The Journal of Supercomputing (2019) 75:6663–6682
https://doi.org/10.1007/s11227-019-02878-7

An image encryption method based on chaos system and AES algorithm

Alireza Arab[1] · **Mohammad Javad Rostami**[1] · **Behnam Ghavami**[1]

Published online: 10 May 2019

Abstract

In this paper, a novel image encryption algorithm is proposed based on the combination of the chaos sequence and the modified AES algorithm. In this method, the encryption key is generated by Arnold chaos sequence. Then, the original image is encrypted using the modified AES algorithm and by implementing the round keys produced by the chaos system. The proposed approach not only reduces the time complexity of the algorithm but also adds the diffusion ability to the proposed algorithm, which make the encrypted images by the proposed algorithm resistant to the differential attacks. The key space of the proposed method is large enough to resist the brute-force attacks. This method is so sensitive to the initial values and input image so that the small changes in these values can lead to significant changes in the encrypted image. Using statistical analyses, we show that this approach can protect the image against the statistical attacks. The entropy test results illustrate that the entropy values are close to the ideal, and hence, the proposed algorithm is secure against the entropy attacks. The simulation results clarify that the small changes in the original image and key result in the significant changes in the encrypted image and the original image cannot be accessed.

Keywords AES encryption algorithm · Arnold chaos sequence · Linear conversion · Correlation

✉ Alireza Arab
alirezaarab@eng.uk.ac.ir

Mohammad Javad Rostami
rostami@uk.ac.ir

Behnam Ghavami
ghavami@uk.ac.ir

[1] Shahid Bahonar University of Kerman, Kerman, Iran

1 Introduction

Recently, with the rapid advances in the communication technology, the digital image transmission has become a popular issue. Digital images form 70% of the transmitted data through the Internet. However, the advanced computer processors have made it easy to illegally access the transmitted data on the Internet.

Not only limited to everyday life of the common people, image transmission has military, medical and industrial applications too. In these applications, the image security against the different attacks is of high importance. The most important method of providing the images security is the image encryption. On the other hand, the time interval in which the image is sent from the sender to the receiver is very prominent, because irreparable damages may be happened, if the delay is more than the threshold. Hence, the encryption algorithm used for such applications must provide high security and low running time in order to meet the desired requirements. For these reasons, all the existing image encryption algorithms are not appropriate for these applications.

Several standard encryption algorithms have been proposed for the text encryption. Due to the high volume, correlation between adjacent pixels and redundancy of the visual data, these algorithms are encountered with very low security and high encryption time. Hence, these algorithms are not suitable for the image encryption. Further to these, due to the mentioned features of the visual data, these image encryption algorithms cannot resist statistical, differential and other attacks and easily fail [1]. To overcome these problems, various image encryption algorithms have been introduced. If the image encryption algorithm can successfully overcome the above-mentioned problems, it can ensure the security of the image. In the image encryption, several evaluation criteria must be considered including the information entropy, correlation between adjacent pixels, the number of pixels change rate (NPCR) and unified average changing intensity (UACI). If the values of these criteria meet the desired expectancy, this means that the algorithm can resist the statistical and differential attacks [2]. Besides, an image encryption algorithm must have a big key space and high sensitivity to the initial conditions in order to resist the brute-force attacks [2]. In addition, the algorithm must be fast in real-time applications.

Combining the chaos system and standard encryption algorithm of AES, this paper proposes an image encryption algorithm. First, the encryption key is built using Arnold chaos system, and then, the image is encrypted by using the proposed algorithm (we name it as CCAES (*c*ombining the chaos and *AES*) in the rest of the paper) which is the modified AES one. The difference between the modified AES and standard one is that the operational block of the modified algorithm is of the same size as the image and the substitution and column integration operations in this algorithm are replaced by other operations. These modifications have made the proposed algorithm faster than the initial AES one and even resistant to all kinds of attacks. These results are explained in detail in the following sections. Therefore, the proposed image encryption algorithm can be an appropriate candidate for the confidential and real-time image data.

The paper is organized as follows: Sect. 2 reviews the literature. Section 3 explains the initial AES and chaos system. Section 4 illustrates the proposed algorithm in detail. Section 5 presents the analysis of the results and discussion and a comparison between the proposed method and other applied ones. Finally, Sect. 6 provides the conclusions.

2 Related work

In this section, the previously conducted studies are investigated in two different categories.

2.1 Encryption algorithms using the chaos system

An encryption algorithm has been presented by Norouzi et al. [1] according to the hyper-chaotic systems. The advantages of this suggestive approach include the need for only one round of diffusion processing and the simple calculations. High security, severe sensitivity to the key and high sensitivity to the original text are the other features of this method. The key stream generated by the hyper-chaotic systems is related to the original image. In addition, for encrypting each pixel, the set of pixels before that pixel are used. The algorithm uses different sets for encrypting various input images. This, in turn, improves the resistance of the encryption system against the differential, known-plain text and chosen-plain text attacks. In this paper, the NPCR and UACI are high. Also, the results of the experimentations such as the key space analysis, histogram, correlation coefficient, information entropy, the highest proportion of signal to noise, key sensitivity analysis, and differential analysis and decryption quality clarify that the proposed image encryption algorithm is secure and reliable and can be used for secure image communication applications.

A beta-based chaos map was used for generating the chaos sequence [3]. This approach is divided into three steps: permutation, diffusion and substitution. The pseudorandom sequence is generated in order to replace the image pixel locations to eliminate the relation between the original and encrypted images. Hence, the severity of the resistance of the encrypted image increases against the attacks.

Wang et al. [4] proposed a hyper-chaotic plan and bit area permutation for the colorful image encryption. First, the colorful image of $M \times N$ size is converted to the grayscale image of $M \times 3N$. Then, this image is converted to an even matrix and the matrix changes into an irregular linear plot at bit level with mapping combination. Next, the Chen system is applied in order to simultaneously encrypt the combinations of red, green and blue. The experimental results and security analyses indicate that not only the plan can provide good encryption achievements, but also the original space is large enough which enables this method for resisting against attacks.

Guan et al. [5] proposed a novel image encryption plan. In this algorithm, first, Arnold cat mapping is used to identify the locations of the image's pixels in the spatial domain. Then, the output signal is preprocessed using Chen chaos mapping. After that, the converted image due to Arnold mapping is encrypted with

the preprocessed signal in a pixel-to-pixel manner. The experiment results show that the original space is so large to resist the attacks. Also, the grayscale parts of the encrypted image are distributed randomly. The encryption algorithm of this approach has three advantages: (1) the key space is large enough which makes it resistant against all kinds of attacks, (2) the encrypted image has an appropriate statistical feature, and (3) the encryption algorithm is very sensitive to the keys.

An efficient image encryption algorithm with Arnold chaos map is presented in [6], which uses substitution and diffusion steps. Instead of the traditional location substitution, this approach uses a circular function. Then, in the diffusion step, a double diffusion function is used by implementing the new key stream generator. The key stream depends on the processed image.

Patro and colleagues propose an effective and simple digital image encryption scheme that combines one-dimensional chaos mapping to carry out multi-mode rotation based on permutation operations and the various stages of publishing operations [7].

In 2018, Patro and Acharya provide an image encryption technique based on multi-level permutation operations, which is different from the current multiple image encryption techniques. This method uses three-level permutation. Patro et al. propose a cryptographic technique based on the combination of chaos and super-chaos for providing image security [8].

Among many algorithms, when the images are encrypted using chaotic techniques, the output of algorithms provides a randomized image, which makes it possible to reduce the possibility of breaking the encryption. Hence, cryptographic algorithms for digital images based on chaos techniques have become an important principle of digital image encryption [9].

In 2019, Sravanthi et al. provide a bit-plane-based image encryption technique using piece-wise linear chaos mapping (PWLCM) and logistic-adjusted-sine two-dimensional mapping [10].

2.2 AES-based encryption algorithms

In this method, multi-step bitwise permutation operations are performed with a round of propagation to obtain better cryptographic results. The main purpose of the method introduced in [11] is to design a dynamic S-box to achieve nonlinear properties and low automatic correlation. In this study, they introduced a dynamic sub-key-dependent S-box to overcome the stagnant S-box weaknesses.

In the image encryption by AES, which is a block encryption approach, since the adjacent pixels have high correlation, a shadow of the original image is left in the encrypted image after the encryption. To overcome this problem, in a key stream generator has been introduced in [12]. There are two kinds of the stream generators including the A5/1 and W7 key stream generators. These generators are made of some register shifts and a series of functions, and W7 shows a better encryption performance rather than A5/1.

The chaotic AES encryption algorithm is explained in [13], in which a chaotic S-box is used which is highly random and sensitive to the initial conditions.

Sensitivity to the initial conditions enables the algorithm to use the initial conditions as another key to provide more security and confidentiality.

In [14], first the original image is used as the input. Then, the rows and columns of the image's pixels are right-shifted to a certain value in order to remove the correlation between the adjacent pixels. The next step is to create the keys based on the location of the mouse on the screen. Given these keys as the primary keys and using the key expansion function, 11 round keys of AES algorithm are generated. These keys are sequentially given to AES algorithm to convert the original image to the encrypted one. This algorithm provides better encryption results regarding the security against the statistical attacks.

In the image encryption, the image is initially divided into the blocks, each consisting of several pixels. The rows and columns corresponding to the original image are distorted using the shift technique which reduces the correlation between the adjacent pixels [15]. This method has been examined using the histogram analysis, information entropy, correlation analysis and differential analysis. The obtained results show that the proposed algorithm provides better security and performance rather than the AES one without shifting technique. As a result, this technique provides appropriate encryption of the multimedia data. Furthermore, the encrypted image by this algorithm meets uniform histogram, reduced pixels correlation and high entropy.

In [16], AES algorithm with mixed approach, dynamic key and S-box generation is proposed. The dynamic key is generated using the time function. This key is randomly generated based upon the time in which the sender is connected to the system. Using the encryption key, the static S-box is converted to the dynamic one. Using the mixed approach, the proposed algorithm provides high security for the data transfer. Also, it adds more complexity to AES algorithm for increasing the substitution and diffusion characteristics. In addition, this approach protects well from the message against the brute force, differential, algebraic and linear attacks.

An image encryption approach is proposed in [17], according to the 2-D logistic map and AES algorithm. First, the image is encrypted using the 2-D logistic system, and then, the encrypted image is sent to AES algorithm for re-encrypting. This approach provides better security level for colorful images. In addition, this algorithm is highly sensitive to the key volume so that only the accurate key volume can decrypt the image.

According to the magic cube turning, an encryption algorithm has been proposed for protecting the image security [18]. In this approach, the original image is divided into six sub-images and each sub-image is added to one side of the magic cube. Then, using the hash function and confidential key, the turn table is generated by which one could turn the rows and columns of the magic cube's surfaces. The turned image is added to AES algorithm for the re-encryption process. The smaller the size of the image blocks given to the magic cube's surfaces, the better the encryption. This algorithm provides an appropriate security level against various attacks.

There are symmetric key encryption techniques which need only one key for data encryption and decryption. They are easy in design but easily decrypted by brute-force attacks. If the attacker can access the key, the whole encryption security is at risk. On the other hand, asymmetric key-based encryption techniques use a pair of

keys: one for encryption and the other for decryption. The latter has a better security than the former; however, it is more time-consuming. Besides, it is also difficult to manage such huge keys efficiently and securely. The study conducted in [19] focuses on implementing a system capable of encrypting and decrypting the multimedia data. This system uses a mixed model based on the integration of symmetric encryption techniques such as AES and asymmetric ones such as ECC.

With the change in the shifting step of the rows in AES algorithm, a more secure and better image encryption algorithm has been proposed [20]. In the shifting step, this algorithm investigates whether the (0, 0) component of the state matrix is even or odd. If the value is odd, then the first and third rows remain unchanged and the second and fourth rows go under one and three cyclic shifting units to the left, respectively. If the value is even, the first and fourth rows do not change and the second and third rows go under three and two cyclic shifting units to the right, respectively. The results show that the proposed algorithm has a better encryption performance against the statistical attacks.

3 Primarily: AES and chaos system

3.1 AES algorithm

The standard AES is an advanced encryption which has been introduced in 2000 by NIST. The data length in AES is 128 bits, i.e., 16 bytes. However, the key can acquire different lengths (for example, 128, 192, 256 bits). AES has 10, 12 and 14 rounds for 128-bit, 192-bit and 256-bit keys, respectively. Figure 1 shows the block diagram of AES algorithm.

AES has four main operational blocks:

1. Substitute byte transformation: An S-box is used to substitute each data block byte with another block.
2. Shift transformation of rows: Each row of the state matrix is given a cyclic shift to the right side according to its location.
3. Mix Transformation of Columns: It is a matrix multiplication operation where each column of the state matrix is multiplied by that of the fixed matrix.
4. Add Round Key Transformation: XOR operation is performed between the new state matrix and the round key one.

3.2 Chaos system

Chaos theory is a branch of mathematics which investigates the extremely complicated systems. In these systems, applying small (seemingly ignorable) changes in the input results in the significant changes in the output.

Chaos system has the following features:

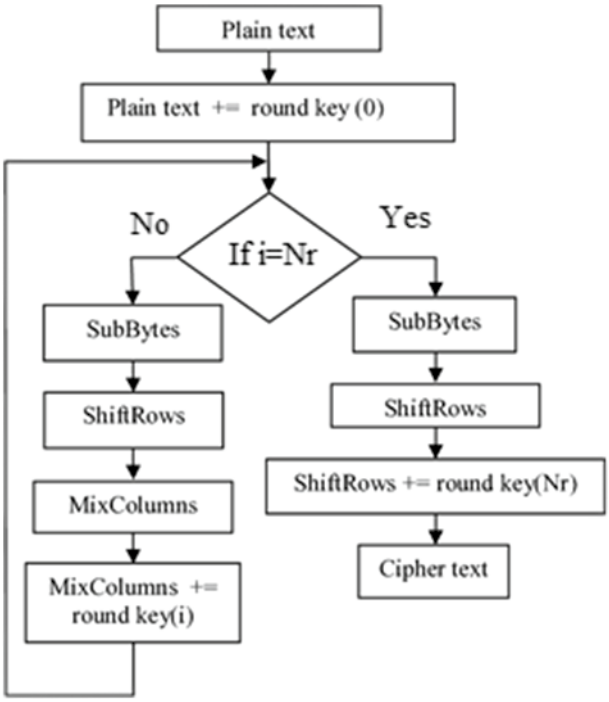

Fig. 1 Block diagram of AES [16]

1. Sensitivity to the initial value: Small changes in the initial value lead to a totally different sequence which is achieved through repetitive computations on a chaos map with the parameters.
2. Sensitivity to the parameters: Small changes in the parameters yield a totally different sequence which is achieved through repetitive computations on a chaos map with the input values.
3. Randomness: The generated chaos sequences using the chaos maps are mostly pseudorandom sequences and their structures are very complex for analysis and prediction.

If an unauthorized person does not know the correct control parameters and initial values, he cannot guess the chaos sequence. In other words, chaos systems can improve the safety of the image encryption systems.

4 The proposed image encryption method

Three important factors must be considered for designing an algorithm:

- The algorithm must be simple enough to be evaluated and analyzed easily and completely.

- An encryptor must provide security margin more than the required value against the known attacks.
- Well-known, well-examined and reliable instruments and ideas must be used for the design.

According to the above-mentioned points, using the combination of modified AES algorithm and Arnold chaos mapping, an image encryption algorithm is proposed here which is an efficient one from both security and speed aspects.

This paper uses the overall structure of the standard AES algorithm. Some modifications have been made to make the proposed method suitable for the image encryption. These terms include two modifications to the original AES encryption algorithm: The first modification is the replacement of proposed propagation operations to permutable operation in the standard encryption algorithm, and the second modification is to replace the linear transformation operation with the column integration operation. Figure 2 depicts the block diagram of the proposed encryption method. The details of the proposed algorithm are explained step by step in the following.

4.1 Generating the round key using the chaos system

Arnold chaos system is used in the proposed encryption algorithm for generating the key. Assume that the original image is of M×N size and n rounds are needed for the encryption. Therefore, $n+2$ arrays of N×M size are generated here using Eqs. (1) and (2). Each array stands for the round key of the CCAES algorithm:

$$\begin{aligned} X1_{n+1} &= \mathrm{mod}\big(\big(X1_n + \big(a \times X2_n\big), 256\big)\big) \\ X2_{n+1} &= \mathrm{mod}\big(b \times X1_n + \big(\big(a \times b + 1\big) \times X2_n\big)\big), 256\big) \end{aligned} \tag{1}$$

$$K(j,k,i) = \mathrm{floor}(\mathrm{mod}\big(\big(k(j,k,i) * \big(10^{14}\big)\big), 256\big) \tag{2}$$

Here, $X1 = 0.0215$, $X2 = 0.5734$, $a = 255.9998$, and b is equal to 0.

4.2 Encryption process

Step 1 The original image is placed in a state matrix with the same size. All the operations are performed on this matrix.

Step 2 First, the bytes of the state matrix are XOR with the corresponding bytes of zero round key, and the round value is set as 1.

Step 3 For round = 1: number of rounds.

First of all, the summation of the state matrix pixels is obtained by the initial value of Sum = 0.

$$\mathrm{Sum} = \sum_{i=1}^{N} \sum_{j=1}^{M} \mathrm{State}(i,j) \tag{3}$$

Step 4 If rounds = even; $i = 1, j = 1$

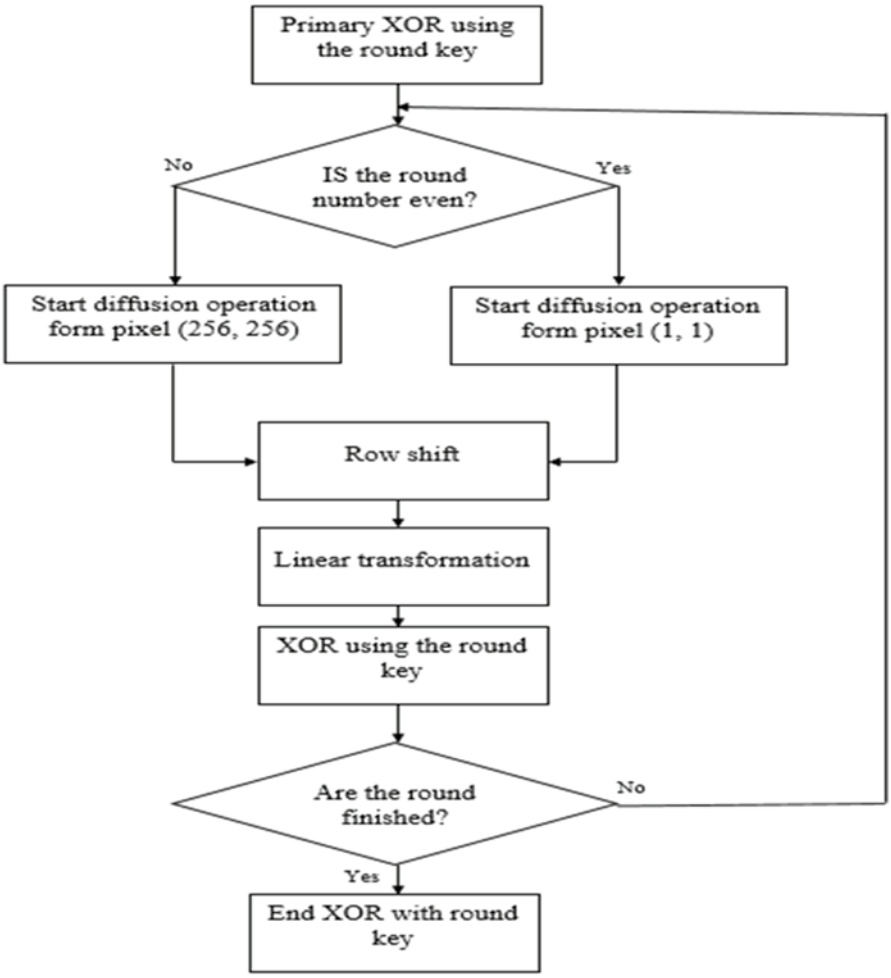

Fig. 2 The block diagram of the proposed encryption algorithm

$$\text{Sum} = \text{Sum} - \text{State}(i,j) \tag{4}$$

$$V = \text{floor}\left(\text{mod}\left(\frac{\text{Sum}}{256^5} \times 10^{10,256}\right)\right) \tag{5}$$

Not that, based on Ref. [5], in order to increase the sensitivity to small variations, the form of 10^{10} is used, and then, the remainder of the division to 256 is calculated where the value of generated number will be in the range of value of pixels in the image.

If $i = 1$ and $j = 1$:

A0 = 124

$$\text{State}(i,j) = \text{State}(i,j) \oplus v \oplus A_0 \tag{6}$$

Otherwise

$$\text{State}(i,j) = \text{State}(i,j) \oplus v \tag{7}$$

While $i < N$: $i = i+1$ and go to step 4.
While $j < M$: $j = j+1$, $i = 1$ and go to step 4.
If rounds = odd; $i = N$, $j = M$
Equations (4) and (5) are repeated.
Step 5
Then, if $i = N$ and $j = M$: $A0 = 124$ and Eq. (6); otherwise, Eq. (7) is repeated.
While $i > 1$: $i = i - 1$ and go to step 5.
While $j > 1$: $j = j - 1$, $i = N$ and go to step 5.
Step 6 The cyclic shifting of the rows:
Each row of the state matrix is given a cyclic shift to the right to an amount of one unit less than the row count.
Step 7 Linear conversion operation:
Figure 3 shows the block diagram associated with the linear conversion operation. Here, the symbol $\ll<$ denotes the cyclic shift, and $\ll$ and $\oplus$ stand for the ordinary shift and XOR operation, respectively. This operation is performed with the data of the state matrix to the amount of 16 bytes. This means that the linear operation is performed on the first 16 bytes and then the second 16 bytes, and this procedure is accomplished for the whole state matrix.
Step 8 The state matrix is XORed by the round key, and the round value increases one unit. If round $<= n$, go to step 3.
Step 9 The state matrix is XORed by the last round key. Considering the mentioned steps, the current state matrix is the encrypted image of the proposed method.

The decryption procedure is the same as the encryption one. The only difference is that some steps are performed reversely. The decryption process initially creates the key by Arnold's mapping, and the number of iterations is set to 10, and then the decryption operation begins. The reversal of the XOR operation is the same as the XOR operation, so only it is enough to XOR the encrypted image with the last key to eliminate the XOR changes in the end. Then, the inverse of the proposed encryption algorithm is executed; in this operation, initially the encrypted image is XORed with the key. In the second step, the inverse of the linear transformation operation is applied to the cipher image. In the next step, the inverse of the row shift operation is performed so that if a row in the encryption operation is rotated to the right by n in the operation, the decoding of the same row is shifted by n units to the left. In the last step, a condition is checked; this condition is such that if the number of rounds is odd, it is the last pixel, and otherwise, the operation of propagation is performed. This process is repeated regarding the number of rounds. Then, the image from the previous steps is XORed by the first key. The resulted image is the same as the original image.

The receiver only needs the initial values and can access the similar key of the encryption procedure via these values.

Various chaos systems were investigated during the present experimentations. The results of Arnold chaos system were better than other systems. That is why this

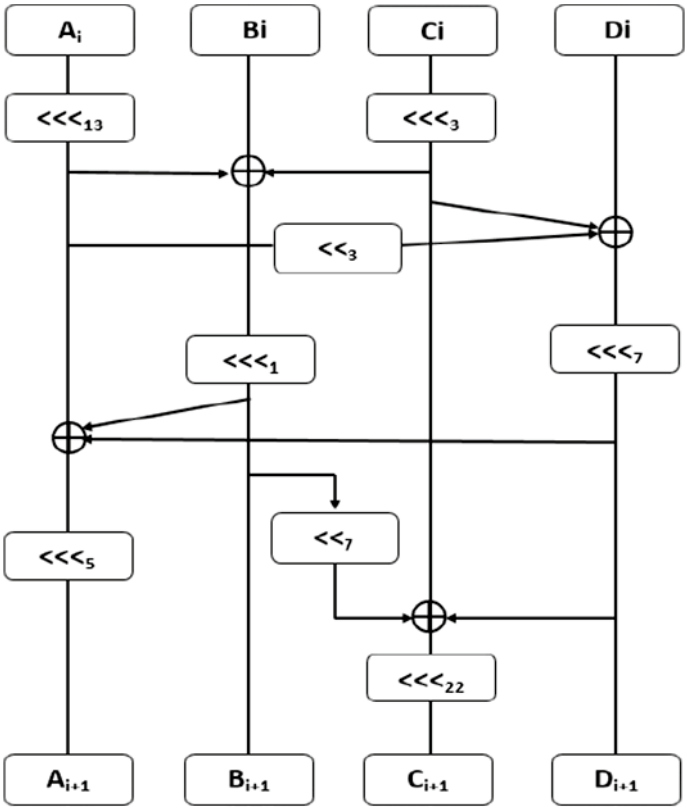

Fig. 3 Block diagram of linear conversion

paper uses Arnold chaos system for producing the pseudorandom sequences for confidential key generation.

5 Results and discussion

In this section, the common security analyses such as the statistical and differential analyses are examined on the CCAES algorithm.

5.1 Histogram analysis of the encrypted image

Four grayscale images (256×256) were chosen and their histograms calculated. Figure 4 depicts the histogram of images before and after the encryption. In this figure, column A represents the main image; column B represents the corresponding cipher image of the original image; column C depicts histogram of the main image; and the column D shows the histogram of the encoded image using the CCAES algorithm, and the last column on the right (column E) shows the histogram of encrypted

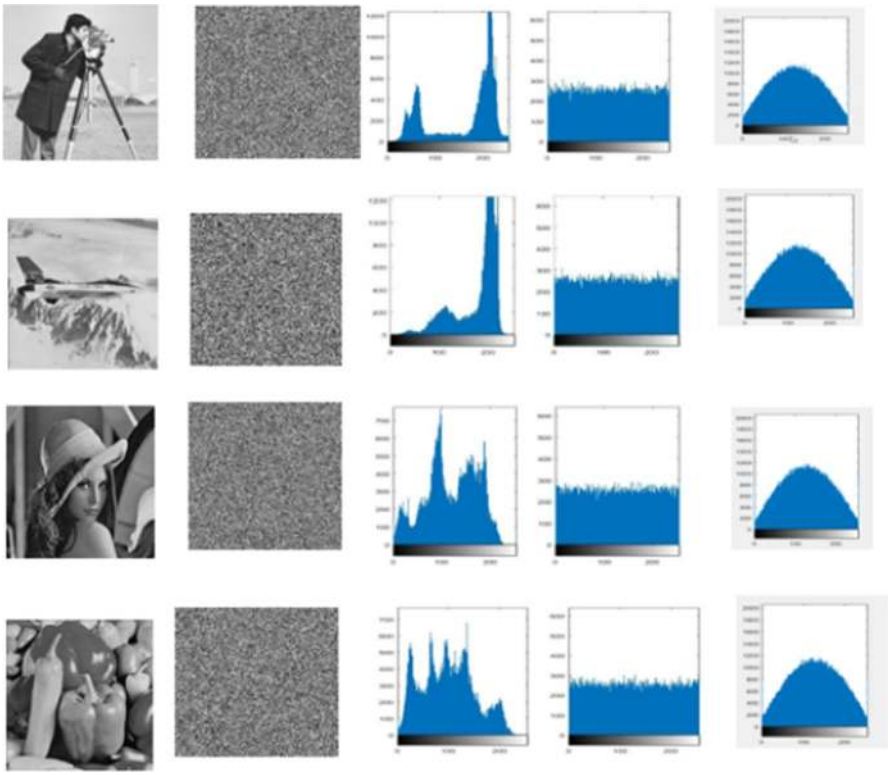

Fig. 4 Histogram of images

image using the AES standard algorithm. As would be observed, the histogram of the encrypted image is uniform and significantly differs from that of the original one. Therefore, no sign of the original image is existent to be used by the statistical attacks.

The histogram uniformity is assessed by Chi-square test which can be defined as:

$$X^2 = \sum_{K=1}^{256} \frac{\left(v_k - 256\right)^2}{256} \tag{8}$$

where k represents the number of grayscale areas and V_k stands for each area's repetition.

Table 1 lists the values of the Chi-square test for the images before and after encryption with the proposed method and the one presented in [21].

5.2 Information entropy analysis

Information entropy is a randomness criterion of the images. Equation (9) is used for calculating the entropy of information:

Table 1 Chi-square value

Chi-square	Lena	Cameraman	F16	Pepper
Image before encryption	29,384	179,819	176,403	30,810
Ref. [21]	263	257	265	274
CCAES algorithm	238.6719	236.6953	241.7656	253.2969

$$H(x) = \sum_{i=1}^{n} p(x_i) \log_2 p(x_i) \tag{9}$$

Here, $p(x_i)$ denotes the probability of X_i. The information entropy has been evaluated for 4 encrypted images. The maximum value of entropy is 8 for the grayscale images.

A comparison of the obtained entropy from the proposed method, the original AES and algorithms presented in [22, 23] is given in Table 2. The results show that the proposed encryption plan can resist the entropy attacks.

5.3 The analysis of the adjacent pixels correlation

To evaluate the correlation between the two adjacent pixels, the following equations are used:

$$E(X) = 1/N \sum_{i=1}^{N} X_i \tag{10}$$

$$\operatorname{cov}(x, y) = 1/N \sum_{i=1}^{N} \big(X_i - E(X)\big)\big(Y_i - E(Y)\big) \tag{11}$$

$$D(X) = 1/N \sum_{i=1}^{N} \big(X_i - E(X)\big)\big(Y_i - E(Y)\big) \tag{12}$$

$$r(x, y) = \frac{\operatorname{cov}(x, y)}{\sqrt{(D(X))}\sqrt{(D(Y))}} \tag{13}$$

Table 2 The value of information entropy

Entropy	Lena	Cameraman	F16	Pepper
AES	7.8693	7.8761	7.8705	7.8734
Ref. [22]	7.9970	7.9970	7.9968	7.9973
Ref. [23]	7.9977	7.9969		7.9973
CCAES algorithm	7.9974	7.9971	7.9973	7.9972

where x and y denote the values of the grayscale areas corresponding to the two adjacent pixels and N is the number of selected adjacent pixels for the correlation calculation. The maximum correlation coefficient is 1 which indicates the high correlation between the adjacent pixels. Hence, a good encryption algorithm must encrypt the image in such a way that the correlation coefficients of the adjacent pixels in the encrypted image are very low and close to zero so that the attacker cannot access useful information. Figure 5 shows the correlation distribution of the adjacent pixels. The first column from left side shows the original and encrypted images, respectively. Columns two, three and four from left show the correlation coefficient of adjacent pixels in vertical, horizontal and diagonal directions for the image in the column. Also, Table 3 gives the correlation distribution values in the vertical, horizontal and diagonal directions for the original and encrypted images.

Table 3 further compares the correlation coefficient of the CCAES algorithm with that obtained via the algorithms in [22, 24] and standard AES one. These coefficients are very low in the encrypted image and approach zero. This proves the efficiency of the algorithm in eliminating the high correlation among pixels of the original image. Further to these, this table shows that the CCAES algorithm has a better correlation compared to the other algorithms. Therefore, the proposed method can resist better against the statistical attacks compared to the other ones.

5.4 Algorithm's sensitivity analysis to the original image

For the sensitivity evaluation, first, the original image is encrypted. Then, one pixel of the original image is randomly changed. The resultant image is encrypted again, and finally, the two encrypted images are compared using Eqs. (15) and (16).

The two measurement criteria of NPCR and UACI are used for investigating the influence of changing one pixel of the original image on the encrypted image. NPCR indicates the average number of the pixels of the encrypted image which have changed due to the pixel change in the original image. For the two encrypted images $C1$ and $C2$ whose original images differ only in one pixel, the 2-D array of $D(i, j)$ is calculated according to Eq. (14) as:

$$D(i,j) = \begin{cases} 1 & c_1(i,j) \neq c_2(i,j) \\ 0 & c_1(i,j) = c_2(i,j) \end{cases} \tag{14}$$

where $c_1(i,j)$ and $c_2(i,j)$ define the grayscale area's value of a pixel in the (i, j) coordinate of the encrypted images $c1$ and $c2$.

Then, NPCR is calculated as follows:

$$\text{NPCR} = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{15}$$

The parameters M and N indicate the dimensions of the original image.

The unified average changing intensity (UACI) between the two images is calculated as follows:

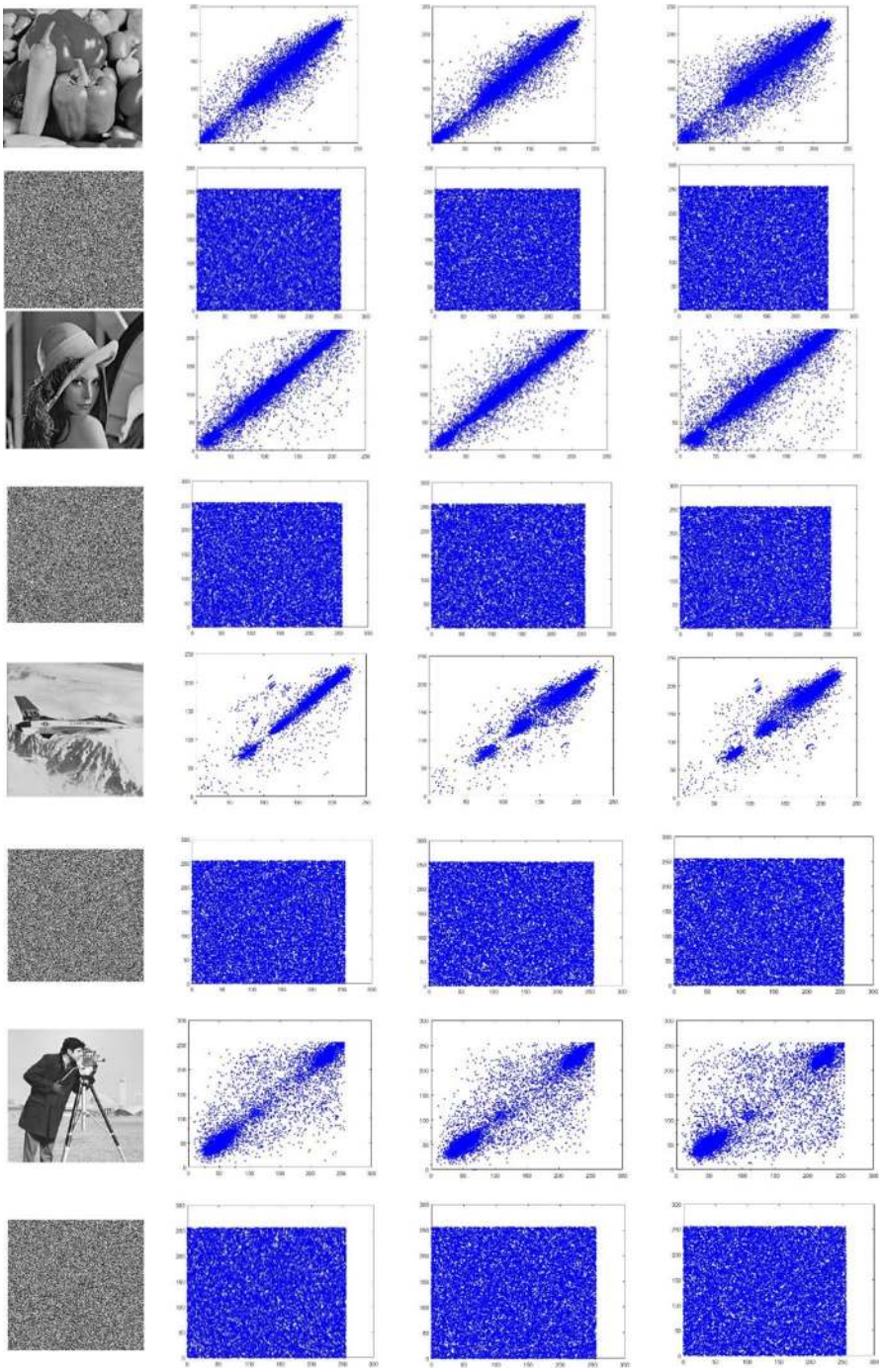

Fig. 5 Correlation distribution of adjacent pixels

Table 3 Correlation values in horizontal, vertical and diagonal directions

Correlation of two adjacent pixels		Ref. [22]	Ref. [24]	AES algorithm	CCAES algorithm
Lena	Horizontal	0.0055002	0.0047	0.2724	0.0027
	Vertical	0.0041189	0.0015	0.2681	0.0012
	Diagonal	0.0002136	0.0030	0.0765	0.0003105
Cameraman	Horizontal	0.0046892	0.0047	0.2729	0.0002267
	Vertical	0.0147580	0.0054	0.2723	0.0007220
	Diagonal	0.0139760	0.0016	0.0682	0.0048
F16	Horizontal	0.004492	0.0033	0.2740	0.0077
	Vertical	0.0005435	0.0002	0.2691	0.0005899
	Diagonal	0.0032230	0.0019	0.0815	0.0026
Pepper	Horizontal	0.0114200	0.0023	0.2704	0.0020
	Vertical	0.0045059	0.0021	0.2709	0.0080
	Diagonal	0.0081210	0.0003	0.0736	0.0008398
Baboon	Horizontal			0.2656	0.0009269
	Vertical			0.2734	0.0047
	Diagonal			0.0723	0.0050
Barbara	Horizontal	0.01818	0.0033	0.1868	0.0094
	Vertical	0.0091	0.0032	0.3561	0.0028
	Diagonal	0.0072	0.0025	0.0659	0.0014
Tank	Horizontal		0.0033	0.0049	0.0012
	Vertical		0.0002	0.2635	0.0006086
	Diagonal		0.0019	0.0186	0.0076
Fishing boot	Horizontal	0.0077			0.0042
	Vertical	0.0086			0.0037
	Diagonal	0.0171			0.0046
House	Horizontal	0.0015	0.0004	0.0519	0.0048
	Vertical	0.0016	0.0012	0.3393	0.0039
	Diagonal	0.0039	0.0006	0.0651	0.0002507
Dog	Horizontal			0.1794	0.0068
	Vertical			0.4199	0.0054
	Diagonal			0.0845	0.0010
Flower	Horizontal			0.0212	0.0021
	Vertical			0.1401	0.0027
	Diagonal			0.0213	0.0032

$$\mathrm{UACI} = \frac{1}{M \times N}\left[\frac{\sum i,j\left|C_{1(i,j)} - C_{2(i,j)}\right|}{2^{l}-1}\right] \times 100 \tag{16}$$

Table 4 NPCR values

NPCR	Lena	Cameraman	F16	Pepper
AES	0.0778	0.0870	0.0809	0.0885
Ref. [22]	99.655	99.625	99.608	99.593
Ref. [24]	99.6253	99.6124	99.6459	99.6040
CCAES algorithm	99.6368	99.5697	99.5712	99.6414

Table 5 UACI values

UACI	Lena	Cameraman	F16	Pepper
AES	0.0093	0.0097	0.0111	0.0101
Ref. [22]	33.561	33.461	33.574	33.635
Ref. [24]	33.4807	33.6551	33.4188	33.4628
CCAES algorithm	33.4724	33.4767	33.3877	33.5864

Table 6 The running time of the CCAES algorithm and the original AES

Run time of encryption + decryption	Pepper	F16	Cameraman	Lena
CCAES algorithm	2.88S	2.9S	2.9S	2.9S
AES	452.3S	515.2S	446.8S	454.1S

where L is the number of used bits for displaying the image, which is equal to 8 here.

The NPCR changing interval is (0,1). When its value is in the vicinity of 1, the encryption security is high. Obviously, the UACI interval is [0,1]. However, the appropriate UACI for the two ideal encrypted images is unknown. The greater values of UACI and NPCR ensure the security of the encryption. Figures 4 and 5 present the UACI and NPCR values of the present and other algorithms (Tables 4 and 5).

Comparing the NPCR and UACI values of the present algorithm with those of algorithms proposed in [22, 24] and the original AES, it can be concluded that the security of the CCAES algorithm and those of [22, 24] against the differential attacks is more than that in the original AES one. Also, due to the satisfactory values of UACI and NPCR, the present algorithm meets the requirements for resisting the differential attacks.

5.5 Comparing the run time of the CCAES algorithm with that of the original AES

After encrypting the Elena, Cameraman, F16 and Pepper images with the CCAES algorithm and the original AES, it is observable that the CCAES algorithm is very faster than the original AES one. According to the results given in Table 6, it can

Table 7 Symbols and notations

Symbols and notations	Description
$\lll$	Cyclic shift
$\ll$	Ordinary shift
$\oplus$	XOR operation
AES	Advanced encryption standard
ECC	Elliptic curve cryptography
NIST	National Institute Of Standards And Technology
NPCR	Number of pixels change rate
UACT	Unified average changing intensity

be claimed that the CCAES algorithm is more appropriate for the real-time applications. All the implementation processes have been conducted using a system with the following configurations (Table 7):

CPU: Intel(R) Core (TM) i7-6500U @ 2.50 GHz 2.59 GHz.
RAM: 8.00 GB (7.87 GB usable).
Windows: 10×64-bit operating system.

6 Conclusion

Combining the chaos sequence and the modified AES algorithm, a novel image encryption algorithm is presented in this paper. In this method, the encryption key is generated by Arnold chaos sequence. Then, the original image is encrypted using the modified AES algorithm and by implementing the round keys produced by the chaos system. The modified AES consists of 10 rounds for encrypting, and the substitution and integration operations of the columns have been replaced by the linear conversion and pixel values summation. These operations not only reduce the time complexity of the algorithm but also add the diffusion ability to the CCAES algorithm, which make the encrypted images by the CCAES algorithm resistant to the differential attacks. The key space of the proposed method is large enough to resist the brute-force attacks. This method is so sensitive to the initial values and input image so that the small changes in these values can lead to significant changes in the encrypted image. This feature also prevents unauthorized persons from decrypting the encrypted image. Statistical analyses show that this approach can protect the image against the statistical attacks. In addition, this approach is highly sensitive to the input values, which enables the algorithm to resist the differential attacks. The histogram distribution of the encrypted image is uniform. The Chi-square test is used to justify the histogram uniformity. The correlation analysis shows a significant decrease in the correlation coefficient between the adjacent pixels after encrypting. The entropy test results illustrate that the entropy values are close to the ideal value, i.e., 8. Therefore, the CCAES algorithm is secure against the entropy attacks. UACI and NPCR are used as the evaluation parameters of the resistance against the differential attacks. The results clarify that the small changes in the original image and

key result in the significant changes in the encrypted image and the original image cannot be accessed.

References

1. Norouzi B et al (2014) A simple, sensitive and secure image encryption algorithm based on hyper-chaotic system with only one round diffusion process. Multimed Tools Appl 71(3):1469–1497
2. Kumari M, Gupta S, Sardana P (2017) A survey of image encryption algorithms. 3D Res 8(4):37
3. Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 1(96):39–49
4. Liu Hongjun, Wang Xingyuan (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. Opt Commun 284(16-17):3895–3903
5. Guan Zhi-Hong, Huang Fangjun, Guan Wenjie (2005) Chaos-based image encryption algorithm. Phys Lett A 346(1-3):153–157
6. Ye G, Wong KW (2012) An efficient chaotic image encryption algorithm based on a generalized Arnold map. Nonlinear Dyn 69(4):2079–2087
7. Patro K, Banerjee A, Acharya B (2017) A simple, secure and time efficient multi-way rotational permutation and diffusion based image encryption by using multiple 1-D chaotic maps. In: International Conference on Next Generation Computing Technologies. Springer, Singapore, pp 396–418
8. Patro K, Acharya B (2018) Secure multi–level permutation operation based multiple color image encryption. J Inf Secur Appl 40:111–133
9. Hailan Pan, Lei Yongmei, Jian Chen (2018) Research on digital image encryption algorithm based on double logistic chaotic map. EURASIP J Image Video Process 2018(1):142
10. Sravanthi D et al (2019) A secure chaotic image encryption based on bit-plane operation. Soft computing in data analytics. Springer, Singapore, pp 717–726
11. Partheeban P, Kavitha V (2018) Dynamic key dependent AES S-box generation with optimized quality analysis. Cluster Comput. https://doi.org/10.1007/s10586-018-2386-6
12. Zeghid M, Machhout M, Khriji L, Baganne A, Tourki R (2007) A modified AES based algorithm for image encryption. In: International Conference on Computer, Information and Systems, pp 526–531
13. ElBadawy ESAM, El-Masry WA, Mokhtar A, Hafez AES (2010) A new chaos advanced encryption standard (AES) algorithm for data security. In: International Conference on Signals and Electronic Circuits
14. Mondal Subijit, Maitra Subhashis (2014) Data security-modified AES algorithm and its applications. ACM SIGARCH Comput Archit News 42(2):1–8
15. Bashir A, Hasan AS, Almangush H (2012) A new image encryption approach using the integration of a shifting technique and the AES algorithm. Int J Comput Appl 975:8887
16. D'souza FJ, Panchal D (2017) Advanced encryption standard (AES) security enhancement using hybrid approach. In: 2017 International Conference on Computing, Communication and Automation (ICCCA). IEEE, pp 647–652
17. Jha Y, Kaur K, Pradhan C (2016) Improving image encryption using two-dimensional logistic map and AES. In: 2016 International Conference on Communication and Signal Processing (ICCSP). IEEE, pp 0177–0180
18. Ahmed BA, Abd SB, Hamida A (2012) A novel image encryption using an integration technique of blocks rotation based on the magic cube and the AES algorithm. IJCSI 9(4):41–47
19. Iyer SC, Sedamkar RR, Gupta S (2016) A novel idea on multimedia encryption using hybrid crypto approach. Proc Comput Sci 1(79):293–298
20. Shtewi AA, Hasan BE, Hegazy AE (2010) An efficient modified advanced encryption standard (MAES) adapted for image cryptosystems. IJCSNS Int J Comput Sci Netw Secur 10(2):226–232

21. Borujeni SE, Eshghi M (2013) Chaotic image encryption system using phase-magnitude transformation and pixel substitution. Telecommun Syst 52(2):525–537
22. Song C-Y, Qiao Y-L, Zhang X-Z (2013) An image encryption scheme based on new spatiotemporal chaos. Opt Int J Light Electron Opt 124(18):3329–3334
23. Zhu C (2012) A novel image encryption scheme based on improved hyperchaotic sequences. Opt Commun 285(1):29–37
24. Zahmoul R, Ejbali R, Zaied M (2017) Image encryption based on new Beta chaotic maps. Opt Lasers Eng 96:39–49