



Improved affine encryption algorithm for color images using LFSR and XOR encryption

Ayşegül Ihsan¹ · Nurettin Doğan²

Received: 31 August 2021 / Revised: 27 April 2022 / Accepted: 25 August 2022 /

Published online: 3 September 2022

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract

In this study, a novel Improved Affine Algorithm (IAA) for color image encryption is proposed. Affine Algorithm (AA) is generally known as an algorithm used for plain text encryption. In the proposed IAA algorithm, Linear Feedback Shift Register (LFSR), XOR encryption, and the AA are combined for color images encryption. The plane image is firstly split into three channels: R, G, and B. The RGB channel image is encrypted using AA encryption with ten keys based on pixel locations and pixel values. The rows and columns of the image are encrypted with LFSR keys and XOR encryption procedures. Finally, the proposed algorithm is tested in Matlab environment to obtain the Histogram, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), Number of Pixel Change Rate (NPCR), and Entropy analyses. The values are compared with other algorithms. The results show that the proposed image encryption algorithm is secure and powerful, outperforming other algorithms.

Keywords Affine algorithm · Image encryption · Linear feedback shift register · XOR encryption

1 Introduction

Today, the internet is effective in every aspect of our lives. During the Covid-19 pandemic that we are currently experiencing, people had to stay at home more. Now, the internet is being used more intensively than ever before. All the transactions, such as shopping, banking, and

✉ Nurettin Doğan
ndogan@ymail.com

Ayşegül Ihsan
aysegulih sann@gmail.com

¹ Department of Information Technologies Engineering, Graduate School of Natural and Applied Sciences, Selçuk University, Alaeddin Keykubat Campus, Konya 42075, Türkiye

² Department of Computer Engineering, Faculty of Technology, Selçuk University, Alaeddin Keykubat Campus, Konya 42075, Türkiye

remote working were carried out through the Internet. Apart from these, the use of social media platforms has increased very rapidly. Computers, mobile phones, smartwatches, devices connected to the Internet, security cameras in the areas we live in, and many other devices are all connected to the Internet. These devices send great amounts of data to different parts of the world with high-speed data transfers. Accessing a large amount of data over the Internet creates high-security risks. Many countries have enacted laws on the protection of personal data. In addition to personal data, the security of states is also crucial when sending data over the Internet. One way to securely send digital data over the Internet is encryption and the other is using steganography. The information to be encrypted can be plain text or an image.

Affine Algorithm is one of the encryption techniques used by cryptographers for plain text. However, it is possible to use AA for image encryption as well. Because the AA includes several operations including translation, scaling, rotation, and truncation, it can also be used for pixel scrambling in image encryption. However, despite these features, the use of AA alone for image encryption is not enough to make good encryption. Therefore, stronger encryption processes are required. Many researchers tried to develop stronger image encryption methods by using AA, LFSR, XOR encryption and other methods together. Lone et al. encoded the image using a random Affine encryption matrix, 2D Hénon, and a chaotic map [18]. Sayed et al. studied Affine encryption with six parameters [25]. Wang et al. combined AA encryption with the zigzag method [29]. They represented secure image encryption with pixel and AA encryption in this study [30]. Chen et al. proposed an encryption algorithm using the AA and Fractional Fourier Encryption [6]. Multilayer resilient color image encryption with random matrix AA was studied [24]. Khan et al. used an S8 permutation of double-AA in S-boxes and a nonlinear Lorentz dynamics system for image encryption [11]. Deb and Bhuyan proposed a new medical image encryption system using a special nonlinear filter function based on Linear Feedback Shift Register (LFSR) [8]. Momeni et al. proposed color image encryption method using LFSR by three dimensional permutation and substitution operations [20]. Masood et al. proposed a lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations [19]. Thinnukool et al. double encryption algorithm using trigonometric chaotic map and XOR of an image [28].

In this study, a new color image encryption algorithm is proposed using LFSR technique known as a random number generator and XOR encryption together with AA, and this algorithm is called Improved Affine Algorithm (IAA). In image encryption, the LFSR is used for key generation. The XOR encryption method is preferred because it is a simple and complex structure. The XOR encryption method is used with LFSR keys.

The main contributions of this study can be summarized as follows:

- In this study, the IAA algorithm developed for color image encryption is used. The user selects ten different keys for AA encryption. The original image is split into three channels: R, G, and B. The image is encrypted with AA using four keys based on pixel locations and six keys based on pixel values.
- The rows and columns of the image are encrypted using the LFSR 256-key and XOR encryption.
- The proposed algorithm is tested with the Histogram, MSE, PSNR, UACI, NPCR, and Entropy. A comprehensive analysis is provided by comparing IAA with other encryption algorithms in the literature. The IAA achieves remarkable improvement and outperforms other encryption algorithms compared in this study.

The content provided in the rest of this paper is organized as follows: In Section 2, Affine Algorithm, Linear Feedback Shift Register, and XOR encryption with LFSR are briefly explained. Section 3 describes the proposed encryption algorithm in detail. In Section 4, the experiments and comparisons are presented, and the results are discussed. Finally, conclusions and future works are given in Section 5.

2 Background

Affine Algorithm (AA), Linear Feedback Shift Register (LFSR), and XOR encryption with the LFSR approach is examined in this section. Following that, the proposed algorithm is examined.

2.1 Affine algorithm

Affine cipher is a type of classical substitution cipher used in cryptography. It was initially created to encrypt a set of 26 English characters. AA is a widely used and well-known encryption method. AA is a multi-key encryption algorithm. The structure of AA is more complex and secure than that of single-key encryption algorithms [18, 25, 29, 30]. AA is used for both text encryption and image decryption. In this study, AA is used for image encryption. For $M \times N$ pixel sizes images, AA formula is shown in Eq. (1) and AA decryption formula is shown in Eq. (2).

$$y = ax + b \pmod{N} \quad (1)$$

$$\bar{y} = a^{-1}(x-b) \pmod{N} \quad (2)$$

where y is the encryption operation and \bar{y} is the decryption operation. The keys used in AA (Eq. 1 and Eq. 2) are denoted as the a -key and the b -key. For decryption, the Greatest Common Divisor (GCD) must be equal $(a, N) = 1$. Consequently, the a -key should not have a common divisor of N and the b -key should be selected from 0 to $N-1$.

2.2 Linear feedback shift register

A perfectly random series of integers is required when encrypting images with LFSR [1]. After all subsequent numbers have been generated, the first numbers are traced. During this process, the digits are carried over the register. The bits are shifted one position to the left, and the shifted bit and the bit previously at a particular step position in the register replace the released bit. The length of the LFSR is $[q_0, q_1, q_2, \dots, q_j]$, where q is the number of circuits and j is the number of registers in the LFSR and the flip-flop circuits can be increased or decreased arbitrarily. It is represented by the clock (c) of the LFSR, where (c_i) is the number of records in the LFSR.

In LFSR, the first numbers are randomly generated. The first numbers are used to generate the second numbers with the XOR operation. To generate the second numbers, the first numbers are shifted in the register. While shifting, the value of the q_0 is shifted to the q_1 . The value of q_0 is then XORed by the value of the q_1 and the result obtained is used as the new

value of the q_2 . The identical actions are performed again and again until the last number is generated. In Fig. 1, the LFSR shift operations and operations to generate new numbers are specified with colors and the colors can be used to track the shifts.

In Fig. 1, the LFSR is 3 bits long and is represented by q_0, q_1 , and q_2 . The LFSR time is represented by c_i . In this example, the q_0 and the q_1 are created randomly ($q_0 = 0$ and $q_1 = 1$). The initial time ($c_{initial}$) is the result of the XOR operation of the q_0 and the q_1 ($(c_{initial}) q_0 = 0 \oplus q_1 = 1 \rightarrow q_2 = 1$). Then, the q_0 on $c_{initial}$ is shifted to q_1 on c_1 , and the green color is used to describe this operation on $c_{initial}$ and c_1 . In c_1 , q_0 and q_1 are XORed, and q_2 is updated as a result ($(c_1) q_0 = 1 \oplus q_1 = 0 \rightarrow q_2 = 1$). After that, q_0 on c_1 is shifted to q_1 on c_2 and the blue color is used to describe this operation on c_1 and c_2 . To produce ten distinct integers, nine feedback shift operations (c_9) are conducted. All operations can be understood by following the colors. The LFSR is commonly used to generate encryption keys. Key generation using LFSR is used in various encryption techniques in the literature.

2.3 XOR encryption with LFSR

XOR encryption is a text and image encryption algorithm. Random keys are generated by LFSR, and the key and pixel values are encrypted in XOR encryption. The XOR operation is preferred by many cryptographers because it is more secure. The LFSR is used to generate the key in the XOR encryption. The flowchart of encryption algorithms with XOR encryption with LFSR is shown in Fig. 2.

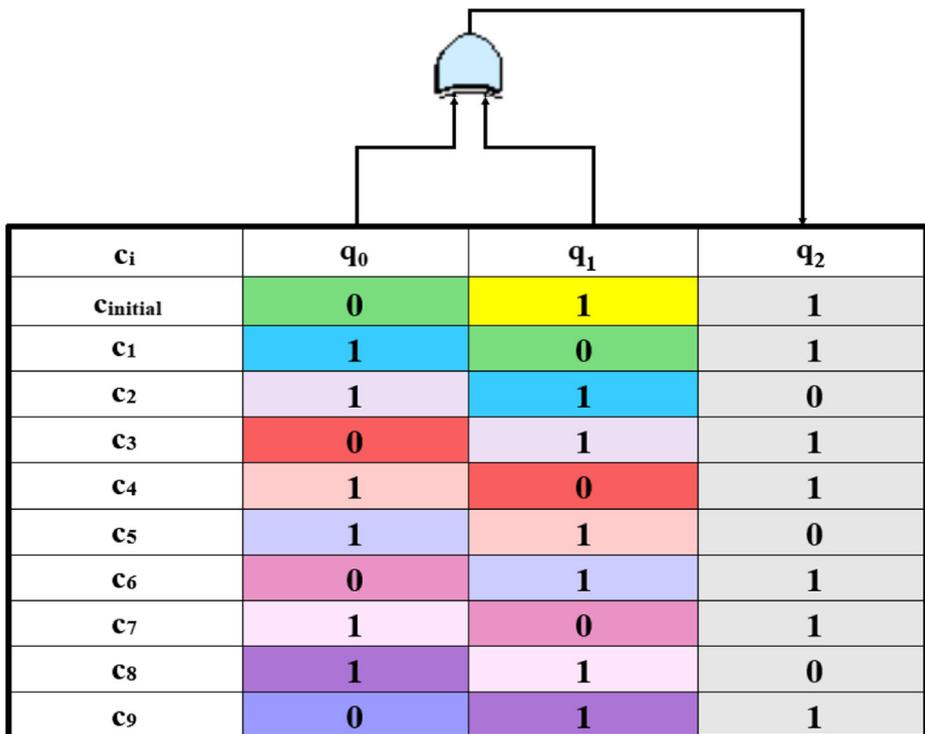


Fig. 1 An example of the LFSR in a numerical procedure

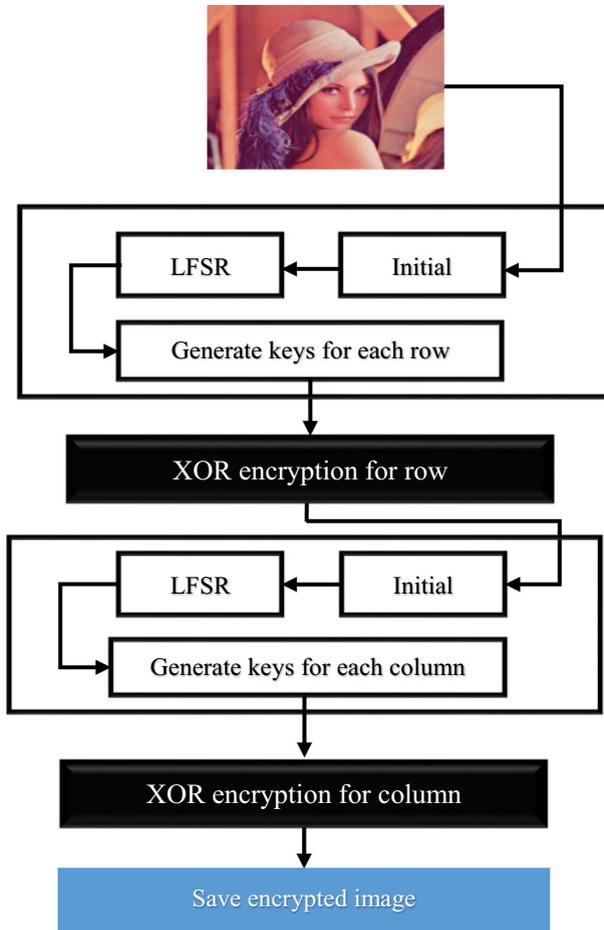


Fig. 2 Combination of XOR encryption with LFSR

In Fig. 2, XOR encryption with LFSR, the color image is selected first. In LFSR, random numbers are first used for key generation, and LFSR is tuned to generate keys for each column. New pixel values are found with random numbers. After shuffling the pixels, a row encryption image is obtained. The decryption step uses the same key as the encryption step. For column encryption, a sequence of random numbers is generated, which is to be converted into a matrix. This method rearranges or swaps the pixel values of the image by using the random matrix. Column encryption is studied on the row-encrypted image. As a result, the image is encrypted using XOR encryption with LFSR encryption methods. Encryption is column-wise and row-wise, and multiple keys are used.

3 Proposed approach

In this study, the images named Lena, Baboon, Airplane, and Pepper are used. The size of each image is 256×256 pixels. For this reason, in this study, explanations will be made for images

with a resolution of 256×256 pixels from now on. The algorithm is applied to the RGB channels of the color image separately. The algorithm is developed in three steps: (i) Pixel Locations Encryption using AA, (ii) Pixel Values Encryption using AA, (iii) XOR encryption with LFSR.

(i) Pixel locations encryption using AA

The plain image is split into three RGB channels. The algorithm is applied to each RGB channel of the color image separately. The four keys: a_1 , b_1 , a_2 , and b_2 are used in this step. Since the size of each image is 256×256 pixels, b_1 and b_2 should be chosen between 0 and 255. a_1 , and a_2 should be chosen so that $GCD(a, 256) = 1$. In this stage, firstly Pixel locations of the image are encrypted using Eq. (1) for the a_1 and b_1 keys. Secondly, Pixel locations of the image are encrypted using Eq. (1) for a_2 and b_2 keys. The encryption processes are visualized in Fig. 3.

The original image is shown in Fig. 3a and the encryption of the original image is shown in Fig. 3b by encrypting pixel positions with two keys. Finally, the pixel locations are encrypted a second time using two keys, as shown in Fig. 3c.

(ii) Pixel values encryption using AA

The pixel values of the image in each channel of the color image are encrypted with AA, and the encryption is performed with Eq. (1). A total of six keys are used for pixel value encryption. The a_3 , b_3 keys are used for the R channel, the a_4 , b_4 keys are used for the G channel, and the a_5 , b_5 keys are used for the B channel. In this step, a total of six keys are utilized for encryption.

In Fig. 4, the image is divided into RGB channels and AA encryption is applied to the image pixel values with a total of six keys: two keys for the R channel, two keys for the G channel, and two keys for the B channel. The encrypted image is concatenated after the channels are encrypted. Encrypting channels individually and with different keys improved the security.

(iii) XOR encryption with LFSR

LFSR generates a total of 256 different keys for a 256×256 image. LFSR key is used to XOR encrypt each pixel of the image. At this stage, XOR encryption is applied twice. In the first step, the rows of the image are encrypted with XOR using the key generated with LFSR.

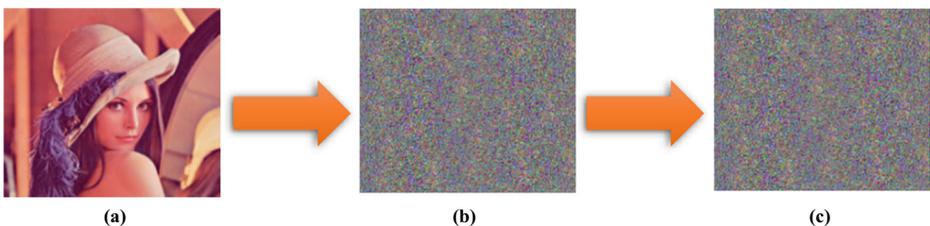


Fig. 3 AA encryption for the color Lena image's pixel locations

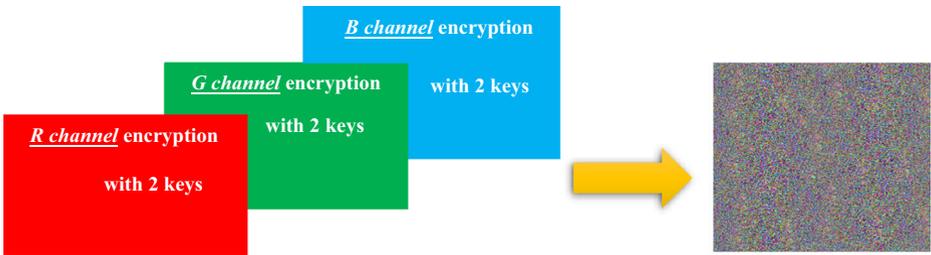


Fig. 4 AA pixel values encryption for RGB channels

In the second step, the columns of the image are encrypted with XOR. Then, all the operations are repeated and the encryption process is completed. Therefore, a strongly encrypted image is obtained with IAA.

The image is encrypted and decrypted using the same keys. The decryption procedure occurs in the opposite direction of the encryption procedure. The block diagram of the image encryption algorithm is shown in Fig. 5. The block diagram of the image decryption algorithm is shown in Fig. 6. The procedures of the encryption algorithm are shown in Fig. 7 whereas the procedures of the decryption algorithm are shown in Fig. 8.

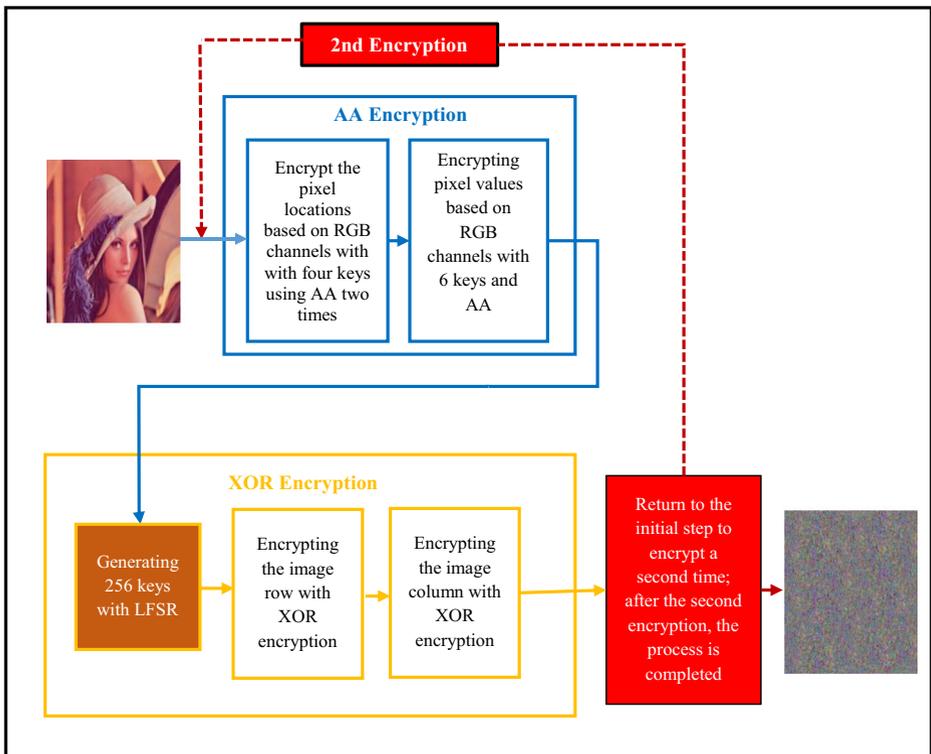


Fig. 5 Block diagram of the encryption of the IAA

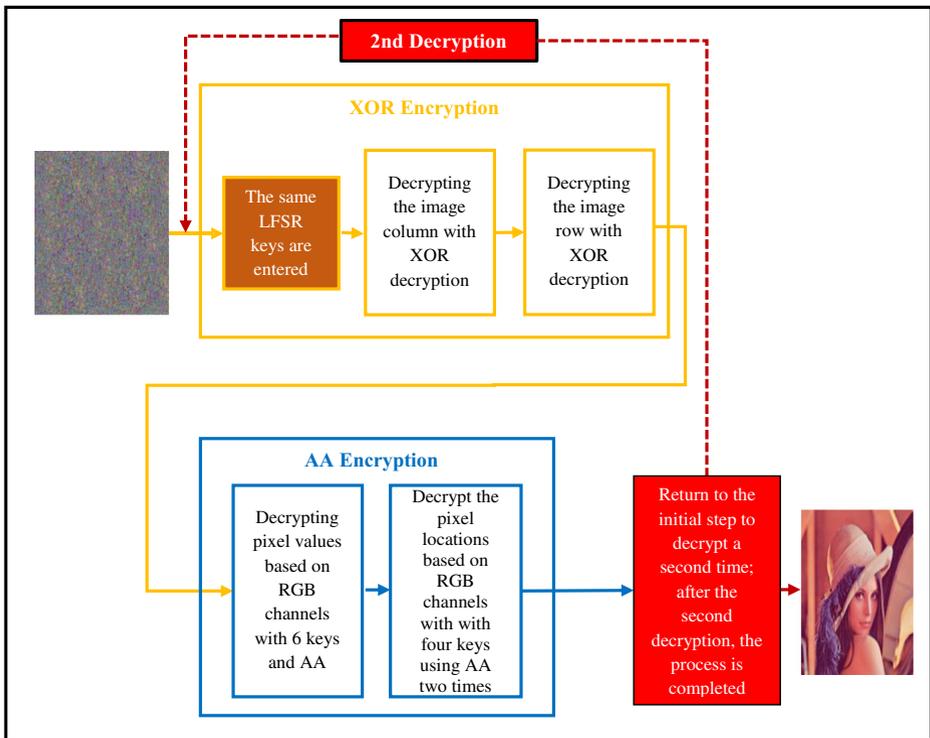


Fig. 6 Block diagram of the decryption of the IAA

Input: The RGB image with a size of 256×256 pixels is selected.

Initiate the process

Step 1: Ten different keys are selected. The pixel locations of the image RGB channels are encrypted using Eq. (1) and two keys. This operation is repeated two times. Two different keys are utilized for each encryption operation, for a total of four different keys.

Step 2: The pixel values of the image RGB channels are encrypted using six keys from RGB channels. As a consequence, the pixel values are encrypted a total of six different keys and Eq. (1).

Step 3: LFSR is used to generate 256 keys. The image is encrypted from row and column with 256-key XOR encryption.

Step 4: After the initial encryption, proceed to step 1 to encrypt for a second time. Encryption is terminated when it is performed a second time.

End

Output: The encrypt image.

Fig. 7 The image encryption procedures of the IAA

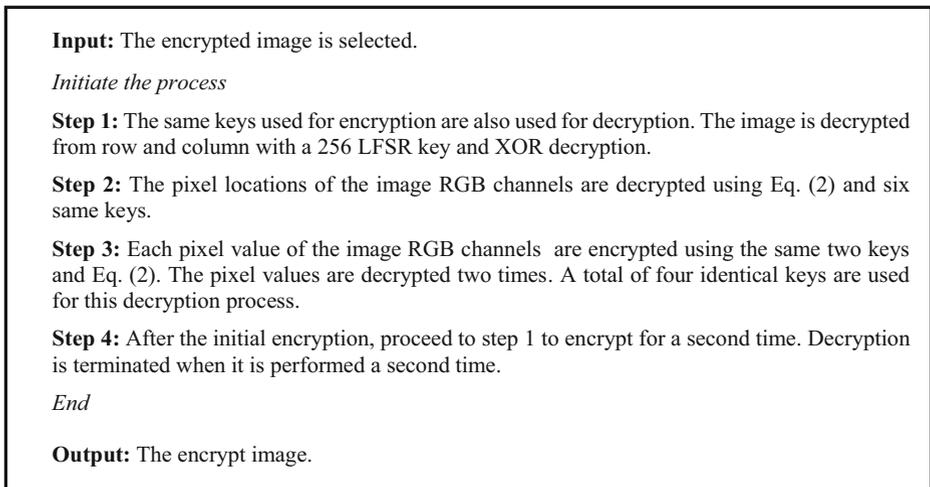


Fig. 8 The image decryption procedures of the IAA

4 Results and analysis

The proposed algorithm is tested with the Histogram, MSE, PSNR, UACI, NPCR, and Entropy analyses. After the encryption tests, the structural content is examined to determine the best algorithm for image encryption and the success of the proposed algorithm is compared with other encryption algorithms. It is explained in detail in this section.

The content provided in the rest of this section is organized as follows: In Section 4.1, Experimental Analysis is briefly summarized. In Section 4.2, the proposed algorithm is compared using the Histogram, MSE, PSNR, NPCR, UACI, and Entropy analyses. The experiments and comparisons are presented, and the results are discussed. Tests and analyses of the proposed algorithm are performed in Section 4.3.

4.1 Experimental analysis

In this study, the images named Lena, Baboon, Airplane, and Pepper are used. The size of each image is 256×256 pixels. Image encryption is performed with ten different keys. The pixel keys are represented by $a_1, b_1, a_2,$ and $b_2,$ and the RGB keys are represented by $a_3, b_3, a_4, b_4, a_5,$ and $b_5.$ For LFSR, “11,011,001” is selected as the initial value and set to 8 bits (0 to 255). The keys used in this study are shown in Table 1. The original images, the encrypted images, and the decrypted images are shown in Table 2.

Table 1 Keys determined for IAA

The Key's Name	Key	The Key's Name	Key
The Initial Value of the LFSR	11,011,001	b_3	97
a_1	19	a_4	133
b_1	133	b_4	19
a_2	29	a_5	256
b_2	100	b_5	100
a_3	39		

Table 2 The original image, the encrypted image, and the decrypted image with IAA

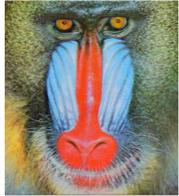
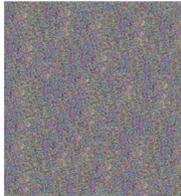
Image Name	Original Image	Encrypted Image	Decrypted Image
Lena			
Baboon			
Airplane			
Pepper			

Table 2 shows that the encryption and decryption operations are successful. The performance of the proposed algorithm is analyzed in the following section.

4.2 Experimental results

The Histogram, MSE, PSNR, NPCR, UACI, and Entropy analyses are explained in this section. Finally, the Histogram, MSE, PSNR, NPCR, UACI, and Entropy analyses are utilized to evaluate the performance of the proposed algorithm.

4.2.1 Histogram analysis

The distribution of the pixel intensities of an image is represented by the Histogram. Also, the analysis of the Histogram shows the probability of hacker-encrypted images being hacked by using frequency data and statistics. The quality of the algorithm used is shown by the homogeneous distribution of the Histogram of the encrypted image [22].

4.2.2 Mean square error and peak signal to noise ratio

The original and encrypted images are compared with Mean Square Error (MSE) [2]. MSE is the mean squared error estimate used to compare possible image differences. In general, the lower the value of MSE, the better the results. In this study, the success of the encrypted image is examined using the MSE value. The original image is represented by $I_{R,G,B}$, the decrypted image by $\hat{I}_{R,G,B}$, the image size by $M \times N$, Δx , and Δy by the pixel size. MSE formula is as shown in Eq. (3).

$$MSE_{R,G,B} = \frac{1}{M \times N} \sum_{i=1}^{M-1} \sum_{j=1}^{N-1} \left[|I_{R,G,B}(m\Delta x, n\Delta y) - \hat{I}_{R,G,B}(m\Delta x, n\Delta y)|^2 \right] \quad (3)$$

Peak Signal to Noise Ratio (PSNR) shows similarities between images. After encrypting the image, PSNR value is used to measure the image deformations [26]. PSNR value is low after successful encryption. PSNR is expressed in decibels (dB) [4]. PSNR is calculated together with MSE values. PSNR test is performed to measure the security of the encrypted images. Achieving a high score on the PSNR test indicates a successful encryption process. The formula for PSNR is shown in Eq. (4).

$$PSNR(I_{R,G,B}, \hat{I}_{R,G,B}) = 10 \log_{10} \left(\frac{(M-1) \times (N-1)}{\sum_{M,N} [I_{R,G,B}(M,N) - \hat{I}_{R,G,B}(M,N)]^2} \right) \quad (4)$$

4.2.3 Number of pixels change rate and unified average changing intensity

Differential attack analysis is performed to detect changes in encrypted images. The hackers are unable to make any meaningful association with the original images based on a small change in the encrypted images because the small change in the original images is created a large change in the encrypted images. The Number of Pixels Change Rate (NPCR) and Unified Average Change Intensity (UACI) are commonly used to measure the effectiveness of this type of attack. NPCR, pixel change with the original image comparison of the encrypted image shows the change in several pixels of the encrypted image and the rate. UACI rate, the encryption technique against various attacks, is defined as the resistance ratio. The average density difference between the original image and the encrypted image is UACI value [23]. Eq. (5) represents the calculation of the NPCR and Eq. (6) represents the calculation of UACI.

Table 3 Histogram analysis of the images

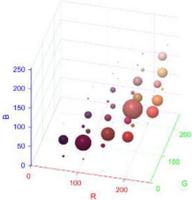
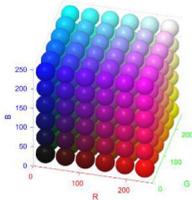
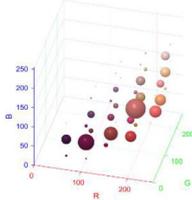
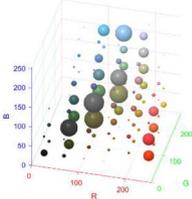
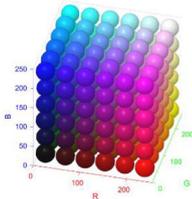
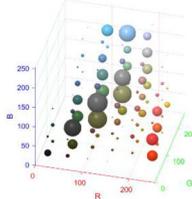
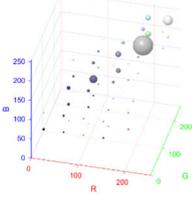
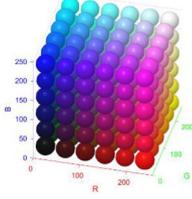
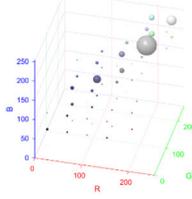
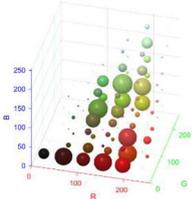
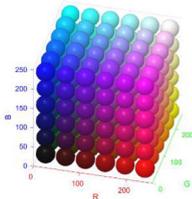
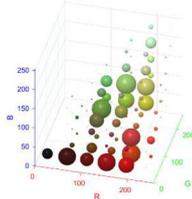
Image Name	Histograms of the Original Images	Histograms of the Encrypted Images	Histograms of the Decrypted Images
Lena			
Baboon			
Airplane			
Pepper			

Table 4 MSE, PSNR, NPCR and UACI results of the proposed algorithm

Image Name	RGB Channels	PSNR	MSE	NPCR	UACI
Lena	R	19.1185	8.3816E5	99.6965	33.5588
	G	20.5472	5.3211E5	99.6574	33.5774
	B	19.8751	5.3357E5	99.6588	32.6485
Baboon	R	20.1994	1.277E3	99.6972	33.6589
	G	19.2476	5.5812E4	99.6675	33.5812
	B	18.8123	2.2271E4	99.6479	33.6127
Airplane	R	20.2581	6.1771E4	99.6972	33.4779
	G	20.1347	6.1213E5	99.6477	33.5538
	B	20.1023	8.8741E5	99.6371	33.6271
Pepper	R	18.3412	8.5741E4	99.6986	33.4599
	G	19.8522	6.4251E5	99.6915	33.5471
	B	20.0178	6.7732E5	99.6278	33.6367

$$NPCR_{R,G,B} = \frac{\sum_{i=1}^{i=M} \sum_{j=1}^{j=N} D_{R,G,B}(i,j)}{M \times N} \times 100\% \quad D_{R,G,B}(i,j) = \begin{cases} 0 & \text{if } I_{R,G,B} = \hat{I}_{R,G,B} \\ 1 & \text{if } I_{R,G,B} \neq \hat{I}_{R,G,B} \end{cases} \quad (5)$$

$$UACI_{R,B,G} = \frac{1}{M \times N} \left[\sum_{i=1}^{i=M} \sum_{j=1}^{j=N} \frac{|\hat{I}_{R,G,B}(i,j) - I_{R,G,B}(i,j)|}{255} \right] \times 100\% \quad (6)$$

where M and N are the width and height of the image. The original image is represented by I , the decrypted image by \hat{I} , the image size by $M \times N$, The difference array $D(i, j)$ is defined as follows: if $I = \hat{I}$, $D(i, j) = 0$; otherwise, $D(i, j) = 1$ [3].

4.2.4 Entropy analysis

Entropy is a significant property that represents the degree of disorder in a system. Entropy is used to calculate the probability of obtaining the original image without knowing the key [5, 14]. Eq. (7) represents the calculation of the value of the Entropy [9].

$$H(m) = \sum_{i=0}^{2^N-1} P(m_i) \times \log_2 \left(\frac{1}{P(m_i)} \right) \quad (7)$$

Table 5 MSE results of the proposed algorithm and other encryption algorithms

Algorithm	RGB Channels	Lena	Baboon	Airplane	Pepper
Proposed Algorithm	R	8.3816E5	1.277E3	6.1771E4	8.5741E4
	G	5.3211E5	5.5812E4	6.1213E5	6.4251E5
	B	5.3357E5	2.2271E4	8.8741E5	6.7732E5
Li et al. [13]	R	1.062E4	8.618E3	9.978E3	7.962E3
	G	9.046E3	7.749E3	1.066E4	1.123E4
	B	7.111E3	9.531E3	1.043E4	1.115E4
Etemadi Borujeni et al. [10]	R	1.032E4	8.518E3	9.651E3	7.828E3
	G	9.115E3	7.625E3	1.040E4	1.107E4
	B	7.056E3	9.439E3	1.009E4	1.124E4

Table 6 NPCR and UACI results of the proposed algorithm and other encryption algorithms

Algorithm	NPCR			UACI		
	R	G	B	R	G	B
Proposed Algorithm	99.6965	99.6574	99.6588	33.5588	33.5774	32.6485
Murillo et al. [21]	99.6300	99.6000	99.6100	33.3100	33.3400	33.4300
Kumar et al. [12]	99.5659	99.5658	99.5959	33.2829	33.3459	33.3270
Teng et al. [27]	99.6429	99.6140	99.6277	33.3935	33.5637	33.4814
Chidambaram et al. [7]	99.6124	99.6140	99.6201	33.4235	33.4838	33.5983

where N is the number of bits to represent a symbol $m_i \in m$. Entropy is measured in bits, where $P(m_i)$ is the probability of the symbol m_i and the \log is the logarithm to base 2. For a source emitting 2^N symbols at random, $H(m) = N$ is the Entropy value. The entropy value result is expected to be about 8 ($H(m) \approx 8$).

4.3 Test and analysis

In this section, MSE, PSNR, UACI, NPCR, and Entropy values are performed to prove that IAA is a successful encryption algorithm. First, the Histograms of the images are analyzed. A homogeneous structure in the encrypted image's histogram is required for effective encryption. The proposed algorithm is used for the encryption of the color images of Lena, Baboon, Airplane, and Pepper. Table 3 shows the original image histogram, the encrypted image histogram, and the decrypted images. Table 3 compares the histograms of the original image and the decrypted image, and the encrypted images of the Histograms are appeared to be fairly evenly distributed. As a result, IAA is recognized as an efficient form of cryptography.

MSE, PSNR, UACI, and NPCR metrics are computed to measure success and resistance to attack, and all results are obtained for each RGB channel of images. PSNR is measured in decibels (dB). UACI and NPCR are calculated in percentages (%). In Table 4, MSE, PSNR, UACI, and NPCR values of RGB channels of images are compared to show the performance of the proposed encryption algorithm. In Table 4, MSE results prove that the original image is obtained after decryption with only minor errors. PSNR results show that IAA encryption is secure for the images. The suggested encryption algorithm is successful in differential attack

Table 7 Entropy of the proposed algorithm

Image Name	RGB Channels	Original Image	Encrypted Image
Lena	R	7.228639	7.999488
	G	7.549785	7.999514
	B	6.967501	7.999428
Baboon	R	7.647045	7.999425
	G	7.361939	7.999561
	B	7.682947	7.999358
Airplane	R	6.773730	7.999412
	G	6.861568	7.999389
	B	6.331334	7.999457
Pepper	R	7.328042	7.999375
	G	7.603665	7.999563
	B	7.144957	7.999544

Table 8 The Entropy of the encrypted images

Algorithm	Image Name	RGB Channels		
		R	G	B
Proposed Algorithm	Lena	7.999488	7.999514	7.999428
Proposed Algorithm	Baboon	7.999425	7.999561	7.999358
Proposed Algorithm	Airplane	7.999412	7.999389	7.999457
Proposed Algorithm	Pepper	7.999375	7.999563	7.999544
Liu et al. [16]	Lena	7.989825	7.989120	7.990007
Liu et al. [16]	Pepper	7.988899	7.989486	7.989519
Liu et al. [16]	Airplane	7.989357	7.989472	7.990092
Liu et al. [17]	Lena	7.989567	7.988533	7.989931
Liu et al. [17]	Pepper	7.988881	7.988873	7.988577
Zhang et al. [31]	Lena	7.997300	7.997000	7.997200
Zhang et al. [31]	Pepper	7.997200	7.997000	7.997200
Zhang et al. [31]	Baboon	7.999300	7.999300	7.999300

analysis if NPCR is above 99% and UACI is above 33% [14]. The average NPCR value for all color test images considered in this study is 99.67% and the average UACI value is 33.58%. UACI and NPCR results show that encryption is effective, and the keys are secure. All tests show that IAA's image encryption algorithm and image decryption algorithm are extremely secure.

Table 5 compares the MSE results of the proposed algorithm to the results of other image encryption algorithms available in the literature. IAA outperforms the other two algorithms in MSE results. Table 6 shows UACI and NPCR results obtained for Lena, Baboon, Airplane, and Pepper images of the proposed algorithm and various image encryption algorithms in the literature.

The Entropy values of RGB channels of images are compared to show the performance of the proposed encryption algorithm. Table 7 shows the entropy results of the proposed algorithm. Table 8 shows the proposed algorithm and the results of other algorithms published in the literature.

The minimum value of information Entropy analysis is zero, whereas the maximum value is eight [15]. Table 7 shows the RGB channel information entropy values for the proposed algorithm. Entropy analysis of the proposed algorithm is calculated as $H(m) \approx 8$. The entropy analysis of the suggested algorithm is compared with the entropies of various encryption algorithms in Table 8.

Table 8 shows that IAA is a more highly secure cryptographic procedure than other encryption algorithms. All tests and analyses proved that IAA is a safe encryption algorithm. As a consequence, the proposed algorithm is extremely robust against Entropy attacks on image predictions.

5 Conclusion

In this study, a novel color image encryption algorithm named Improved Affine Algorithm (IAA) is developed. IAA is performed in three procedures. In the first step, the plain image is split into three channels: R, G, and B. The RGB channel pixel locations are encrypted two times with four different keys using Affine Algorithm (AA). In the second step, the RGB channel pixel values are encrypted separately with a total of six different keys using AA.

Finally, the rows and columns of the image are XOR encrypted with 256 keys using LFSR. The decryption procedure occurs in the opposite direction of the encryption procedure. The proposed algorithm is used for the encryption of the color images of Lena, Baboon, Airplane, and Pepper. IAA has successfully performed encryption operations and decryption operations. Further, the Histogram, MSE, PSNR, UACI, NPCR, and Entropy values are measured the purpose algorithm's performance. The experimental results are compared to other encryption algorithms. The analyses and comparisons show that the proposed encryption algorithm is highly secure against various attacks.

Acknowledgments We would like to thank the referees who read this study and made the necessary criticisms and contributed to the writing of the study in a better way.

Declarations

Competing interests The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Abu-Issa AS, Quigley SF (2009) Bit-swapping LFSR and scan-chain ordering: a novel technique for peak-and average-power reduction in scan-based BIST. *IEEE Trans Comput Aided Des Integr Circ Syst* 28(5): 755–759
2. Bani MA, Jantan A (2008) Image encryption using block-based transformation algorithm. *IJCSNS Int J Comput Sci Netw Secur* 8(4):191–197
3. Behnia S, Akhavan A, Akhshani A, Samsudin A (2013) Image encryption based on the Jacobian elliptic maps. *J Syst Softw* 86(9):2429–2438
4. Brahim AH, Pacha AA, Said NH (2020) Image encryption based on compressive sensing and chaos systems. *Opt Laser Technol* 132:106489
5. Çelik H, Doğan N (2021) A color image steganography using a chaotic map based on K-least significant bits. *J Polytech (Politeknik Dergisi)*. <https://doi.org/10.2339/politeknik.1008594>
6. Chen H, Liu Z, Tanougast C, Ding J (2019) Optical hyperspectral image cryptosystem based on affine transform and fractional fourier transform. *Appl Sci* 9(2):330
7. Chidambaram N, Raj P, Thenmozhi K, Amirtharajan R (2020) Advanced framework for highly secure and cloud-based storage of colour images. *IET Image Process* 14(13):3143–3153
8. Deb S, Bhuyan B (2021) Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR. *Multimed Tools Appl* 80(13):19803–19826
9. Doğan N, Çelik H (2021) A hybrid color image encryption method using a scan pattern. *J Polytech (Politeknik Dergisi)*. <https://doi.org/10.2339/politeknik.902661>
10. Etemadi Borujeni S, Eshghi M (2013) Chaotic image encryption system using phase-magnitude transformation and pixel substitution. *Telecommun Syst* 52(2):525–537
11. Khan M, Jamal SS, Hazzazi MM, Ali KM, Hussain I, Asif M (2021) An efficient image encryption scheme based on double affine substitution box and chaotic system. *Integration* 81:108–122
12. Kumar M, Powduri P, Reddy A (2014) An RGB image encryption using diffusion process associated with chaotic map. *J Inf Secur Appl* 21:20–30
13. Li P, Zhao Y (2017) A simple encryption algorithm for quantum color image. *Int J Theor Phys* 56(6):1961–1982
14. Liu H, Wang X (2011) Color image encryption using spatial bit-level permutation and high-dimension chaotic system. *Opt Commun* 284(16–17):3895–3903
15. Liu H, Kadir A, Liu J (2019) Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system. *Opt Lasers Eng* 122:123–133
16. Liu H, Zhang Y, Kadir A, Xu Y (2019) Image encryption using complex hyper chaotic system by injecting impulse into parameters. *Appl Math Comput* 360:83–93

17. Liu H, Kadir A, Xu C (2020) Color image encryption with cipher feedback and coupling chaotic map. *Int J Bifurcation Chaos* 30(12):2050173
18. Lone PN, Singh D, Mir UH (2021) A novel image encryption using random matrix affine cipher and the chaotic maps. *J Mod Opt* 68(10):507–521
19. Masood F, Driss M, Boulila W et al (2021) A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wirel Pers Commun*. <https://doi.org/10.1007/s11277-021-08584-z>
20. Momeni Asl A, Broumandnia A, Mirabedini SJ (2021) Color image encryption using linear feedback shift registers by three dimensional permutation and substitution operations. *Int J Nonlinear Anal Appl* 12:903–921
21. Murillo-Escobar MA, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez RM, Del Campo OA (2015) A RGB image encryption algorithm based on total plain image characteristics and chaos. *Signal Process* 109:119–131
22. Naveenkumar SK, Panduranga HT (2013) Triple image encryption based on integer transform and chaotic map. In: 2013 International Conference on Optical Imaging Sensor and Security (ICOSS), 1–6
23. Rhouma R, Meherzi S, Belghith S (2009) OCML-based colour image encryption. *Chaos, Solitons Fractals* 40:309–318
24. Sabir S, Guleria V (2021) Multi-layer color image encryption using random matrix affine cipher, RP2DFrHT and 2D Arnold map. *Multimed Tools Appl* 80(18):27829–27853
25. Sayed WS, Radwan AG, Fahmy HA, Elsedek A (2021) Trajectory control and image encryption using affine transformation of Lorenz system. *Egypt Inform J* 22(2):155–166
26. Shehab A, Elhoseny M, Muhammad K, Sangaiah AK, Yang P, Huang H, Hou G (2018) Secure and robust fragile watermarking scheme for medical images. *IEEE Access* 6:10269–10278
27. Teng L, Wang X, Meng J (2018) A chaotic color image encryption using integrated bit-level permutation. *Multimed Tools Appl* 77(6):6883–6896
28. Thinnukool O, Panityakul T, Bano M (2021) Double encryption using trigonometric chaotic map and XOR of an image. *CMC-Comput Mater Continua* 69(3):3033–3046
29. Wang H, Hu Y, Yu L, Wang Q (2018) The optimal scrambling algorithm based on zigzag and affine transformation. In: 2018 IEEE International Conference on Mechatronics and Automation (ICMA), 1189–1193
30. Yadav SS, Singh Y, Sriwas S (2017) Gray code (n, k, p) based pixel substitution and affine transform based gray code bit plane permutation technique for secure image encryption. *ARNP J Eng Appl Sci* 12(11): 3500–3508
31. Zhang D, Chen L, Li T (2021) Hyper-chaotic color image encryption based on transformed zigzag diffusion and RNA operation. *Entropy* 23(3):361

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.