International Journal of Engineering and Applied Computer Science (IJEACS)
Volume: 02, Issue: 08, ISBN: 978-0-9957075-9-7, August 2017

An Advance Approach of Image Encryption using AES, Genetic Algorithm and RSA Algorithm

Avinash Ray
Department of Electrical & Electronics Engineering
NITTTR, Bhopal, India

Anjali Potnis
Department of Electrical & Electronics Engineering
NITTTR, Bhopal, India

Prashant Dwivedy
Department of Electrical & Electronics Engineering
NITTTR, Bhopal, India

Shahbaz Soofi
Department of Electrical & Electronics Engineering
NITTTR, Bhopal, India

***Abstract*— In current scenario the entire world is moving towards digital communication for fast and better communication. But in this a problem rises with security i.e. when we have to store information (either data or image) at any casual location or transmit information through internet. As internet is an open transmission medium, security of data becomes very important. To defend our information from piracy or from hacking we use a technique and i.e. known as Encryption Technique. In this paper, we use image as information and use an advance approach of well-known encryption techniques like AES, Genetic Algorithm, and RSA algorithm to encrypt it and keep our information safe from hackers or intruders making it highly difficult and time consuming to decipher the image without using the key.**

Keywords-AES, Communication, Decrptyion, Encryption, Genetic, Information, Open Transmission Medium, RSA, Security.

I. INTRODUCTION

In recent scenario information or data transmission is done through electronic means or we can say with the help of internet. Internet is an open transmission medium, so there is chance of data hacking or data piracy while it is being transmitted. Another problem arises with the data storage. That is sometimes we save some crucial messages in such devices which are operated by many people. So, at that time there is chance of Piracy of data. To stop these all piracy and hacking a technique is used to protect our information and is known as Encryption Technique. Encryption is a technique 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 algorithm normally requires a set of characters 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 Asymmetric Algorithm which is also called Asymmetric cryptography. It is usually implemented by the use of one-way functions. In mathematical terms, these are functions that are easy to compute in one direction but very difficult to compute in reverse manner. This is what allows you to publish your public key, which is derived from your private key. A common one-way function used today is factoring large prime numbers. It is easy to multiply two prime numbers together and get a product. However, to find out the factors there are numerous possibilities, and it is one of the great mathematical difficulties e.g. RSA Algorithm

And second one is Symmetric Algorithm which is also called as called symmetric cryptography or shared secret encryption [2]. This form of encryption uses a secret key, called the shared secret, to mix up the data into impenetrable twaddle. The person on the receiver end needs the shared secret (key) to unlock the message. It is called symmetric cryptography because the same key is used on both ends (i.e. at the sender end and at receiver end) for both encryption and decryption e.g. Genetic Algorithm.

In this paper, we take an image as input and perform different encryption technique over it. Here we encrypt a single image with three different encryption techniques [3] one by one in which some techniques are of symmetric algorithm and some are of asymmetric algorithm (like Genetic, AES, and RSA). Here all encryption techniques are used one by one that is output of one encryption technique is converted in input, of another encryption technique, or it is better to say all encryption technique is used in cascade manner. After execution of all encryption technique over input image, we get a highly encrypted image which is very difficult to decrypt without the authorization of its generator because of its dual nature i.e. symmetric and asymmetric encryption technique. Here to decrypt the image users need 'key', because of secret key algorithm, and the key must be provided by generator only.

II. METHODOLOGY

Here a list of the several encryption techniques are given which are used in this hybrid model of image encryption technique.

A. AES Algorithm

It is also known as Rijndael [2]. The AES algorithm [7] was developed by Vincent Rijmen and Joan Daemen. In October 2000 NIST acknowledged that AES algorithm is one of best algorithm in security, performance, efficiency, ability

of implementation, and also flexibility. The AES is a symmetric key algorithm, in this both sender and receiver uses identical key to encrypt data into cipher and then 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. It [3] is an iterative algorithm. It is composed of 4 basic operational blocks. For complete 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.

1) Encryption: In the 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.

a) *Initial Round:* Add Round Key, each byte of the state is combined with a block of the round key using bitwise XOR.

b) *Iterative Round's:* In the iterative round four operations are performed which include sub bytes operation which is a non-linear substitution step where each byte is replaced with another according to a lookup table. Shift rows is a transposition step where the last three rows of the state are shifted cyclically a certain number of steps. Mix columns is a mixing operation which operates on the columns of the state, combining the four bytes in each column. Finally, addition of round key is performed.

c) *Final Round:* In the final round all the above operations are repeated except in the final round mix columns is not performed.

2) Decryption: Inverse sub bytes, inverse shift rows and inverse mix columns are used in reverse order instead of sub bytes, shift rows, and mix columns. The key expansion remains the same.

B. Genetic Algorithm

Genetic Algorithm (GA) is a penetrating technique used in computer science to find out approximate solution to optimization problems. Genetic Algorithm [8] (GA) is first proposed by John Holland and his contemporaries at the University of Michigan in 1975. Genetic Algorithm is a particular class of evolutionary algorithm that used techniques inspired from human evolution *or* evolutionary biology like inheritance, mutation, natural selection and recombination (also called crossover).

B. 1) Encryption: Take an image as input. Calculate its Height (H) and Width (W) of the input image [9]. Find (H mod 8) and (W mod 8), if they are equal to zero then go to next step

$$H = H + (8 - (H \bmod 8)) \quad (3)$$
$$W = W + (8 - (W \bmod 8)) \quad (4)$$

Divide input image in two blocks, each block size is of (8x8). Perform crossover operation. Perform mutation operation get an encrypted block. Repeat last two steps for each block to get an encrypted image.

2) *Decryption:* Take encrypted image as input. Go to encrypted block. Perform mutation operation followed by crossover operation to get decrypted block [10]. Repeat last two steps for each block to get decrypted image.

C. RSA Algorithm

RSA is an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman [4]. 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 [5].

The RSA algorithm consists of three major steps in encryption and decryption. The steps are as following

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

2) Encryption: The RSA algorithm [6] 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

$$C = M^e \bmod (n) \quad (1)$$

3) Decryption: The text is decrypted using the private key (n, d) from the

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

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

III. Simulation

The encryption is performed on two images one Lena.bmp shown in figure 1 and other Mandrill.bmp shown in figure 2 both of size 512×512

Figure 1. Test Image Lena

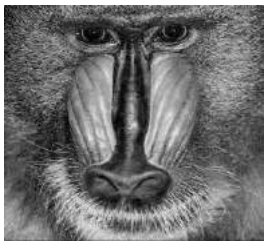

Figure 2. Test Image Mandrill

In the hybrid model, the encryption is done by combining the encryption techniques listed above in the order shown in figure 3 where the output of each technique is the input of the next encryption algorithm.

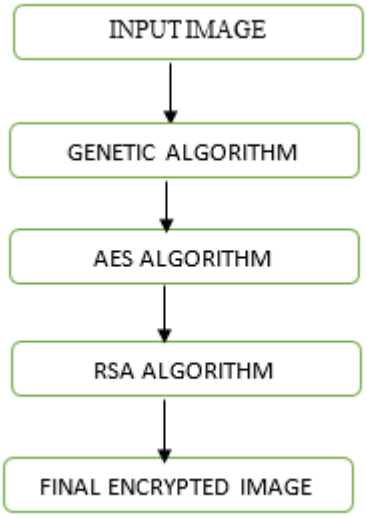

Figure 3. Flowchart for Hybrid Image Encryption

For decryption, the same techniques are applied in the reverse order shown in figure 4.

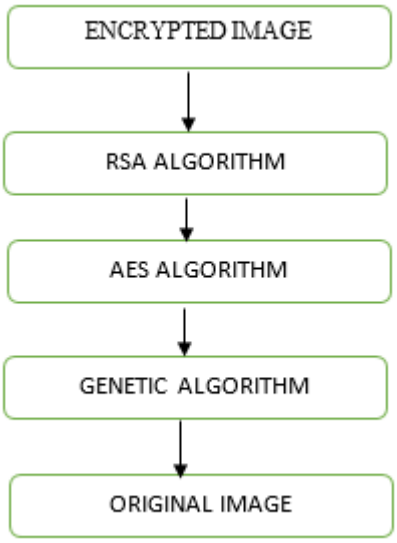

Figure 4. Flowchart for Hybrid Image Decryption

Figure 5. Test Image Lena Encryption. a) Original Image b) Genetic encryption c) AES encryption h) RSA encryption final image.

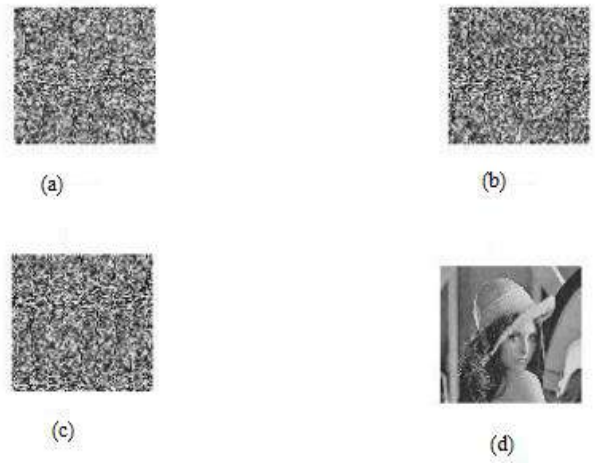

Figure 6. Test image Lena Decryption. a) RSA decryption b) AES decryption c) Genetic decryption d) original image.

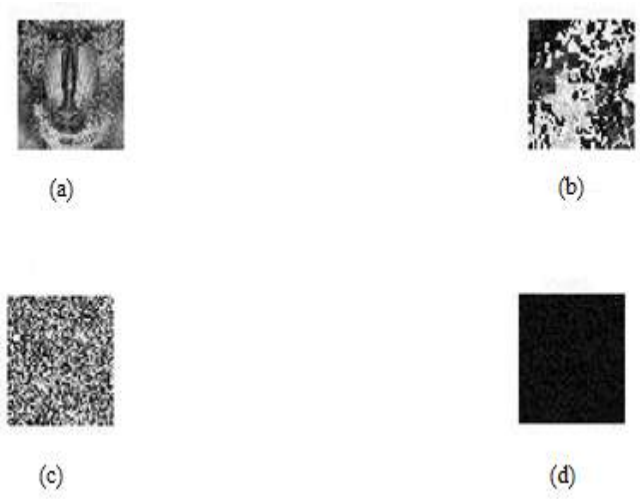

Figure 7. Test Image Mandrill Encryption. a) Original Image b) Genetic encryption c) AES encryption d) RSA encryption final image.

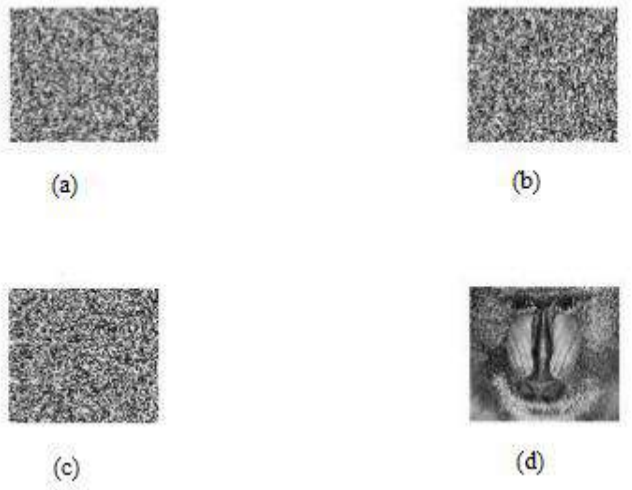

Figure 8. Test image Mandrill Decryption. a) RSA decryption b) AES decryption c) genetic decryption d) original image.

Figure 5 and 6 show the step by step encryption and decryption of the test image Lena. Figure 7 and 8 show the step by step encryption and decryption of the test image Mandrill.

IV. Measurement Parameters

To be able to tell how suitable the hybrid encryption model is the following quality measurement parameters are employed once between original image [10] 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)

Table 1 shows the measurement parameters employed between the test image Lena and the encrypted Image [11] and between the original image and its decrypted image.

TABLE I. QUALITY MEASURMENT PARAMETERS FOR TESTIMAGE 1.

Measuremen t Parameters	**Comparison between Original Image Lena and Encrypted Image**	**Comparison between Original Image Lena and**
MSE	253.80	5.5098
AD	108.5366	1.5029
MD	243	5
NAE	0.8749	0.0121
NK	1	1
SC	1.44	1
PSNR	24.08	40.7195

Table 2 shows the measurement parameters employed between the test image Mandrill and the encrypted Image and between the original image and its decrypted image.

TABLE II. QUALITY MEASURMENT PARAMETERS FOR TESTIMAGE 2

Measuremen t Parameters	**Comparison between Original Image Lena and Encrypted Image**	**Comparison between Original Image Lena and Decrypted Image**
MSE	245.67	. 5.5150
AD	93.06	1.5023
MD	238	5
NAE	0.8584	0.0139
NK	1	1
SC	1.4266	1.0004
PSNR	24.2271	40.7154

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.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.

[3] H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. IEEE Trans. Signal Process. 48 (8), 2439–2451, 2000.

[4] 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.

[5] H. Cheng, X.B. Li, Partial encryption of compressed image and videos, IEEE Trans. Signal Process. 48 (8) (2000) 2439–2451.

[6] S. Li, X. Zheng, Cryptanalysis of a chaotic image encryption method, in: Proceedings of the IEEE International. symposium on circuits and systems, Scottsdale, AZ, USA, 2002.

[7] 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.

[8] Sandeep Bhowmik, Sriyankar Acharyya, "Image cryptography: the Genetic algorithm approach", IEEE, vol. 3, pp. 223-227, 2011.

[9] Mohammed A.F. Al-Husainy, "Image encryption using Genetic algorithm", Information Technology Journal, vol. 3, pp. 516-519. 2006.

[10] P. Blomgren and T. F. Chan, "Color TV: Total variation methods for restoration of vector-valued images," IEEE Trans. Image Process, vol. 7, no. 3, pp. 304–309, Mar. 1998.

[11] M. Lebrun, M. Colom, and J. M. Morel, "The noise clinic: A universal blind denoising algorithm," in Proc. IEEE Int. Conf. Image Process, Oct. 2014, pp. 2674–2678.