

Image Cryptography with Least Squares Approximations

¹Mustafa K. Ramadhan and ²Adil AL-Rammahi

¹Department of Computer Techniques Engineering, Al-Safwa College University, Iraq

²Department of Mathematics, Faculty of Mathematics and Computer Science, University of Kufa, Iraq

Article history

Received: 22-08-2019

Revised: 12-10-2019

Accepted: 19-11-2019

Corresponding Authors

Adil AL-Rammahi

Department of Mathematics,
Faculty of Mathematics and
Computer Science, University
of Kufa, Iraq

Email: adil.m.hasan@uokufa.edu.iq

Abstract: Security of digital images has become one of the most important issues in network technologies. Different techniques have been evolved over the past few years to provide security for digital images through concealing information, image scrambling and image encryption. The aim of this work is to enhance the network security level by using the cryptographic method based on the Least Square Approximation technique (LSA). This work is one of the first attempts due to the use of the least squares polynomial of fifth degree technique as data interpolation in the image cryptography process. It has been proven in this study that a high level of correlation exists amongst the original and the corresponding decrypted images. The achieved high values of the measured Peak Signal to Noise Ratio (PSNR) for the decrypted images in this study are an indication to the high accuracy of the proposed technique in comparison to other cryptographic techniques. The output of the encrypted technique in this study reveals its reliability and robustness against security attacks.

Keywords: Index Terms-Image Encryption, Least Squares Approximations, Peak Signal to Noise Ratio, Coefficient Correlations

Introduction

Information security is an increasingly important concern in the social networking era. Cryptography plays a crucial role in different popular applications of multimedia technology such as smart phones communications, electronic commerce, exchange of private emails, ATM security, transmitting financial information, etc. Cryptography can be described as a process of converting particular data into unreadable format for secure electronic transmitting and then retransforming it back to its original form. Different encryption methods have been proposed to protect the confidential data from unauthorized use such as discrete logarithm (Odlyzko, 2000), Rivest-Shamir-Adleman (RSA) public key (Rivest *et al.*, 1970), knapsack (Merkle and Hellman 1978) and the alike. Those techniques depended on the Galio field construction technique which is considered a difficult one to employ (Merkle and Hellman, 2017). They are based on highly complicated concepts represented in algebra modular, prime number, operators, vector spaces and orthogonal basis. To overcome those difficulties and complexities, different methods have been introduced, such as a hybrid chaotic map for image encryption and hiding problems. In that method, the ciphered image is embedded into several carrier images

(Cao, 2013). Based on the composition of the three classic chaotic maps: The logistic map, the Henon map and the Ikeda map, the hybrid chaotic map demonstrates a more complex chaotic characteristic than that of the single chaotic maps. Younes and Jantan presented a block-based transformation algorithm. They combined the process of image transformations and the well known Blowfish encryption and decryption algorithm (Younes and Jantan, 2008). That technique introduced lower correlations and higher entropies due to the increase in the number of blocks owing to the use of smaller block sizes. El Abbadi *et al.* (2014) introduced an image encryption using the Singular Values Decomposition (SVD). Elabbadi utilised the spectral diagonal matrices of two images to produce a new third one. Al-Rammahi (2015) used mutual two images for crypto one image via SVD technique. Mutual singular value decomposition approach can perform well with simple images, but it is not an appropriate method to be employed with complex images due to the simplicity of the SVD method. To overcome the associated drawbacks with that method, (Al-Rammahi, 2014a; 2014b) proposed another two methods for image encryption/decryption operation, see. However, limitations still associated with those two methods when they were applied to the very complex digital images.

Several other methods based on Least Squares Approximation (LSA) have also been developed to overcome the complexities associated with the aforementioned methods, such as, (Elrabeay *et al.*, 2012) technique that is based on the LA interpolation of fused MR. A major drawback of that technique is represented by giving a large number of coefficients in all scales corresponding to the edges of the image. Divya also introduced a method using a least-squares interpolation step. In that method, the image encryption operation was carried out by breaking down the image into 8x8 blocks. Then, domain transformation have been applied to those blocks from the spatial to the frequency domain using the Discrete Cosine Transformation (DCT) method (Divya *et al.*, 2012). The drawback of this method is limited to the homogeneous images. Kekre *et al.* (2014) proposed a hybrid method to secure digital images. The basis of Kekre's method was a combination of hiding information and image encryption processes. Kekre employed four different algorithms based on Least Significant Bit (LSB) for hiding information process. Kekre's technique showed low quality in the decryption process when it was applied to complex images. Al-khassaweneh and Aviyente (2008) proposed an encryption/decryption image technique based on the first-degree polynomial interpolation LSA. In this technique, the original images are encrypted using randomly generated method. In the decrypted stage, the LSA method is utilised to decrypt the encrypted images. The major problem with Al-khassaweneh's technique is the sensitivity to the effect of the outliers. In addition to that, there was no information provided about the coefficient Correlations (COR) and PSNR of the examined images. Shreef and Hoomod (2013) utilized technique based on first-degree LS interpolation method for image encryption. Shreef's technique does not take into account the variances of the observations due to the sensitivity to the effect of the outliers.

In this study we are addressing these problems, including the sensitivity to the effect of outliers, by using a robust and highly accurate technique based on the LSA method. This method interpolates all mesh points when the number of mesh points is equal to the degree of the LSA. The performance of the proposed method in this study is compared to the performances of the introduced methods by both Al-khassaweneh and Shreef. The newly employed technique in this study has been proven more efficient than other previously introduced techniques due to its encryption/decryption accuracy.

The rest of this paper is organised as follows: Section 2 presents a brief description about the least squares method. Section 3 demonstrates some information about the proposed cipher method using least squares interpolation. The statistical analysis and discussion are presented in section 4. Section 5 outlines the conclusions from this work.

Least Squares Method

A Least Squares (LS) method is introduced as a statistical technique to find the best fit line for a model. It is used to examine the nature of the relationship between any two variables. This idea can be achieved by determining an approximate solution to a system of linear equations with no exact solution. The concept of LS is to find the best fit that is a straight line $y = ax + b$ by measuring the values of y for given values of x . Suppose n points have been given where (Kolman, 1993): $(x_1, y_1), (x_2, y_2), \dots, (x_n, y_n)$ with $x_1 < x_2 < \dots < x_n$. The polynomial $y = b_0 + b_1x + b_2x^2 + \dots + b_mx^m$ of degree m represents the best fit for the given data points. To determine the values of the constants $b_0, b_1, b_2, \dots, b_m$, the y polynomial can be formatted as follows:

$$y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{bmatrix}, b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}, A = \begin{bmatrix} 1 & x_1 & x_1^2 & \vdots & x_1^m \\ 1 & x_1 & x_2^2 & \vdots & x_2^m \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_1 & x_n^2 & \vdots & x_n^m \end{bmatrix} \quad (1)$$

Then, the value of b can be computed as follows:

$$b = (A'A)^{-1} A'y \quad (2)$$

Passive Threat in Wireless Networks

Confidentiality, integrity and availability are important elements in order to ensure secure wireless networks. Confidentiality of the wireless network traffics is highly influenced by passive attacks, while integrity and availability are affected by active attacks. A passive attack is the first stage of a hacking process. For launching an active attacks against the wireless networks, passive attacks is needed. Passive attacks are silent in nature as it does not present any alteration to the network traffic or normal network operations. In this type of the attack, the network traffic is simply can be sniffed and analyzed by the attackers based on the objective of capturing sensitive information of the victims. Passive attack is very difficult to detect as an illegal access can be gained by the unauthorized users to the network traffic without modifying the traffic (Khan *et al.*, 2008). Based on that, this work is concerned with the passive attacks which is laying down a foundation for later launching an active attacks.

Proposed Cipher Method using Least Squares Interpolation

It is known that the LSA method is classified as an approximation data technique. It causes noticeable errors when it is utilized in image cryptography. To overcome

this problem, a new technique has been introduced in this study based on the least square interpolation method. In this technique, the number of mesh points is exact equal to the degree of least squares polynomial. Applying this technique to encrypt and decrypt different types of images result in minimal errors, Fig. 1 and 2.

In the proposed cryptography method of this work, the columns of an image have been partitioned to represent the key, say n . The gray levels which represent the number of Bits Per Pixel (BPP) can be classified based on the selected n key into dependent values (y_1, y_2, \dots, y_n) and independent values (x_1, x_2, \dots, x_n) as the x 's have been chosen at any interval. In this study, m is assumed to be equal to n in order to interpolate (x, y) otherwise LSA approximates the values and results in errors. Equation (2) has been employed to calculate the value of b . An example of this process can be explained by the representation of image values in the matrix T as follows:

$$T = \begin{bmatrix} 20 & 22 & 22 & 24 & 44 & 45 & 44 & 55 & 33 & 12 \\ 65 & 77 & 21 & 89 & 55 & 34 & 22 & 23 & 55 & 34 \\ 34 & 23 & 10 & 56 & 39 & 90 & 77 & 78 & 99 & 67 \\ 91 & 78 & 20 & 90 & 30 & 70 & 88 & 90 & 66 & 89 \\ 78 & 93 & 30 & 12 & 10 & 23 & 90 & 80 & 88 & 70 \\ 46 & 40 & 40 & 51 & 909 & 78 & 30 & 50 & 22 & 23 \\ 89 & 20 & 50 & 58 & 80 & 45 & 23 & 36 & 44 & 54 \\ 40 & 10 & 60 & 42 & 70 & 29 & 4 & 72 & 66 & 64 \\ 20 & 45 & 77 & 69 & 56 & 70 & 5 & 90 & 89 & 76 \\ 34 & 78 & 98 & 78 & 77 & 34 & 89 & 30 & 54 & 12 \end{bmatrix} \quad (3)$$

Each row can be divided into two vectors where the key $k = 5$. For interpolating second row $[65, 77, 21, 89, 55, 34, 22, 23, 55, 34]$, two vectors are interpolated, $y_1 = [65, 77, 21, 89, 55]$ and $y_2 = [34, 22, 23, 55, 34]$, for independent vector $x = [1, 2, 3, 4, 5]$. By applying Equation (2) on $\{x, y_1\}$, we get:

$$b = -105 * [0.0062, -0.1337, 0.8356, 2.0617, 1.7417]$$

The value of b represents the code of y_1 , since b is not part of the grey level's values. Below are the implemented algorithms in this study for encryption and decryption images:

For Encryption

1. Given key = n .
2. Divide the columns into n -vectors.
3. Form independent and dependent variables x and y respectively, where $x = 1:1: n$ and $y = [m_1, \dots, m_n]$.
4. Calculate b using Equation (2) via LSA of x and y .
5. Take the coefficients of LSA as encrypted

vector b .

6. Transform new matrix B of b vectors to an encrypted image file.

For Decryption:

1. Given key = n .
2. Read encrypted image matrix B .
3. Divide the columns into n -vectors.
4. Calculate the inverse LSA of x and b .
5. Take the coefficients of decrypted vector q .
6. Transform the new matrix to the decrypted image Q .

To explain the operation of the proposed method in this study, a simple example can be introduced as follows:

Assume that 20, 30 and 40 represent image values. Then, the (1,20), (2,30) and (3,40) points represent the interpolated mesh points. To encrypt the image, the LSA interpolating method can be applied as follows:

$$A = \begin{bmatrix} 1 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 3 & 9 \end{bmatrix} \text{ and } y = \begin{bmatrix} 20 \\ 30 \\ 40 \end{bmatrix}$$

Then:

$$b = (A'A)^{-1} A'y = \begin{bmatrix} 10 \\ 10 \\ 0 \end{bmatrix} \text{ and } y = 10 + 10x + 0x^2 = 10 + 10x$$

The $\begin{bmatrix} 10 \\ 10 \\ 0 \end{bmatrix}$ is the encryption of $\begin{bmatrix} 20 \\ 30 \\ 40 \end{bmatrix}$.

The image cryptography process depends on two separate stages. The first stage is an encryption and the other one is a decryption which is the inverse operation of the encryption.

Mathematically, it is known that when minor changes occur during the encryption operations it results in large alterations in the original data. This leads to the need of implementing an accurate algorithm to prevent or reduce the alterations in the original data during encryption and decryption operations. The statistical measurements of an image are determined by the coefficient correlations (COR), $PSNR$, Number of Pixels Change Rate ($NPCR$) and the Unified Average Changing Intensity ($UACI$). It is noted that $PSNR$ is strongly related to the number of vanishing moments (Abhilash, 2015). The sparsity of the transformation is strongly affected by the vanishing moments (Wu and Noonan, 2011). Higher vanishing moments means more complex functions can be represented by the scaling function.















Image	Original image T	Decrypted image Q
Ice		
Balloon		
Children		
Freeways		
Lena		
Tahreer		
Stadium		

Fig. 1: Encrypted and decrypted images of the proposed method

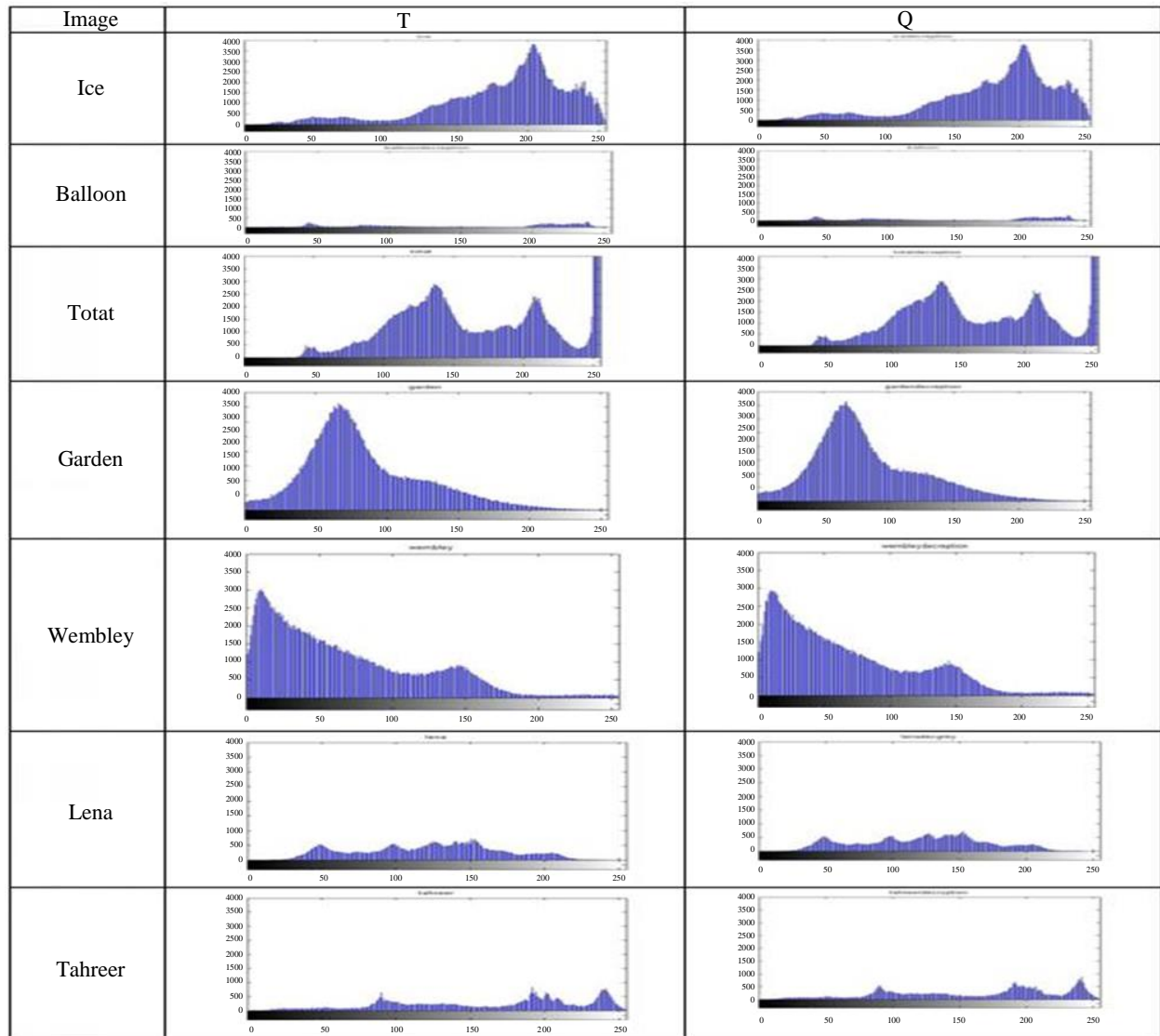


Fig. 2: Histogram of the examined images in this study

The *PSNR*, *NPCR*, *UACI* and *COR* can be calculated as follows:

$$PSNR = 10 * \log_{10} \left(\frac{255 * 255}{MSE} \right) \quad (4)$$

$$MSE = \frac{1}{M * N} \sum_{i=1}^N \sum_{j=1}^M (X(i, j) - Y(i, j))^2 \quad (5)$$

where, *X* refers to the origin image with dimension of *N* * *M* and *Y* refers to its corresponding encryption with the same dimension. A lower value of *MSN* means less error which is in turn means a higher value of *PSNR*. Based on the high values of *CRO* and *PSNR*, the performance of the newly introduced technique has proven higher accuracy of the examined images in comparison to the previously introduced cryptography techniques:

$$NPCR = \frac{\sum D}{M * N} * 100\% \quad (6)$$

$$UACI = \frac{1}{M * N} \left[\sum \frac{|X - Y|}{255} \right] * 100\% \quad (7)$$

$$COR = \frac{\sum_{i=1}^N \sum_{j=1}^M (X(i, j) - E(X))(Y(i, j) - E(Y))}{\left[\sum_{i=1}^N \sum_{j=1}^M (X(i, j) - E(X))^2 \sum_{i=1}^N \sum_{j=1}^M (Y(i, j) - E(Y))^2 \right]^{\frac{1}{2}}} \quad (8)$$

$$E(X) = \frac{\sum_{i=1}^N \sum_{j=1}^M (X(i, j) - E(X))}{M * N} \quad (9)$$

where, *D* denotes the array bipolar, *D*(*i*, *j*) = 0 if *X*(*i*, *j*) = *Y*(*i*, *j*), otherwise *D*(*i*, *j*) = 1. It is known that the *NPCR* and

UACI are the most commonly utilised parameters to assess the strength of image encryption/decryption technique in the sense of differential attacks (Wu and Noonan, 2011). In other words, high values of *NPCR* and *UACI* are usually used as an indication to a high resistance to differential attacks. Based on that, the high values gained of *NPCR* and *UACI* are an indication of the strength of the employed technique in this study against differential attacks.

Statistical Analysis and Discussion

In order to examine the accuracy of the utilized algorithms in this study, different images, including medical ones, have been encrypted and then decrypted. The performance of the proposed algorithms in this study is compared to the performance of Al-khassaweneh and Shreef's algorithms. The examined algorithm in this study exhibits a very few errors in the decryption process owing to the high correlation between the decrypted and origin images, in addition to the high *PSNR* values achieved by the proposed method. It has been shown that the achieved *COR* values are very close to 1. In other words, the newly introduced technique in this study has demonstrated higher correlation between the decrypted and the origin images in comparison to Al-khassaweneh and Shreef. In addition to that, high *PSNR* values (average value of *PSNR* is around 45) have been gained in comparison to the *PSNR* values introduced by Al-khassaweneh and Shreef, Table 1 to 3. For example, the attained *COR* and *PSNR* values in this study are 0.9994 and 43.7342 respectively for Tahreer's image, see Table 1, while the achieved *COR* and *PSNR* values by Al-khassaweneh for the same image were 0.9014 and 40.7342, Table 2.

Usually, hackers may seek to observe variations at the encrypted image to find the correlation between the plaintext and the encrypted image. Generally, the *NPCR* and the *UACI* can be utilised as an indication to the ability to resist to the differential attacks. As higher the measured values of *NPCR* and *UACI* as, the better resistance to the differential attacks. The proposed algorithms in this study have been applied to different types of images of different complexities, Fig. 2. In that figure, *T* denotes the original image and *Q* refers to the decrypted one. The measured *NPCR* and *UACI* for the examined images provide very acceptable results in terms of the method's strength against the differential attacks, Table 1. In other words, the implemented decryption algorithm in this study effectively detects that alteration to the original image, i.e., it detects the attack and resists it.

Further examination to the accuracy of the introduced method in this study, grayscale and coloured medical images are tested, Fig. 3. Al-khassaweneh and Shreef's techniques are also applied to those medical images for the purpose of comparison. Higher values in terms of *COR*, *PSNR*, *NPCR* and *UACI* parameters are achieved in this study in comparison to Al-khassaweneh and Shreef's works. For example, the *PSNR* value is 52.4470 when the proposed method in this study is applied to the grayscale image. While, for the same image, the values of *PSNR* are 26.5230 and 18.8080 for Al-khassaweneh and Shreef respectively. The achieved *COR* in this study for the grayscale image is 0.9697, while the achieved *COR* values by both Al-khassaweneh and Shreef are 0.9091 and 0.9011 respectively. The measured *NPCR* and *UACI* for the examined images provide very acceptable results in terms of the method's strength against the differential attacks.

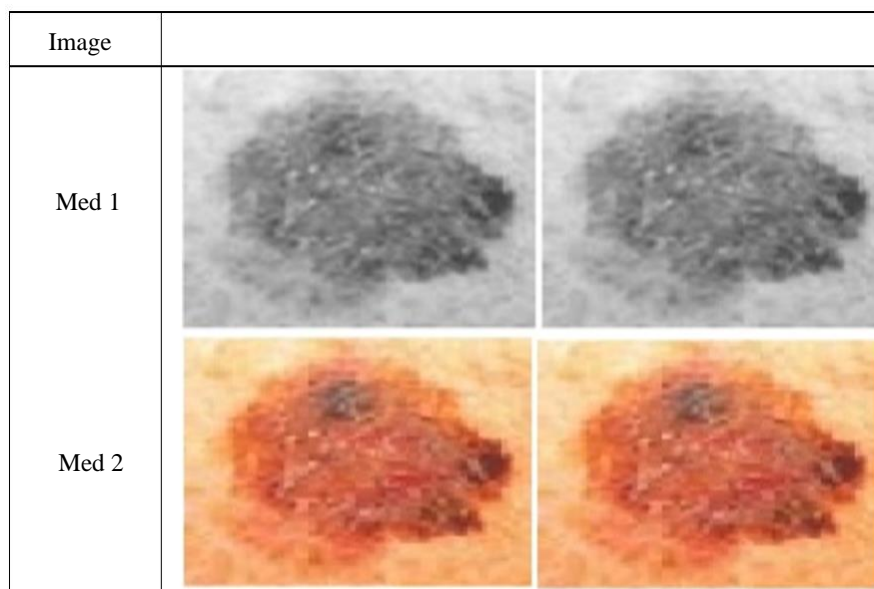


Fig. 3: Examined medical images

Table 1: Statistical parameters of the examined images.

Image	COR	PSNR	NPCR	UACI
Ice	0.9999	50.3175	99.60	77.9170
Balloon	0.9999	45.6005	97.80	65.4512
Children	0.9998	46.9898	99.90	77.8900
Freeways	0.9979	39.6203	99.991	72.9981
Stadium	0.9977	37.0469	99.90	60.5151
Tahreer	0.9994	43.7342	99.98	66.616
Lina	0.9997	47.667	99.9995	72.9970
Med (grey)	0.9697	52.4470	92.9995	62.9970
Med (color)	0.9497	36.4156	90.9995	60.9970

Table 2: Statistical parameters measured by Al-khassaweneh

Image	COR	PSNR	NPCR	UACI
Ice	0.9799	46.3075	98.60	74.9770
Balloon	0.9699	42.6005	97.80	61.4512
Children	0.9591	40.9088	98.90	74.8900
Freeways	0.9479	35.6203	97.991	70.9981
Stadium	0.9171	35.0461	95.90	55.5151
Tahreer	0.9014	40.7342	94.95	61.616
Lina	0.9091	42.667	95.99	70.9870
Med (grey)	0.9091	26.5230	88.9095	55.9970

Table 3: Statistical parameters measured by Shereef

Image	COR	PSNR	NPCR	UACI
Ice	0.9799	46.3075	98.60	74.9770
Balloon	0.9699	42.6005	97.80	61.4512
Children	0.9591	40.9088	98.90	74.8900
Freeways	0.9479	35.6203	97.991	70.9981
Stadium	0.9171	35.0461	95.90	55.5151
Tahreer	0.9014	40.7342	94.95	61.616
Lina	0.9091	42.667	95.99	70.9870
Med (grey)	0.9091	26.5230	88.9095	55.9970

Table 4: Table of attempts

No. of decrypted values	No. of attempts
2	4.6663 e ¹⁵⁷
3	3.5554 e ¹⁵⁷
4	3.8886 e ¹⁵⁶
5	7.7772 e ¹⁵⁵
6	1.2962 e ¹⁵⁵
7	1.8517 e ¹⁵⁴
8	2.3146 e ¹⁵³
9	2.5718 e ¹⁵²
10	2.5718 e ¹⁵¹

Based on the examinations to the large number of images of different textures and complexities, it can be stated that the newly introduced technique is robust and more accurate comparing to the previously introduced cryptography techniques.

Robustness of Proposed Method

Assume that the attacker can gain access and read the crypto values [-10, 15, 5]. Suppose that the attacker is knowledgeable about the presented algorithm in this study, with respect to the method's algebraic type and

key, the attacker has to manipulate the following methods and using the attacker's table, Table 5, to find the plain values of x and y :

$$a + bx + cx^2 = y(x) \text{ then } -10 + 15x + 5x^2 = y(x)$$

By choosing 200 variables for x on interval [-100, 99], the attacker needs: $100!/3! = 1.5554 \times 10^{157}$ attempts. Table 4 refers to the number of attempts of 100 decrypted values, All the 200 values for x and y are shown in the appendix section, see Appendix.

Conclusion

Mathematical concepts play an essential role in image cryptography. The proposed algorithms in this study employ interpolated *LSA* which results in a very few errors. In this method, all mesh points are interpolated when the number of mesh points is equal to the degree of the *LSA*. This means that all dependent points pass through the curve of the *LSA*. In order to examine the accuracy of the utilized algorithms in this study, different images, including grayscale and colored medical images, have been encrypted and then decrypted. It has been revealed that the newly introduced technique in this study has proven high correlations between the decrypted and the origin images. High *COR* and *PSNR* values have been gained when the proposed technique in this study is applied to a very large number of images of different textures and complexities. In comparison to the introduced techniques by both Al-khassaweneh and Shreef, high *NPCR* and *UACI* are achieved by the proposed technique in this study. The high values of *NPCR* and *UACI* indicate the strength of the employed technique in this study in terms of the high resistance to differential attacks.

Acknowledgment

This paper was supported by the faculty of computer science and mathematics of university of Kufa, Iraq. We thank all reviewers for deep reading on this paper.

Author's Contributions

Adil Alrammahi: Achieved the theory of the proposed method, implementation, comparing of results, and discussion.

Musrafa Ramadhan: Achieved the introduction, related works, references, and Proof reading.

Conflict of Interest

The authors declare that they have no conflict of interest.

References

- Abhilash, T.B., 2015. Effect of vanishing moments on the quality attributes of an image in digital watermarking system. *Int. J. Innova. Technol. Res.*
- Al-khassaweneh, M. and S. Aviyente, 2008. Image encryption scheme based on using least square approximation techniques. *Proceedings of the IEEE International Conference on Electro/Information Technology*, May 18-20, IEEE Xplore Press, Ames, IA, USA, pp: 108-111.
 DOI: 10.1109/EIT.2008.4554276
- Al-Rammahi, A., 2014a. Encryption image using small order linear systems and repeated modular numbers. *Proc. World Congress Eng.*
- AL-Rammahi, A., 2014b. Calculus logarithmic function for image encryption. *World Academy Sci., Eng. Technol. Int. J. Math., Comput. Sci. Eng.*
- Al-Rammahi, A., 2015. Encryption image via mutual singular value decomposition. *Proceedings of the International conference of digital image processing, World Academy of Science and Engineering Technology, (SET' 15).*
- Cao, A., 2013. A new hybrid chaotic map and its application on image encryption and hiding. *Math. Problems Eng.*, 1: 1-13.
 DOI: 10.1155/2013/728375
- Divya, V.V., S.K. Sudha and V.R. Resmy, 2012. Simple and secure image encryption. *Int. J. Comput. Sci.*, 9: 286-289.
- El Abbadi, N., A. Mohamad and M. Abdul-Hameed, 2014. Image encryption based on singular value decomposition. *Int. J. Comput. Sci.*, 10: 1222-1230.
- Elrabeay, S., F.E. Elsami, N. Elfishawi and S.E. Elkhamy, 2012. Least-squares interpolation of fused Mr and ct images in the wavelet domain. *Int. J. Comput. Applic.*
- Kekre, H.B., T. Sarode and P. Halarnkar, 2014. A hybrid approach for information hiding and encryption using multiple LSB's algorithms. *Int. J. Applic.*, 3: 42-51.
- Khan, S., N. Mast, K.K. Loo and A. Silahuddin, 2008. Passive security threats and consequences in IEEE 802.11 wireless mesh networks. *GlobalCIS Digital Library.*
- Kolman, B., 1993. *Introductory Linear Algebra with Applications*. 12th Edn., MacMillan Publishing Company, ISBN-10: 0023660325.
- Merkle, R. and M.E. Hellman, 1978. Hiding information and signatures in trapdoor knapsacks. *IEEE Tran. Inform. Theory*, 24: 525-530.
 DOI: 10.1109/TIT.1978.1055927
- Merkle, R. and M. Hellman, 1978. Hiding information and signatures in trapdoor knapsacks. *Tran. Inform. Theory*, 24: 525-530.
 DOI: 10.1109/TIT.1978.1055927
- Odlyzko, A.M., 2000. Discrete logarithms: The past and the future. *Designs Codes Cryptography*, 19: 129-145.
 DOI: 10.1023/A:100835000
- Rivest, R.L., A. Shamir and L. Adleman, 1970. On digital signatures and public key cryptosystems. *Technical Memo.*
- Shreef, M.A. and H.K. Hoomod, 2013. Image encryption using lagrange-least squares interpolation. *Int. J. Adv. Comput. Sci. Inform. Technol.*, 2: 35-55.
- Wu, Y. and J.P. Noonan, 2011. *NPCR and UACI* randomness tests for image encryption. *Multidisciplinary J. Sci. Technol. J. Selected Areas Telecommun.*
- Younes, M.A. and A. Jantan, 2008. Image encryption using block-based transformation algorithm. *Int. J. Comput. Sci.*, 35: 1-9.

Appendix

Table 5: Attacker' table

x	y	x	y
-100	48490	-50	11740
-99	47510	-49	11260
-98	46540	-48	10790
-97	45580	-47	10330
-96	44630	-46	09880
-95	43690	-45	09440
-94	42760	-44	09010
-93	41840	-43	08590
-92	40930	-42	08180
-91	40030	-41	07780
-90	39140	-40	73900
-89	38260	-39	7.100
-88	37390	-38	6.400
-87	36530	-37	62800

Table 5: Continue

-86	35680	-36	59300
-85	34840	-35	55900
-84	34010	-34	52600
-83	33190	-33	49400
-82	32380	-32	46300
-81	31580	-31	43300
-80	30790	-30	40400
-79	30010	-29	37600
-78	29240	-28	34900
-77	28480	-27	32300
-76	27730	-26	29800
-75	26990	-25	27400
-74	26260	-24	25100
-73	25540	-23	22900
-72	24830	-22	20800
-71	24130	-21	18800
-70	23440	-20	16900
-69	22760	-19	16695
-68	22090	-18	16491
-67	21430	-17	16289
-66	20780	-16	16088
-65	20140	-15	15888
-64	19510	-14	15689
-63	18890	-13	15491
-62	18280	-12	15295
-61	17680	-11	15100
-60	17090	-10	340.0000
-59	16510	-9	260.0000
-58	15940	-8	190.0000
-57	15380	-7	130.0000
-56	14830	-6	80.0000
-55	14290	-5	40.0000
-54	13760	-4	10.0000
-53	13240	-3	10.0000
-52	12730	-2	20.0000
-51	12230	-1	20.0000
0	-10.0000	50	13240
1	10.0000	51	13760
2	40.0000	52	14290
3	80.0000	53	14830
4	130.0000	54	15380
5	190.0000	55	15940
6	260.0000	56	16510
7	340.0000	57	17090
8	430.0000	58	17680
9	530.0000	59	18280
10	0640	60	18890
11	0760	61	19510
12	0890	62	20140
13	1030	63	20780
14	1.180	64	21430
15	13400	65	22090
16	1510	66	22760
17	1690	67	23440
18	1880	68	24130
19	2080	69	24830
20	2290	70	25540
21	2510	71	26260
22	2740	72	26990
23	2980	73	27730
24	3230	74	28480

Table 5: Continue

25	3490	75	29240
26	3760	76	30010
27	4040	77	30790
28	4330	78	31580
29	4630	79	32380
30	4940	80	33190
31	5260	81	34010
32	5590	82	34840
33	5930	83	35680
34	6280	84	36530
35	6640	85	37390
36	7010	86	38260
37	7390	87	39140
38	7780	88	40030
39	8180	89	40930
40	8590	90	41840
41	9010	91	42760
42	9440	92	43690
43	9880	93	44630
44	10330	94	45580
45	10790	95	46540
46	11260	96	47510
47	11740	97	48490
48	12230	98	49480
49	12730	99	50480
