International Journal of Electrical and Computer Engineering (IJECE)
Vol. 12, No. 1, February 2022, pp. 1040~1047
ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp1040-1047

Asymmetric image encryption scheme based on Massey Omura scheme

Najlae Falah Hameed Al Saffar, Inaam R. Al-Saiq, Rewayda Razaq Mohsin Abo Alsabeh
Department of Mathematics, Faculty of Computer Science and Mathematic, University of Kufa, Najaf, Iraq

Article Info

Article history:

Received Feb 11, 2021
Revised Aug 4, 2021
Accepted Aug 21, 2021

Keywords:

Asymmetric key cryptosystem
Image encryption
Massey Omura cryptosystem
Mean square error
Peak signal to noise ratio
Unified average changing intensity

ABSTRACT

Asymmetric image encryption schemes have shown high resistance against modern cryptanalysis. Massey Omura scheme is one of the popular asymmetric key cryptosystems based on the hard mathematical problem which is discrete logarithm problem. This system is more secure and efficient since there is no exchange of keys during the protocols of encryption and decryption. Thus, this work tried to use this fact to propose a secure asymmetric image encryption scheme. In this scheme the sender and receiver agree on public parameters, then the scheme begin deal with image using Massey Omura scheme to encrypt it by the sender and then decrypted it by the receiver. The proposed scheme tested using peak signal to noise ratio, and unified average changing intensity to prove that it is fast and has high security.

Corresponding Author:

Najlae Falah Hameed Al Saffar
Department of Mathematics, Faculty of Computer Science and Mathematic, University of Kufa
Najaf, Iraq
Email: najlaa.hameed@uokufa.edu.iq

1. INTRODUCTION

Image encryption is the process of converting original image (plain image) to another form of image (cipher image), so that it will be readable to the authorized users only. Image encryption scheme determines how simple or complex the transformation process of the image, it provides confidentiality, integrity and authentication of the images transferred between the users. Cryptosystem technique is one of the common techniques used in securing data or messages by encoding the original message into other characters that can hide the pattern and meaning of the original message. There are two types of cryptosystem technique; symmetric and asymmetric key cryptosystem, the first one (also known as privet key cryptosystem) used the same key for the encryption and decryption process, these keys should be kept secretly between the two parties. The second type (also known as public key cryptosystem) there are two different keys, one of them used in the encryption process, the other used in the decryption process. Massey Omura scheme is one of the asymmetric key cryptosystems, where the key used in the encryption process is different with the key used in the decryption process. The Massey Omura scheme is an asymmetric key cryptosystem that will be the focus of this paper. It was introduced in 1983 by Massey and Omura [1], it is an encryption scheme based on three stages encryption protocol from the improvement of Shamir three pass protocol [2], [3] where the key used in the encryption or decryption process is generated by the sender and receiver based on a mutually agreed value. The hardness of solving the discrete logarithm problem from the adversaries is one of the Massey Omura scheme advantages. In other word, the security of Massey Omura scheme based on solving the discrete logarithm problem.

A little bit of researchers tried to develop or use Massey Omura scheme to be more efficient or to construct new system respectively. For both cases the purpose of their work is to improve its security.

Koblitz [4] in 1987 presented a discussion for elliptic curve analog of the Massey Omura scheme, the security of this system based on solving the elliptic curve discrete logarithm problem which is harder than classical discrete logarithm problem. Winton [5] in 2007 enhanced Massey Omura scheme by introducing two versions. The first version came with replacing the prime modulus with a composite number to be with a same level of security of Rivest–Shamir–Adleman (RSA) scheme. The second version added a digital signature to the first version, which provided an additional aspect of security. In 2012, Winton [6] introduce a three pass system which is hybrid system between symmetric and asymmetric key cryptosystem more secure than both of symmetric and asymmetric. This system based on the two versions that mentioned in [5]. In 2018 Massey Omura scheme was involved in chat application [7], this implementation was very effective to secure the data this due to the encryption applied layered. Another work involved Massey Omura scheme in 2018, Haley [8] replaced cyclic group in a finite field that use in the original Massey Omura scheme with a non abelian group, the purpose of this work is to make the scheme harder to break. In 2019 Massey Omura scheme was a tool to analysis the security of three pass protocols, where the value of the mean squared error (MSE) and the peak signal to noise ratio (PSNR) was zero and infinite respectively, which means, the scheme can maintain data integrity [9]. The latest work where the Massey Omura scheme was involved was in 2021, Massey Omura protocol was a tool together with Vernam cipher [10] to do implementations for three methods for number generation [11]. Actually, no work for involving Massey Omura scheme with image encryption.

This work describes how to use the Massey Omura scheme to encrypt image where the three pass protocols in this scheme can maintain the security of keys used both in the process of encryption and decryption images. Implementation of this proposed scheme is expected to minimize the misuse of images that have been distributed by parties who are not given access. The new scheme will be implemented and tested on the gray images. The efficiency and performance of the new scheme will be assessed by using some security measures like MSE, PSNR, and unified average changing intensity (UACI). Matrix laboratory (MATLAB) R2014a (8.3.0.532) 32-bit software on a workstation Intel® Core™ i3 with CPU 2.13 GHz and RAM 4 GB with Microsoft Windows 7 as an operating system will be used for encryption and decryption processes.

This paper is coordinated as follows: Image encryption is presented in section 2. Section 3 describes the Massey Omura scheme. Section 4 explains the proposed image encryption scheme. An implementation example of the proposed scheme will introduce in section 5. Section 6 will contain the security analysis for some measures MSE, PSNR, and UACI, the conclusion and future works of the proposed scheme are displayed in section 6.

2. IMAGE ENCRYPTION

A gray image can be expressed as a matrix of dimension $n \times m$, all inputs values are in $[0, 255]$. Nowadays, images are transferred everyday across the network. Some of these images are confidential and they require to be transferred securely. Recently, many image encryption techniques have been proposed to verify interactive media data before transmission over insecure channels. We will list the most recent ones; in 2018 and 2020, [12] and [13] respectively have been are involved Hill [14] and Elliptic Curve cryptosystem [4], [15] in technique to encrypt and decrypt, they have been proved that it was more hard for the interloper attackers Wang and Tu [16] in 2020, involved concepts of chaotic system [17] to do encryption for medical image, they protected them in the process of transmission and utilization. Concepts of chaotic system was also involved in image encryption in 2020 [18], image encryption was applied with numbers were generated in LabVIEW software [19], Depending on the metrics used, the proposed method was acceptable. Yanhong Wei [20] in the same year used concepts of chaotic system to propose a scheme for image encryption, it was simple, easy to program and implement. Private key and segment map table was involved in 2020 [21] to encrypt and decrypt a color image, it was simple and highly secure method according to the time of execution. Matrix semi tensor product with a compound secret key was a base for an algorithm of a chaotic image encryption in 2020, they proved that the proposed algorithm is secure and effective and can use for a color image [22]. Image encryption has been implementing for fractional-order of dimension three in 2020, where the proposed algorithm was effective according to the security analysis [23]. Finally, elliptic curves were a tool to construct an asymmetric image encryption scheme in 2021 in two different works [24], [25], they were fast and secure in term of generating points on an elliptic curve. In the same year (2021), an approach of image encryption based the time delay of chaotic system has been proposed [26], where they proposed a type of time delay chaotic system to achieve the purpose of the image encryption. A high-speed image encryption has been proposed as an implementation also in 2021, where chaotic map has been involved, they propose a new fractional with one dimension chaotic map in a large chaotic space [27]. In this work, asymmetric image encryption scheme will propose based Massey Omura scheme.

3. MASSEY OMURA SCHEME

Massey Omura scheme is an exponential based cryptosystem by Messey and Omura [1] in 1983. It was based on three pass protocols. The advantage of this cryptosystem is not it is necessary to distribute and exchange keys between the two communicating parties, this mean Massey Omura scheme allows two users (sender and receiver) which do not share their private keys to exchange their information over insecure channel. Massey Omura scheme in brief is as follows: If the sender (Part A) wants to send a message M to the receiver (Part B) using Massey Omura scheme, they must agree with a trusted party on prime p and a prime field F_p. Part A encrypts M with his key (say $e_A \in (0, p-1)$, with $\gcd(e_A, p-1) = 1$) and sends the result (M^{e_A}) to Part B; B encrypts what he has received with his key (say $e_B \in (0, p-1)$, with $\gcd(e_B, p-1) = 1$) and sends the new result ($M^{e_A e_B}$) back A. Now, A decrypts B's response by computing $M^{e_A e_B d_A} = M^{e_B}$ where $d_A = d_A^{-1} \bmod (p-1)$ and sends the result (M^{e_B}) to B. Finally, B will get the message by computing $M^{e_B d_B} = M$ where $d_B = d_B^{-1} \bmod (p-1)$. The Massey Omura scheme is summarized in Figure 1.

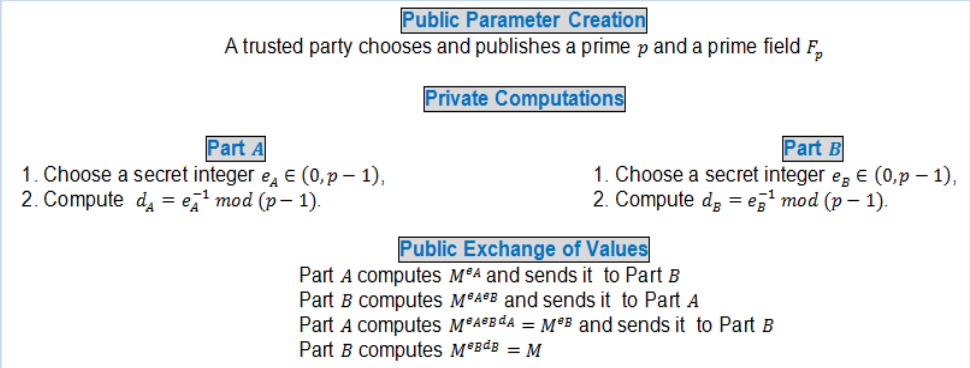


Figure 1. Massey Omura scheme

4. PROPOSED IMAGE ENCRYPTION SCHEME

A new proposed scheme for image encryption based on Massey Omura scheme has been introduced in this section. This scheme increases the security and makes the system more efficient than the original Massey Omura scheme. This scheme can be in brief as follows: if the sender (Part A) wants to send an image $\text{plain}_{\text{image}}$ to the receiver (Part B) using the proposed scheme, they must agree with a trusted party on prime p and a prime field F_p. When we trying to deal with the $\text{plain}_{\text{image}}$ we have to convert this image to matrix-in this work we will consider gray image-the maximum value of the generating matrix will be 255. So, as not to lose the features of the original image, the prime p have to be more than 255. So, as Massey Omura scheme as shown in Figure 1 choosing the prime p is followed by choosing e_A, e_B and calculation d_A, d_B by Part A and Part B respectively. The proposed scheme will illustrate in the following steps:

Step 1 : Part A selects the $\text{plain}_{\text{image}}$, then represent is as a matrix of pixels (denoted by M).
Step 2 : Then he detriments the size of new matrix as $M_{n \times m}$.
Step 3 : Part A computes M^{e_A} and sends it as an encrypted image for the first round (denoted by encrypted I_{image}) to Part B.
Step 4 : Part B computes $M^{e_A e_B}$ and sends it as an encrypted image for the second round (denoted by encrypted II_{image}) to Part A.
Step 5 : Part A computes $M^{e_A e_B d_A} = M^{e_B}$ and sends it as an encrypted image for the third round (denoted by encrypted III_{image}) to Part B.
Step 6 : Part B computes $M^{e_B d_B} = M$ which is the corresponding matrix of the $\text{decrypted}_{\text{image}}$.

5. IMPLEMENTATION EXAMPLE

Assume that Part A wants to send an image (mandrill.png) which is a $\text{plain}_{\text{image}}$ with size 161×164 to Part B using the proposed scheme, they must agree with a trusted party on prime $p = 257 > 255$, and a prime field F_{257}. Both of two users have to chooses and compute their keys ($e_A = 223, e_B = 141$ and $d_A = 31, d_B = 69$) respectively as Figure 1. Now the processing of the example will be as follows:

Part A represents the $\text{plain}_{\text{image}}$ image as a matrix M as:

$$M=\begin{bmatrix} 83 & 111 & 103 & 76 & \cdots \\ 95 & 131 & 109 & 94 & \cdots \\ 50 & 75 & 58 & 85 & \cdots \\ 50 & 75 & 58 & 85 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}_{161\times164}$$

So, he will do the first round of the proposed scheme by computing a matrix M^{e_A} as:

$$M^{e_A}=\begin{bmatrix} 83^{223}\bmod257\equiv233 & 111^{223}\bmod257\equiv213 & 103^{223}\bmod257\equiv237 & 76^{223}\bmod257\equiv230 & \cdots \\ 95^{223}\bmod257\equiv211 & 131^{223}\bmod257\equiv77 & 109^{223}\bmod257\equiv56 & 94^{223}\bmod257\equiv93 & \cdots \\ 50^{223}\bmod257\equiv195 & 75^{223}\bmod257\equiv251 & 58^{223}\bmod257\equiv239 & 85^{223}\bmod257\equiv161 & \cdots \\ 50^{223}\bmod257\equiv195 & 75^{223}\bmod257\equiv251 & 58^{223}\bmod257\equiv239 & 85^{223}\bmod257\equiv161 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}_{161\times164}$$

Then represents it as encrypted I_{image} and sends it to Part B. Part B computes $M^{e_Ae_B}$ after convert the received image to matrix as:

$$M^{e_Ae_B}=\begin{bmatrix} 233^{141}\bmod257\equiv181 & 213^{141}\bmod257\equiv88 & 237^{141}\bmod257\equiv147 & 230^{141}\bmod257\equiv160 & \cdots \\ 211^{141}\bmod257\equiv146 & 77^{141}\bmod257\equiv33 & 56^{141}\bmod257\equiv192 & 93^{141}\bmod257\equiv194 & \cdots \\ 195^{141}\bmod257\equiv135 & 251^{141}\bmod257\equiv19 & 239^{141}\bmod257\equiv196 & 161^{141}\bmod257\equiv47 & \cdots \\ 195^{141}\bmod257\equiv135 & 251^{141}\bmod257\equiv19 & 239^{141}\bmod257\equiv196 & 161^{141}\bmod257\equiv47 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}_{161\times164}$$

and sends it as an encrypted image for the second round (denoted by encrypted II_{image}) to Part A. Part A computes $M^{e_Ae_Bd_A}$ after convert the encrypted II_{image} to matrix as:

$$M^{e_Ae_Bd_A}=\begin{bmatrix} 181^{31}\bmod257\equiv82 & 88^{31}\bmod257\equiv73 & 147^{31}\bmod257\equiv82 & 160^{31}\bmod257\equiv212 & \cdots \\ 146^{31}\bmod257\equiv44 & 33^{31}\bmod257\equiv37 & 192^{31}\bmod257\equiv86 & 194^{31}\bmod257\equiv151 & \cdots \\ 135^{31}\bmod257\equiv215 & 19^{31}\bmod257\equiv186 & 196^{31}\bmod257\equiv173 & 47^{31}\bmod257\equiv108 & \cdots \\ 135^{31}\bmod257\equiv215 & 19^{31}\bmod257\equiv186 & 196^{31}\bmod257\equiv173 & 47^{31}\bmod257\equiv108 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}_{161\times164}$$

and sends it as an encrypted image for the third round (denoted by encrypted III_{image}) to Part B. Finally, Part B will be able to see the $plain_{image}$, by converting the encrypted III_{image} to matrix and computing $M^{e_Ae_Bd_Ad_B}$ as:

$$M^{e_Ae_Bd_A}=\begin{bmatrix} 82^{69}\bmod257\equiv83 & 73^{69}\bmod257\equiv111 & 82^{69}\bmod257\equiv103 & 212^{69}\bmod257\equiv76 & \cdots \\ 44^{69}\bmod257\equiv95 & 37^{69}\bmod257\equiv131 & 86^{69}\bmod257\equiv109 & 151^{69}\bmod257\equiv94 & \cdots \\ 215^{69}\bmod257\equiv50 & 186^{69}\bmod257\equiv75 & 173^{69}\bmod257\equiv58 & 108^{69}\bmod257\equiv85 & \cdots \\ 215^{69}\bmod257\equiv50 & 186^{69}\bmod257\equiv75 & 173^{69}\bmod257\equiv58 & 108^{69}\bmod257\equiv85 & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{bmatrix}_{161\times164}$$

It is $decrypted_{image}$. Figure 2 will summarize the output of execution of this example. Different gray images with 256×256 as their sizes are used to implement the proposed scheme. Table 1 summarizes their execution.

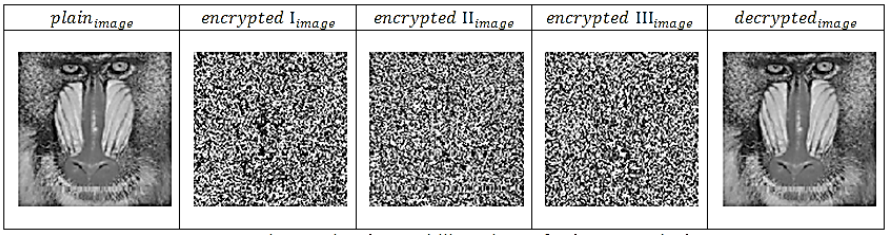
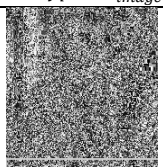
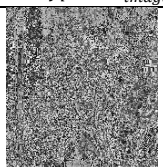
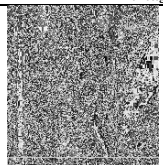
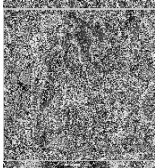
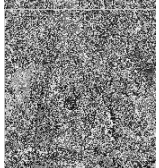
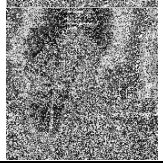
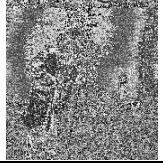
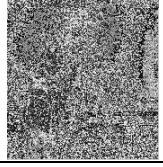


Figure 2. Implementation the mandrill.png image for the proposed scheme

Table 1. Execution the proposed scheme using different gray images

Image Name	$plain_{image}$	$encrypted\ \mathrm{I}_{image}$	$encrypted\ \mathrm{II}_{image}$	$encrypted\ \mathrm{III}_{image}$	$decrypted_{image}$
Lena					
Peppers					
Cameraman					

6. SECURITY ANALYSIS

Security performance of the proposed scheme is analyzed by calculating MSE, PSNR, and UACI, these measures are utilized to evaluate gray image that has been encrypted and compare it with the original image. The results will be an excellent indicator to measure the efficiency of the proposed scheme and evaluate the ability of the proposed scheme to resist statistical attacks. Mean square error and peak signal to noise ratio: MSE and peak signal-to-noise ratio (PSNR) [28] are tools to check the data integrity. So MSE and PSNR will be used to evaluate the quality of plain image with respect to the encrypted images. The equation of the PSNR is as: $\mathrm{PSNR} = 10\log_{10}\frac{255\cdot 255}{\mathrm{MSE}}$ where $\mathrm{MSE} = \frac{1}{\mathrm{m}*\mathrm{n}}\sum_{\mathrm{i}=1}^{\mathrm{m}}\sum_{\mathrm{j}=1}^{\mathrm{n}}(\mathrm{X}(\mathrm{i},\mathrm{j}) - \mathrm{Y}(\mathrm{i},\mathrm{j}))^2$, $\mathrm{X}(\mathrm{i},\mathrm{j})$ and $\mathrm{Y}(\mathrm{i},\mathrm{j})$ are the pixel value of encrypted image and original image respectively both have size $\mathrm{m}\times\mathrm{n}$. Obviously, that calculating the MSE will affect the value of PSNR, if PSNR is decreasing means that the MSE is increasing this fact in term of the processing of image encryption, in other words the high value of MSE and low value of PSNR indicates that the two images are totally different, and this leads to the efficiency of the proposed scheme.

In this work we get 12002.3 and 7.36791 as an average value of the values of the MSE and PSNR respectively of the $\mathrm{encrypted\ I}_{\mathrm{image}}$, $\mathrm{encrypted\ II}_{\mathrm{image}}$ and $\mathrm{encrypted\ III}_{\mathrm{image}}$ with respect to the $\mathrm{plain}_{\mathrm{image}}$ which is Lena, it is so hard for an attacker to recover the plain image. Unified average changing intensity (UACI): It is one of differential analyses used to evaluate the strength of image encryption, where it is estimated the contrast between the encrypted image and plain image [13]. The highest value of the UACI (approximately 33.46%) implies that the proposed procedure is safe against differential assaults. The equation of the UACI is as: $\mathrm{UACI} = \frac{1}{256*256}\sum_{\mathrm{i}=1}^{256}\sum_{\mathrm{j}=1}^{256}\frac{\mathrm{X}(\mathrm{i},\mathrm{j})-\mathrm{Y}(\mathrm{i},\mathrm{j})}{255}\cdot 100\%$, $\mathrm{X}(\mathrm{i},\mathrm{j})$ and $\mathrm{Y}(\mathrm{i},\mathrm{j})$ are the pixel value of plain image and decrypted image respectively. In this work we get 33.47067 as an average value of the values of the UACI of the $\mathrm{encrypted\ I}_{\mathrm{image}}$, $\mathrm{encrypted\ II}_{\mathrm{image}}$ and $\mathrm{encrypted\ III}_{\mathrm{image}}$ with respect to the $\mathrm{plain}_{\mathrm{image}}$ which is Lena, it is so hard for an attacker to recover the plain image.

According to Table 2 the MSE, PSNR and UACI as an average value of the values of the MSE, PSNR, and UACI of the $\mathrm{encrypted\ I}_{\mathrm{image}}$, $\mathrm{encrypted\ II}_{\mathrm{image}}$ and $\mathrm{encrypted\ III}_{\mathrm{image}}$ with respect to the $\mathrm{plain}_{\mathrm{image}}$ that have been tested. The values of PSNR were very low while the values of MSE were very high and this means that the proposed scheme is efficient. The values of UACI for tested images were much closed to the expected value 33.46 and this demonstrates the strength of the proposed scheme against the attackers. Indeed, these results pointed that the encrypted images hardly be perceived, and this leads to an efficient encryption technique. A comparison of the proposed scheme and some other recently algorithms over security measures for different gray image with size 256×256 are shown in Table 3. It is clear that the MSE in the proposed scheme is higher than [12], [13], [23] schemes. PSNR and UACI values in the proposed scheme are also much better than other existing work. As a result, it can be concluding that the proposed scheme is more efficient than the other schemes.

Finally, Table 4 summarized the time consumed in encryption and decryption processes over the four gray images-that considered in this work. Time of execution all steps of the proposed scheme considered as measuring the efficiency of this scheme, Table 2 shows that the proposed scheme needs very the low time for execution. Again, this work is time efficient.

Table 2. The performance of the proposed scheme using various security measures for different gray image with size 256×256

$plain_{image}$ Name	Measures	$encrypted$ I_{image}	$encrypted$ II_{image}	$encrypted$ III_{image}	Average	$decrypted_{image}$
Lena	MSE	10167.8	12876.7	12962.4	12002.3	0
	PSNR	8.06704	7.03275	7.00394	7.36791	Inf
	UACI	32.5566	33.9044	33.951	33.47067	0
Peppers	MSE	10942.3	11997.9	13125.5	12021.9	0
	PSNR	7.73971	7.33975	6.94964	7.343033	Inf
	UACI	32.5755	33.7086	33.9099	33.398	0
Cameraman	MSE	12947.9	13296.3	13562.7	13268.97	0
	PSNR	7.00881	6.89349	6.80734	6.903213	Inf
	UACI	32.9009	33.9278	34.5693	33.79933	0
Mandrill	MSE	7490.3	7089.2	8865.9	7815.133	0
	PSNR	9.38581	9.62483	8.65357	9.221403	Inf
	UACI	31.7739	32.6801	32.9567	32.47023	0

Table 3. Comparison of the proposed scheme with other methods over security measures for different gray image with size 256×256

Schemes	$plain_{image}$ Name	MSE	PSNR	UACI
This Study	Lena	12002.3	7.36791	33.47067
	Peppers	12021.9	7.343033	33.398
	Cameraman	13268.97	6.903213	33.79933
	Mandrill	7815.133	9.221403	32.47023
Dawahdeh [12]	Lena	8985.8	8.5952	30.3842
	Peppers	–	–	–
	Cameraman	12974	6.9999	35.5263
	Mandrill	6934.2	9.7208	27.3588
Rajvir [13]	Lena	11015.636	7.7107	33.5844
	Peppers (Red Stream)	11720.228	7.4414	34.6475
	Cameraman	–	–	–
	Mandrill	6949.448	9.7113	27.3642
Obaid [23]	Lena	7640.4	9.2996	28.1854
	Peppers	–	–	–
	Cameraman	8167.8	9.0097	26.9897
	Mandrill	6806.6	9.8015	27.0906

Table 4. Encryption and decryption time for the proposed scheme for different gray image with size 256×256

$plain_{image}$ Name	Encryption/ and Decryption time in seconds
Lena	2.746180
Peppers	2.277766
Cameraman	2.262432
Mandrill	2.319871

7. CONCLUSION AND FUTURE WORKS

Recently the information security considered as the most important issues in the world. Massey Omura scheme considered as an asymmetric key cryptosystem based on the difficulty of solving the discrete logarithmic problem, where it is considered as one of the advantages of using the Massey Omura scheme. Asymmetric key cryptosystem has been proposed in this paper using the standard Massey Omura scheme to improve and raise the security of the original Massey Omura scheme for image encryption. A good result displayed at Table 2 for four gray images with size 256×256, and this supports the efficiency of the proposed scheme. Table 3 indicates that the proposed scheme on the same four gray images gives good results for MSE, PSNR, and UACI better than other existing schemes. The MSE values in the proposed scheme were higher than the other existing schemes. PSNR values were lower than the others which is mean that it is better in the proposed scheme than the referred schemes. Also, UACI values were nearest to 33.46 which is the expected value. Table 4 indicates the little execution time in the encryption and decryption processes, and this also indicates that the proposed scheme need not a long time in its computations. This work offered here can be subject to future studies, colored images can be used to a modification of the proposed scheme. Due to modest of it structure and quicker of its calculations, this work it can be a new line to implement the proposed scheme in wireless applications.

REFERENCES

[1] J. L. Massey and J. K. Omura, "A new multiplicative algorithm over finite fields and its applicability in public key cryptography," EUROCRYPT'83 Udine, Italy, 1983.
[2] A. G. Konheim, "Cryptography, a primer," John Wiley and Sons, 1981.
[3] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone, "Handbook of applied cryptography," CRC press, 2018.
[4] N. Koblitz, "Elliptic curve cryptosystems," *Mathematics of computation*, vol. 48, pp. 203-209, 1987, doi: 10.1090/S0025-5718-1987-0866109-5.
[5] R. Winton, "Enhancing the massey–omura cryptosystem," *Journal of Mathematical Sciences and Mathematics Education*, vol. 2, no. 1, pp. 21-29, 2007.
[6] R. Winton, "Combining public and private key cryptography," *Journal of Mathematical Sciences and Mathematics Education*, vol. 7, no. 1, pp. 1–10, 2012.
[7] T. Zebua, R. K. Hondro, and E. Ndruru, "Message security on chat app based on massey omura algorithm," *International Journal of Information System and Technology*, vol. 1, no. 2, 2018, doi: 10.30645/ijistech.v1i2.11.
[8] S. Haley, "Non-commutative massey-omura encryption with symmetric groups," Student Research Submissions, 2018.
[9] D. Rachmawati, M. A. Budiman, and M. A. Rikzan, "Analysis of file security with three-pass protocol scheme using massey-omura algorithm in android," *Journal of Physics Conference Series*, vol. 1235, 2019, doi: 10.1088/1742-6596/1235/1/012075.
[10] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraphic communications," in *Transactions of the American Institute of Electrical Engineers*, vol. XLV, pp. 295-301, 1926, doi: 10.1109/T-AIEE.1926.5061224.
[11] V. Manjunatha, A. Rao, and A. Khan, "Complex key generation with secured seed exchange for Vernam cipher in security applications," *Materials Today: Proceedings*, vol. 35, part 3, pp. 497-500, 2021, doi: 10.1016/j.matpr.2020.03.132.
[12] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349-355, 2018, doi: 10.1016/j.jksuci.2017.06.004.
[13] C. Rajvir, S. Satapathy, R. Soundrapandiyan, and R. Lakshmanan, "Image encryption using modified elliptic curve cryptography and hill cipher," *Smart Intelligent Computing and Applications*, pp. 675-683, 2020, doi: 10.1007/978-981-13-9282-5_64.
[14] L. S, Hill, "Cryptography in an algebraic alphabet," *The American Mathematical Monthly*, vol. 36, no. 6, pp. 306-312, 1929, doi: 10.1080/00029890.1929.11986963.
[15] V. S. Miller, "Use of elliptic curves in cryptography," *Conference on the theory and application of cryptographic techniques*, 1985, pp. 417-426.
[16] X. Wang and C. Tu, "A chaos-based medical image encryption method," *Indonesian Journal of Electrical Engineering and Computer Science (IJEECS)*, vol. 19, no. 3, pp. 1316-1324, 2020, doi: 10.11591/ijeecs.v19.i3.pp1316-1324.
[17] L. M. Pecora, T. L. Carroll, G. A. Johnson, and D. J. Mar, "Fundamentals of synchronization in chaotic systems, concepts, and applications," *Chaos: An Interdisciplinary Journal of Nonlinear Science*, vol. 7, no. 4, pp. 520-543, 1997, doi: 10.1063/1.166278.
[18] B. Gürevin, M. Yıldız, E. Güleryüz, M. Kutlu, and O. Sorgun, "A chaos-based image encryption on LabVIEW," *Chaos Theory and Applications in Applied Sciences and Engineering*, vol. 2, no. 2, pp. 69-76, 2020.
[19] T. Jeffrey and J, Kring, "LabVIEW for everyone: graphical programming made easy and fun," Prentice Hall PTR, 2006.
[20] Y. Wei, "Application of chaos theory in image encryption," *IOP Conference Series: Materials Science and Engineering*, vol. 750, no. 1, 2020, doi: 10.1088/1757-899X/750/1/012197.
[21] M. Khrisat, Khawatreh, O. Majed, A. Dwairi, A. Hindi, and Z. alqadi, "Color image encryption-decryption using SMT," *International Journal of Engineering Technology Research and Management*, vol. 4, no. 5, pp. 32-40, 2020.
[22] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Information Sciences*, vol. 539, no. 9, 2020, doi: 10.1016/j.ins.2020.06.030.
[23] L. Chen, H. Yin, T. Huang, L. Yuan, S. Zheng, and L. Yin, "Chaos in fractional-order discrete neural networks with application to image encryption," *Neural Networks*, vol. 125, pp. 174-184, 2020, doi: 10.1016/j.neunet.2020.02.008.
[24] N. A. Azam, I. Ullah, and U. Hayat, "A fast and secure public-key image encryption scheme based on Mordell elliptic curves," *Optics and Lasers in Engineering*, vol. 137, pp.106371, 2021, doi: 10.1016/j.optlaseng.2020.106371.
[25] Z. K. Obaid and N. F. H. Al Saffar, "Image encryption based on elliptic curve cryptosystem," *International Journal of Electrical and Computer Engineering (IJECE)*, vol. 11, no. 2, pp. 1293-1302, 2021, doi: 10.11591/ijece.v11i2.pp1293-1302.
[26] B. Wang, B. F. Zhang, and X. W. Liu, "An image encryption approach on the basis of a time delay chaotic system," *Optik*, vol. 225, 2021, doi: 10.1016/j.ijleo.2020.165737.
[27] M. Z. and X. Wang, "A new fractional one-dimensional chaotic map and its application in high-speed image encryption," *Information Sciences*, vol. 550, pp. 13-26, 2021, doi: 10.1016/j.ins.2020.10.048.
[28] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR–a comparative study," *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8-18, 2019, doi: 10.4236/jcc.2019.73002.

BIOGRAPHIES OF AUTHORS

Najlae Falah Hameed Al Saffar received her B.Sc. degree from Kufa University-Iraq, in 1999 and M.Sc. Degree from Babylon University-Iraq in 2005. She obtained Ph.D. in Mathematical Cryptography UPM University-Malaysia in 2015. She is serving as Assistant Professor, Department of Mathematics, Faculty of Computer Science & Mathematics University of Kufa Iraq. She has published more than 16 papers in International and National journals and conference proceedings. Her research interests are number theory, cryptography, and their applications also security and algebraic number field. She can be contacted at email: najlaa.hameed@uokufa.edu.iq.

Inaam R. Al-Saiq received her B.Sc. degree from the University of Mustansiriya Iraq, in 1993 and Msc. Degree from the University of Mustansiriya Iraq in 2000. She is serving as Assistant Professor, Department of Mathematics, Faculty of Computer Science & Mathematics University of Kufa Iraq. She has published more than 10 papers in International and National journals. Her research interests are numerical analysis, ordinary differential equations, cryptography and the application of numerical analysis in cryptography and image processing. She can be contacted at email: anaamr.jabr@uokufa.edu.iq.

Rewayda Razaq Mohsin Abo Alsabeh received her B.Sc. degree from Al Mustansiriya University Iraq, in 1993 and MSc. Degree from Al Mustansiriya University Iraq in 2000. She obtained Ph.D. in Mathematics from University of Essex in 2017. She is serving as Assistant Professor, Department of Mathematics, Faculty of Computer Science and Mathematics University of Kufa/Iraq. She has published more than 12 papers in International and National journals and conference proceedings. Her research interests are operations research, functional analysis and applied mathematics. She can be contacted at email: ruwaida.mohsin@uokufa.edu.iq.