# Secure Data Transmission Using Image Encryption

PawanManwatkar, Abhijeet Fate, SushantSakhare, AbhijitWagh, Asst.Prof. PurvaGogte
*Department of Information Technology, Dr. BabasahebAmbedkar College of Engineering& Research, Nagpur*
*Rashtrasanth Tukdoji Maharaj Nagpur University, Nagpur*

***Abstract- With the spread of digital data around the world through the internet, the security of the personal data has also need to increase. In today's world, every person is using the internet for sending the digital data like personal information, bank account information etc. But this information is sending in unsecure environment that's why the data is not secured. For this, many methods are coming up to protect the data from going into hands of attacker. Cryptography is encryption and decryption technique for keep data secure. The main purpose in cryptography is to make message concept unintelligible, while steganography aims to hide personal secret message. For security purpose, digital images are best excellent carriers of hidden information. In this paper, we propose a high-performance text & image Cryptography along with a substitution encryption methodology. The new invented algorithm is use for acquiring the (R, G, B, A, X, Y) value of every pixel of image and the threshold value is added in it for security purpose. Experimental results show that the visual and the statistical values of the image with encrypted data before sending are similar to the values after receiving thus reduces the chance of the confidential message being detected and enables secret communication.***

***Keywords- Cryptography, plaintext, encryption, decryption, ciphertext, substitution cipher, Optical character recognition, AES algorithm, Image encryption algorithm.***

## I. INTRODUCTION

The security of data transmission is a vital problem in communication networks. A communication system is reliable as long as it provides high level of security. Usually, users exchange personal sensitive information or important documents. The security and confidentiality of data provide over the transmission medium. Nowadays, internet multimedia is very popular ; an amount of data has exchanged every second over a non- secured channel, which may not be safe. Therefore, it is essential to protect the data from attackers. To protect the data; cryptography and steganography techniques can be used.

The networks are of two types: wired network and wireless networks. In wired network, the systems/devices are connected with wire i.e. cat6 cable, optic fiber cable. The data is transmitted through a transmission medium. The transmission of the data in wired network is more secure than the data transmission in wireless network. There is no need to encrypt the data.

In wireless network, the data is transmitting over an air. So, this is unsecure way of sending data. The data can easily access by unauthorized person. For this we require to encrypt the data before sending and main of this project is to keep the personal message from unauthorized person using text and image encryption method.

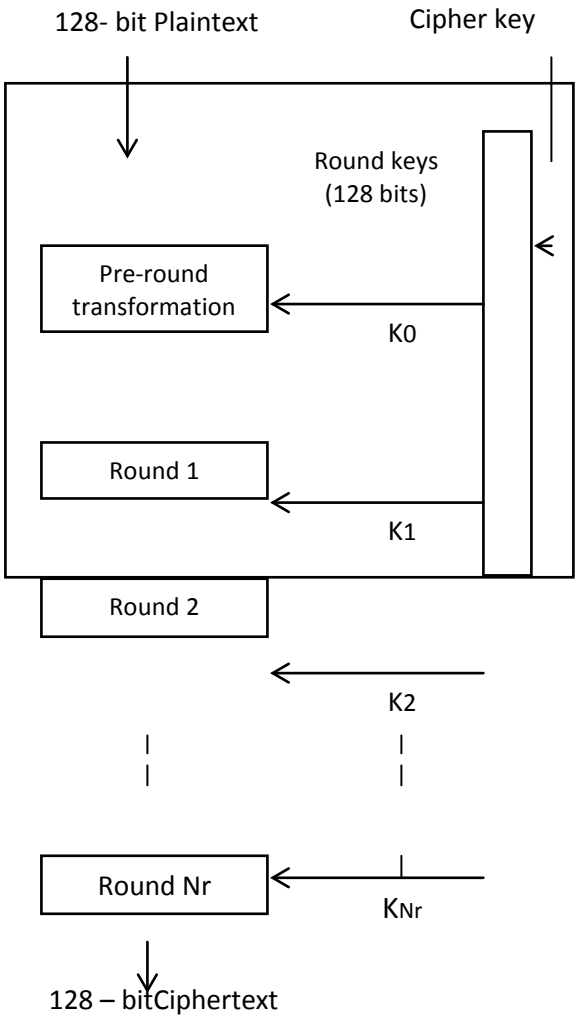
Cryptography is the science of keeping the transmitted data secure. It provides encryption for secure communication. The encryption process is applied before transmission, and the decryption process is applied after receiving the encrypted data. In this project, the AES algorithm is used to encrypt and decrypt the secret text. Steganography is the science of writing secret message inside a different digital content; it conveys the data by concealing it in other medium such as image or audio which is called the cover abject. The information hiding process is applied before transmission and the extraction process is applied after receiving.

We have used image encryption algorithm for image encryption method. In this new algorithm, the threshold value is added to each pixel value of image i.e. (R,G,B) value of an image and alpha value and also added with (X,Y) position of each pixel. But this threshold value should know to only sender and receiver. The receiver will not get original text until he don't get know perfect threshold value set by the sender at the time of image encryption. The threshold value is a numeric value and the sender can take any numeric value as threshold value. As large a threshold value, the complexity to decrypt the image or carrying the perfect pixel value and plot it to get original image for attacker is greater.

Cryptography algorithm has classified as symmetric key algorithm and public key algorithm. Symmetric algorithm uses the same key for encryption and also for decryption, while public Key algorithm uses different keys for encryption and decryption.

*AES Encryption:*

Advance Encryption Standard (AES) is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST) in December 2001. In 1997, NIST standards looking for a replacement for DES, which would be called the Advance Encryption Standard or AES. The AES algorithm required a block size of 128 bits and three different key sizes of 128, 192 and 256 bits.

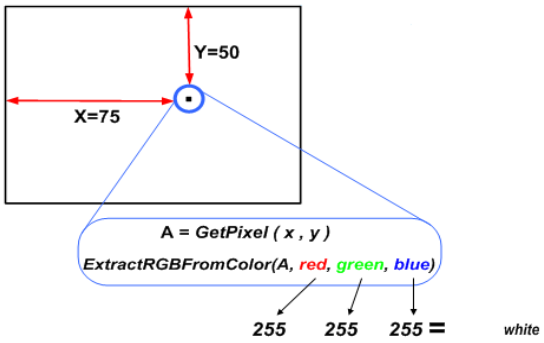



AES is a non Feistel cipher that encrypts and decrypts a data block of 128 bits. AES algorithm uses 10, 12, or 14 rounds for encryption and also decryption. The key size which is 128, 192, or 256 bits, depends on the number of rounds. A below figure shows the general design for the encryption algorithm (called cipher); the decryption algorithm (called inverse cipher) is similar, but the round keys are applied in the reverse order in decryption process.

The number of round keys generated by the plaintext expansion algorithm is always one more than the number of the rounds.

*Image Encryption:*

There are many image encryption algorithm are available. In this, our own image encryption algorithm has used. An image is consisting of number of pixel and it is depend upon the size of an image. Each pixel has RGBA value stands for Red Green Blue Alpha and X, Y position.




While RGBA is sometimes described as a color space, it is actually simply a use of the RGB color model, with extra information. The color is RGB, and may belong to any RGB color space, but an integral alpha value as invented by Catmull and Smith. The alpha channel is normally used as an opacity channel. If pixel has a value of 0% in its alpha channel, it is fully transparent, whereas a value of 100% in the alpha channel gives a fully opaque pixel.

In this image encryption we are acquiring the R, G, B value, alpha value and X, Y position of each pixel of an image. Am image has created from encrypted secret text or message. We will add a threshold value in R, G, B, A, X, Y value in sequence. This will help to increases a complexity against an attacker.

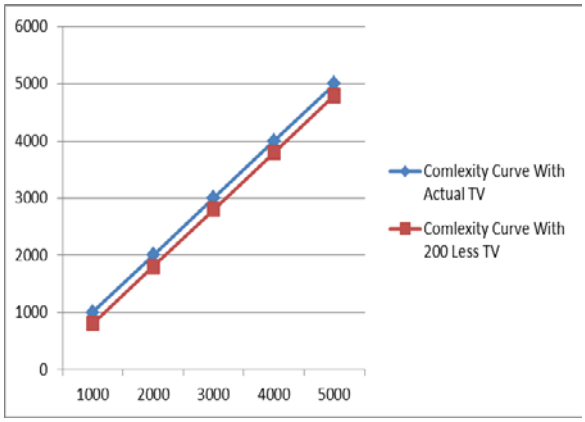
RT= R+TV, G+TV, B+TV, A+TV X+TV, Y+TV

Where, TV is abbreviation for Threshold Value

TV= Numeric Value (Ex. 100 or 1000)

A= Alpha value of an image

RT= Result




In the above graph, it shows a complexity curve between threshold value and time. The attacker can attack on sending data but he need to know the threshold value. Whatever threshold value has entered by sender, up to that value an attacker will try to get perfect value of each pixel of image. The red curve describe that if the sender has set the threshold value 1000, then attacker can get the image on value 800 but this image will be blur image not a perfect image. On the actual value of threshold the receiver/attacker will get the perfect value which has shown in blue curve. But in both cases, the attacker cannot get secret text because the secret text also encrypted with AES algorithm.

## II. LITERATURE SURVEY

*1. Lossless Image Compression and Encryption Using SCAN.*

S.S. Maniccam and N.G. Bourbakis [4] have presented a new algorithm which does two works: lossless compression and encryption of binary pictures. The compression and encryption schemes are based on SCAN patterns generated by the SCAN methodology. The SCAN is formal language-based 2D spatial-accessing methodologies generate a wide range of scanning paths or space filling curves.

*2. New Encryption Algorithm for Image Cryptosystems.*

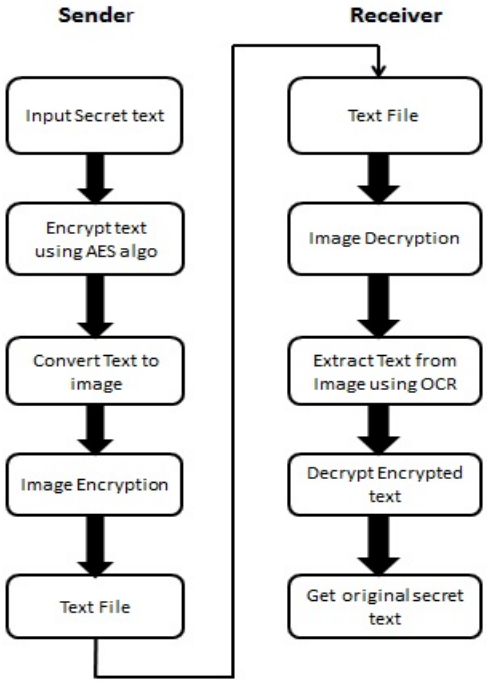
Chin-Chen Chang, Min-Shian Hwang, and Tung-Shou Chen [6] used vector quantization for designing better cryptosystem for images. The scheme was based on vector quantization (VQ), cryptography, and various others number theorem. In vector quantization (VQ) firstly the images are decomposed into vectors and then sequentially encoded vector by vector. . Then traditional cryptosystems from commercial applications can be used.

*3. Technique for Image Encryption using Digital Signatures.*

AlokaSinha and Kehar Singh [4] have proposed a new technique in which the digital signature of the original image is added to the encoded version of the original image. A best suitable error code is followed to do encoding of the image, ex: Bose-ChaudhuriHochquenghem (BCH) code. At the receiver end, after decryption of that image, the digital signature verifies the authenticity of the image.

## III. IMPLEMETATION

The main objective of this paper is to introduce a secure communication system that employs cryptography to encrypt and embed the secret message to be transmitted over a non-secure channel




In this system, the encryption process is achieved using the AES and Image encryption algorithm, which presents a high speed and level of security. The proposed system consists fromfour stages as shown in Figure Note that the main stages are encryption, embedding, extractionand decryption. The following algorithm describes these stages.

*Algorithm:*

Sender Module

Input: Embed the message.

Output: Message is embedded safely in an image and sending properly.

*Begin*

*1. Input Message.*

*2. Encrypt message using AES.*

*3. Set threshold value*

*3. Create image from encrypted message using steganography.*

*4. Encrypt (R,G, B) value of each pixel, alpha value and its (X,Y) position of an image using threshold value.*

*5. Sending data*

*End*

Receiver Module

Input: Receive data.

Output: Get original message.

*Begin*

*1. Receive pixel value of image.*

*2. Set same threshold value.*

*3. Construct image.*

*4. Extract message from image using OCR.*

*5. Decrypt message using AES.*

*6. Get original message.*

*End*

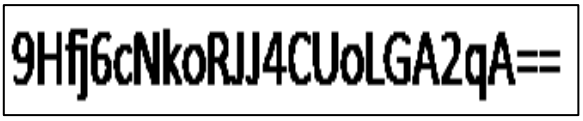
As shown in the above block diagram, there is sender and receiver. From this it can specify that it is server-client concept. The server is acts as a sender and client is acts as a receiver. In server, the sender will first type a secret message, then encrypt this secret message using AES algorithm.

*Example :*

Plain Text = “pawan”

CipherText=“9Hfj6cNkoRJJ4CUoLGA2qA=”

Convert this encrypted message into image. Then set the threshold value. Acquire the R, G, B, A, X, Y value adding with threshold value using customized algorithm. Setup the sever-client module, connect them and send data from server to client.




Example.

Left side shows (R, G, B, A, X, Y) values without adding threshold value and also adding and subtracting some numeric value.

Right side shows (R, G, B, A, X, Y) values with adding threshold value 100 and also adding and subtracting numeric value.

| R,G,B,A,X,Y | R , G , B , A, X , Y |
|---|---|
| 0,0,0,0,0,0 | 111,88,113,86,115,84 |
| 0,0,0,0,0,1 | 111,88,113,86,115,85 |
| 0,0,0,0,0,2 | 111,88,113,86,115,86 |
| 0,0,0,0,0,3 | 111,88,113,86,115,87 |
| 0,0,0,0,0,4 | 111,88,113,86,115,88 |
| 0,0,0,0,0,5 | 111,88,113,86,115,89 |
| 0,0,0,0,0,6 | 111,88,113,86,115,90 |
| 0,0,0,0,0,7……. | 111,88,113,86,115,91.. |

In client side, the receiver has connected to server. He will be receiving the data form the server. Then set the threshold value and construct an image. This may be possible when the receiver get know actual threshold value which was set by the sender. After constructing an image the OCR method has used to extract the encrypted message from an image. Then Decrypt an encrypted message using AES symmetric key algorithm. AES algorithm used for both encryption and decryption at sender and receiver side must be same.

## IV. CONCLUSION & SCOPE

In this project a high security model uses cryptography for both text and image has been developed. The image encryption algorithm is used for acquiring the (R, G, B) value of each pixel with its (X,Y) position and alpha value of image in text file and add threshold value and some numeric value with both (R,G,B) and (X,Y) and alpha values (A) of each pixel of an image before sending it. This algorithm increases the security level of data transmission with cryptography. Here we embed the confidential message into an image file in such a manner that the degradation in quality of the carrier image is not noticeable.

- It is expected that this text &image encryption technique will be deployed in military sector and banking sector for sending secret message from one place to another place securely.
- This techniques can be also use in other fields where the rendering of the original message is required or desired.

## REFERENCES

[1] Obaida Mohammad Awad Al-Hazaimeh, (2013) "A New Approach for Complex Encrypting andDecrypting Data" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.2.

[2] Katzenbeisser, S. and Petitcolas, F.A.P. 2000, Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Inc., Boston, London.

[3] Xinpeng Zhang and Shuozhong Wang, (2005), "Steganography Using MultipleBase Notational System and Human Vision Sensitivity", IEEE signal processing letters, Vol. 12, No. 1.

[4] PiyushMarwaha, PareshMarwaha, (2010), "Visual Cryptographic Steganography in images", IEEE, 2nd International conference on Computing, Communication and Networking Technologies.

[5] Hemalatha S, U Dinesh Acharya, Renuka A and Priya R. Kamath, (2012), " A Secure and High Capacity Image Steganography Technique", Signal & Image Processing : An International Journal (SIPIJ) Vol.4, No.1.

[6] Mandal J.K. and Sengupta M., (2010), “Authentication/Secret Message Transformation Through Wavelet Transform based Subband Image Coding (WTSIC).”, Proceedings of International Symposium on Electronic System Design, IEEE Conference Publications, pp 225 – 229.

[7] Septimiu F. M., MirceaVladutiu and Lucian P., (2011),"Secret data communication system using Steganography, AES and RSA", IEEE 17th International Symposium for Design and Technology in Electronic Packaging.

[8] Y. Huang, B. Xiao, H. Xiao, (2008), "Implementation of Covert Communication Based on Steganography", IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing, pp. 1512-1515.

[9] Cheddad, A, Condell, Joan, Curran, K and McKevitt, Paul,(2008), "Securing Information Content using New Encryption Method and Steganography", IEEE Third International Conference on Digital Information Management.

[10] Saraireh S. and Benaissa M., (2009), “A Scalable Block Cipher Design using Filter Banks and Lifting over Finite Fields” In IEEE International Conference on Communications (ICC), Dresden, Germany.