PAPER

A new method of image encryption using advanced encryption Standard (AES) for network security

To cite this article: Saba Inam *et al* 2023 *Phys. Scr.* **98** 126005

Physica Scripta

PAPER

A new method of image encryption using advanced encryption Standard (AES) for network security

Saba Inam[1,*], **Shamsa Kanwal**[1], **Rabia Firdous**[1], **Khansa Zakria**[1] and **Fahima Hajjej**[2]

[1] Department of Mathematical Sciences, Fatima Jinnah Women University, The Mall, Rawalpindi, Pakistan
[2] Department of Information Systems, College of Computer and Information Sciences, Princess Nourah bint Abdulrahman University, P. O. Box 84428, Riyadh 11671, Saudi Arabia
[*] Author to whom any correspondence should be addressed.

E-mail: saba.inam@fjwu.edu.pk

RECEIVED
21 September 2023

REVISED
25 October 2023

ACCEPTED FOR PUBLICATION
2 November 2023

PUBLISHED
16 November 2023

Keywords: advance encryption standard, image encryption, chaotic maps, arnold map

Abstract

With the rapid increase in the use of technology, images have become a major source of sharing personal, confidential and official information and there is a dire need to protect this secret data. Image encryption plays major role in the security of images and there are many techniques developed for this purpose. Chaos based image encryption has now become most applicable and beneficial technique for image encryption. The purpose of this paper is to highlight a new method of image encryption with the use of advanced encryption standard (AES) and chaotic maps. This technique is composed of substitution and permutation phases. AES is found to be most secure cipher until now against different kinds of attacks. The round keys are generated by AES using key expansion algorithm. The sensitivity of this technique is that it is dependent on initial values and input image. S-boxes in AES introduce non-linearity, confusion, and an avalanche effect, enhancing security and resistance to cryptographic attacks by substituting bytes in the encryption process. The combination of AES and chaotic maps in encryption schemes provides a two-tiered approach to enhance security. AES offers a strong and well-established encryption method, while chaotic maps introduce randomness and complexity, making it more difficult for attackers to decipher encrypted data. This combination is often used to achieve a higher level of encryption security in various applications, including data transmission and storage. Different kinds of analysis and tests are performed on the technique which includes information entropy, number of pixel change rate (NPCR), and peak signal-to-noise ratio (PSNR), unified average changing intensity (UACI) and histogram correlation of adjacent pixels. The results of these tests show that this technique is secure and resistant towards attacks.

1. Introduction

Digital images, and digital video-based digital images, have become an important medium for information storage and transmission in the computer network in the civil and military fields in recent years, along with the fast promotion and rising popularity of network technology and digital communication technology around the world. Network security challenges, on the other hand, have been a significant factor that has hindered and limited the advancement of network technology [1]. Some images may contain personal or commercial information that is not intended for public use. To resist unauthorized access, revision, and other threats, image security should be given a high priority. Data shielding and encryption, as well as decryption, are two frequently applied methods. Watermarking, anonymity, and steganography are all methods for hiding data. Encryption of multimedia content can be a quick and easy way to secure data from unauthorized access. Such techniques needed the encryption of data using mathematical procedures, with only the real party sharing the data would be able to decrypt it in order to use it [2]. Some of such image encryption techniques include data encryption standard (DES) [3], triple data encryption standard (3DES) and AES [4].

Classical image encryption techniques, on the other hand, are not very ideal for image encryption due to some particular characteristics of digital images, such as large storage capacity, high redundancy, and strong correlation among adjacent pixels. Many researchers developed new image encryption algorithms in addition to standard image encryption techniques in order to improve image encryption. Chaos-based algorithms have demonstrated extraordinary qualities in numerous areas, including security, complexity, speed, processing power, and computational overhead, among others. Chaos-based encryption isn't a novel concept. A chaotic function was utilized to develop a cryptographic algorithm back in 1989 [5]. Although there aren't many specific chaos-based image encryption techniques in the literature, there are a few, which are briefly reviewed here.

The CKBA (chaotic key-based algorithm) encryption method was proposed [6]. The technique creates a time series based on a chaotic map, which is then used to build a binary sequence as a key. Image pixels are rearranged according to the binary sequence generated, and then XOR or XNOR operations are performed with the selected key. This method is incredibly easy, but it has significant security flaws, as recently pointed out in [7]. This technique is vulnerable to a chosen/known-plain-text attack that uses only one plain-image, and its security against a brute-force attack is also debatable. Dang *et al* [8] introduced a joint image compression and encryption method in 2000, applying the Discrete Wavelet Transform (DWT) for compression as well as DES for encryption.

[9] presented a novel image encryption scheme. This approach involves the utilization of an encryption key derived from the Arnold chaos sequence. Subsequently, the initial image undergoes encryption through a modified AES algorithm, employing the round keys generated by the chaos system. The modified AES encryption process encompasses ten rounds, wherein the conventional column substitution and integration operations are replaced by linear transformations and pixel value summation procedures.

[10] introduces an image encryption scheme that combines a discrete-time alternating quantum walk (AQW) with the advanced encryption standard (AES). Quantum properties are leveraged to enhance the AES algorithm, employing a keystream generator linked to AQW parameters for creating a probability distribution matrix. Key derivation involves extracting specific singular values from this matrix to replace the Rcon in the AES algorithm. Furthermore, the ascending order of the cloned probability distribution matrix reorders the mapping rules for the S-box and ShiftRow transformations within the AES algorithm. This approach utilizes a probability distribution matrix alongside a plaintext XOR operation for preprocessing and employs a modified AES algorithm to accomplish the encryption process.

For image encryption, mathematical algorithms are used to convert the original images into ciphered images which are hard to interpret. Hence to increase resistance against security attacks, such as statistical [11] and differential attacks [12] and to meet the said security constraints, several image encryption techniques have been developed. Some of these includes digital watermarking techniques [13], image scrambling methods [14], image steganography [15] and image cryptography [16]. In the last few decades, the manipulation of chaos in cryptography has shown keen interest due to its major property of sensitivity to initial conditions give the form of randomness. To design efficient image encryption systems, numerous Chaos-based cryptographic models [17–19] have been used to develop novel methods which exhibits remarkably good features in many aspects regarding speed, cost, computational power, computational overhead, complexity, etc.

The following is a summary of the paper's structure:

Section 2 describes the AES algorithm, chaos systems and maps especially Arnold map. Section 3 presents the proposed image encryption algorithm. Section 4 explains the results and analysis of the proposed algorithm. Section 5 includes conclusion.

2. Preliminaries

2.1. Chaos theory

Chaos theory is a developing branch of mathematics that analyses nonlinear systems. When these systems are properly initiated, they exhibit chaotic behavior during iterations. Chaotic behavior is a type of state behavior that is irregular and hence appears to have noise-like features. Despite the fact that it is aperiodic, the chaotic trajectory never exactly repeats itself, it is entirely predictable given the precise initial conditions with parameter values. These chaotic qualities are utilized to produce an aperiodic sequence that will be used as the keystream in the encryption system.

The chaos system includes the following characteristics:

(1) Initial value sensitivity: minor changes in the initial value result in a completely new sequence, which is done through repeated calculations on a chaos map using parameters.

(2) Parameter sensitivity: minor changes in the parameters result in a completely different sequence, which is achieved through repetitive calculations on a chaos map with the input data.

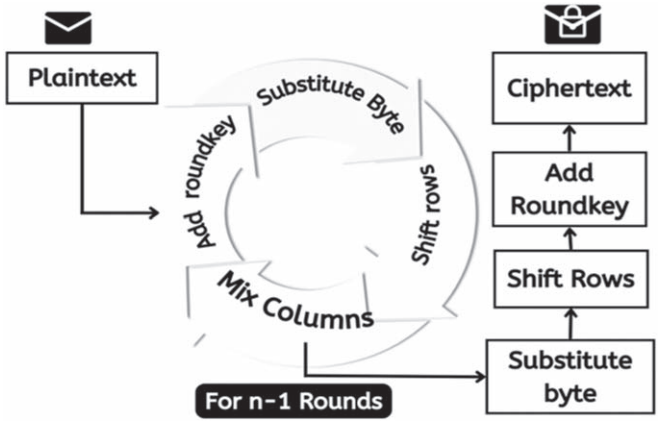

Figure 1. Basic working of AES.

(3) Randomness: the chaotic sequences generated by the chaos maps are generally pseudorandom sequences with extremely complicated structures for analysis and prediction.

2.2. Arnold scrambling

Scrambling is an important topic in image encryption. The scrambling transformation changes the pixel location of original image from the original pixel position. The old and new pixel positions determine the 'degree of scrambling.' The larger the distance, the larger is the degree of scrambling. Not the pixel grey values but only the pixel coordinates are changed during scrambling, as a result, the image's actual components appear to be buried, making it difficult for the interceptor to detect them. Arnold scrambling is one of the most extensively utilized scrambling strategies which is defined below:

$$\begin{pmatrix} s' \\ t' \end{pmatrix} = \begin{pmatrix} 1 & a \\ b & 1+ab \end{pmatrix} \begin{pmatrix} s \\ t \end{pmatrix} (\mathrm{mod}\ M) \text{ where } a \geqslant 1 \text{ and } b \geqslant 1 \tag{1}$$

2.3. Advanced encryption standard

The Advanced Encryption Standard (AES) is the most popular and commonly used symmetric encryption algorithm available nowadays. Discovered in 2000, AES is found to be six times faster than DES. The following are the characteristics of AES:

- Symmetric block cipher with symmetric key.
- Data is in 128 bits, key size is 128/192/256 bits and has 10, 12 and 14 rounds for key size 128, 192 and 256 respectively [20].
- It is stronger and faster than Triple-DES.
- Specifications and design specifications are fully provided.

Figure 1 describes the block diagram of AES and its rounds:
There are four primary operational blocks in AES, which are as follows:

(1) Sub byte Substitution: This is a nonlinear byte substitution that uses a substation table (s-box) that is constructed using multiplicative inverse and affine transformations.

(2) Shift rows: is a straightforward byte transposition. The bytes in the state's last three rows are cyclically shifted; the left shift offset ranges from one to three bytes.

(3) Mix columns transformation: This is the same as a matrix transformation. The states' columns are multiplied by a predetermined matrix.

(4) Add round key: Is it just a simple XOR between the round key and the working state.

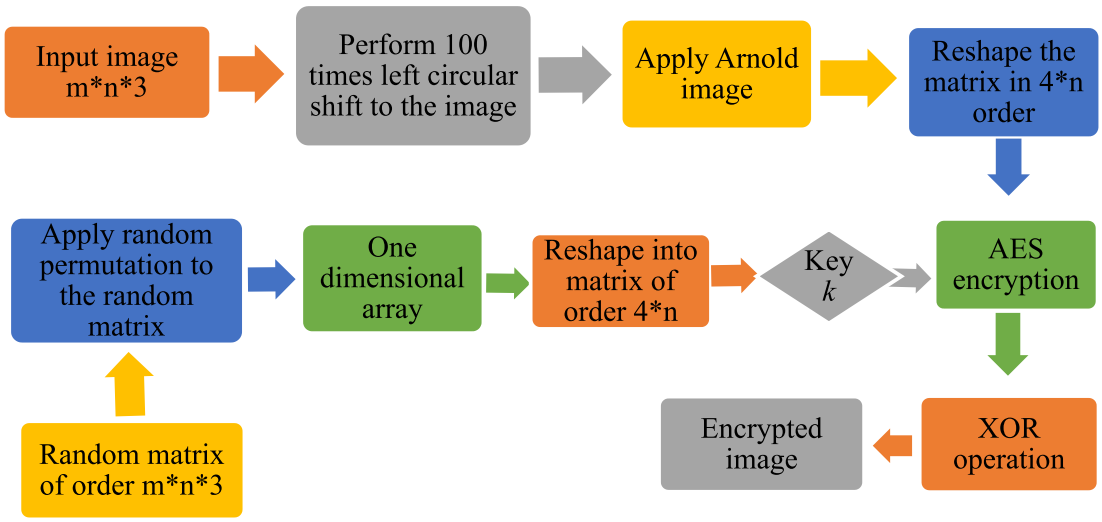

Figure 2. Flowchart of proposed encryption algorithm.

3. Proposed image encryption scheme

Three vital aspects should be considered while developing an algorithm:

- The algorithm must be simple to be tested and evaluated fully and rapidly.
- The design must make use of well-known, tested, and reliable techniques and concepts.
- An encryption algorithm must provide a security margin against possible attacks that is higher than the required number [21].

Our suggested encryption system is being built while taking into account all of these aspects. Application of Arnold map with AES has been carried out.

3.1. Image encryption and decryption scheme

Three steps make up the method we suggest. Key generation is done first using a random matrix and random permutation. After saving this key, further use of this key is made by using it in the rounds of AES encryption and decryption. Next, an input image is taken and circularly left shifted 100 times. Then this rotated image into a 4 x N matrix, where N is the input image's number of columns. The image is then permuted using an Arnold map. After that AES encryption algorithm is applied using generated.

The flowchart of our proposed encryption scheme is presented in figure 2.

Our suggested encryption algorithm employs the random matrix to generate the key which is being used in AES algorithm and then further using the permutation for more randomness. Suppose that the original image is of $p \times q \times 3$ pixels in size and that the encryption will take n rounds. So we need a key matrix of the same size in AES algorithm.

3.1.1. Algorithm 1 (Key generation)

Input: Random matrix having order $p \times q \times 3$

Output: Encryption key k

Step 1. Give an input of a random matrix having order $p \times q \times 3$

Step 2. Transform this random matrix in an array of random integers having no repeating values using random permutation command.

Step 3. Rearrange this array in order of $4 \times n$ where n is the number of columns of random matrix.

Step 4. Save this key as k.

3.1.2. Permutation and implementation of AES

This stage involves reshaping the initial pixels of an image. The input image is hundred times rotated to left and then Arnold map is used to permute the pixel values. The key k which was generated in the algorithm 1 of our scheme, is utilized in the AES algorithm.

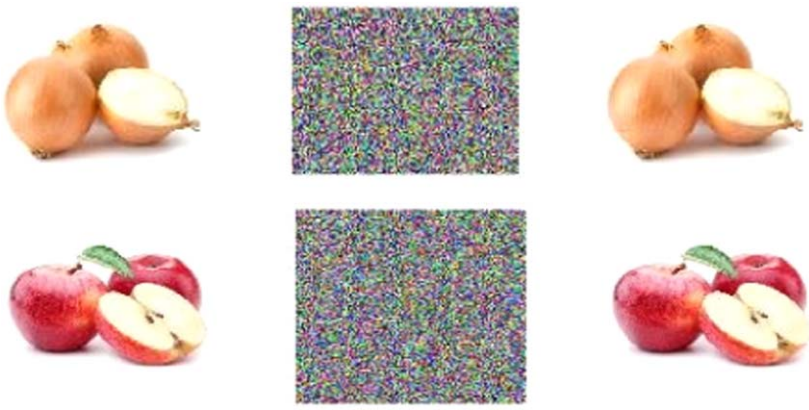

Figure 3. Original, encrypted and decrypted image of Onion and Apple (256 × 256) from our proposed scheme.

3.1.3. Algorithm 2 (AES with the generated key)

Input: An image M of $p \times q \times 3$, key k generated by Algorithm 1.

Output: Encrypted image of order $p \times q \times 3$.

Step 1. Input the image having order $m \times n \times 3$.

Step 2. Apply hundred times left circular shift to the inserted image.

Step 3. Perform iterations of the Arnold map mentioned in equation (1) on above rotated image.

Step 4. Reshape this chaotic image into matrix of order $4 \times q$, and q denotes the number of columns of the matrix.

Step 5. Apply all rounds of AES encryption to the image produced in above step using the key generated in algorithm 1.

Step 6. After that, apply XOR operation to the image.

Step 7. Reshape the resultant matrix in the order $p \times q \times 3$.

Step 8. Save the resultant matrix as an encrypted image.

3.1.4. Image decryption algorithm

The encryption and decryption procedures are quite similar but just differ in a way that all the stages of encryption are to be performed in reverse direction. The decryption algorithm initially involves the XOR operation and uses the same key generated by the algorithm 1, used in the encryption procedure and then the decryption process begins.

Input: Encrypted image of order $p \times q \times 3$.

Output: The original image

Step 1. Apply inverse XOR operation.

Step 2. Apply all rounds of AES decryption algorithm with the generated key.

Step 3. Apply inverse Arnold map to the resultant matrix.

Step 4. Reshape the state array in a matrix of order of input image.

Step 5. Perform 100 times right circular shift to the reshaped image.

Step 6. The resultant image is saved and it is similar to original image.

Our proposed encryption technique is analyzed using MATLAB 2018a. The encrypted image is obtained by going through the processes of pixel permutation, AES with generated key and diffusion. The original image is obtained by the decryption technique of AES. We used the image of Onion and Apple (256×256 pixels) for testing our proposed encryption technique. During encryption, we have used key generated through random matrix and permutation operations.

The tests and analysis are performed on the sample image of Onion and Apple for comparison of our scheme with other image encryption schemes. The original image, encrypted image and decrypted image of Onion and Apple (256 × 256) obtained from our proposed algorithm is shown below (figure 3).

4. Results and analysis

Differential and statistical analysis of the proposed encryption scheme is described in detail throughout this section. The proposed technique is compared using different tests. These tests are the parameters for proving our proposed encryption and decryption technique to be correct and applicable.

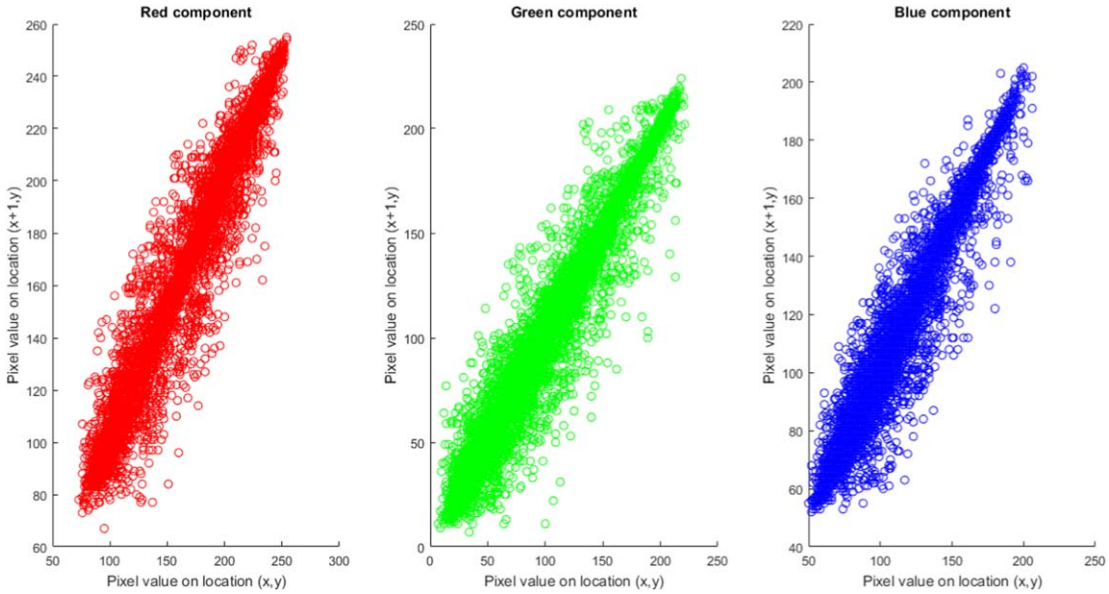

Figure 4. Correlation of Onion image (256 × 256).

4.1. Correlation analysis of adjacent pixels

The correlation coefficient of neighboring pixels tells the relation of adjacent pixels of an image with one another. The adjacent pixels of plain image in all three dimensions (vertical, horizontal and diagonal) have high correlation which is about 1. On the other hand, an encrypted image should have minimum correlation which is approximately 0 [22]. The correlation value is calculated by the following formula:

$$C_r = \frac{n(\sum_{i-1}^{n} r_i t_i - \sum_{i-1}^{n} t_i)}{(n\sum_{i-1}^{n}(r_i)^2 - (\sum_{i-1}^{n} r_i)^2\left(\left(n\sum_{i-1}^{n}(t_i)^2 - (\sum_{i-1}^{n} t_i)^2\right)\right)} \tag{2}$$

Here r_i and t_i are the two pixel values in the adjacent position and n is the total number of pixel values used to calculate the relationship of these pixel values.

The following figures 4–6 show the correlation of original image, diagonal wise and row wise correlation of encrypted image respectively.

The following table 1 shows the correlation coefficient values of image of Onion and Apple (256 × 256).

4.2. Statistical analysis of histogram

To highlight the irregularity in encrypted images, the histogram analysis is performed which must show that histogram of encrypted image is considerably different from plain image and homogeneous in all red, blue and green levels, making it impossible for attackers to obtain any meaningful information. The pixels in any input image are not uniform and differ widely at each part of the image, indicating that the data is immensely vulnerable to attack, but when we look at the image pixels of the encrypted image (figure 7), it is clear that each pixel is much focused and uniform in all directions. The concentrated uniformity of pixels indicates that the image is secure to statistical attacks.

4.3. Mean square error analysis

This test is performed to determine the accuracy and variance between plain and encrypted images. A higher MSE value means that there is a larger variation between the original and the cipher image. This analysis is performed using the following formula:

$$MSE = \frac{1}{p \times q \times 3}\sum_{i=0}^{r-1}\sum_{i=0}^{q-1}(J_o(x, y) - J_c(x, y))^2 \tag{3}$$

Where p denotes the rows and q denotes the columns of the image J. J_o and J_c represents the original and cipher image respectively. MSE should always be greater or equal to 30 *db* for the difference between the input and the output image. Table 2 shows the mean square ration for our proposed algorithm.

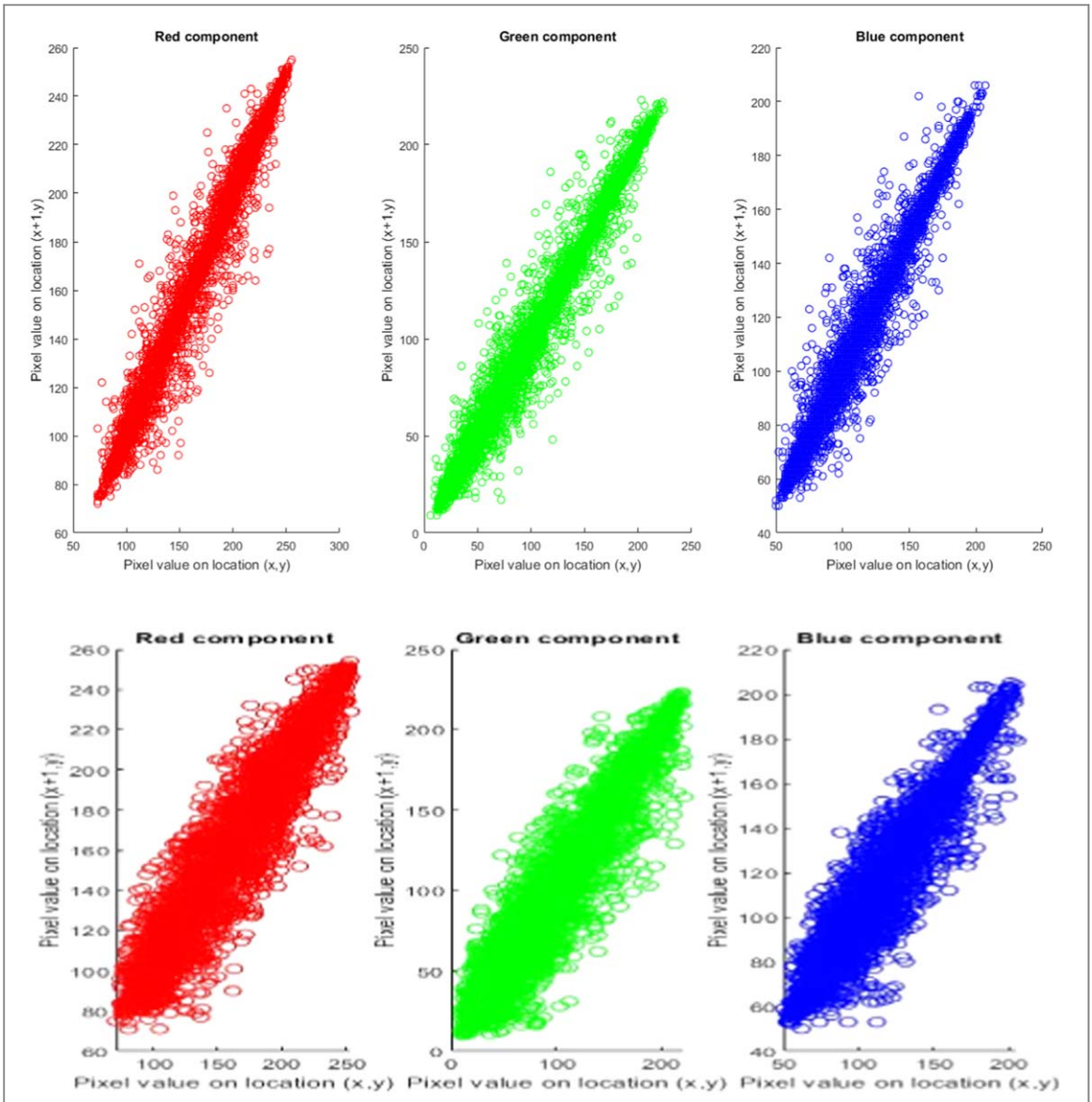

Figure 5. (a) Diagonal wise Correlation of Onion image (256 × 256). (b) Row wise correlation of original image of Onion (256 × 256).

4.4. Peak signal to noise ratio analysis (PSNR)

In this analysis, we examine how good or bad our plain and cipher images are i.e. to measure the quality of these images. The formula in the equation (3.4) is used to calculate its value.

$$PSNR = 10.\log\frac{255^2}{MSE}(db) \tag{4}$$

The PSNR between both the plain and encrypted image should be as low as possible for the encryption technique to succeed. Table 2 displays the PSNR value related to our proposed encryption technique. For good security of encrypted image, it should be limited to a minimal number.

4.5. Sensitivity analysis or differential evaluation

The image after encryption must be noticeably different from the actual image, which is a difficult problem for all cryptosystems to achieve. In our proposed technique, we apply NPCR (Number of Pixel Changing Rate) and UACI (Unified Average Changing Intensity) to measure the difference of original image and encrypted image. When the value of NPCR is increased, a more effective cryptosystem is built, which will guarantee resistance to various threats. Both of these tests can be calculated using the formulas shown in the equations (5) and (6) respectively.

$$NPCR = \frac{\sum_{i,j} M(i,j)}{b \times h} \times 100 \tag{5}$$

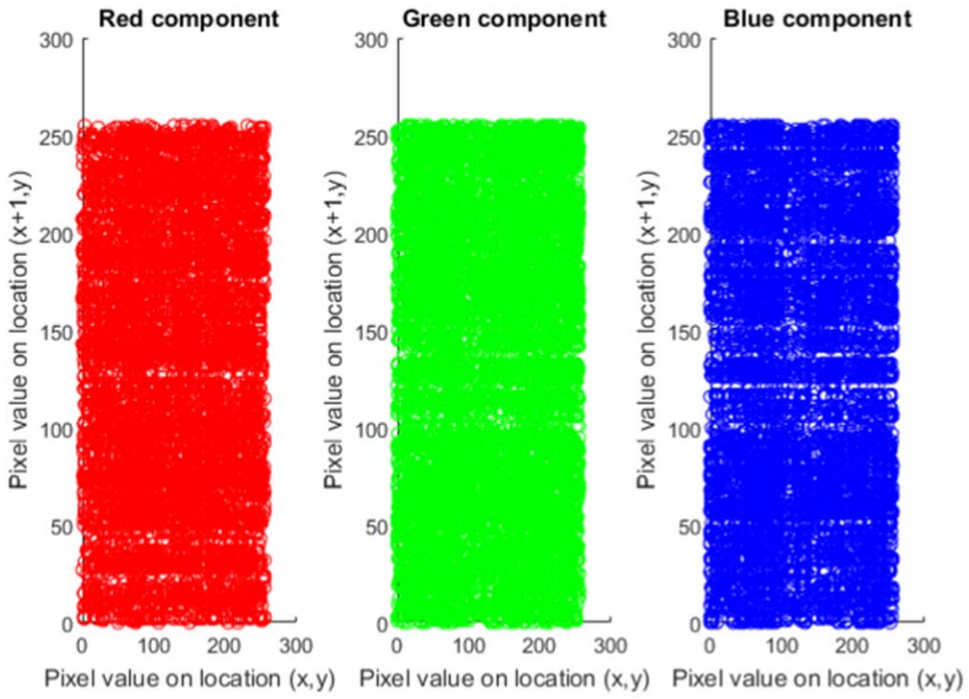

Figure 6. Row-wise correlation of encrypted image of Onion.

Table 1. Correlation coefficient of original onion and apple image.

		Red		Green		Blue	
	Direction\color	Original image	Encrypted image	Original image	Encrypted image	Original image	Encrypted image
Onion	Vertical	0.9574	−0.00290	0.95891	−0.00630	0.92380	−0.00144
	Horizontal	0.97933	0.000391	0.98051	−0.00141	0.96051	0.00744
	Diagonal	0.9366	−0.00491	0.93991	−0.000191	0.89001	0.00630
Apple	Vertical	0.9564	−0.00280	0.95791	−0.00641	0.93270	−0.00324
	Horizontal	0.97833	0.000381	0.98250	−0.00130	0.95451	0.00655
	Diagonal	0.9356	−0.00391	0.93590	−0.000281	0.89101	0.00636

$$UACI = \frac{1}{b \times h}\left[\sum_{i,j}\frac{|Z(i,j) - Z'(i,j)|}{255}\right] \times 100 \tag{6}$$

In above equation, b shows the width and h represents the height of the encrypted image, respectively. Z is representing the image that has been encrypted while Z' is representing the one pixel change in original image.

$$If \quad Z \neq Z',\ Z(i,j) = 1;$$

$$else,\ Z(i,j) = 0$$

The NPCR value should be greater than the ideal value to improve encryption quality. Table 3 shows the comparison of NPCR and UAIC valuse of our proposed technique with some of the recent studies.

4.6. Information entropy analysis

This analysis calculates the irregularity of concentrations of pixels in an encrypted image. Also this is used to analyze the unpredictability of encrypted images. The entropy is calculated using the following formula:

$$H(c) = \sum_{i=0}^{255} P(c_i)\log_2\frac{1}{P(c_i)} \tag{7}$$

Where $H(c)$ is the entropy of cipher image c, $P(k)$ is the probability of the occurring of symbol k. The entropy of an image after encryption according to NIST criteria must be approximately 8 for improved encryption quality and image security. The entropy value of our proposed scheme is 7.9980. Table 4 enlists the entropy values of

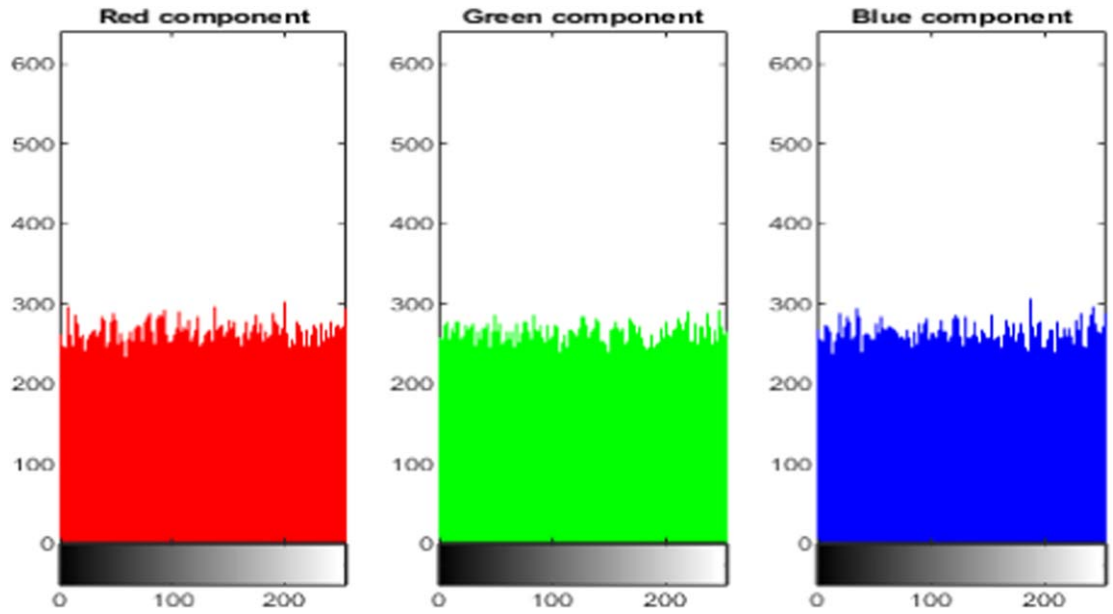

Figure 7. Histogram of encrypted image (Onion).

Table 2. PSNR and MSE value of our suggested scheme.

	Onion		Apple	
Criteria(approximate value)	PSNR	MSE	PSNR	MSE
Suggested Algorithm	8.36940	8763.11	8.70123	8769.15

Table 3. Comparison of various NPCR and UACI.

Image encryption techniques	NPCR	UACI
[21]	99.6368	33.4724
[23]	99.66	33.622
[24]	99.366	32.721
[25]	99.6491	30.52370
Proposed Technique (Onion)	99.590	33.390

Table 4. Entropy values of different encryption schemes.

Image encryption techniques	Entropy values
[21]	7.9975
[23]	7.9834
[24]	7.9800
[25]	7.9976
Proposed Technique (Onion)	7.9990

different encryption techniques. The entropy of our proposed scheme shows that our encryption technique produces more irregularity in encrypted image which means that encryption gives better results.

4.7. Key space analysis

The key space should be large enough to give a greater security level or to prevent brute-force attack. However, it must not be less than 10^{30} [24]. The suggested approach employs a 128-bit AES key and two initial conditions for

Table 5. NPCR, Entropy, UACI, MSE and PSNR analysis of current scheme.

Analysis of image encryption technique	NPCR	Entropy	UACI	MSE	PSNR
Proposed Scheme	99.59	7.9991	33.39	8783.6	8.3694

Arnold scrambling. Considering the computing complexity of a 64-bit double-precision parameter to be 10^{15} in accordance with the IEEE floating-point standard. The total number of possible keys will be:

$$\text{Total key space} = 10^{128} \times 10^{15} \times 10^{15} = 10^{158}$$

As key size of our proposed algorithm is large enough, so it is highly strong to be safe from brute force attack.

4.8. Key sensitivity analysis

Any encryption scheme has a crucial part known as secret key which acts as a core of that scheme. One key is used in our suggested encryption technique. The current technique entirely affects the output of the decryption algorithm even for very little variations in the components of the secret key. It implies that if we are adding 10^{-16} in the key k, we will not be able to decrypt the original picture utilizing that similar key. It is evident that not a single clue of plain or input image is there in the cipher or output image. Our suggested encryption and decryption algorithms are extremely sensitive to secret keys. The entropy value, NPCR, MSE, UACI, and PSNR values of our suggested image encryption scheme is presented in the following table 5.

5. Conclusion

In our research, we presented a novel image encryption technique which utilizes AES (Advanced encryption standard) and Arnold map. In AES encryption scheme, key is generated by permuting a random matrix and Arnold's map helps to convert the matrix of original image into more complex form. The proposed technique is resistant to many cryptographic attacks which we have shown in the security analysis. The security analysis includes, key sensitivity analysis, NPCR, UACI, key space analysis and entropy analysis. The result of these analysis shows that our proposed technique is secure and more efficient than the traditional AES technique and it may have application in the encryption of digital media sent over internet.

Acknowledgments

Princess Nourah bint Abdulrahman University Researchers Supporting Project number (PNURSP2023R236), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia.

Data availability statement

The data cannot be made publicly available upon publication because no suitable repository exists for hosting data in this field of study. The data that support the findings of this study are available upon reasonable request from the authors.

Conflicts of interest

The authors declare that they have no conflicts of interest.

ORCID iDs

Saba Inam https://orcid.org/0000-0003-3218-1427
Shamsa Kanwal https://orcid.org/0000-0001-6392-2406

References

[1] Pan H, Lei Y and Jian C 2018 Research on digital image encryption algorithm based on double logistic chaotic map *EURASIP Journal on Image and Video Processing* **2018** 1–10
[2] Taleb S M, Fakhri M A and Adnan S A 2020 Optical investigations of nanophotonic LiNbO3 films deposited by pulsed laser deposition method *In Defect and Diffusion Forum* **398** 16–22 Trans Tech Publications Ltd
[3] Smid M E and Branstad D K 1988 Data encryption standard: past and future *Proc. IEEE* **76** 550–9

[4] NIST FIPS 197-upd 1 2023 Advanced Encryption Standard (AES), National Institute of Standard and Technology (https://doi.org/10.6028/NIST.FIPS.197-upd1)
[5] Matthews R 1989 On the derivation of a 'chaotic' encryption algorithm *Cryptologia* **13** 29–42
[6] Chen G, Mao Y and Chui C K 2004 A symmetric image encryption scheme based on 3D chaotic cat maps *Chaos, Solitons Fractals* **21** 749–61
[7] Li S and Zheng X 2002 Cryptanalysis of a chaotic image encryption method *2002 IEEE Int. Symp. on Circuits and Systems. Proc. (Cat. No. 02CH37353) (Vol. 2, pp. II-II). IEEE*
[8] Dang P P and Chau P M 2000 Image encryption for secure internet multimedia applications *IEEE Trans. Consum. Electron.* **46** 395–403
[9] Arab A, Rostami M J and Ghavami B 2019 An image encryption method based on chaos system and AES algorithm *The Journal of Supercomputing* **75** 6663–82
[10] Liu G, Li W, Fan X, Li Z, Wang Y and Ma H 2022 An image encryption algorithm based on discrete-time alternating quantum walk and advanced encryption standard *Entropy* **24** 608
[11] Hurley N, Cheng Z and Zhang M 2009 Statistical attack detection *In: Proc. of the Third ACM Conf. on Recommender Systems* 149–56
[12] Lu J, Dunkelman O, Keller N and Kim J 2008 New impossible differential attacks on AES *International Conference on Cryptology in India* (Springer) 279–93
[13] Shah T, Jamal S S *et al* 2020 An improved chaotic cryptosystem for image encryption and digital watermarking *Wireless Personal Communication* **110** 1429–42
[14] Zeng W and Lei S M 2003 Digital image scrambling for image coding systems *US Patent* 6,505,299
[15] Morkel T, Eloff J H and Olivier M S 2005 An overview of image steganography *In: ISSA* **1** 1–11
[16] Bhowmik S and Acharyya S 2011 Image cryptography: the genetic algorithm approach *In: 2011 IEEE Int. Conf. on Computer Science and Automation Engineering, IEEE* **2** 223–7
[17] Kanwal S, Inam S, Othman M T B, Waqar A, Ibrahim M, Nawaz F and Hamam H 2022 An effective color image encryption based on Henon Map, Tent Chaotic Map, and orthogonal matrices *Sensors* **22** 4359
[18] Kanwal S, Inam S, Cheikhrouhou O, Mahnoor K, Zaguia A and Hamam H 2021 Analytic study of a novel color image encryption method based on the chaos system and color codes *Complexity* **21** 1–17
[19] Kanwal S, Inam S, Hajjej F, Cheikhrouhou O, Nawaz Z, Waqar A and Khan M 2022 A new image encryption technique based on sine map, chaotic tent map, and circulant matrices *Security and Communication Networks* **22** 4152683 17
[20] Stallings W 2002 The advanced encryption standard *Cryptologia* **26** 165–88
[21] Arab A, Rostami M J and Ghavami B 2019 An image encryption method based on chaos system and AES algorithm *The J. Supercomput.* **75** 6663–82
[22] Pisarchik A N and Zanin M 2008 Image encryption with chaotically coupled chaotic maps *Physica D* **237** 2638–48
[23] Ahmad J and Hwang S O 2016 A secure image encryption scheme based on chaotic maps and affine transformation *Multimedia Tools Appl.* **75** 13951–76
[24] Ahmad J and Hwang S O 2015 Chaos-based diffusion for highly autocorrelated data in encryption algorithms *Nonlinear Dyn.* **82** 1839–50
[25] Shadangi V, Choudhary S K, Patro K A K and Acharya B 2017 Novel Arnold scrambling based CBC-AES image encryption *International Journal Control Theory and Applications* **10** 93–105