RESEARCH ARTICLE OPEN ACCESS

Hybrid model for Image Encryption and Decryption using RSA, AES, and Affine with XOR Operation

Avinash Ray*, Anjali Potnis**, Sanjeet Kumar***, Prashant Dwivedy****, Shahbaz Soofi*****
*(Department of Digital Communication Engineering, NITTTR, Bhopal - 462002
Email: atulasn03@outlook.com)
** (Department of Digital Communication Engineering, NITTTR, Bhopal - 462002
Email: apotnis@nitttrbpl.ac.in)
*** (Department of Digital Communication Engineering, NITTTR, Bhopal - 462002
Email: tnk@live.in)
**** (Department of Digital Communication Engineering, NITTTR, Bhopal - 462002
Email: dwivedyfamily@gmail.com)
***** (Department of Digital Communication Engineering, NITTTR, Bhopal - 462002
Email: shahbaz_261@yahoo.com)

ABSTRACT
In present scenario, whole world is moving towards digital communication for fast and better communication. But in this a problem arises with security i.e. when we have to transmit information (either data or image) over internet or to store information at any random location then its security is very important. To protect our information from hackers we use a technique i.e. Encryption. In this paper, we use image as information and use different types of encryption techniques to encrypt it and protect it from hackers. Here we use different types of encryption tecghniques (i.e. RSA, AES, and Affine with XOR Operation) in cascade form to make image highly secure, and it will be difficult as well as time taking for hackers or intruders to decrypt the image without using the approprite key.

Keywords – AES, Affine Transform with XOR encryption algorithm, Image decryption, Image encryption, Open Medium, RSA Algorithm, PSNR, MSE.

Date of Submission: 26 -07-2017 Date of acceptance: 05-08-2017

I. INTRODUCTION

In recent scenario information transmission is being done through electronic means such as internet. Internet is an open medium, so there is chance of data hacking while it is being transmitted. Another problem arises with data storage. That is sometimes some crucial information is stored in devices which are of public use. So, at that time there is chance of piracy of data. To protect the data from attack a technique called encryption is used.

Encryption is a process which uses finite set of instructions called an algorithm [1] to convert original message known as plain text, into encrypted form (or coded form) known as cipher text.

Cryptographic algorithms require a set of character called as 'key' to encrypt or decrypt data. With the help of key and algorithm we can encrypt or decrypt plain text into cipher text and then cipher text to plain text.

Encryption is of two types. One is Symmetric Algorithm which is also called as shared secret encryption. This form of encryption uses a secret key, called the shared secret, to convert data into cipher text. The person on the other end needs the shared secret (key) to unlock the data. It is called symmetric cryptography because the same key is used on both ends for both encryption and decryption e.g.: - Genetic algorithm. The other is Asymmetric Algorithm which is also called Asymmetric cryptography. It is usually implemented by the use of one-way functions that are easy to compute in one direction but very difficult to compute in reverse. This is what allows you to publish your public key, which is derived from your private key e.g.: - RSA algorithm.

In this paper, we take an image as our information and try to encrypt it with different image encryption technique. After encryption, we use some parameters such as PSNR, MSE, Normalized

Absolute Error, Average Difference, Structural content, Maximum Difference to check which one technique is most suitable for image encryption encryption.

II. THE PROPOSED IMAGE ENCRYPTION TECHNIQUES

The result of error in image acquisition process [2] that results in pixel values that do not reflect true intensities of the real picture is called noise. Using probability density functions, we can define a set of noise models. The most occurring noises in digital images are Poisson noise, Exponential noise, Multiplicative noise, and Erlang noise or Gamma noise. Following, these noises are discussed at stretch.

2.1 RSA Algorithm

RSA is an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman[2]. In such a cryptosystem, the encryption key is a public one and the decryption key which is different from the encryption key is kept private. As two different keys are being used in encryption and decryption the RSA algorithm is also called as an asymmetric cryptographic algorithm. The RSA algorithm consists of three major steps in encryption and decryption. The steps are as Following

Key Generation:

The RSA contains a public key and a private key. Of these two keys, the public key is used for encrypting messages and can be known to everybody. The messages encrypted with the public key are decrypted using the private key. The method for key generation is as follows. First choose two distinct prime numbers p and q and then compute n=pxq where n is the modulus for the public key and the private keys. Next compute $\phi(n) = (p-1)(q-1)$. Choose an integer 'e' such that $1 < e < \phi(n)$ and GCD $(e, \phi(n)) = 1$. The pair (n, e) is the public key. The private key is a unique integer d obtained by solving the equation $d\,e \equiv 1 \pmod{\phi(n)}$.

Encryption:

The RSA algorithm is used here for encrypting an image. So, the message text (m) is in the form of pixels lying in the range 0 to 255. The pixels are stored and operated upon in an array format. The text is encrypted using the public key (n, e) from the equation

$$c = m^e \bmod (n) \quad (1)$$

Decryption:

The text is decrypted using the private key (n, d) from the equation

$$m = C^d \bmod (n) \quad (2)$$

The decrypted pixels are obtained in the array format and subsequently the decrypted image.

Fig 3 shows the original, encrypted and decrypted image in Matlab. Table 1 is an evaluation of different quality parameters using RSA algorithm.

2.2 Affine Transform and XOR Operation

Affine Transformation [3] is a technique in which we can change the original pixel value to a different location with the help of an 8-bit key. Then the image which is to be transmitted is divided into 2x2 pixel blocks and then each block is encrypted with the XOR Operation by four 8 bit keys. The total key size used in this algorithm is 64 bits. The relationship [5] between plain text (P) and cipher text (C) is

$$C = (K_0 + K_1 \times P) \bmod N \quad (5)$$

$$P = (C + (-K_0) \times 1/K) \bmod N \quad (6)$$

1/K is the multiplicative inverse of K_1 and $(-K_0)$ = additive inverse of K_0.

The HCF of $(K_1, N) = 1$

Encryption:

Take an image S of size M x N and a secret key of 64 bits. Break 64 bits key into eight equal parts i.e. (K_0, K_1, K_2, K_3, K_4, K_5, K_6, and K_7). The four sub keys (K_0, K_1, K_2 and K_3) are used for location change of pixel value and next four keys (K_4, K_5, K_6 and K_7) are used for encryption using XOR Operation. For every pixel P x, y changes the location (X, Y) in S to (X', Y') in C by formula

$$X' = (K_0 + K_1 \times X) \bmod M \quad (7)$$

$$Y' = (K_2 + K_3 \times Y) \bmod N \quad (8)$$

Break C into M/2 x N/2 number of 2 x 2 blocks. Now XOR Operation is performed for each block according to the following equations

$$P'_{1,1} = P_{1,1} \text{ XOR } K_4 \quad (9)$$

$$P'_{1,2} = P_{1,2} \text{ XOR } K_5 \quad (10)$$

$$P'_{2,1} = P_{2,1} \text{ XOR } K_6 \quad (11)$$

$$P'_{2,2} = P_{2,2} \text{ XOR } K_7 \quad (12)$$

Decryption:

Take a cipher image C [4] of size M x N and a secret key of 64 bits. Break the 64 bits key into

eight equal parts i.e. (K_0, K_1, K_2, K_3, K_4, K_5, K_6, and K_7). Break C into M/2 x N/2 number of 2 x 2 blocks. Then XOR Operation is performed for each block

Decrypt $P'_{1,1}$ as $P_{1,1} = P'_{1,1}$ XOR K_4 (13)
Decrypt $P'_{1,2}$ as $P_{1,2} = P'_{1,2}$ XOR K_5 (14)
Decrypt $P'_{2,1}$ as $P_{2,1} = P'_{2,1}$ XOR K_6 (15)
Decrypt $P'_{2,2}$ as $P_{2,2} = P'_{2,2}$ XOR K_7 (16)
For every pixel P x', y' changes the location (X', Y') in C to (X, Y) in S by formula [10]
X = (X' + (-K0)) x 1/K1) mod (17)
Y = Y' + (- K2)) x 1/K3) mod N (18)
Fig 4 shows the original, encrypted and decrypted image in Matlab. Table 2 is a comparison of different quality parameters using affine with XOR algorithm.

2.3 AES Algorithm

It is also known as Rijndael [6]. The AES algorithm was developed by Vincent Rijmen and Joan Daemen. In October 2000 NIST acknowledged that AES algorithm is the best algorithm in security,
performance, efficiency, ability of implementation, and also flexibility. The AES algorithm is symmetric
key algorithm, in this both sender and receiver uses same key to encrypt data into cipher and to decrypt cipher into original data. In this algorithm it has a fixed block length of 128 bits, while the length of key
size can be of 128, 192, or 256 bits. AES [7] is an iterative algorithm. It is composed of 4 basic operational blocks. For entire encryption iteration is performed up to "N" times. The total number of
iteration i.e. N can be 10, 12, and 14 based on key length i.e. 128, 192, and 256 respectively.

Encryption

Key Expansion Round keys are derived from the cipher key using Rijndael's key schedule. AES requires a separate 128-bit round key block for each round plus one more. Initial Round

- Add Round Key, each byte of the state is combined with a block of the round key using bitwise XOR

Iterative Round's

☐Sub Bytes, a non-linear substitution step where each byte is replaced with another according to a lookup table.
*Shift Rows, a transposition step where the last three rows of the state are shifted cyclically a certain number of steps.
*Mix Columns, a mixing operation which operates on the columns of the state, combining the four bytes in each column.
*Add Round Key

Final Round
Sub Bytes
Shift Rows
Add Round Key

Decryption

Inverse sub bytes, inverse shift rows and inverse mix columns is used in reverse order instead of sub bytes, shift rows, and mix columns. The key expansion remains the same. Fig 1 shows the original, encrypted and decrypted image in Matlab. Table 1 is a comparison of different quality parameters using AES algorithm.

EXPERIMENTAL RESULTS

In the hybrid algorithm used the image is encrypted using the encryption techniques in the following order-
1. RSA
2. AES
3. Affine with XOR

Figure 1 shows the encrypted image using the hybrid algorithm and the decrypted image. The image used for experimental analysis is cameraman.tif which is an in built Matlab image file.

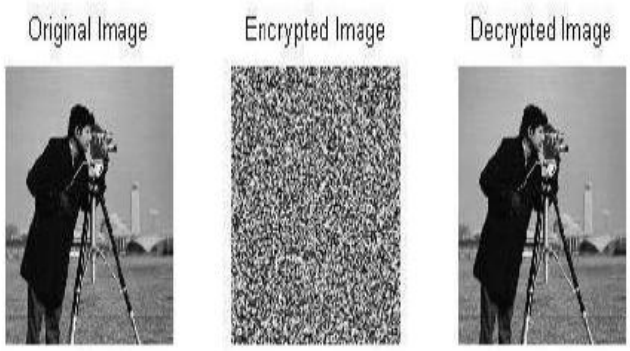

Fig 1. Encrypted and decrypted image using hybrid algorithm

IV. PERFORMANCE MEASUREMENT PARAMETERS

To be able to tell which the most suitable encryption technique [13] the following quality measurement parameters are employed once between original image and encrypted image and once between original image and decrypted image.
• Mean Square Error (MSE)
• Peak signal to Noise Ratio (PSNR)
• Normalized Absolute Error (NAE)

• Normalized cross correlation (NCC)
• Average difference (AD)
• Structural content (SC)
• Maximum difference (MD)

Quality Parameters	Comparison between Original Image and Encrypted Image	Comparison between Original Image and Decrypted Image
Mean Square Error	252	5.505
Peak Signal to Noise Ratio	24.208	40.7159
Normalized Absolute Error	0.2484	0.0104
Normalized cross correlation	1	1
Average Difference	101.06	1.5029
Structural Content	1.45	1.0003
Maximum Difference	241	5

Table 1. Performance measurement parameters for hybrid algorithm

Consider an image of dimensions M and N. If f(x, y) is the original image and g(x, y) is the distorted image then the various measurement parameters are described as follows.

4.1 Mean Square Error (MSE)

The MSE [19] is cumulative squared error between the compressed and the original image. It is calculated using

$$MSE = \frac{1}{MN}\sum_{0}^{M-1}\sum_{0}^{N-1}||f(x,y) - g(x,y)|| \quad (10)$$

4.2 Peak Signal to Noise Ratio (PSNR)

The PSNR is used to determine the ratio between the maximum power of a signal and power of corrupting noise. The formula of PSNR is given as

$$PSNR = 10\,log_{10}\left[\frac{M*N}{MSE}\right] \quad (11)$$

4.3 Average Difference (AD)

The average difference is given by the formula

$$AD=|f(x,y) - g(x,y)| \quad (12)$$

4.4 Maximum Difference (MD)

The maximum difference is given by the formula

$$MD= \max|f(x,y) - g(x,y)| \quad (13)$$

4.5 Normalized Absolute Error (NAE)

The normalized error is given by

$$y = NAE = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N}(f(x,y) * g(x,y))}{\sum_{x=1}^{M}\sum_{y=1}^{N}(f(x,y))^2} \quad (14)$$

4.6 Structural Content (SC)

SC is correlation based measure and measures the similarity between two images. It is given by the equation

$$SC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(y(i,j))^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}(x(i,j))^2} \quad (15)$$

V. CONCLUSION

This paper presents a new image encryption method based on a hybrid model of encryption using various encryption techniques. Experimental results show that our model yields high random cipher image measured by various quality measurement parameters such as MSE, AD, MD and PSNR thus making it difficult to recover the original image without the key.

REFERENCES

[1] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.
[2] J.C. Yen, J.I. Guo, An efficient hierarchical chaotic image encryption algorithm and its

VLSI realization, IEEE Proc. Vis. Image Process. 147 (2000) 167–175.
[3] Chin-Chen Chang, Min-Shian Hwang, Tung- Shou Chen, "A new encription algorithm for image cryptosystems", The Journal of Systems and Software 58 (200 I), 83-9 I.
[4] Mohammed A.F. Al-Husainy, "Image encryption using Genetic algorithm", Information Technology Journal, vol. 3, pp. 516-519. 2006.
[5] Sandeep Bhowmik, Sriyankar Acharyya, "Image cryptography: the Genetic algorithm approach", IEEE, vol. 3, pp. 223-227, 2011
[6] J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.
[7] H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. IEEE Trans. Signal Process. 48 (8), 2439–2451, 2000.
[8] Amol R. Madane, K.T Talele,M.M Shah, "Watermark Logo in Digital Image using DWT, Proceedings of SPIT-IEEE Colloquium and International Conference,Vol.1.

International Journal of Engineering Research and Applications (IJERA) is **UGC approved** Journal with Sl. No. 4525, Journal no. 47088. Indexed in Cross Ref, Index Copernicus (ICV 80.82), NASA, Ads, Researcher Id Thomson Reuters, DOAJ.

Avinash Ray " Hybrid model for Image Encryption and Decryption using RSA, AES, and Affine with XOR Operation " International Journal of Engineering Research and Applications (IJERA) 7.8 (2017): 90-94.