Journal of Engineering and Applied Sciences 14 (2): 464-469, 2019
ISSN: 1816-949X

Modified Mathematical Method to Improve RSA Image Cryptosystem Algorithm

Abbas Fadhil Mahdi, Shahid Adil Taher and Mohammed Ridha Nsaif
Department of Computer Science, Faculty of Computer Science and Mathematics,
University of Kufa, Kufa, Iraq

Abstract: This study focuses on protecting information against any broke attempts to known the data contents by transforming it into an unintelligible and secure format that allows information to be kept secret, so, we improved one of the most important methods used in the field of cryptography the asymmetric which uses a pair of keys that called RSA (Rivest-Shamir-Adleman) by multiplying the number of (public, private) keys to some extend "k" in the cryptosystem process and as well as how to apply proposal modified on set of digital gray images using MATLAB language, the practical results showed after comparative between traditional and modified algorithm, that (RSAM) gives more powerful security in the encryption process instead of conventional RSA and a high match ratio between original and decrypted images during data retrieval in the decryption process because it depends on computational hardness of the algorithm that based on "k" number of chosen (public, private) keys. Therefore, (RSAM) modified more confidential and safe for data privacy from unauthorized access attempts to detect or corrupt information.

Key words: RSA cryptosystem, cryptography, public key cryptosystem, data, privacy, algorithm

INTRODUCTION

Cryptography depends heavily on mathematics and the keys used to secure data during transform it into network and according to of keys used for encryption (k_e), respectively for decryption (k_d), the cryptosystems are classified into symmetric key (use the same key for cryptosystem process) and asymmetric (different keys), so, depending on this categories show many ways of cryptography algorithms such as (Dhakar *et al*., 2012). Hill cipher, Vignere cipher, Affine cipher algorithms are the symmetric cryptography examples and RSA algorithm is the asymmetric cryptography examples which are the interest of this study, its invented the first public key cryptography as well as called also asymmetric cryptography by Ron Rivest, Adi Shamir and Len Adleman shortened as RSA in 1977 and many researchers have modified the mathematical properties of the algorithm. the study by Hassan *et al.* (2014), the reseachers have integrated the RSA algorithm with concept genetic algorithms to encrypt and decrypt data and other reseachers in study (Dhakar *et al*., 2012), additive some homomorphisms features to increase the security of algorithm in study of Patidar and Bhartiya (2013), the researchers increase by one the numbers of large prime (third key) to make the modified algorithm very difficult to decompose against hackers. While the researchers in the study of Abudin *et al.* (2014) suggest encrypting the value (n) that generated by (p*q) by choosing two pairs of the key, the small size of the pair used to encrypt data and large size of the pair used to encrypt the value (n) of the small size of the pair.

Work of RSA cryptography: In RSA cryptography there is a pair of different keys, the first is called public key that used for encryption procedure and available to whomever to send a message and the other is called private key that used for decryption procedure and must be kept secret by the creator and the following steps describes the concept of work it.

The key generation of conventional RSA algorithm:

- Select two numbers a and b are large prime and chosen by each user to evaluate the value (n), n = a*b
- Compute as following β (n) = β (a*b) =(a-1)*(b-1)
- Suppose (x, y) are chosen such that (y) is an inverse of (x) modulo β(n) where 1<x, y<β (n), g c d (x, β (n)) = 1
- The pair (x, n) is pronounced and announced for everyone but should be keep (y, n) secret by the creator (Milanov, 2009)

The procedure of RSA encryption:

- Declared sender's public key (x, n) used to encrypt a serial of data plaintext as a block m
- The procedure of encryption compute as following equation e (m) = y ≡ m^x (mod n) by the sender
- The sender will be transmitted ciphertext as a set of blocks (Rosen, 2005)

Corresponding Author: Abbas Fadhil Mahdi, Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Kufa, Iraq

The procedure of RSA decryption:

- The private key of the receiver (y, n) being used to decrypts the cipher data
- $D(y) = m \equiv y^y \pmod n$ is calculated for each single block (Hoffstein *et al*., 2008)

MATERIALS AND METHODS

Proposed method (RSAM algorithm): In this study, we focused on the process of optimizing one of the algorithms asymmetric cryptography that called (RSA) by manipulating certain mathematical properties to increasing the numbers of public keys (x_1, x_2, x_3, ..., x_k, n) in the encryption procedure and as well as corresponding private keys (y_1, y_2, y_3, ..., y_k, n) in decryption procedure to upgrade level security as will be explained in the following example instead of choosing one public key are (x, n) and another private key is (y, n) for cryptosystems, we can applied the proposed modification over mathematical matrices as well as can be applied over any type of image like (color or gray level image) in image processing, since, the proposed system offers a more robust encryption method than traditional encryption and data integrity during the decryption process as we will demonstrate during the search (Hussain, 2015).

Key generation of proposal algorithm:

- Two large prime numbers a and b are chosen by RSA's user to from n = a*b
- Computes β (n) where β (n) = β (a*b) = (a-1)(b-1)
- Pick a positive integer numbers (k) such as (x_1, x_2, x_3, ..., x_k) to refer public keys and then calculate the private keys such as (y_1, y_2, y_3, ..., y_k) are chosen such that y_h is an inverse of x_h modulo β (n) with $1<x_h$, $y_h<\beta$ (n), GCD (x_h, β (n)) = 1, for $1 \le h = k$
- (x_1, x_2, x_3, ..., x_k, n) for everyone will be declared as the public key and (y_1, y_2, y_3, y_4, ..., y_k, n) should be kept secret as the corresponding private key (Ivy *et al*., 2012)

An example of proposed cryptosystem on matrices: Suppose Alice wants to send encrypted message as a matrix on unsecured channel:

$$T = \begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$$

which is a part of an image, Alice have five public key as following ($x_1 \cdot x_2 \cdot x_3 \cdot x_4 \cdot x_5$, n) = (7, 11, 13, 23, 53, 143) and harmonious keys of private following ($y_1 \cdot y_2 \cdot y_3 \cdot y_4 \cdot y_5$, n) = (103, 11, 37, 47, 77, 143)

Encryption process: Use the above public keys and arrange it as a corresponding block of the plain matrix to make up the encryption key matrix (x_{ixj}) as the following:

K_e = matrix x_{ixj}

$$x_{4\times4} = \begin{bmatrix} 07 & 11 & 13 & 23 \\ 53 & 07 & 11 & 13 \\ 23 & 53 & 07 & 11 \\ 13 & 23 & 53 & 07 \end{bmatrix}$$

To encrypt plain matrix ($T_{4\times4}$) using following defined encryption format. We denoted to the x_{ixj} is the power of T_{ixj} by $(x_{ixj}®T_{ixj})$ for all matrix n×n:

$$C_R = (x_{ixj}®T_{ixj}) \pmod{143} \equiv \begin{bmatrix} 07 & 11 & 13 & 23 \\ 53 & 07 & 11 & 13 \\ 23 & 53 & 07 & 11 \\ 13 & 23 & 53 & 07 \end{bmatrix}®$$

$$\begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix} = \begin{bmatrix} (20)^7 & (02)^{11} & (08)^{13} & (25)^{23} \\ (05)^{53} & (11)^{07} & (04)^{11} & (28)^{13} \\ (11)^{23} & (22)^{53} & (09)^{07} & (08)^{11} \\ (06)^{13} & (12)^{23} & (23)^{53} & (10)^{07} \end{bmatrix}$$

$$\pmod{143} \equiv \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}$$

Finally, Alice transmitted the encryption message as a matrix to Jack as following by un-secure channel:

$$\text{Channel } C_R = \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}$$

Decryption process: Jack has the following private keys to decrypt the message as a matrix ($y_1 \cdot y_2 \cdot y_3 \cdot y_4 \cdot y_5$, n) = (103, 11, 37, 47, 77, 143) a organize the keys conforming decryption as following, so:

$$y_{ixj} = \begin{bmatrix} 103 & 11 & 37 & 47 \\ 77 & 103 & 11 & 37 \\ 47 & 77 & 103 & 11 \\ 37 & 47 & 77 & 103 \end{bmatrix} \text{ as respectively}$$

The matrix:

$$C_R = \begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix}$$

received by jack to acquire the plain matrix T_{ixj}, use the algorithm of (RSA) modified:

$$T_{4\times4} = y_{4\times4} \circledR C_r \,(\text{mod}143) = \begin{bmatrix} 103 & 11 & 37 & 47 \\ 77 & 103 & 11 & 37 \\ 47 & 77 & 103 & 11 \\ 37 & 47 & 77 & 103 \end{bmatrix} \circledR$$

$$\begin{bmatrix} 136 & 46 & 138 & 38 \\ 70 & 132 & 114 & 106 \\ 110 & 55 & 48 & 96 \\ 84 & 12 & 56 & 10 \end{bmatrix} = \begin{bmatrix} (136)^{103} & (46)^{11} & (138)^{37} & (38)^{47} \\ (70)^{77} & (132)^{103} & (114)^{11} & (106)^{37} \\ (110)^{47} & (55)^{77} & (48)^{103} & (96)^{11} \\ (84)^{37} & (12)^{47} & (56)^{77} & (10)^{103} \end{bmatrix}$$

$$(\text{mod}\ 143) \equiv \begin{bmatrix} 20 & 02 & 08 & 25 \\ 05 & 11 & 04 & 28 \\ 11 & 22 & 09 & 08 \\ 06 & 12 & 23 & 10 \end{bmatrix}$$

At last, note retrieval original matrix after decryption process as above matrix shown.

RESULTS AND DISCUSSION

Practical work: Using the MATLAB@2014 program to execute both traditional (RSA) and modified (RSAM) algorithms on some various computerized gray images, the practical aspect appears (encrypted, decrypted) images and the histogram of them as shown. And make a comparison between the two methods (RSA, RSAM) with original images as that clear in Fig. 1. And that important to refer to the mathematical definition of the PSNR and SSIM that we calculated it in Table 1 and 2 (Srivastava and Singh, 2015):

$$\text{PSNR}(A,T) = 10\log_{10}\frac{255^2}{\text{MSE}(A,T)} \quad (1)$$

- Given references image A and T a test image, both of size m×n
- For the maximum intensity of 256*256 images is 255 (0-255)

Where mean square error is given by:

$$\text{MSE} = \frac{1}{MN}\sum_i^M\sum_j^N (A_{ij}-T_{ij})^2 \quad (2)$$

and structural similarity index contains three comparison functions known for luminance comparison, contrast comparison and structure comparison between two signals l and g:

$$k(l,g) = \frac{2\mu_l\mu_g+c_1}{\mu_l^2+\mu_g^2+c_1}, c(l,g) = \frac{(2\sigma_l\sigma_g+c_2)}{\sigma_l^2+\sigma_g^2+c_2}, s(l,g) = \frac{\sigma_{lg}+c_3}{\sigma_l\sigma_g+c_3} \quad (3)$$

which the relative importance of the three components defines as:

$$\text{SSIM}(l,g) = \frac{\left((2\mu_l\mu_g+c_1)(2\sigma_{lg}+c_2)\right)}{(\mu_l^2+\mu_g^2+c_1)(\sigma_l^2+\sigma_g^2+c_2)} \quad (4)$$

Where:

μ_l, μ_g = The means of l and g
σ_l, σ_g = The standard deviations of l and g, respectively
σ_{lg} = The correlation coefficient between l and g

The constants c_1-c_3 are used to stabilize the algorithm when the denominators approach to zero, s.t (Wang *et al*., 2004):

$$\mu_l = \frac{1}{S}\sum_{i=1}^S l_i,\ \mu_g = \frac{1}{S}\sum_{i=1}^S g_i,$$
$$\sigma_l = \left[\frac{1}{S\text{-}1}\sum_{i=1}^S (l_i-\mu_l)^2\right]^{1/2}, \sigma_g = \left[\frac{1}{S\text{-}1}\sum_{i=1}^S (g_i-\mu_g)^2\right]^{1/2} \quad (5)$$

We implemented the proposed system (RSAM) that uses public keys (7, 11, 13, 23, 53, 143) and private keys (103, 11, 37, 47, 77, 143) as well as the traditional system that uses public key (7, 143) and private keys (103, 143) on some gray images to the inference which of the two methods is better in terms of strength of encryption and data security by using some criterion where applying performance coefficients Peak Signal-to-Noise Ratio

Table 1: The difference between the original image and the image shows encoded in terms of PSNR, SSIM

Image (org)	PSNR (RSA, org)	PSNR (RSAM, org)	SSIM (RSA, org)	SSIM (RSAM, org)
A	-41.3109	-41.3113	0.0132	-3.1638e-05
D	-40.8717	-40.8719	0.0192	4.3523e-04
B	-42.5189	-42.5200	0.0179	-5.3055e-07

Table 2: The difference between the original image and the decoded images shows in terms of PSNR, SSIM

Image (ORG)	PSNR (RSA, org)	PSNR (RSAM, org)	SSIM (RSA, org)	SSIM (RSAM, org)
A	-27.4525	Inf	0.9005	1
D	-31.0847	Inf	0.8471	1
B	-23.5485	Inf	0.9434	1

(PSNR) and Structural Similarity Index (SSIM) between the RSA Method and modified method (RSAM) for the original image, we found both of methods have the convergent performance in terms of (PSNR), although, the

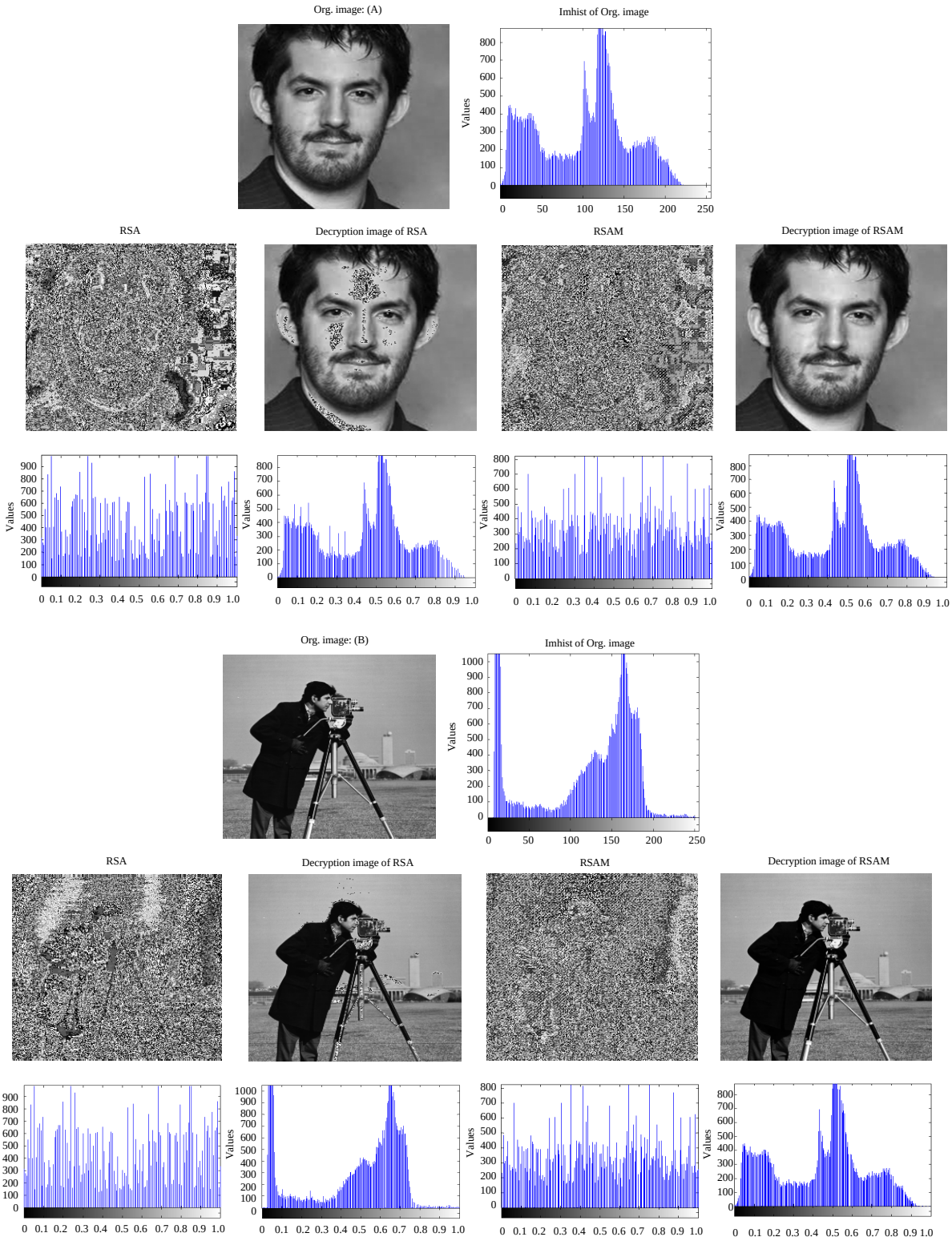

Fig. 1: Continue

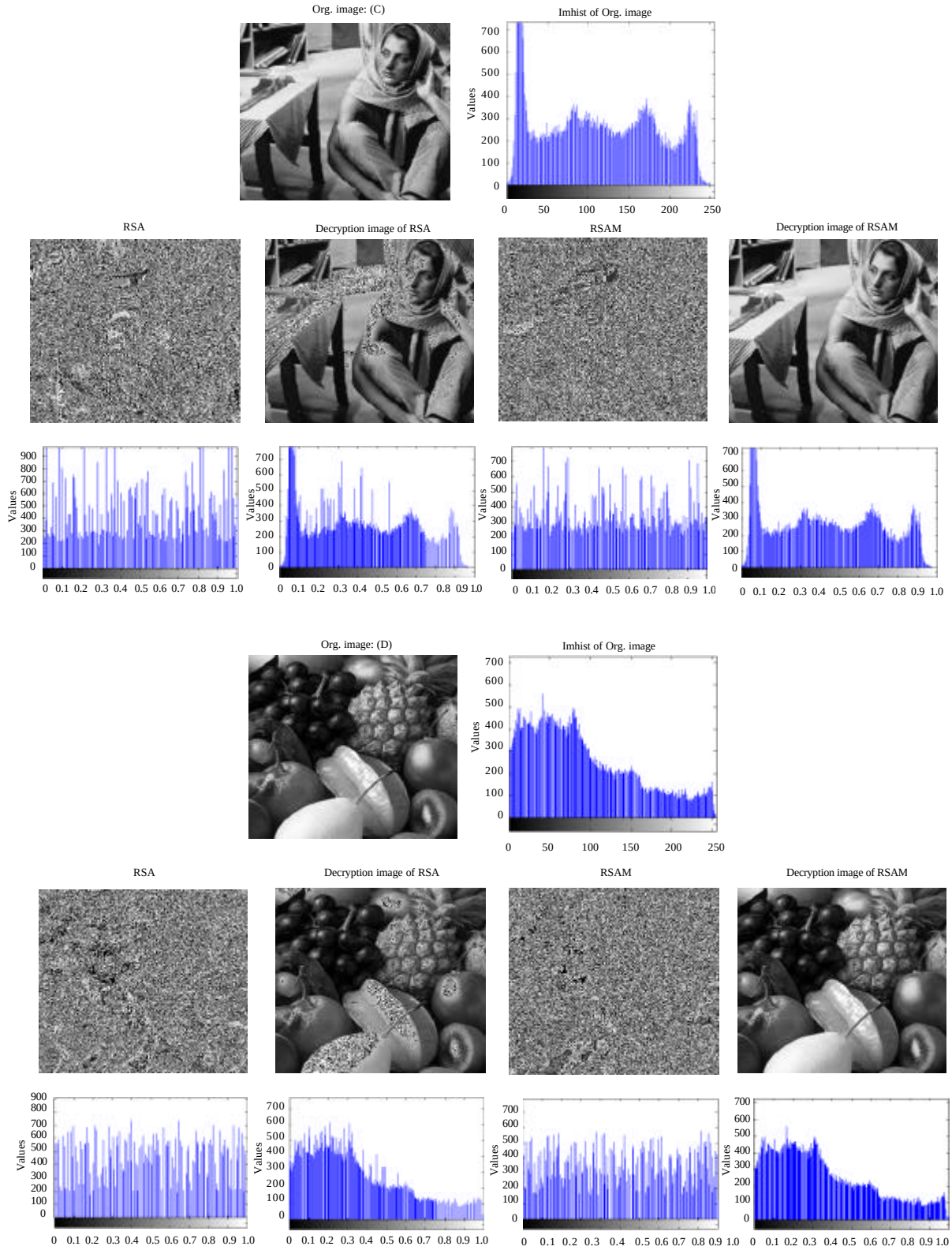

Fig. 1: The original image is shown with the coded images in the classical and modified methods with the histogram statement for each case

Table 3: The most important difference between the proposed system (RSAM) and the conventional system (RSA)

RSA	RSAM
Use pair keys for a cryptosystem	Use "k" keys for a cryptosystem
Less secure	More secure
Less vulnerable to brute force attack	More vulnerable to brute force attack
Consume less time	More consume time
Weak data integrity and retrieval	High data integrity and retrieval

modified method has a stronger algorithm than the traditional method because it uses to increase the numbers of keys while traditional RSA algorithm use pair of keys only as shown in Table 1, (SSIM) criterion of similarity shows a large difference between the original image and the encoded image of a proposed system far outweigh the traditional method as described Table 1.

In Table 2 also shows (PSNR) and (SSIM) between decrypted images by the RSA method and decrypted images by modified method (RSAM) for the original image and proves the efficiency of the proposed method, since, the (PSNR) of it equal to infinity because the difference between it and original image equal to zero and by equation no 1 appears that the inverse relation between PSNR and MSE and the congruence or the similarity between them (original and decrypted by RSAM images) is equal to the maximum value reached by this amount which is 1 and also mention general differences between the traditional method and modified according to the result obtained as shown in Table 3 (Sharma *et al*., 2012; Ayele and Sreenivasarao, 2013).

CONCLUSION

This study presents improved RSA image cryptosystem rely on multiple the keys of private and as well as the conformable public keys in order to increase the security and give more ability to defend against any attackers try to hacking cryptosystem in addition to provides high integrity of information when retrieved in decryption process but at the expense of time as the proposed system (RSAM) consumes more time than the conventional method known.

REFERENCES

Abudin, J., S.K. Keot, G. Malakar, N.M. Borah and M. Rahman, 2014. Modified RSA public key cryptosystem using two key pairs. Intl. J. Comput. Sci. Inf. Technol., 5: 3548-3550.

Ayele, A.A. and V. Sreenivasarao, 2013. A modified RSA encryption technique based on multiple public keys. Intl. J. Innovative Res. Comput. Commun. Eng., 1: 859-864.

Dhakar, R.S., A.K. Gupta and P. Sharma, 2012. Modified RSA Encryption Algorithm (MREA). Proceedings of the 2012 2nd International Conference on Advanced Computing and Communication Technologies (ACCT), January 7-8, 2012, IEEE, Rohtak, Haryana, India, ISBN:978-1-4673-0471-9, pp: 426-429.

Hassan, A.K.S., A.F. Shalash and N.F. Saudy, 2014. Modifications on RSA cryptosystem using genetic optimization. Intl. J. Res. Rev. Appl. Sci., 19: 150-155.

Hoffstein, J., J.C. Pipher, J.H. Silverman and J.H. Silverman, 2008. An Introduction to Mathematical Cryptography. Vol. 1, Springer, New York, USA., ISBN:978-0-387-77993-5, Pages: 426.

Hussain, A.K., 2015. A modified RSA algorithm for security enhancement and redundant messages elimination using K-Nearest neighbor algorithm. Intl. J. Innovative Sci. Eng. Technol., 2: 159-163.

Ivy, B.P.U., P. Mandiwa and M. Kumar, 2012. A modified RSA cryptosystem based on 'n' prime numbers. Int. J. Eng. Comput. Sci., 1: 63-66.

Milanov, E., 2009. The RSA algorithm. RSA Laboratories, Hebron, Connecticut. https://sites.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf

Patidar, R. and R. Bhartiya, 2013. Modified RSA cryptosystem based on offline storage and prime number. Proceedings of the 2013 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), December 26-28, 2013, IEEE, Enathi, India, ISBN:978-1-4799-1594-1, pp: 1-6.

Rosen, K.H., 2005. Elementary Number Theory and its Applications. 5th Edn., Addison Wesley, Boston, USA., ISBN:9780321237071, Pages: 721.

Sharma, S., J.S. Yadav and P. Sharma, 2012. Modified RSA public key cryptosystem using short range natural number algorithm. Intl. J. Adv. Res. Comput. Sci. Software Eng., 2: 134-138.

Srivastava, R. and O.P. Singh, 2015. Performance analysis of image encryption using block based technique. Intl. J. Adv. Res. Electr. Electron. Instrum. Eng., 4: 4266-4271.

Wang, Z., A.C. Bovik, H.R. Sheikh and E.P. Simoncelli, 2004. Image quality assessment: From error visibility to structural similarity. IEEE Trans. Image Process., 13: 600-612.