Asymmetric key, Encryption, Decryption, AES.**

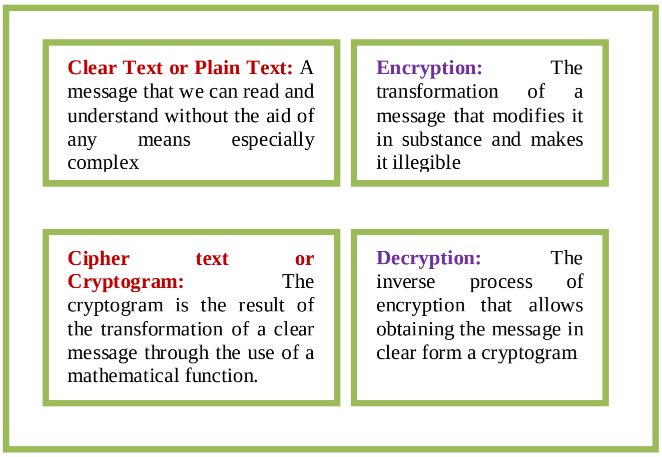
I. INTRODUCTION

With the increasing growth of network applications, security has become an important factor in communication and transferring data on a public network. To make the network secure there are different methodologies used from the ancient time which are still very effective in present scenario. Some of the network security techniques are as under:

Substitution: In cryptography the substitution techniques is an older but yet powerful method to hide the original text, this method deals with the replacement of alphabets with some other alphabets or set of alphabets as well as numbers. One method was developed by Julius Caeser[12] here the characters of plain text message are replaced by other characters, numbers or symbols. Caesar Cipher is a special case of substitution techniques where in each alphabet in a message is replaced by an alphabet three places down the line. Another technique mono-alphabetic Cipher here rather using a uniform scheme for all the alphabets in a given plain text message, we decided to use the random substitution. One more technique Homophonic Substitution Cipher is also used as a substitution method which involves substitution of one plain text character with a cipher text character at a time; however the cipher text character can be any one of the chosen set. In Polygram substitution cipher technique replaces one block of plain text with a block of cipher text i.e. it does not work on a character by character basis. Poly-alphabetic Substitution Cipher is another technique which uses a set of related mono alphabetic substitution rules & also uses a key that determines which rule is used for which substitutions.

Transposition: Transposition techniques differ from the substitution techniques in the way that they do not simply replace one alphabet with another[12]; they also perform some permutation over the plain text alphabets. The most popular technique used over here is rail fence technique which involves writing the plain text as sequence of diagonals and then reading it row by row to produce cipher text. Another technique is Simpler Columnar Transposition Technique which simply arranges the plain text as a sequence of rows & columns randomly. A widely used technique Vernam cipher method which uses a one-time pad, which is discarded after a single use and therefore, is suitable only for short messages.

Encryption: In cryptography [10], encryption is the process of converting readable information into unreadable information. From past many decades companies and individual users with an extraordinary need for protection are using encryption as a secure technique for protecting their data. During 1970s, encryption technique included as strong security of secretive government organization into the public domain, and is now employed in protecting widely-used systems, like Internet, mobile telephone networks and bank automatic teller machines. Encryption is very useful in protecting information, but some other techniques are still needed to make security, particularly to verify the message authenticity and integrity; for example, a Message Authentication Code (MAC) or digital signatures. Message Authentication Code is helpful in providing message integrity on the other hand digital signatures provides message authentication, the MAC and digital signatures promises that the message has been originated from the genuine sender itself while the MAC promises that the message has not been altered in between the transmitting network. Figure 1 is showing a simple cryptography process.



Clear Text or Plain Text: A message that we can read and understand without the aid of any means especially complex

Encryption: The transformation of a message that modifies it in substance and makes it illegible

Cipher text or Cryptogram: The cryptogram is the result of the transformation of a clear message through the use of a mathematical function.

Decryption: The inverse process of encryption that allows obtaining the message in clear form a cryptogram

Fig-1: Cryptography Process

Key: In cryptography, to encrypt or decrypt data from one format to another a key value is required. In modern encryption techniques, file information is needed to encrypt or decrypt the information to be sent or being received and this can be done by two popular techniques public key encryption which uses a public key, and it is available to anyone, another is private key, which is used by the owner of the key pair only. If we want to send a message to the receiver side, we must encrypt it using the public key. At the time of receiving message owner must decrypt it using his private key. On the other hand symmetric encryption uses only a single key which should be kept secret, but this can be shared with other clients those will be exchanging messages with the key owner [10].

Private Key Encryption: In symmetric encryption or private Key encryption only one single key is used for encryption and decryption of the message which is to be transferred. The advantage of this technique is fast execution speed because a single key is used on both the ends of the public network. Systematic key security management is the primary concern at the time using private key encryption [11].

Public Key Encryption: In Asymmetric encryption or public key encryption pair of keys is used as a public and as a private key. To privately communicate with the other user the public key is distributed to everyone. Hence this approach solves most perceived problem of the private key encryption which is key exchanging between users. In this technique each user has the private key, which is paired to the public key. In this technique private key is never shared between the users while public key is widely available. Asymmetric key encryption is slower as compared to private key encryption because of multiple key distribution management between users [11].

AES Algorithm: Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen[13]. The algorithm is very flexible as it supports any combination of data and key size of 128, 192, and 256 bits. However, AES mandates that the plain text must be 128 bit long which can be divided into four basic operation blocks. These blocks operate on array made up of bytes organized in a 4×4 matrix which is called the state. For total encryption, the data is passed through Nr number of rounds (Nr = 10, 12, 14) .These rounds performs the following transformations:

Subbyte Transformation: This includes a non linear byte Substitution which uses a substitution table (s-box), this substitution table is constructed with the help of Affine Transformation and multiplicative inverse

Shift rows transformation: It is a simple byte transposition method where the bytes in the last three rows of the state are cyclically shifted; on the other hand offset of the left shift varies from one to three bytes.

Mix columns transformation: It is similar to the multiplication of columns of the matrix; here each column vector is multiplied by a fixed matrix. One thing should be kept in mind that the bytes are treated as polynomials rather than numbers.

Add round key transformation: It is a simple XOR operation between the working state and the round key. This transformation is its own inverse.

Inverse Substitute Bytes: It is the reverse procedure of the Substitute Bytes transformation; here the inverse S-box is applied on each byte of the State. This is obtained by taking the inverse of the affine transformation followed by taking the multiplicative inverse

Inverse Shift rows: Ii is the inverse of the shift rows in which the first row of the state array remains unaffected. The bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the right respectively.

Inverse Mix columns: In the Inverse Mix Columns transformation, every column of the state array is considered a polynomial. After multiplying modulo x4+1 with a fixed polynomial the result is the corresponding column of the output state.

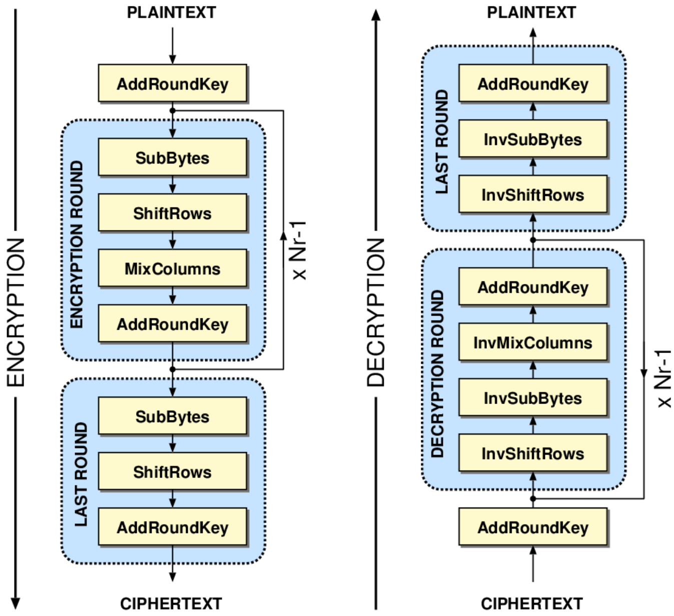


Fig-2: Diagram of AES Encryption Algorithm

As AES is a symmetric key encryption technique the secret key is known to both the sender and the receiver. The key cannot be determined by any known means, even if an eavesdropper knows the plaintext and the cipher text AES algorithm remains secure. The design of AES algorithm supports the use one of any three key sizes (Nr). AES-128, AES-196 and AES-256 use 128 bit (16 bytes, 4 words), 196 bit (24 bytes, 6 words) and 256 bit (32 bytes, 8 words) key sizes respectively. AES when compared to DES, have no known weaknesses. All key values are equally secured thus no value will render one encryption more vulnerable than another. The keys are expanded via a key expansion routine which is used in the AES cipher algorithm. This key expansion routine is quite flexible & can be performed all at once or on the fly calculating words as per the need of the user.

AES is extremely fast as compared to other block ciphers. (Though there are mismatch between size and speed), in dedicated hardware AES allows even faster execution as the round transformation is parallel by design. AES was designed to be amenable to pipelining. The cipher has no bias towards big or little endian architectures as it do not use arithmetic operations. AES Does not use SBoxes of other ciphers, bits from Rand tables, or any other such problem hence it is fully self-supporting.

II. Literature Survey

This paper is based on the work done by Ahmad Abusukhon and Mohammad Talib [1]. In their Algorithm, there are mainly two levels of data encryption. The first level contains Text-To-Image Encryption which is designed by the authors of the paper while the second level contains Image-Shuffle Encryption which is based on Efficient digital encryption algorithm based on matrix scrambling technique [2]. These two levels of encryption are performed on the receiver side and decryption is performed on the client side. In the first level i.e. Text-To-Image Encryption each letter in the text file is transformed into three random integers say R for Red, G for Green and B for Blue where each random number ranging from 0 to 255. The three random numbers represent one pixel in the image file. In their algorithm, they generated a random pixel (R, G, and B values calling them RGB value) for each letter. During this process the random numbers RGB for all letters are combined and stored in one string (key 1) then they have used key1 to transform the plaintext into cipher text. The result of this process is a two dimensional array or Matrix of Pixels MP in which each 3 contiguous columns in a given row represent one letter. In order to make it difficult to attack the data they execute the second level of encryption, here they determine the number of times the matrix is shuffled[2]; say N. where N is equal to the number of column of MP. Each time the matrix MP is shuffled two random numbers are generated say R1, and R2, where R1 represents row/column number and R2 represents another row/column number. R1 is replaced by R2 and *vice-versa*. The Shuffled matrix, say SP, is finally sent to the client. On receiving SP, client uses key 2 to retrieve the original matrix MP and then each pixel in MP is decomposed into R, G, and B values. Then using key 1 each 3 contiguous values (R, G, and B) are transformed to a specific letter.

In the proposed algorithm there is an AES encryption stage in which the image is encrypted using a key following AES algorithm, the AES has been widely adapted to encrypt data but now a days frequently used for encrypting images as well.

Praveen.H.L , H.S. Jayaramu, M.Z.Kurian [9] Has developed a model which can easily encrypt the images obtained from satellites. Even If faulty data occurs then satellite needs not to wait for long time to receive next data. To prevent this error free encryption scheme is proposed in On-Board. They also states that AES provides an error-free encryption system and error is much more reduced even in radiation in satellites.

Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush[8] has also used AES algorithm to encrypt image, they have first rotated the plain image to generate another image with the help of magic cube. The original image is divided into six sub-images and these sub-images are divided amongst a number of blocks and attached to the faces of a Magic Cube and to confuse the relationship between the plain image and the encrypted image, the rotated image is fed into an AES algorithm which is applied to each pixel of the image to encrypt the image even further.

Jawad Ahmad and Fawad Ahmed [6] have compared two encryption algorithms namely Advanced Encryption Standard (AES) and Compression Friendly Encryption Scheme (CFES). They have explored the security estimations of AES and CFES for digital images against brute-force, statistical, and differential attacks, the results they have calculated to test the security of these algorithms for digital images shows some weaknesses in CFES. These weaknesses were mainly related to low entropy and horizontal correlation in encrypted images, the authors also states that the image encrypted by CFES has correlation in horizontal direction while AES encrypted image has very less correlation in all directions. The algorithm which has less correlation values indicates that it has higher security.

Manoj. B, Manjula N Harihar[5] also states that Image Encryption and Decryption using AES can be designed and implemented to protect the confidential image data from an unauthorized access the authors found that Successful implementation of AES algorithm is one of the best encryption and decryption standard available in market.

P. Radhadevi, P. Kalpana[7] has also presented the encryption & decryption of an image using AES algorithm, they have concluded that the AES can be used very efficiently to secure image transmission.

P.Karthigaikumar ,Soumiya Rasheed[4] has also used AES algorithm for simulation of image encryption they have successfully implemented the AES algorithm in MATLAB on Xilinx platform, Timing simulation is also performed which verifies the functionality of the designed circuit.

III. PROPOSED MODEL

This section, describes the proposed encryption algorithm. This technique is designed to improve the algorithm proposed by the Ahmad Abusukhon and Mohammad Talib [1]. First of all their algorithm does not solve the key exchange process. Another loop hole is that they have to transfer the whole key, this is quite big in size (key1) as every character in plain text has been replaced by three random numbers. Hence it requires to transfer at least three times more data as compared to actual data just for decrypting the packet. Fig.3 shows the block diagram of proposed technique. Since encryption is better option as compared to simple shuffling of bits, Hence proposed technique employs an encryption stage rather than shuffling the bit positions by matrix scrambling technique [2]. The sender & receiver side has a combination database that contains various combinations of text to digit mapping. It has various for transforming characters into equivalent RGB values, where each combination is assigned a unique number ranging from 1 to N where N denotes the total number of combinations. Now starting from the sender side, the sender generates a random number between 1 to N, which represents the combination number to be applied. Using the corresponding combination, transformation proposed in [1] is applied for generating the resultant image. Now this image is encrypted by a key using an AES algorithm [13], which generates an encrypted image. On this encrypted image, one more pixel is added, which stores the value of the combination number that was used to transform text into the image. Now the key which was used in AES algorithm is transformed to its equivalent RGB resultant value. Finally these resultant values and the final image generated are transferred to the destination host. Upon receiving the final image, the first task is to read the last pixel that was added to get the combination number. Once this number is obtained the received key is transformed

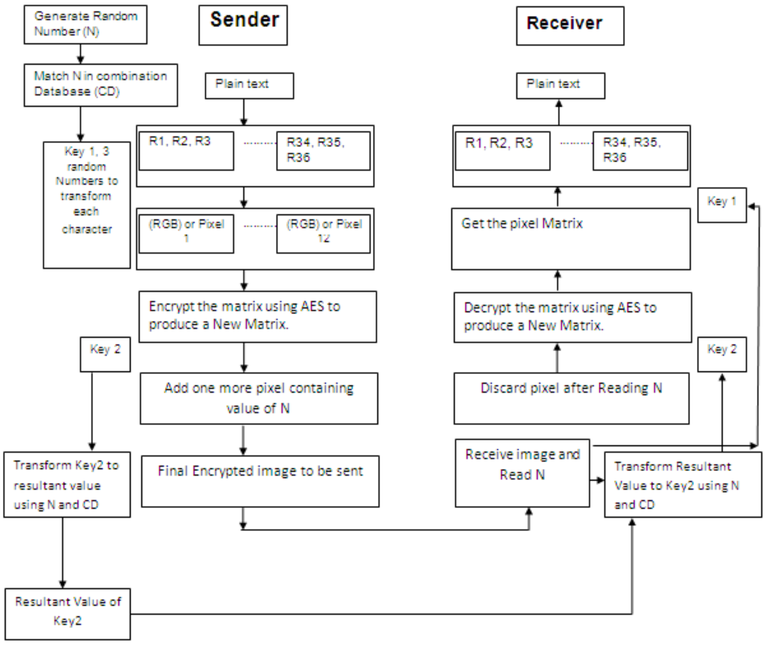

Generate Random Number (N)
Sender
Receiver
Match N in combination Database (CD)
Plain text
Plain text
Key 1, 3 random Numbers to transform each character
R1, R2, R3
R34, R35, R36
R1, R2, R3
R34, R35, R36
Key 1
(RGB) or Pixel 1
(RGB) or Pixel 12
Get the pixel Matrix
Encrypt the matrix using AES to produce a New Matrix.
Decrypt the matrix using AES to produce a New Matrix.
Key 2
Key 2
Add one more pixel containing value of N
Discard pixel after Reading N
Transform Key2 to resultant value using N and CD
Final Encrypted image to be sent
Receive image and Read N
Transform Resultant Value to Key2 using N and CD
Resultant Value of Key2

Fig-3: Proposed Model

to its original value by using the combination number. After this, corresponding transformation is applied with the help of various combination databases. Now receiver discards the last pixel from the image and then applies AES on image (using previously obtained key), which was generated after discarding the last pixel. When receiver obtains the decrypted image it applies the transformation with same combination number that was found in the last pixel of received image and generates the original text.

IV. CONCLUSION

This paper proposes a method which when implemented will lead to a highly secure transmission of text. If a hacker any how decrypts the image then he gets another image, which further confuses him whether the actual information is in text or in image format, the blend of text to image transformation and then AES encryption makes actual information (plain text) highly secure for transmitting it on extremely vulnerable and insecure network environment.

REFERENCES

[1] Ahmad Abusukhon Mohammad Talib "A Novel Network Security Algorithm Based on Private Key Encryption" *IEEE International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012*.

[2] Kiran Kumar, M., Mukthyar Azam, S., and Rasool, S. (2010) "Efficient digital encryption algorithm based on matrix scrambling technique". *International Journal of Network Security and its Applications (IJNSA), 2(4).*

[3] Komal D Patel, Sonal Belani "Image Encryption using different Techniques" *International Journal of Emerging Technology and Advanced Engineering Volume 1, Issue 1, November 2011.*

[4] P.Karthigaikumar Soumiya Rasheed "Simulation of Image Encryption using AES Algorithm" *IJCA Special Issue on Computational Science - New Dimensions & Perspectives" NCCSE, 2011.*

[5] Manoj.B, Manula N Harihar "Image Encryption and Decryption using AES" *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-1, Issue-5, June 2012.*

[6] Jawad Ahmad and Fawad Ahmed "Efficiency Analysis and Security Evaluation of Image Encryption Schemes" *International Journal of Video & Image Processing and Network Security IJVIPNS-IJENS Vol:12 No:04.*

[7] P. Radhadevi, P. Kalpana "Secure Image Encryption Using AES" *International Journal of Research in Engineering and Technology Volume: 1 Issue: 2.*

[8] Ahmed Bashir Abugharsa, Abd Samad Bin Hasan Basari and Hamida Almangush "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm" *International Journal of Computer Science Issues (IJCSI); Vol. 9 Issue 4, p41 Jul2012.*

[9] Praveen.H.L , H.S Jayaramu, M.Z.Kurian "Satellite Image Encryption Using AES" *International Journal of Computer Science and Electrical Engineering (IJCSEE), Vol-1, Iss-2, 2012.*

[10] Stalling, W. (2005) "Cryptography and network security principles and practices, 4th edition Prentice Hall". Available at: http://www.filecrop.com/cryptography-andnetwork- security-4th-edition.html.

[11] Dr. Mahesh Motwani "Cryptography & Network Security" Balaji Learning Book.

[12]Atul Kahate, Cryptography and Network Security, Second Edition, Tata McGraw-Hill Edition 2008.

[13] AES.pdf http://www.facweb.iitkgp.ernet.in/~sourav/AES.pdf.