

Color Image Encryption using AES and RSA



Peyyala Venkata Jaswanth, Baddam Ranga Reddy, Marturi Surya Pavan Kumar, M. Jasmine Pemeena Priyadarsini

Abstract— Information security is an important task on multimedia and communication world. During storing and sharing maintaining a strategic distance from the outsider access of information is the difficult one. There are many encryption algorithms that can provide data security. In this paper two of the encryption algorithms namely AES and RSA are implemented for color images. AES (Advanced Encryption Standard) is a symmetric key block cipher published in December 2001 by NSIT (National Institute of Standards and Technology). RSA (Rivest-Shamir-Adleman) is an asymmetric key block cipher. It uses two separate keys, one for encryption called the public key and other for decryption called the private key. Both the implementation and analysis are done in Matlab. The quality and security level of both the algorithms is analysed based on various criteria such as Histogram analysis, Correlation analysis, Entropy analysis, NPCR (Number of Pixel Change Rate), UACI (Unified Average Changing Intensity), PSNR (Peak Signal-to-Noise Ratio).

Index Terms—AES (Advanced Encryption Standard), NPCR (Number of Pixel Change Rate), PSNR (Peak Signal-to-Noise Ratio), RSA (Rivest-Shamir-Adleman), UACI (Unified Average Changing Intensity)

I. INTRODUCTION

We can represent a digital image as an array. The elements of the array or matrix are known as pixels. The size of the image can be decided from the dimensions of the array of pixels. The number of columns in the array is the height of the image and the number of rows is the width of the image. Every pixel of the array has an intensity value. We use these intensity values to encrypt and decrypt an image. Before encrypting and decrypting an image one must know about the types of images. The binary image has only two-pixel values 0 which is black and 1 which is white. There are different formats for different type of images. For a n-bit image there are 2^n intensity values. The 2, 3, 4, 5 and 6-bit color format images are rarely used in recent times. They were used in old times for televisions and monitor screens. The standard digital images use an 8-bit format. The range of the colors in 8-bit vary from 0-255, Where 0 stands for black, and 255 stands for white, and 127 stands for Gray color.

Revised Manuscript Received on May 15, 2020.

* Correspondence Author

Peyyala Venkata Jaswanth*, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India

Baddam Ranga Reddy, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India

Marturi Surya Pavan Kumar, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India

M. Jasmine Pemeena Priyadarsini, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore, India

© The Authors. Published by Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP). This is an open access article under the CC BY-NC-ND license (<http://creativecommons.org/licenses/by-nc-nd/4.0/>)

Gray scale images have intensity from the darkest Gray which is black to lightest Gray which is white. Since they are of 8-bit color format they have 2^8 (256) different shades of colors in it. Color images have intensity from the darkest and lightest of three different colors, Red, Green, and Blue. The mixtures of these color intensities produce a color image. Since Color images have three different color planes each of them is 8-bit intensities so they are also called as 24-bit color images.

II. PROPOSED ALGORITHMS

A. AES ALGORITHM

AES [1][2][4] was developed by Vincent Rijmen and John Daemen. It was published by NSIT in 2001. It is a symmetric key cipher which means it uses the same key for both encryption and decryption. AES is a block cipher which uses substitution, transformation and permutation for providing security. It is block cipher which encrypts and decrypts data block, also called as state. A state is a group of 128 bits and can be represented as a matrix. Each column and row of the matrix is referred as a word. AES is available in three different versions; 10 rounds with a key size of 128 bits, 12 rounds with a key size of 192 bits and 14 rounds with a key size of 256 bits, but round key size and block size is always the same which is 128 bits. AES uses four operations

1. SubBytes operation: SubBytes operation substitutes each byte of the state with a new byte using an 8-bit S-box.
2. ShiftRows operation: ShiftRows operation makes the i^{th} row of the state to shift left by i number of bits.
3. MixColumns operation: MixColumns operation operates on columns of the state, each column is transformed individually using an operation matrix.
4. AddRoundKey operation: In AddRoundKey operation each column of the state is combined with the round key using XOR the operation.

While encryption the plain text is converted into a state then AddRoundKey operation is performed and passed onto further rounds. All the rounds have four operations except for last round which has only three, last round does not have MixColumns operation. Round keys used in the AddRoundKey operation are generated by Key Expansion process [3]. The cipher key is different from the round key. Decryption is like encryption, but the only difference is we use inverse of operations that are used in the encryption except the AddRoundKey operation.

B. RSA Algorithm

Ron Rivest, Adi Shamir and Leonard Adleman designed RSA algorithm in 1977. RSA is an asymmetric key cipher which means it uses two keys public and private.



Public key is used in the encryption process and the private key is used in the decryption process. RSA algorithm can be divided into three main steps

1. *Key Generation:* Key generation [8] is the very first step in RSA algorithm as we already knew that RSA algorithm uses two keys, we need to calculate both keys. Key generation in RSA involves four simple steps

- i. First step is to choose two different prime numbers p and q then compute $n=p \times q$.
- ii. Second step is to calculate $\phi(n) = (p - 1)(q - 1)$.
- iii. Third step is to choose e such that $1 < e < \phi(n)$ and $\text{GCD}(e, \phi(n)) = 1$ where (e,n) is our public key.
- iv. Fourth step is to find d such that $ed=1 \pmod{\phi(n)}$ where d is our private key.

2. *Encryption:* The sender encrypts the original text using the public key and the formula

$$C = P^e \pmod{n} \quad (1)$$

3. *Decryption:* The cipher text obtained from the encryption is decrypted by the receiver using the private key and the formula

$$P = C^d \pmod{n} \quad (2)$$

III. IMPLEMENTATION

To encrypt a gray scale image we used the pixel intensity values of the image, we already knew an image can be represented as an array of pixels, the intensity values of the pixels are encrypted using the algorithm and pixels with those encrypted intensity values are arranged in the same order to get the encrypted image. Decryption is opposite to the encryption, the intensity values of the encrypted image are taken and decrypted using the same algorithm and the pixels with those decrypted intensity values are arranged in the same order to get the decrypted image. On the other hand, pixels of a color image have three values of red, green and blue colors, we split each color image into three different gray scale images then encrypt each one individually and combine them back again to make the final encrypted image. Decrypting is reverse of the encryption, we split the encrypted image then decrypt them individually and combine them back again to get the decrypted color image. Encryption and decryption are done using MATLAB [1][5][6][7][9]. Fig.2 shows the encrypted images of Fig.1 using AES and RSA algorithms.



Fig.1 Original image



(a) AES algorithm



(b) RSA algorithm

Fig.2 Encrypted images using different algorithms

IV. STATISTICAL ANALYSIS PARAMETERS

A. Histogram analysis

Image histogram is a graph that tells us how many numbers of pixels there with an intensity value are. The intensity values are represented using the horizontal axis of the graph while the number of pixels with that intensity value are represented using the vertical axis of the graph. For a color image there will be three graphs for each color. The image histogram analysis is one of the simple methods to check the quality of encryption algorithm. For a good encryption algorithm the encrypted image will have a histogram which is uniformly distributed.

B. NPCR and UACI

NPCR (Number of Pixel Change Rate) value tells the rate of change of number of pixels in an encrypted image when a pixel of original image is changed. NPCR of an image can be defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{m \times n} \times 100\% \quad (3)$$

UACI (Unified Average Changing Intensity) value calculates the average intensity of differences between the poriginal image and the encrypted image. UACI of an image can be defined as

$$UACI = \frac{1}{m \times n} \left[\sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \right] \times 100\% \quad (4)$$

$$D(i,j) = \begin{cases} 1, & C_1(i,j) \neq C_2(i,j) \\ 0, & C_1(i,j) = C_2(i,j) \end{cases} \quad (5)$$

NPCR and UACI are used to measure the strength of encryption algorithm against different kind of attacks. For a better encryption algorithm, the ideal value of NPCR is 99.61% [4]and that of UACI is 33%.

C. PSNR

PSNR is the peak signal to noise ratio between the original and a compressed image or a reconstructed image. It is a measurement of quality between the two images. The PSNR value will be very high for two similar images and vice versa. For example, two same images will have a PSNR value of infinity and two completely different images will have a very low PSNR value. To find the PSNR value we need to find the MSE (Mean Squared Error) value. MSE of an image is defined as

$$MSE = \frac{\sum_{x,y} [I_1(x,y) - I_2(x,y)]^2}{x \times y} \quad (6)$$

x is the number of rows and y is the number of columns in the two images. PSNR of an image is defined as

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \quad (7)$$

R is the maximum fluctuation in the input image data type.

D. Correlation analysis

Correlation is a statistical relationship between two measured quantities. Correlation coefficient is the numerical measurement of correlation. The correlation coefficient is defined as

$$r = \frac{\sum_i (x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\sum_i (x_i - \bar{x})^2} \sqrt{\sum_i (y_i - \bar{y})^2}} \quad (8)$$

x_i is the intensity value of i^{th} pixel in 1st image and y_i is the intensity value of i^{th} pixel in 2nd image. \bar{x} is the mean of pixel intensity values in the 1st images and \bar{y} is the mean of pixel intensity values in the 2nd image. For two identical images correlation coefficient is 1 and for two different images correlation coefficient value ranges between 1 and -1 or equal to -1. Correlation can also be used to relate two adjacent pixels of an image. An Encrypted image should have less correlation between its adjacent pixels.

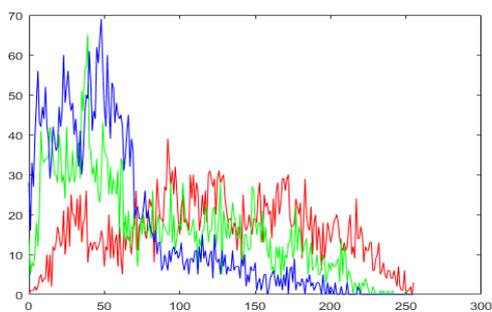
E. Entropy analysis

In cryptography, entropy is used to measure the randomness of the cipher text so that it cannot reveal any information regarding the plain text. Entropy tells us how randomly the pixels of cipher image are arranged. For a encryption algorithm, the ideal entropy value is 8[2]. The information entropy of an image I is defined as

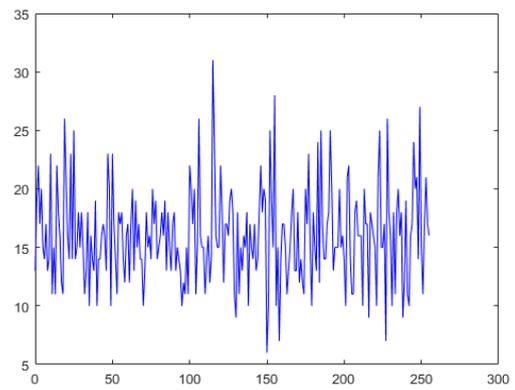
$$H(I) = \sum_{i=0}^{255} p(I_i) \log \frac{1}{p(I_i)} \quad (9)$$

where I_i is the i^{th} gray value of the image and $P(I_i)$ is the probability of I_i .

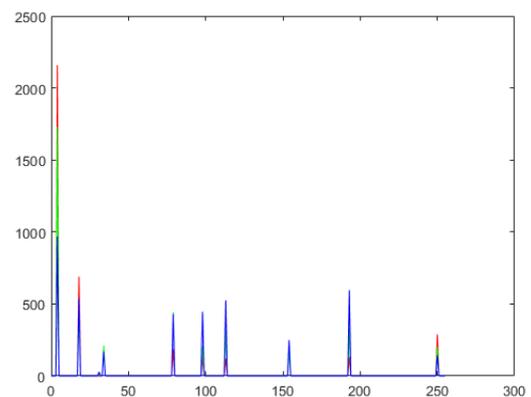
V. RESULTS



(a) Original image



(b) AES Encrypted image



(c) RSA Encrypted image

Fig.3 Histogram of Original and encrypted images

TABLE-I: Comparison of Analysis Parameters between Encrypted Images Using AES and RSA

Analysis Parameters	AES	RSA
PSNR	76.94dB	-41.27dB
UACI	33.71	38.14%
NPCR	99.59%	100%
Correlation of horizontally adjacent pixels	0.023	0.367
Correlation of vertically adjacent pixels	0.091	0.537
Entropy	7.954	2.747
Cross Correlation	-0.020	-0.473

Histograms of original image and encrypted images using AES and RSA algorithms is shown in Figure 3. Histogram of AES encrypted image is uniformly distributed, but RSA encrypted images is not uniformly distributed.

Table 1 shows the comparison of analysis parameters between AES encrypted image and RSA encrypted image. PSNR, NPCR and UACI values are approximately ideal so both the algorithms provide better security against attacks. Correlation analysis shows that the correlation between adjacent pixels is high in RSA encrypted image than in AES encrypted image, so from correlation analysis we can say that RSA encrypted image may leak small amount of information.

VI. CONCLUSION

In this work, we used AES and RSA algorithms for encrypting and decrypting images. Encryption, decryption and analysis is done using MATLAB 9.0 VERSION R2016a. we use the image intensity values to encrypt and decrypt the image, as an image can be represented as an array of pixels and each pixel has its own intensity values. As a color image is has 3 different color combined, it can be split into 3 different gray scale images. We encrypt each color plane individually using the algorithms and then combine them to form the encrypted image. Decryption is exactly the reverse process. We compared both the algorithms using different analysis methods. we conclude that AES is faster than RSA, both the algorithms provide better security against attacks, but encrypted images of RSA algorithm may leak tiny amounts of information.

REFERENCES

1. Q. Zhang and Q. Ding, "Digital Image Encryption Based on Advanced Encryption Standard (AES)," 2015 Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control (IMCCC), Qinhuangdao, 2015, pp. 1218-1221, doi: 10.1109/IMCCC.2015.261.
2. S. H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, "A new modified version of Advanced Encryption Standard based algorithm for image encryption," 2010 International Conference on Electronics and Information Engineering, Kyoto, 2010, pp. V1-141-V1-145, doi: 10.1109/ICEIE.2010.5559902.
3. B. Subramanyan, V. M. Chhabria and T. G. S. Babu, "Image Encryption Based on AES Key Expansion," 2011 Second International Conference on Emerging Applications of Information Technology, Kolkata, 2011, pp. 217-220, doi: 10.1109/EAIT.2011.60.
4. A. Singh, P. Agarwal and M. Chand, "Image Encryption and Analysis using Dynamic AES," 2019 5th International Conference on Optimization and Applications (ICOA), Kenitra, Morocco, 2019, pp. 1-6, doi: 10.1109/ICOA.2019.8727711.
5. V. S. Aparna, A. Rajan, I. Jairaj, B. Nandita, P. Madhusoodanan and A. A. S. Remya, "Implementation of AES Algorithm on Text And Image using MATLAB," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2019, pp. 1279-1283, doi: 10.1109/ICOEI.2019.8862703.
6. A. Chaouch, B. Bouallegue and O. Bouraoui, "Software application for simulation-based AES, RSA and elliptic-curve algorithms," 2016 2nd International Conference on Advanced Technologies for Signal and Image Processing (ATSIP), Monastir, 2016, pp. 77-82, doi: 10.1109/ATSIP.2016.7523051.
7. S. Mukherjee, S. Sinha, S. Chakrabarti and T. Mukhopadhyay, "A meticulous implementation of RSA Algorithm using MATLAB for image encryption," 2017 1st International Conference on Electronics, Materials Engineering and Nano-Technology (IEMENTech), Kolkata, 2017, pp. 1-6, doi: 10.1109/IEMENTECH.2017.8076979.
8. H. Wang, Z. Song, X. Niu and Q. Ding, "Key generation research of RSA public cryptosystem and Matlab implement," PROCEEDINGS OF 2013 International Conference on Sensor Network Security Technology and Privacy Communication System, Nangang, 2013, pp. 125-129, doi: 10.1109/SNS-PCS.2013.6553849.
9. H. Agrawal, "Matlab implementation, analysis & comparison of some RSA family cryptosystems," 2010 IEEE International Conference on Computational Intelligence and Computing Research, Coimbatore, 2010, pp. 1-3, doi: 10.1109/ICCIC.2010.5705873.

AUTHORS PROFILE



Peyyala Venkata Jaswanth did his B.Tech in Electronics and Communication Engineering from Vellore Institute of Technology, Vellore. His areas of interest are VLSI, Microcontroller and Embedded System. He has done so many projects based on Microcontroller and Embedded System. He has been awarded for his project called dual-axis sun light tracking solar panel system.



Marturi Surya Pavan Kumar did his B.Tech in Electronics and Communication Engineering from Vellore Institute of Technology, Vellore. His areas of interest are Sensors, Digital Communication and Analog Communications and done so many projects based on them.



Baddam Ranga Reddy did his B.Tech in Electronics and Communication Engineering from Vellore Institute of Technology, Vellore. His areas of interest are Microcontroller, Digital Communication and Analog Communications and done so many projects based on them.



Dr. M.Jasmine Pemeena Priyadarsini obtained B.E. degree from Madras University in 1992 and M.E. degrees from Madurai Kamaraj University, Madurai in 1995.. She earned his Ph.D. from Vellore Institute of Technology, Vellore, INDIA in 2014. She has published more than 45 research papers in National and International journals and reputed conferences. She has a teaching experience of about 25 years in Vellore Institute of Technology, Vellore in India. Presently, she is serving as Professor at Vellore Institute of Technology, India. She is a life member of Indian Society for Technical Education, IEEE society Membership, Fellow of Institution of Engineers, Fellow of Institution Electronics and Telecommunication Engineers. She has authored about four technical books. His research areas include Digital Image Processing, Digital signal processing,, Optical Signal Processing, Light wave Communication Systems, Optical Coding Theory and Biometric Image Processing. She is a reviewer of several international conferences and journals.