

# An Image Feature Extraction to Generate a Key for Encryption in Cyber Security Medical Environments

<https://doi.org/10.3991/ijoe.v19i01.36901>

Abeer Salim Jamil<sup>1</sup>(✉), Raghad Abdulaali Azeez<sup>2</sup>, Nidaa Flaih Hassan<sup>3</sup>

<sup>1</sup>Department of Computer Technology Engineering, Al-Mansour University College, Baghdad, Iraq

<sup>2</sup>Information Technology Unit, Collage of Education for Human Science-Ibn Rushed, University of Baghdad, Baghdad, Iraq

<sup>3</sup>Department of Computer Science, University of Technology, Baghdad, Iraq  
abeer.salim@muc.edu.iq

**Abstract**—Cyber security is a term utilized for describing a collection of technologies, procedures, and practices that try protecting an online environment of a user or an organization. For medical images among most important and delicate data kinds in computer systems, the medical reasons require that all patient data, including images, be encrypted before being transferred over computer networks by healthcare companies. This paper presents a new direction of the encryption method research by encrypting the image based on the domain of the feature extracted to generate a key for the encryption process. The encryption process is started by applying edges detection. After dividing the bits of the edge image into (3×3) windows, the diffusions on bits are applied to create a key used for encrypting the edge image. Four randomness tests are passed through NIST randomness tests to ensure whether the generated key is accepted as true. This process is reversible in the state of decryption to retrieve the original image. The encryption image that will be gained can be used in any cyber security field such as healthcare organization. The comparative experiments prove that the proposed algorithm improves the encryption efficiency has a good security performance, and the encryption algorithm has a higher information entropy 7.42 as well as a lower correlation coefficient 0.653.

**Keywords**—cyber security, medical image encryption, feature extraction, diffusion, randomness, key generation

## 1 Introduction

Businesses utilize the cyber security as well as the physical security measures for preventing unauthorized access to the data centers and the else electronic systems. One aspect of cyber security that this protection is aimed at defending is the privacy, stability, and availability of digital information. The demand for instantaneous, high-quality content security for digital medical pictures is rising with the proliferation of computing and networking technologies that make it feasible to distribute such images [1, 2].

The widespread availability of digital devices has facilitated the easy distribution of digital photographs to anybody. Conventional encryption approaches are ineffective in directly protecting e-health data due to size, redundancy, and capacity constraints, particularly when the patient data is provided via open channels [3]. The digital picture is one of the most important techniques of conveying vast quantities of information, however to transfer this format safely, some cryptographic approach is required. Multiple methods of encryption have emerged in recent years, greatly enhancing the safety of online picture sharing. Images have a high pixel high redundancy and correlation, but the traditional encryption techniques, like International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES), Advanced Encryption Standard (AES), and Rivest Shamir Adleman (RSA) being created for text information. Thus, the other lightweight encryption technique has become one of the most prominent picture encryption method [4, 5] and is frequently employed in cryptosystems. Some photos are very sensitive, some images include secret data, and some images are delivered through insecure transmission channels, therefore protecting them from any assault is necessary [6]. Visual cryptography is one technique to ensure the image data security. By using visual cryptography, images may be encrypted in such a manner that they cannot be decoded during the transmission. In order to prevent the frequency attacks, most lightweight cryptography relies on the notion of diffusion/confusion of the image bits [7, 8]. There are two potential dangers for picture data: First, the sensitive information might be leaked from the image itself. Second, the picture data must be protected during the transmission since it may be stolen and altered before being sent across a network [9]. The efficacy of an encryption method is dependent on the quality of its key. On the other hand, the expanded key presents several challenges, such as a higher risk of forgetting and a higher barrier to storage. The external nature of the key also introduces a security risk into the encryption algorithm [5, 10, 11], and the present research is centred on the encrypting patient x-ray images, so they could be securely transmitted over a network. To do this, the diffusion principle has been followed which is applied to the pixels of the original images to generate the secret key, tested its randomness, and then used it to encrypt the image.

## **2 Related works**

Now more than ever, the information security must be bolstered due to the prevalence of defensive data being kept and communicated digitally across insecure channels. The visual component of data is crucial. The need to secure the images from prying eyes has led to several adaptations of various encryption methods by researchers. As an example, [12] presented a technique for a two-dimensional chaotic map and two secrets, both of which are relevant to the many different kinds of studies now being conducted on substitutions, permutations, chaotic maps, spatial domains, diffusion, etc. Picture encryption keys are generated by first slicing the image into four sections, then encrypting each section individually  $n$  times, then reversing the keys for each section, and finally repeating the process  $n$  times. As introduced by Al-Haj A. et al. in [13],

the watermark picture may be embedded in the source image by using the Histogram Shifting RDH technique in the spatial domain. A partially encrypted picture was produced. Pixel permutation was used to produce the key, and another spatial domain watermark picture was utilized to encrypt the key using the RDH Histogram shifting technique. Finally, the watermarked image and the encrypted watermarked image of 8-bit planes were merged to form 16-bit planes. By treating the generation of keys as a 5D conservative hyper-chaotic system, Zhou M., et al. [14] created a novel, safe technique of encrypting images. When using a diffusion mechanism that relies on both plaintext and ciphertext, from encrypting the 1st. plaintext pixel block to encrypting the final pixel block and then modernizing the 1st. cypher text block, the chaotic system utilized for generating the pseudorandom orders must remain unchanged, and the important encryption model's streams must be random. In [15], the Josephus sequence, two hyper chaotic systems (1-D and 6-D), LFSR generator, and SHA-512 hash function and were all employed together. Three efficient scrambling operations were utilized for permuting the columns and rows locations. With studies, like differential attacks and fault propagation, their method is able to achieve a great performance and a high resistance to a wide variety of security threats. When encrypting a picture, a special key is utilized, and both the encryption and decryption steps from [16] must be taken into account. For this reason, the idea of partial picture encryption has been investigated. For the original picture to be recovered after encryption, the receiving end must have access to the same key. In contrast, the approach presented by Zhou B. et al. in [6] uses a fractal diagram to encrypt pictures by transforming them into a series of random patterns whose shapes are determined by the parameters used in the pattern's production. Using the inverse technique, it may recover the original picture using these keys by analyzing the form's shape pattern. Fractal images of various forms may be generated by performing this transformation, with the original images' security assured. According to the findings, the proposed system is both efficient and secure in its execution, requiring little time for calculations. An example of an elliptic curve cryptosystem was provided by the method of picture encryption described in [17]. An elliptic curve is shared by the two communicating parties. The sender first aggregates the pixel data and transforms them to large integers, and then the sender encrypts the big integers using ECC and the chaotic system, resulting in shorter encryption times. In the end, the encrypted large numbers are used to create the encrypted picture. While the suggested approach provides more security and greater accuracy, the encrypted message is larger in size. To manage the encrypted data transfer over open networks, in [8], a visual cryptography system, whose central principle is the encryption of an image that disperses a secret across  $m$  different image shares, is found in this work. This method makes it difficult for hackers to recover the original picture data. There is also a need to use the effective encryption technique to protect the original image's privacy and security. Using this theory, a novel method of picture encryption and decryption that use the diffusion technique and a mix of chaotic maps is created in the current study.

### **3 Image encryption**

The most advanced encryption technology [1] will ensure that the businesses are properly secured from cyber threats. Most security systems use encryption because it is one of the most effective means of keeping sensitive information safe. The subtleties of biometrics vary from one person to the next, making it difficult to construct a security system that relies on them; however, when the biometric system is used, it is important to be aware of the risks involved, such as what happens if the reference template is exposed by a meddler [18, 19]. This issue is addressed by cryptography, the encrypted data security is reliant upon (2) factors: The cryptographic algorithm robustness and the key secrecy and how a secret key method being distributed [11, 20]. This categorises the crypto-systems as either private-type (symmetric) key or public-type (asymmetric) key. When employing a public key to encrypt plaintext, the resulting ciphertext must be decrypted using a corresponding private key. Private-key cryptography uses a single key that is shared by the sender / receiver for both encryption and decryption [5].

When it comes to information security, the studies focusing on protecting the digital images are a promising new area. The existing picture encryption algorithms distort the original image into a meaningless random noise signal, making it more vulnerable to attack [6]. In order to ensure the safety of data in interactive media prior to transmission over an unsecured channel, numerous picture encryption algorithms have been developed recently. In the realm of picture encryption, the starting value of pseudo randomness, chaos, ergodicity, and parameters, in addition to the process technique that is utilised, are very sensitive [17, 21].

### **4 Features extraction**

Processing that characterises' borders, a crucial and fundamental characteristic in image processing is called "Edge Detection and Feature-Extraction," and it is essential to the motion identification process. By pinpointing abrupt changes in pixel values, the edge detection helps define the image's areas, lowers the data and filters out the noise without sacrificing the image's essential structural qualities. With most photos degraded by noise or certain data possession devices, lighting circumstances, etc., an enhanced image is necessary for understanding. Most edge detection techniques start with the premise that the edges are detectable anywhere there is a break in the picture. Using this premise, one can derive the derivative of the image's intensity value and find the spots where the derivative is maximal, pinpointing the edges [22–30].

## 5 Sobel edge detectors

Using edge detection, one may decrease the amount of data in a picture while still retaining the crucial features. The proposed method uses Sobel edge detection, which aims to maximise the accuracy with respect to the following criteria: (1) accurately identifying the true edges while minimising the likelihood of false positives; (2) ensuring that the detected edges are as visually alike to the true edges into the original image as likely; and (3) ensuring that only a single false positive is generated for each true edge point. Sobel edge detection masks incorporate the information about the edges in the horizontal and vertical planes into a single metric. The masks look like this:

$$\begin{array}{cc} \text{Row} & \text{Mask} \\ \begin{bmatrix} -1 & -2 & -1 \\ 0 & 0 & 0 \\ 1 & 2 & 1 \end{bmatrix} & \begin{array}{cc} \text{Column} & \text{Mask} \\ \begin{bmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{bmatrix} \end{array} \end{array}$$

Each of these masks is convolved with the corresponding picture. A row mask result (S1) and a column mask result (S2) are now available for each pixel position. Using these values, one gets the following definitions for the edge magnitude and edge direction matrices:

$$\text{Edge Magnitude} = \sqrt{(S1^2 + S2^2)} \tag{1}$$

$$\text{Edge Direction} = \text{Tan}^{-1} \left[ \frac{S1}{S2} \right] \tag{2}$$

## 6 Proposed system

The purpose of this work is to hide any medical significance in the picture. To begin the encryption procedure, the bits of the medical picture undergo a series of diffusions and modifications to get a scrambling condition helpful for gaining access to the maximal blurring of the image; the Sobel filter is then used to identify the edges. The edge image is a two-by-two matrix whose cells are individually divided into 3\*3 squares, and then their values are transformed to integers. Since there are 9 bits per window, the highest possible integer number is 767, which indicates that there can only be a maximum of three significant digits in an integer. Then, the total of each group of three decimal places is added to the sum of the neighbouring groups, and the average of these integer values is converted into binary to serve as the key for the encryption procedure. The created key is XORed with each window of the edge picture and then subjected to NIST randomness tests to verify its legitimacy. The proposed approach for encrypting the medical images is elucidated in both algorithm 1 and Figure 1.

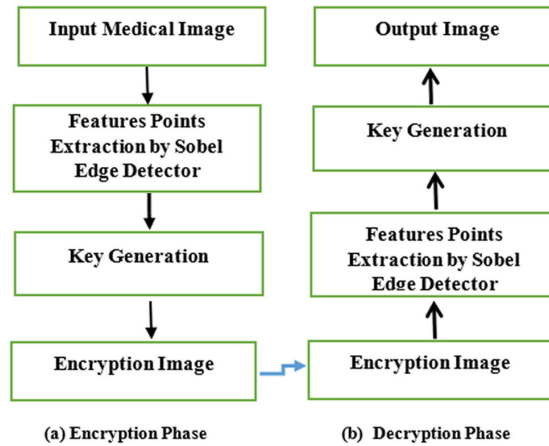


Fig. 1. The general stages of the proposed medical image encryption technique

| <i>Algorithm (1) General algorithm</i>   |
|--|
| Input: Original Image  |
| Output: Encryption Image   |
| Begin  |
| Step_1. Convert the original image into edge image using Sobel edge.   |
| Step_2. Convert the edge image into binary two-dimensional array.  |
| Step_3. Divide the array in the previous step to windows of (3×3).   |
| Step_4. Each window in the previous step is converted into an integer no., each number isn't exceeded 3 decimals places.       |
| Step_5. Create 1D array for storing the nos. made in the preceding step, each number has 3 cells from 1D array.                |
| Step_6. Sum each three cells in the previous step with the adjacent three cells and so on until the end of array               |
| Step_7. Calculate the average resulting in the previous step.  |
| Step_8. Convert the result of the previous step to binary bits, these bits represent the key generated for encryption process. |
| Step_9. Xored the generated key with all the windows in the matrix of edge image in step 3.                                    |
| Step_10. The result of the previous step is the encryption image.  |
| End  |

### 6.1 Feature extraction by Sobel edge detector

Since Sobel edge detection is so efficient at extracting structural information from a wide range of visual objects, and since it greatly reduces the amount of data to be processed, it is utilised to locate the feature points, as manifested in Figure 2. After using the Sobel technique, the selected pixel is represented as a feature extraction vector.

The following steps are applied to extract a feature by Sobel edge detector:

- Transform the image into grayscale
- Convolve the grey image with Sobel-x filter
- Convolve the grey image with Sobel-y filter
- Compute the gradient magnitude and direction

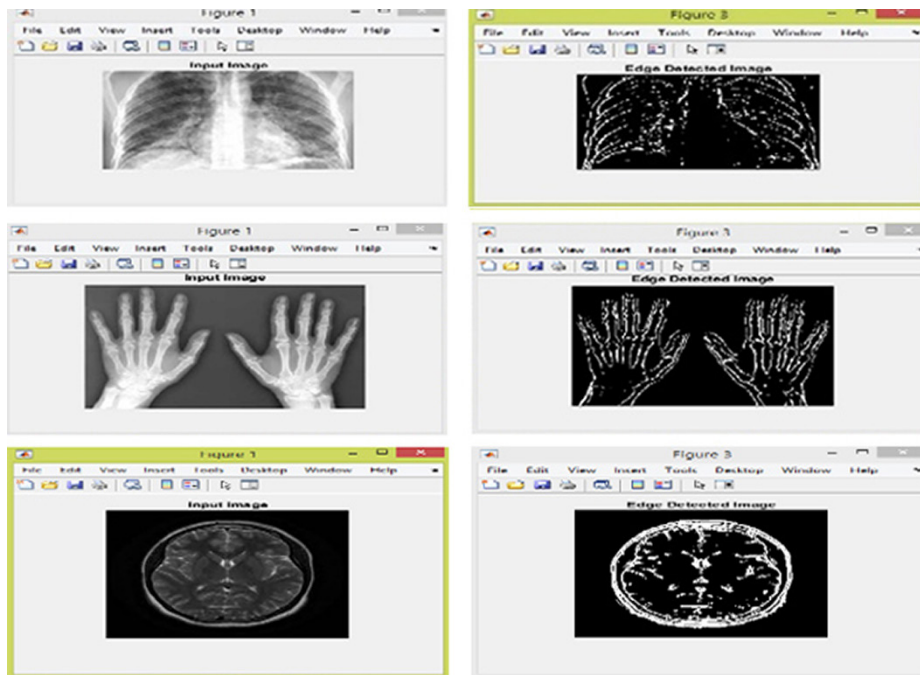


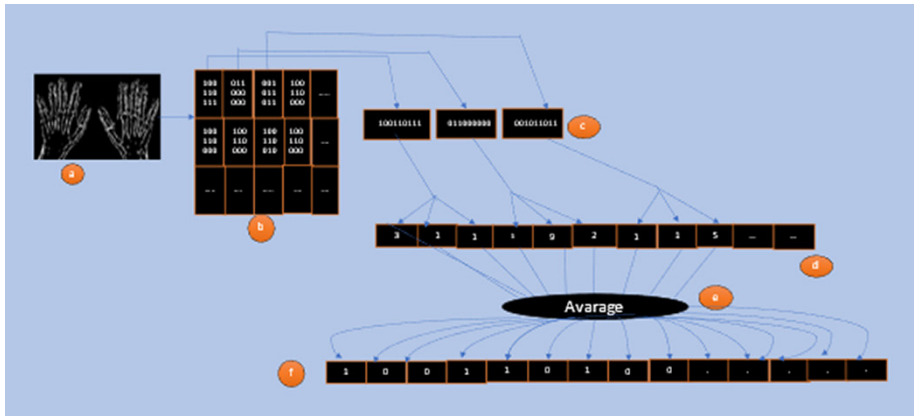
Fig. 2. Sobel edge detector

## 6.2 Key generation

Several security studies agree that generating random keys is the most crucial step in the encryption process. This is due to that an arbitrarily created long key being problematic to remember and, hence, tough to break. The feature extraction vector is used to generate a random cryptographic key (K), as evinced in Algorithm 2. The key generation is followed by testing for randomness. All produced keys have successfully passed the unexpected binary series and the random test; therefore, they can be used effectively.

**Algorithm (2): Random Key Generator**

Input: Image of Edge Detection  
 Output: randomly key  
 Begin  
 Step\_1 Create a binary matrix from edge detection of image (Figure 3(a)).  
 Step\_2 Divide the binary 2-dimensional array into size of (3\*3) window, each one is equal to (9) cells, as depicted in Figure 3(b).  
 Step\_3 Convert the binary value of each window in Figure 3(c) into integer numbers, the value of this number is not exceeding 511.  
 Step\_4 Create one-dimension array, put the result of each window of step\_3 in successive three cells, and this will be illustrated in the Figure 3(d).  
 Step\_5 Compute the average of all numbers in cells of Figure 3(d), as described in Figure 3(e).  
 Step\_6 Create one-dimension binary array by converting the average of cells in Figure 3(e) in the preceding step, such binary array refers as the key for the operation of encryption, and this will be revealed in the Figure 3(f).  
 End



**Fig. 3.** Key generation: “a” An edge image, “b” 2D array, “c” 9 Bits window, “d” 1D of cells, “e” Average, and “f” Binary array (Key)

### 6.3 Medical image encryption

After the encryption equation has been fully implemented, the encrypted picture will be displayed in the second stage of the encryption process, where the key obtained using the Sobel technique will be utilised in the first step.

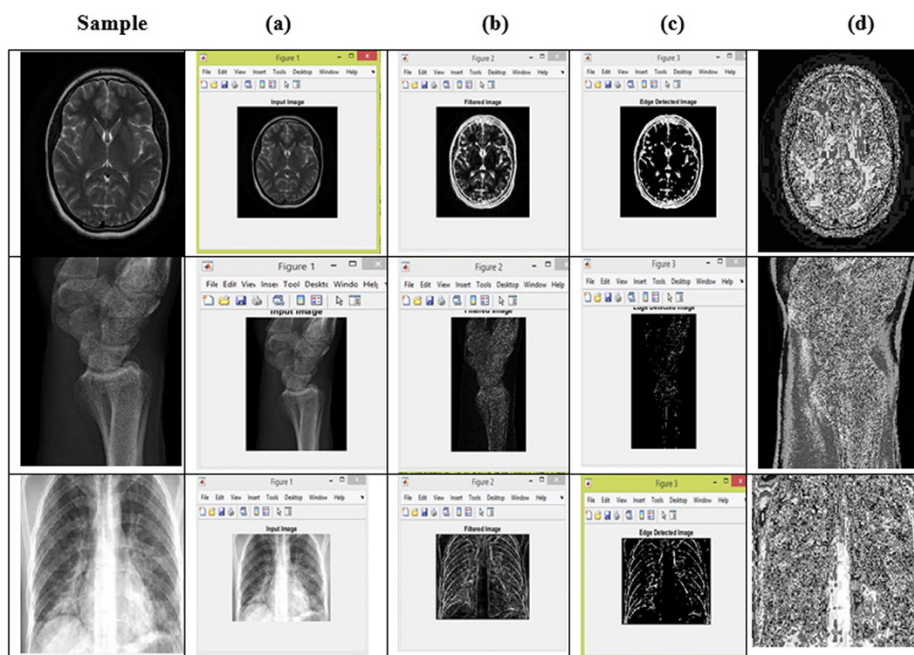
Algorithm (3) illustrates the steps of medical image encryption.



**Algorithm 3: Medical Image Encryption.**  
Input: Points of vector features and key generation  
Output: Image encryption  
Begin  
Step\_1: Apply the key created as clarified in the Figure 3(f) with a window, as illustrated in the Figure 4 (b) by using XOR operator.  
$$C_i = e(i) \text{ XOR } b(i)$$
  
Step\_2: The result is image encryption.  
End

## 7 Experimental results

The suggested technique can be utilized for encrypting the images of each size or kind. As portrayed in the Figure 4a–d, three samples from medical images have been processed via the suggested procedure.



**Fig. 4.** Three samples from medical images, (a) Input image, (b) Filtered image, (c) Sobel detector apply, and (d) Image Encryption

The measures that being utilized to asset the proposal performance include NPCR, Medical image encryption time, Correlation as pointed out Equation 3 [32], Entropy Coefficient as pointed out Equation 4, UACI [32], and Equation 5 reference to Peak Signal to Noise Ratio (PSNR).

$$R_{xy} = \frac{1/N \sum_{i=1}^N (xi - 1/N \sum_{k=0}^n x(k))(yi - 1/N \sum_{k=0}^n y(k))}{\sqrt{\frac{1}{N} \sum_{k=0}^n (xk - E(x))^2} \sqrt{\frac{1}{N} \sum_{k=0}^n (yk - E(y))^2}} \quad (3)$$

$$\text{Entropy} = \sum(p(i)) \left( \log \frac{1}{p(i)} \right) \quad (4)$$

Where:

P(i): Probability of the count of an ith image gray value

$$PSNR = 10 \text{Log}_{10} \left[ \frac{M \times N 255^2}{\sum_{m=1}^M \sum_{n=1}^N |f(m,n) - d(m,n)|^2} \right] \quad (5)$$

Where:

f (m, n): The original- image

(m, n): The decrypted-image

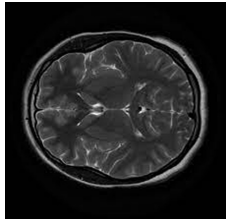

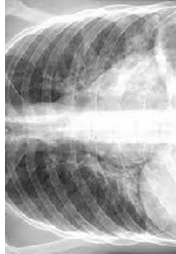
The suggested key generator yields a high resilience, as listed in Table 1, when applied to four randomization tests on three medical pictures. All four of these tests (Serial, Poker, Runs, and Frequency) demonstrated similar results.

**Table 1.** Four randomness tests for three medical images

| Test                  | Accept Degree      | Sample 1  | Sample 2 | Sample 3 |       |
|-----------------------|--------------------|-----------|----------|----------|-------|
| <b>Serial Test</b>    | Should be <=6.3    | 3.27.250  | 1.542    | 1.078    |       |
| <b>Poker Test</b>     | Should be <=11.1   | 4.300     | 0.725    | 1.263    |       |
| <b>Runs Test</b>      | Should be <=15.391 | <b>T0</b> | 12.321   | 8.329    | 7.654 |
|                       |                    | <b>T1</b> | 1.341    | 2.361    | 1.561 |
| <b>Frequency Test</b> | Should be >=0.001  | 0.134     | 0.109    | 0.126    |       |

Table 2 shows the encrypted and encrypted time, the image, Correlation, entropy, NPCR, PSNR, UACI, MSE for the encryption, and the decryption images, correspondingly, as well as the values of entropy for various samples of medical images.

**Table 2.** Evolution measurements for three medical image encryptions

| Medical Image (Samples)   | Encryption Time Full Image(Second) | Entropy Medical Image | Correlation | NPCR   | UACI   | MSE (Medical Image Encryption) | PSNR (Medical Image Encryption) | PSNR (Medical Image Decryption) |
|---|------------------------------------|-----------------------|-------------|--------|--------|--------------------------------|---------------------------------|---------------------------------|
|    | 4.89                               | 7.42                  | 0.653       | 68.52  | 8.108  | 64.48                          | 19.3                            | 85.17                           |
|   | 5.03                               | 7.55                  | 0.762       | 62.38  | 8.946  | 70.50                          | 21.1                            | 81.3                            |
|  | 4.65                               | 7.45                  | 0.628       | 68.136 | 10.729 | 65.82                          | 19.7                            | 83.74                           |

## 8 Conclusions

In this research, the main objective of the process of encrypting medical images is to protect the data of healthcare institutions, customers or employees and any other information stored electronically from any type of cyber-attack. Where, the key was improved by the Sobel edge detection algorithm in addition to that a set of measures was used to calculate the degree of key strength by calculating the Entropy, Correlation, NPCR and UACI. The results were 7.42, 0.653, 68.52 and 8.108, respectively for sample (1a), and this indicates the degree of strength of encryption which ensures the degree of confidentiality. The encrypted image and also when retrieving the original image by doing the process of decrypting, the image turned out to be the image of a high quality and did not induce any loss of information during the process of encryption and decryption.

## 9 References

- [1] P. S. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber security," *Int. J. Adv. Res. Comput. Commun. Eng.*, vol. 7, no. 11, pp. 125–128, 2018. <https://doi.org/10.17148/IJARCCCE.2018.71127>
- [2] J. Li et al., "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 14, pp. 1–16, 2020. <https://doi.org/10.1186/s12911-020-01328-2>
- [3] H. Ayesha et al., "Automatic medical image interpretation: State of the art and future directions," *Pattern Recognit.*, vol. 114, p. 107856, 2021. <https://doi.org/10.1016/j.patcog.2021.107856>
- [4] M. Ghebleh, A. Kanso, and D. Stevanović, "A novel image encryption algorithm based on piecewise linear chaotic maps and least squares approximation," *Multimed. Tools Appl.*, vol. 77, no. 6, pp. 7305–7326, 2018. <https://doi.org/10.1007/s11042-017-4634-9>
- [5] M. S. Mahdi, R. A. Azeez, and N. F. Hassan, "A proposed lightweight image encryption using ChaCha with hyperchaotic maps," *Period. Eng. Nat. Sci.*, vol. 8, no. 4, pp. 2138–2145, 2020.
- [6] S. Bai, L. Zhou, M. Yan, X. Ji, and X. Tao, "Image cryptosystem for visually meaningful encryption based on fractal graph generating," *IETE Tech. Rev.*, vol. 38, no. 1, pp. 130–141, 2021. <https://doi.org/10.1080/02564602.2020.1799875>
- [7] S. Das, S. N. Mandal, and N. Ghoshal, "Diffusion and encryption of digital image using genetic algorithm," in *Proceedings of the 3rd International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA) 2014*, pp. 729–736, 2015. [https://doi.org/10.1007/978-3-319-11933-5\\_82](https://doi.org/10.1007/978-3-319-11933-5_82)
- [8] P. Geetha, V. S. Jayanthi, and A. N. Jayanthi, "Multiple share creation based visual cryptographic scheme using diffusion method with a combination of chaotic maps for multimedia applications," *Multimed. Tools Appl.*, vol. 78, no. 13, pp. 18503–18530, 2019. <https://doi.org/10.1007/s11042-019-7163-x>
- [9] A. Upadhyaya, V. Shokeen, and G. Srivastava, "Image encryption: Using aes, feature extraction and random no. generation," in *2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions)*, pp. 1–4, 2015. <https://doi.org/10.1109/ICRITO.2015.7359286>

- [10] R. Xie, M. Wang, and B. Hai, "Image encryption research based on key extracted from iris feature," *Int. J. Secur. Its Appl.*, vol. 9, no. 6, pp. 157–166, 2015. <https://doi.org/10.14257/ijasia.2015.9.6.16>
- [11] D. D. Salman, R. A. Azeez, and A. M. J. Hossen, "Key generation from multibiometric system using meerkat algorithm," *Eng. Technol. J.*, vol. 38, no. 3, pp. 115–127, 2020. <https://doi.org/10.30684/etj.v38i3B.652>
- [12] K. Gupta, R. Gupta, R. Agrawal, and S. Khan, "An ethical approach of block based image encryption using chaotic map," *Int. J. Secur. Its Appl.*, vol. 9, no. 9, pp. 105–122, 2015. <https://doi.org/10.14257/ijasia.2015.9.9.10>
- [13] A. Al-Haj and H. Abdel-Nabi, "Digital image security based on data hiding and cryptography," in 2017 3rd International conference on information management (ICIM), pp. 437–440, 2017. <https://doi.org/10.1109/INFOMAN.2017.7950423>
- [14] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Processing*, vol. 171, p. 107484, 2020. <https://doi.org/10.1016/j.sigpro.2020.107484>
- [15] M. Naim, A. A. Pacha, and C. Serief, "A novel satellite image encryption algorithm based on hyperchaotic systems and Josephus problem," *Adv. Sp. Res.*, vol. 67, no. 7, pp. 2077–2103, 2021. <https://doi.org/10.1016/j.asr.2021.01.018>
- [16] T. Kumar and S. Chauhan, "Image cryptography with matrix array symmetric key using chaos based approach," *Int. J. Comput. Netw. Inf. Secur.*, vol. 11, no. 3, p. 60, 2018. <https://doi.org/10.5815/ijcnis.2018.03.07>
- [17] X. Zhang and X. Wang, "Digital image encryption algorithm based on elliptic curve public cryptosystem," *IEEE Access*, vol. 6, pp. 70025–70034, 2018. <https://doi.org/10.1109/ACCESS.2018.2879844>
- [18] R. A. Azeez, M. K. Abdul-Hussein, M. S. Mahdi, and H. T. H. S. ALRikabi, "Design a system for an approved video copyright over cloud based on biometric iris and random walk generator using watermark technique," *Period. Eng. Nat. Sci.*, vol. 10, no. 1, pp. 178–187, 2021. <https://doi.org/10.21533/pen.v10i1.2577>
- [19] D. D. Salman and R. A.-A. Azeez, "BUILD CRYPTOGRAPHIC SYSTEM FROM MULTI-BIOMETRICS USING MEERKAT ALGORITHM," *Iraqi J. Comput. Informatics ijci*, vol. 45, no. 2, pp. 1–8, 2019. <https://doi.org/10.25195/ijci.v45i2.46>
- [20] N. F. Hassan, A. E. Ali, and T. W. Aldeen, "Generate random image-key using hash technique," *Eng. Tech. J.*, vol. 28, no. 2, pp. 382–397, 2010.
- [21] Z. K. Obaid and N. F. H. Al Saffar, "Image encryption based on elliptic curve cryptosystem," *Int. J. Electr. Comput. Eng.*, vol. 11, no. 2, p. 1293, 2021. <https://doi.org/10.11591/ijece.v11i2.pp1293-1302>
- [22] K. Lakhani, B. Minocha, and N. Gugnani, "Analyzing edge detection techniques for feature extraction in dental radiographs," *Perspect. Sci.*, vol. 8, pp. 395–398, 2016. <https://doi.org/10.1016/j.pisc.2016.04.087>
- [23] N. Alseelawi and H. T. Hazim, "A novel method of multimodal medical image fusion based on hybrid approach of NSCT and DTCWT," *iJOE*, vol. 18, no. 03, p. 115, 2022. <https://doi.org/10.3991/ijoe.v18i03.28011>
- [24] I. A. Aljazaery and A. H. M. Alaidi, "Encryption of color image based on DNA strand and exponential factor," *iJOE*, vol. 18, no. 03, p. 101, 2022. <https://doi.org/10.3991/ijoe.v18i03.28021>
- [25] H. N. A. H. Haider TH. Salim ALRikabi Saif Hameed Abbood, Mohd Shafry Mohd Rahim, and Abdul Hadi M. Alaidi, "DR-LL Gan: Diabetic Retinopathy lesions synthesis using Generative Adversarial Network," *International journal of online and biomedical engineering*, vol. 18, no. 3, pp. 151–163, 2022. <https://doi.org/10.3991/ijoe.v18i03.28005>

- [26] M. K. Abdul-Hussein and H. Alrikabi, "Evaluation of the interference's impact of cooperative surveillance systems signals processing for healthcare," 2022. <https://doi.org/10.3991/ijoe.v18i03.28015>
- [27] N. F. A.-B. Azhar Al-zubidi, Rajaa K. Hasoun, Soukaena Hassan Hashim, and Haider Th. Salim Alrikabi, "Mobile application to detect Covid-19 pandemic by using classification techniques: Proposed system," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 34–51, 2021. <https://doi.org/10.3991/ijim.v15i16.24195>
- [28] H. T. H. H. Alrikabi, "Enhanced data security of communication system using combined encryption and steganography," *International Journal of Interactive Mobile Technologies*, vol. 15, no. 16, pp. 144–157, 2021. <https://doi.org/10.3991/ijim.v15i16.24557>
- [29] I. A. Aljazeera, H. T. S. Alrikabi, and M. R. Aziz, "Combination of hiding and encryption for data security," *International Journal of Interactive Mobile Technologies*, vol. 14, no. 9, pp. 34–47, 2020. <https://doi.org/10.3991/ijim.v14i09.14173>
- [30] M. R. Wankhade and N. M. Wagdarikar, "Feature extraction of edge detected images," *Int. J. Comput. Sci. Mob. Comput.*, vol. 6, no. 6, pp. 336–345, 2017.
- [31] A. S. Jamil and A. M. S. Rahma, "Image encryption based on multi-level keys on RC5 algorithm," *iJIM*, vol. 16, no. 17, p. 101, 2022. <https://doi.org/10.3991/ijim.v16i17.34335>
- [32] A. Muhammed, A. S. Jamil, and N. F. Hassan, "Partial face encryption based on CAT swarm optimization", 2nd International Conference on Advances in Engineering Science and Technology, 2022.

## 10 Authors

**Abeer Salim Jamil** received the MSc. and PhD. in Computer Science from University of Technology, Iraq, 2004 and 2015 respectively. She has around 24 years of teaching experience and 11 years teaching in Cisco Network Academic (CISCO). Her areas of interests are Digital Image Processing, Video Processing, Security software Engineering, Networking and artificial intelligence applications. She can be contacted at email: [abeer.salim@muc.edu.iq](mailto:abeer.salim@muc.edu.iq).

**Assist. Prof. Dr. Raghad Abdulaali Azeez** received the MSc. from University of Technology, Iraq, 2002 and PhD. in Computer Science from Iraqi Commission for Computers and Informatics / Institute for Postgraduate Studies, 2006. She has around 20 years of teaching experience. Her areas of interest's are computer security and image processing. **SECOND A. AUTHOR** Assist. Prof. Dr. Raghad A. Azeez received the MSc. from University of Technology, Iraq, 2002 and PhD. in Computer Science from Iraqi Commission for Computers and Inforatics / Institute for Postgraduate Studies, 2006. She has around 20 years of teaching experience. Her areas of interest's are computer security and image processing.

**Nidaa Flaih Hassan** received the MSc. and PhD. in Computer Science from University of Technology, Iraq, 1996 and 2005 respectively. She has around 25 years of teaching experience. Her areas of interests are Cyber Security, Multimedia Compression, and Image Processing. She can be contacted at email: [110020@uotechnology.edu.iq](mailto:110020@uotechnology.edu.iq).

Article submitted 2022-10-17. Resubmitted 2022-11-18. Final acceptance 2022-11-19. Final version published as submitted by the authors.