Chapter

Hybrid Encryption Model Based on Advanced Encryption Standard and Elliptic Curve Pseudo Random

Amal Hafsa, Mohamed Gafsi, Jihene Malek and Mohsen Machhout

Abstract

Securing multimedia applications becomes a major challenge with the violation of the information increasing currently. In this paper, a novel method for color image encryption is proposed. The procedure of encryption is performed using cooperation between Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES) with CTR (Counter) mode. In the cryptographic system, we have proposed to take advantage of the Elliptic Curve Random Generator to generate a sequence of arbitrary numbers based on the curve. The random generation step is founded on the public key sharing and a changing point G. Then, the AES-CTR is performed to these sequences using arbitrary keys for image encryption. The use of the AES alongside greatly distributed random results an interesting encryption method. Security analysis is successfully performed and our experiments prove that the suggested technique provides the basis of cryptography with more simplicity and correctness.

Keywords: hybrid scheme, AES, CTR ECC, random generator, image encryption

1. Introduction

Cryptography plays an important role to attain the privacy of images. There exist two main families of cryptographic algorithms. The asymmetric algorithm is inherently slow because of its associated hard calculations, while the symmetric algorithm shines with its rapidity. However, the latter suffers from a serious gap, the keys must be transmitted safely. To overcome these issues, we suggest an efficient version of AES-ECC hybrid encryption scheme which combines the benefits of the symmetric Advanced Encryption Standard (AES) and the asymmetric Elliptic Curve Cryptography (ECC). In [1], C. Junli el al propose an image encryption method using the AES-ECC hybrid cryptographic system. In that paper, the authors focus on the key sharing way. In fact, the AES key encryption is performed using ECC and the securing key is done by the digital signature of the ECC. Then, the AES is utilized for data encryption. An ameliorated version of this way is suggested in [2], an AES-ECC hybrid encryption system is developed for wireless sensor network. In this way, the AES Key is generated and encrypted by the ECC algorithm. After transmission, another pair of the ECC key (Key 2) is generated and ciphered using the symmetric algorithm. This token is transferred to the other part

and the encryption of the data input is performed using the Key 2. Therefore, the cipher ECC is achieved. Finally, the encryption of the cipher-ECC is performed using AES, and ciphertext output is obtained to be transferred via the network. The principle inconvenience of this paper is that the employ of the ECC asymmetric algorithm to encrypt all original text is highly time-consuming. Thus, the system is not efficacious in terms of using energy, particularly for weak sensors. Hajajneh et al. proposed in [3] a cryptographic system that secures multimedia application in FPGA. The goal of this work is to perform authentication and encryption using a Cipher Block Chaining Message Authentication code protocol (CCMP) and a counter (CTR) protocol. Though the results indicate an amelioration on the speed, the overall system risked to be attacked [3, 4] and these techniques do not furnish possibilities of enhancement. Attaya et al. [5] proposed the employ of a hybrid system that combines both chaos and AES algorithms. In the AES, both substitution box and Add-Round key are replaced by a chaos generator which leads to an increase in both diffusion and confusion and decreases the run time when compared with the standard. Yet encryption can outcome a feeble code when compared with the traditional AES since there is only one step that performs the entropy comparing with the different steps in the AES. Although the authors declare that the decryption process is impossible without the key [5]. In [6], K. Shankar et al. propose to encrypt images using an asymmetric encryption key. They utilized the genetic algorithm to get the ideal key. In this way, the ECC is utilized to encrypt all pixels one by one. Although, the employ of an asymmetric algorithm for every pixel and researching for the ideal keys are costly operations. In [7], A.A.A. El. Latif suggested an amalgamation between Elliptic Curve Cryptography (ECC) and a chaotic system. In that paper, authors utilized cyclic elliptic curves with LFSR (Linear Feedback Shift Register) and a chaos system for the keystream sequences generation. Then, image encryption is performed using the key streams. In [8], H. Liu et al. demonstrated that the previous model proposed in [7], is vulnerable to the chosen Plain text attacks. In order to dissolve this issue, they overcast the errors by using the Chirikov standard map [9] for the diffusion and the confusion of the image. Similarly, they employed a preceding stream of the encrypted images to encrypt the next stream. Although, some problems can be produced with the generated logic map because there exists a correlation between Xn values of the chaotic system.

The main contribution of our paper is to propound a way which is secure while addressing the issues of preceding works. In particular, a novel method for image encryption was suggested. The procedure of encryption is performed tacking benefits of Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). The suggested technique utilizes the ECC as a random generator, where a sequence of random numbers is generated founded on Elliptic Curve parameters. Randoms are then employed to be as inputs for the key of the AES which generates the keystream for pixels encryption. The process of random number generation is founded on the NIST (National Institute of Sciences and Technology). Though the NIST way is employed extensively, it has some limitations. In this paper, the suggested random number generation addresses the limitation of this way employing a unique method of generating randoms by X and Y coordinates. Yet, using the Y coordinate, the entropy value of generated random numbers is improved. As known, no preceding works have used both coordinates (X and Y) for random number generation. In the following, proposed cryptographic algorithms are clearly explicated in Section 2. Section 3 details the suggested hybrid method for image encryption. Section 4 furnishes the experimental results followed by complete analysis over the propound technique. Finally, the last section concludes and recommends for future works.

2. Proposed cryptographic algorithms

A cryptographic function is founded on mathematical rulers. As well, a strong cryptographic algorithm requires an effective key that is large enough for the keyspace. The efficient key generation needs the right mathematical foundation. In this paper, the proposed technique utilized for the key generation is clearly explicated.

Nowadays, two fundamentals cryptographic systems are efficient and secure enough for image encryption:

- Advanced Encryption Standard (AES): It is characterized by its speed and its simplicity in implementation.
- Elliptic Curve Cryptography (ECC): Is characterized by its high security and its small key size to be employed in every system.

In this paper, by considering the advantages of both cryptosystems, a novel cooperative framework is proposed.

2.1 Advanced encryption standard (AES)

The Advanced Encryption Standard (AES) was firstly proposed in 2001. No successful attacks have been signalized on the AES. This latter involves key sizes and block sizes. The size of the information block is 128 bits, and the length of the key can be 128, 192, or 256 bits. In this work, the reduced processing time is needed. Then, a 128 bits key size is sufficient. For the encryption operation, round transformation is performed as a set of iterations, which includes the Sub-Bytes, Shift-Rows, Mix-Columns, and Add-Round key operations. For the Sub-Bytes operations, a Table S-box is utilized to substitute every block byte with a novel bloc. For the Shift-Rows, every row of the matrix is performed by a cyclic shift to the right according to its position. The mix-columns transformation consists of binary

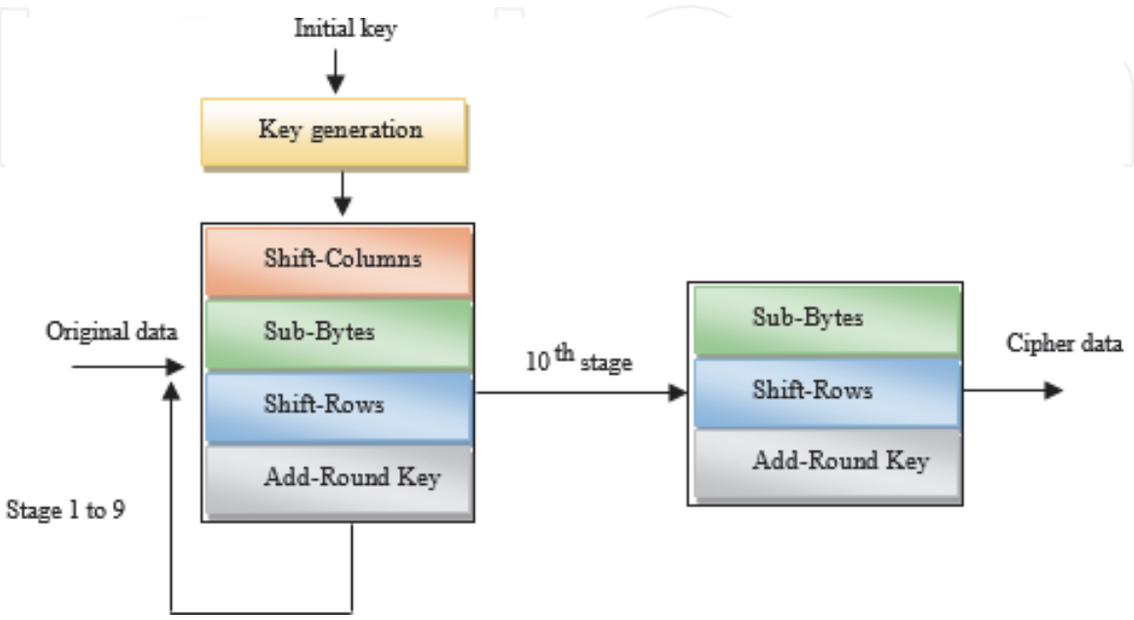


Figure 1.
Flow design of AES algorithm.

multiplying every element of the matrix state with polynomials from an auxiliary matrix. Finally, an exclusive OR between the round key and the matrix state is performed to obtain an intermediate matrix [10] (**Figure 1**).

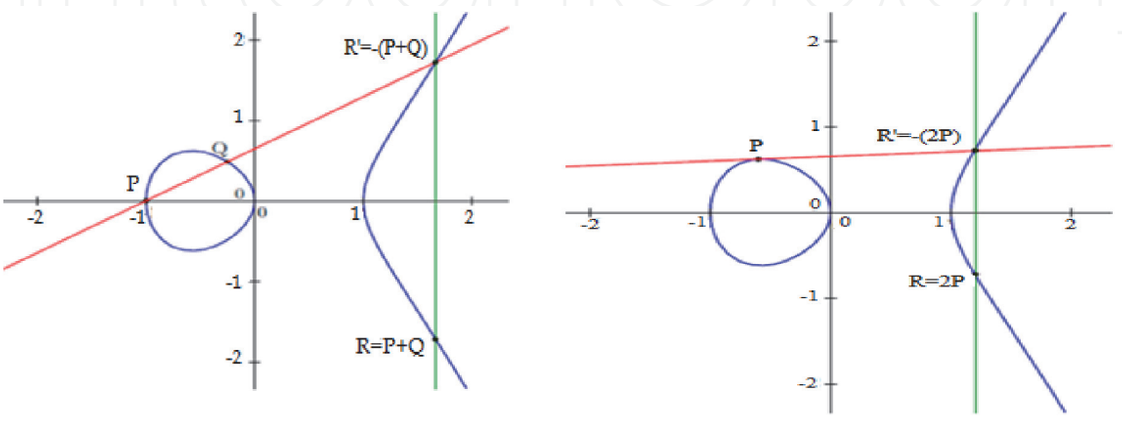
2.2 Elliptic curve cryptography (ECC)

In this section, an overview of the Elliptic Curve Cryptography (ECC) is given. Then the Montgomery scalar multiplication is used due to its resistance to side-channel attack.

2.2.1 Overview

Cryptography based on elliptical curves (ECC) has enjoyed great interest since its introduction by Miller and Koblitz in 1987 [11, 12].

Cryptographic systems based on elliptical curves make it possible to gain efficiency in key management because of the small sizes of the keys used. In addition, the calculation algorithms linked to elliptical curves are faster, and therefore have a much higher key generation and exchange rate. Cryptographic systems based on elliptical curves are increasingly used in protocols using public key cryptography. Elliptic curves are used for encryption (ElGamal ECC), digital signatures (ECDSA), pseudo-random generators and other tasks. The Elliptical curve equation is of the form $y^2 = x^3 + ax + b$, the value of a and b is fixed and x, y belongs to finite field (prime or binary field). Encryption and decryption algorithms are based on point multiplications (usually referred to with kP, where k is the scalar). The base point P on which the point multiplication (a.k.a. scalar multiplication) is done is also fixed. All operations of ECC are done in the finite field (prime or binary field). Two basic operations over the curve are defined: The Point Addition and the Point Doubling. Point addition computes a third point on the curve taking two different input points, while Point Doubling computes a third point on the curve when the two inputs are the same Point as depicted in **Figure 2**. Both Point Addition and Point Doubling operations are built using modular arithmetic, where operations like addition, subtraction, multiplication, etc. are required. In **Figure 3**, the hierarchy of scalar multiplication is presented.



a) Point Addition b) Point Addition

Figure 2.
Point addition and point doubling operations.

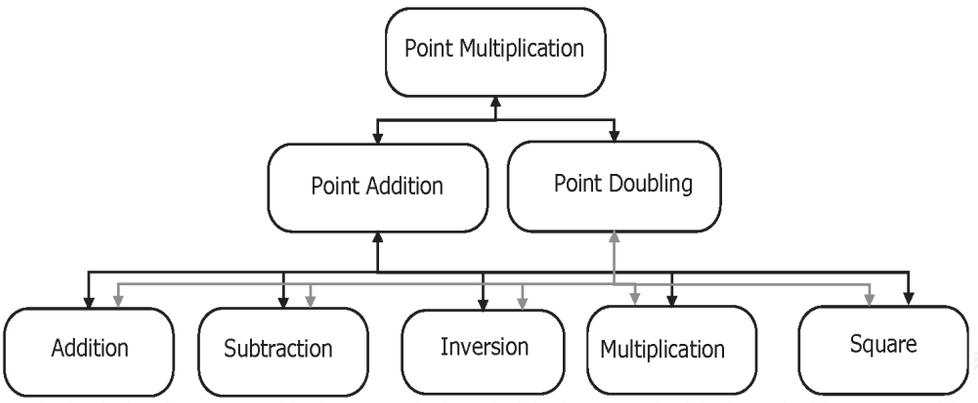


Figure 3.
Hierarchy of scalar multiplication.

2.2.2 ECC montgomery scalar multiplication

Point Multiplication is the base of the ECC. It exists differents algorithms to compute it. The Montgomery scalar multiplication, presented in Listing 1, is the most popular algorithm which is resistant against SCA (Side Channel Attacks) [13].

Listing 1: Montgomery Point multiplication

Input: k = (kn−1, kn−2..., k1, k0) ^{2} with Kn-1=1, P (x, y) ϵ E($F2^m$)
Output: Q = k. P
1: $R_0 \leftarrow 0$ and $R_1 \leftarrow P$
2: For i=n down to 0 do
3: If ki =1 then
4: $R_1 \leftarrow R_{1+} R_0$ Addition step
5: $R_0 \leftarrow 2R_0$ Doubling step
6: Else
7: $R_0 \leftarrow R_{0\ +} R_1$ Addition step
8: $R_1 \leftarrow 2R_1$ Doubling step
9: End if
10: End for
11: Return Q=R

2.2.3 López-Dahab's montgomery scalar multiplication

Using López-Dahab's Montgomery point multiplication, inversion, which consumes a lot of resources in terms of memory as well as execution cycles, and power consumption, is avoided and the number of multiplication operations is optimized. Algorithm 5 gives the Montgomery point multiplication. We can see that, whatever the value of ki, point addition (Madd) and point doubling (Mdouble) are computed simultaneously [14, 15].

Listing 2. López-Dahab's Montgomery scalar multiplication [15]

Input: k = $(k_{n-1}, k_{n-2}..., k1_{,\ k0})_2$ with
Output: Q = k P k_{n-1}=1 P (x,y) E(F_2^m)
Set X_1 = x; Z_1 = 1; $X_2 = x^4 + b$; $Z_2 = x^2$
For i from N -2 down to 0 do
If k_i = 1 then
Madd (X_1; Z_1; X_2; Z_2);

Mdouble (X_2; Z_2); else
Madd (X_2; Z_2; X1; Z1);
Mdouble (X_1; Z1);
End if
End for
$x_3 = X_1/Z_1$
$y_3 = (x+X_1/Z_1).[(X_1+xZ_1)(X_2+xZ_2)+(x^2+y)(Z_1.Z_1)].(xZ_1Z_1)^{-1}$
Return (x_3, y_3)

The point addition Madd (X1; Z1; X2; Z2) is computed as follow:

$$X1 = x\ (X1\ Z2 + X2\ Z1)^2 + X1\ Z1\ X2\ Z2; Z1 = (X1\ Z2 + X2\ Z1)^2$$

The point doubling Mdouble (X2; Z2) is computed as follow:

$$X2 = X^4{}_2 + b\ Z^4{}_2; Z2 = X^2{}_2\ Z^2{}_2$$

2.2.4 Side channel attacks (SCA)

In computer security, a side-channel attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited. Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks. The rise of Web 2.0 applications and software-as-a-service has also significantly raised the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g. through HTTPS or WiFi encryption), according to researchers from Microsoft Research and Indiana University [16] Many powerful side-channel attacks are based on statistical methods pioneered by Paul Kocher [17] Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically considered side-channel attacks: see social engineering and rubber-hose cryptanalysis.

General classes of side channel attack include:

Cache attack: attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service.

Timing attack: attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform.

Power-monitoring attack: attacks that make use of varying power consumption by the hardware during computation.

Electromagnetic attack: attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent to those in power analysis or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.

Acoustic cryptanalysis: attacks that exploit sound produced during a computation (rather like power analysis).

Differential fault analysis: in which secrets are discovered by introducing faults in a computation.

Data remanence: in which sensitive data are read after supposedly having been deleted. (i.e. Cold boot attack).

Software-initiated fault attacks: Currently a rare class of side-channels, Row hammer is an example in which off-limits memory can be changed by accessing adjacent memory too often (causing state retention loss).

Optical: in which secrets and sensitive data can be read by visual recording using a high-resolution camera, or other devices that have such capabilities (see examples below).

One significant advantage of the ECC is that this method can be utilized for random number generation. Dual-EC-DRBG is recommended by the NIST as a random generator standard [18]. But it has a back door in random bit generator algorithm [19].

3. Proposed hybrid method

An image encryption method should be simple to implement, safe, and rapid enough to be used in real applications. In the suggested technique, the image is divided into its original color scheme. This scheme has three color channels having red, green, and blue. Every channel presents a matrix having M × N size which is the input data for the cryptosystem. The mask of the color matrices is performed by the maskers where there are generated utilizing the primary key with the intervention of the ECC and AES algorithms. After the encryption step, channels are combined in order to produce a novel cipher image. The suggested model is effectuated in two steps which are: The key generation and the image encryption.

3.1 Key generation step

In the first, the two parts compromise on the ECC curve. In the second, the shared key is performed utilizing the help of Diffie-Hellman. Because of this latter, is vulnerable to attack, the two parts share values of Diffie-Hellman with its own digital signature to avert the attack. The primary key is utilized as an initial input to generate random numbers. This latter is the primary step to gaining the key.

3.1.1 Random number generation

Random Number Generator utilizes the benefits of Discrete Logarithm Problem (DLP) to generate sequence of number. The DLP in the elliptic curve cryptography permits to obtain irreversible numbers in order of P (a point on the curve) which is hard in the calculation. Ce cryptographic algorithm takes the strengths of the ECC principle operations, addition, and multiplication. Because it is unattainable to obtain the shared primary key; it's a DLP, sharing of point A and point G which are two points bellowing to the curve where A = [*JK*]. G, will not impact the security of the suggested way. The algorithm uses mainly point addition in the place of multiplication because this latter is very costly. In the final, because whole operations in the ECC are safe, the multiplication of X coordinates of points A, B, and C are employed to produce the matrix D. The value of JK is updated utilizing the Y coordinate of points to furnish randomness of the suggested algorithm that covering the back-door issue. The propound method utilized for the random generation is detailed in Listing 3.

Listing 3. The Algorithmic of Random Number Generation Step

1. **Procedure:** RNG (Y, G, k, Primary Key)
2. J $K_1 \leftarrow$ Primary Key
3. for i $\leftarrow$ 1, i $\leq$ k **do**
4. A (x, y) $\leftarrow$ $JK_i * G$ (x, y), where $*$ indicates the point multiplication in ECC
5. B (x, y) $\leftarrow$ A (x, y) $\otimes$ Y (x, y), where $\otimes$ indicates the point addition in ECC
6. C (x, y) $\leftarrow$ B (x, y) $\otimes$ G (x, y)
7. $D_i \leftarrow |x_A \times x_B \times x_C|$, where x_A is the coordinate of point A, x_B is the coordinate of the point B, x_C is the coordinate of the point C
8. J $K_{i+1} \leftarrow y_A + y_B + y_C$, where y_A is the coordinate of point A, y_B is the coordinate of the point B, y_C is the coordinate of the point C
9. end for
10. return D
11. End procedure

When analyzing the proposed algorithmic, we note that the Primary Key consists of shared primary key betwixt parts. Both G and Y bellow on the curve having big orders. The *k* parameter presents the number of randoms needed for the generation where its value dependant on the execution system specifications. It can be defined based on the size of the image. it is preferable to set *k* value founded on the size of image for small images and to fix this value for large images. *J K1* takes the value of the primary key. After that, the point *A (x, y), where x* and *y* are the coordinates of the point on the elliptic curve, is performed using the point multiplication between *J Ki* and the point *G (x, y)*. Then, the point *B (x, y)* is acquired using the point addition of *A (x, y)* and *Y (x, y).* To obtain *C (x, y),* a point addition of *B (x, y)* and *G (x, y)* is performed. In the end, *Di* is acquired using multiplication of $|xA \times xB \times xC|$and the *J Ki* value is updated by the simple addition of *yA + yB + yC. D* is the result of the algorithmic that contains generated numbers needed for the encryption. The D matrix presents the base for maskers' generation and initial ciphers.

3.1.2 Maskers generation step

After the generation, random numbers are utilized to produce maskers' matrices for the encryption process. Every masker is specific for its corresponding channel where it is ciphered using the AES. Maskers present the keyspace for cipher image and their entropy value tests the randomness in order to prove the effectiveness. The D array is utilized to create maskers for image encryption where the elements of Z are ciphered using AES with the primary key. In algorithmic 3, the RMR presents the masker result utilized to encrypt the red channel of the original image. After that, the RMR is employed as input for AES to obtain the green channel masker result (RMG). In the end, by applying the AES on the RMG, the blue channel masker RMB is obtained. An IV parameter is acquired using both Primary Key and β value where:

$$IV = (PrimaryKey) mod (K)$$

By utilizing this parameter, 3*128 bits initial cipher (IC) for every channel and a 128-bit IC_Key are created where:

$$IC_{Key} = D(IV)$$

$$IC_{Key} = RMR(IV)$$
$$IC_{Key} = RMG(IV)$$
$$IC_{Key} = RMB(IV)$$

These values are removed from maskers. The Listing 4 presents the technique maskers and ICs gained.

Listing 4. The Algorithmic of Masker Generation Step

1. **Procedure**: masker (Array D, Primary Key, k**)**
2. for i ← 1, i ≤ k do
3. RM_R ← AES (D, Key)
4. RM_G ← AES (RM_R, Key)
5. RMB ← AES (RM_G, Key)
6. IV= (Primary Key) mod(k)
7. IC red← RM_R (IV)
8. IC green← RM_G (IV)
9.IC blue← RM_B (IV)
10. end for
11. **Return** (RM, IC)
12. End procedure

3.2 Image encryption step

The suggested image encryption procedure is founded on the stream cipher. Firstly, the permutation of the image is performed utilizing a random generator. Then, the image is split into red, green, and blue matrices. Every matrix is converted to 128 bits. After that, an XOR operation is performed between every bit of color matrix and every bit of ICs and maskers. Every information stream is masked utilizing the correspondent key channel matrices created in the proceeding part containing RMR, RMG, RMB, ICred, ICgreen, ICblue and IC_Key. The suggested technique is presented in Listing 5. Here, the matrix of every color channel over keys utilized to cipher every channel is considered as input to the proposed algorithm. After that, every color matrix is split into 128 bits data path. Everyone has 16 pixels of individual color in its data. Then everyone is XORed with its initial cipher (IC) and its masker. When every data on the masker are employed, IC is updated utilizing the AES and XOR operation. At the end, when the encryption procedure is performed, the whole channels are combined to produce 24 bits of color pixels considered as a result of performing every channel side by side to obtain a novel cipher image. The decryption procedure is analogous to the encryption phase. But we must insert encrypted image input.

Listing 5: Algorithmic of Cipher Image Phase

1. Procedure: Image encryption (Mat_{red}, Mat_{blue}, Mat_{green}, RM_R, RM_G, RM_B, IC_{red}, IC_{green}, IC_{blue}, $IC\text{-}_{Key}$)
2. **for** i ← 1, i, ImageS ize/16 **do**
3. $Enc_{red,i}$ ← $S\,tream_{red}$ (i) ⊕ IC_{red} ⊕ RM_R
4. $Enc_{green,i}$ ← $S\,tream_{green}$(i) ⊕ IC_{green} ⊕ RM_G
5. $Enc_{blue,i}$ ← $S\,tream_{blue}$(i) ⊕ IC_{bule} ⊕ RM_B
6. **if** i mod n(RM_R) = 0 where ("n(RMr)" means the length of the RMr) **then**

7. $IC_{red} = AES(IC_{key}, IC_{blue})$
8. $IC_{green} = IC_{green} \oplus IC_{red}$
9. $IC_{blue} = IC_{blue} \oplus IC_{green}$
10. **end if**
11. $i \leftarrow i + 1$
12. **end for**
13. Encrypt_Image = Combine Channels ($S\,tream_{red}$, $S\,tream_{green}$, $S\,tream_{blue}$)
14. **return** Encrypt_Image
15. **end procedure**

4. Security analysis

Images encryption security is a major challenge. Hence the exigency to an enhanced security approach to resist against various attacks. Experimental results are realized in this paper with various different color images. Many standard tests and evaluations are considered in this paper to access and analyze the security of image encryption containing the noise attack, known plain text and chosen plain text attack, the UACI (Unified Average Changing Intensity), NPCR (Number of Pixels Change Rate), correlation of adjacent pixels, histograms, entropy, and the keyspace. The primary key used for the key generation is 897627103061277028662417274331420 15 and the *k = 128*.

4.1 Robustness against noise attack

During the image transmission via a network, the ciphered image can lose information or can be influenced by noise. Various cryptographic systems are sensitive to noise where a small change to the ciphered image can produce a strong distortion into the deciphered picture. **Figure 4** shows that the deciphered pictures keep the global clear image information for the man eye when the ciphered picture is affected by Salt § Pepper noise with various percentages. Therefore, the suggested method is robust and resist versus noise attack.

4.2 Differential attack analysis

Both NPCR (Number of Pixels Change Rate) and UACI (Unified Average Changing Intensity) are utilized for the verification of the performance versus

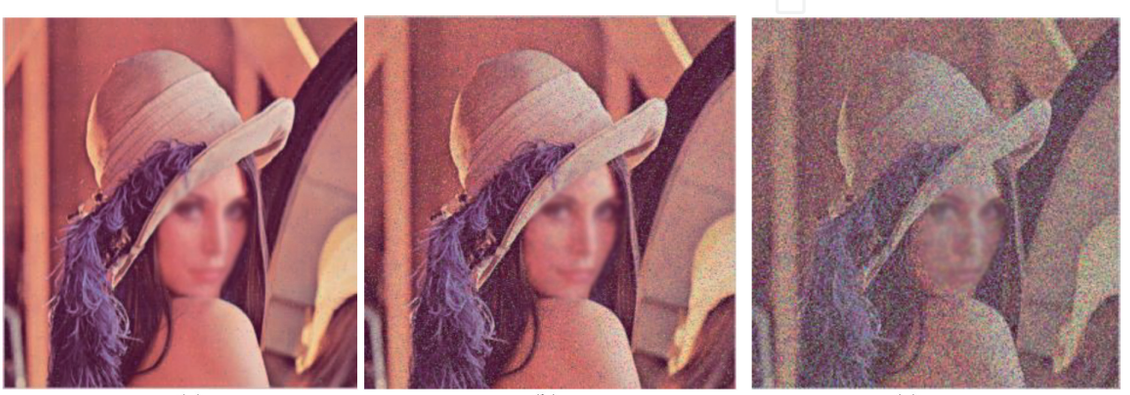


Figure 4.
Decrypted Lena of size 512 × 512 × 3 with salt § pepper noise: (a) d = 0.01, (b) d = 0.1 and (c) d = 0.5.

differential attacks. Only one-bit modification over the clear image can result a considerable modification in the encrypted picture. NPCR and UACI parameters are presented in Eqs. (1) and (2). The desired average values for UACI is 33.46% and for NPCR is 99.56%.

$$NPCR : N(C1, C2) = \sum_{i,j} \frac{D(i,j)}{W * H} * 100\% \tag{1}$$

$$UACI = U(C1, C2) = \frac{1}{W * H} \sum_{i,j} \frac{|C1(i,j) - C2(i,j)|}{225} * 100\% \tag{2}$$

Where:
C1, C2 are the Ciphered pictures.
M is the size of pictures.
D: Bipolar matrix determined from C1 and C2.

The NPCR measures the pixels number that modifies value in differential attack. The elevated value is considered better. The UACI computes the average variance betwixt two paired encrypted pictures where a minimal value is the best. **Table 1** compares both NPCR and UACI results performed on Lena $512 \times 512 \times 3$ using the suggested algorithm with some existing works. Results prove that the propound cryptographic technique has meet desired objective for resisting versus differential attacks.

4.3 Statistical Attack Analysis

Histogram of encrypted picture analysis and correlation of adjacent pixels are two fundamental parameters required to prove that the proposed cryptographic model is resistant versus statistical attacks.

4.3.1 Histogram analysis

The histogram of the picture shows the frequency of every pixel. An improved cryptographic system must produce a uniform color distributed histogram. **Figure 5** shows the histogram of original and ciphered images. As you can see, histograms of ciphered images are uniform. The large dissimilarity between the two histograms from original and ciphered images denotes that images are greatly uncorrelated and no information can be detected from the cipher pictures which proves that the suggested cryptographic model is resistant versus statistical attacks.

4.3.2 Correlation coefficient analysis

The correlation is a performance that evaluates the grade of similitude between two objects. If the original and the encrypted are different, therefore, the correlation factor is well low or highly close to zero. The reduced values prove that the encryption proceedings are capable to cover all characteristics of the transmitted

Algorithm	Proposed Model	[20]	[21]	[22]
NPCR	99.6215	99.6162	99.50	99.61
UACI	33.4631	33.3979	33.30	33.48

Table 1.
Comparison of the NPCR and UACI results with existing methods.

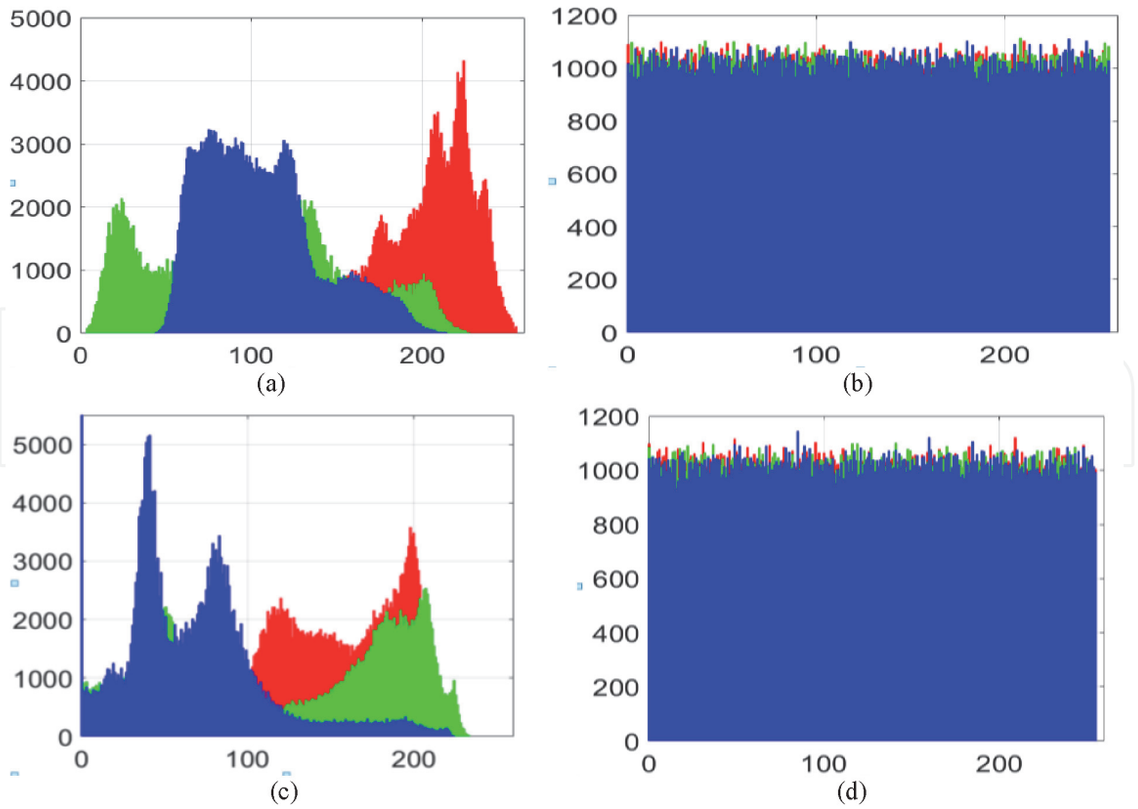


Figure 5.
Histogram of original and cipher images: (a): Histogram of original Lena image, (b): Histogram of Lena cipher image, (c): Histogram of original pepper image, (d): Histogram of pepper cipher image.

image. **Figure 6** shows the distributions of 2000 pairs randomly selected adjacent pixels of the original and encrypted Lena $512 \times 512 \times 3$ image, respectively in the horizontal, vertical, and diagonal direction.

The following equations are utilized for the study of the correlation between two adjacent pixels in the horizontal, vertical, and diagonal orientations for both clear and ciphered images.

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} xi \tag{3}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} (xi - E(x))^2 \tag{4}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N} (xi - E(x))(yi - E(y)) \tag{5}$$

$$rx,y = \frac{cov(x,y)}{\sqrt{D(x)} \times \sqrt{D(y)}} \tag{6}$$

Where x, y are the intensity values of the two adjacent pixels in one image. N is the number of adjacent pixels chosen to compute the correlation.

We measured the correlation factor between the clear and ciphered images in each direction and findings are exposed in **Table 2**.

Findings show that coefficients are very reduced in the ciphered images in all directions and near to zero. On the other hand, the proposed cryptographic method is compared with other methods existing in the literature and results prove that the propound cryptosystem has a better correlation with the smallest coefficients in all

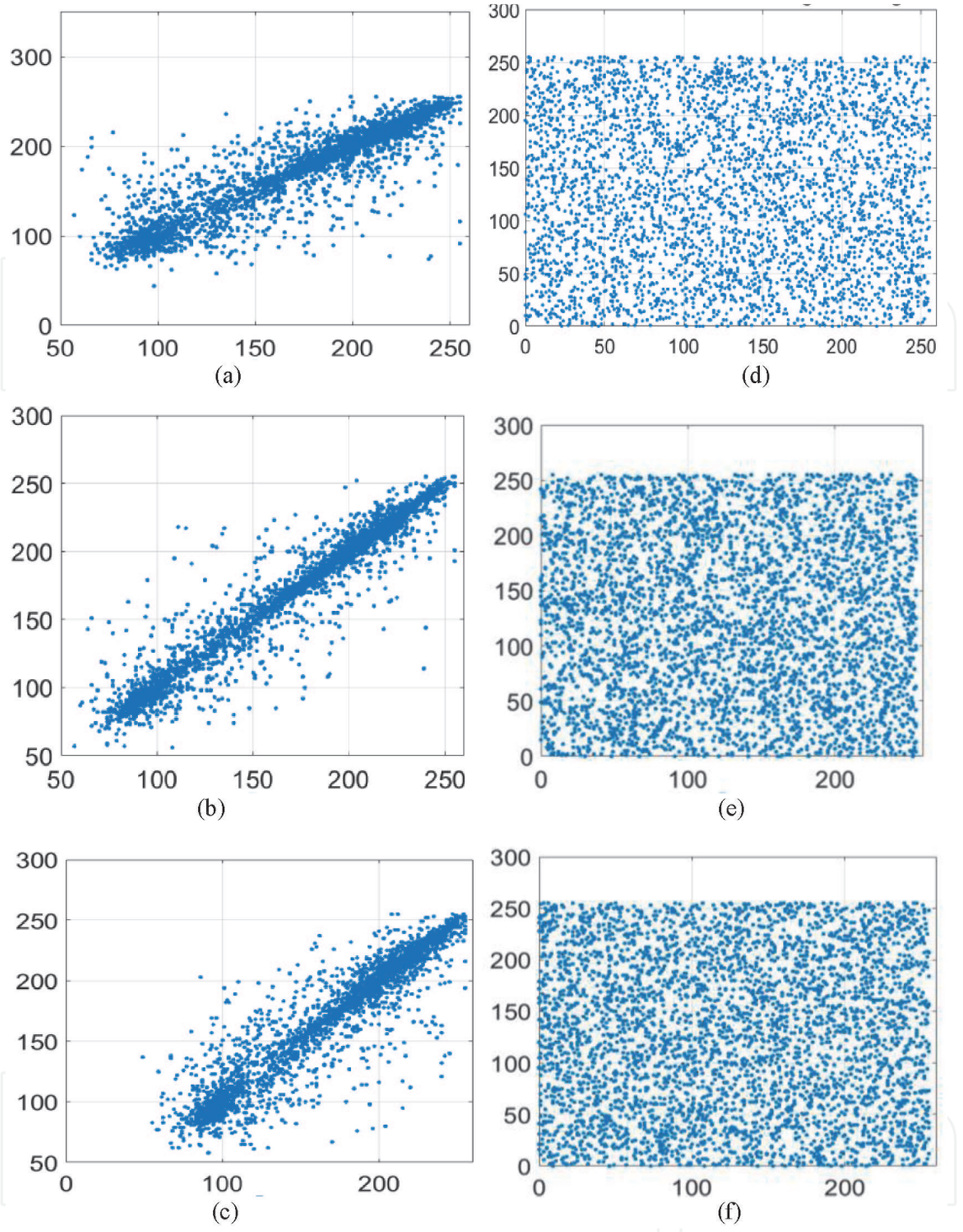


Figure 6.
Correlation distribution of original and cipher Lena 512 × 512 × 3 color image in horizontal, vertical and diagonal directions: (a)-(c): Correlation distribution of original images; (d)-(f): Correlation distribution of cipher images.

directions which prove the effectuality of the algorithm and its capability for resisting statistical attack.

4.4 Information entropy analysis

The entropy parameter is considered as the standard to test randomness. Entropy coefficient is utilized to obtain the incertitude performed in the ciphered image. If the entropy is elevated, the confidentiality is higher. Note that the utmost

Algorithm	Correlation coefficient		
	Horizontal	Vertical	Diagonal
Proposed Method (Lena)	-0.00871	-0.00141	-0.02039
Proposed Method (Baboon)	-0.00796	-0.01509	0.00196
Proposed Method (Peppers)	-0.03619	0.00295	0.013008
Ref. [20]	0.004639	0.006763	0.010818
Ref. [21]	0.00100	0.0017	0.01250
Ref. [22]	0.000101	0.00000958	0.000131

Table 2.
The correlation coefficient comparison with different encryption methods.

Algorithm	Cipher image
Proposed Method (Lena 512*512×3)	7.99951
Ref. [20]	7.9989
Ref. [21]	7.9973
Ref. [22]	7.9994

Table 3.
The entropy value comparison with different encryption methods.

entropy value for a gray scale image is 8 bits/pixel. The average value for H(m) for numerous preceding works was between 7.90 and 7.99. This value is depending on the image, the size of the key and the cryptographic model. Entropy is computed as:

$$H(m) = \sum_{i}^{2N-1} P(m||i)\, log\, 2\left(\frac{1}{P(mi)}\right) \tag{7}$$

Where:
$H(m)$: Entropy image.
$P(mi)$: Probability mass function.
$2N - 1$: number of gray levels.
Table 3 compares the entropy value gained by the proposed model with other cryptographic methods. Results denote that the entropy value of the suggested cryptographic system is much closer the ideal case which prove the randomness of the system.

4.5 Know plain text and chosen plain text attack

In the proposed algorithm, the diffusion process is performed by the XOR operation of the AES. Thus, it is very essential to evaluate its robustness against the chosen plain text attack. This type of attack uses the encrypted image with arbitrary plaintext data to crack the cryptosystem algorithm. According to reference [23], if the Eq. (8) is determined, the algorithm will be vulnerable to chosen plain text attacks. Otherwise, the algorithm resists chosen plain text attacks.

$$C_1(x,y) \oplus C_2(x,y) = P_1(x,y) \oplus P_2(x,y) \tag{8}$$

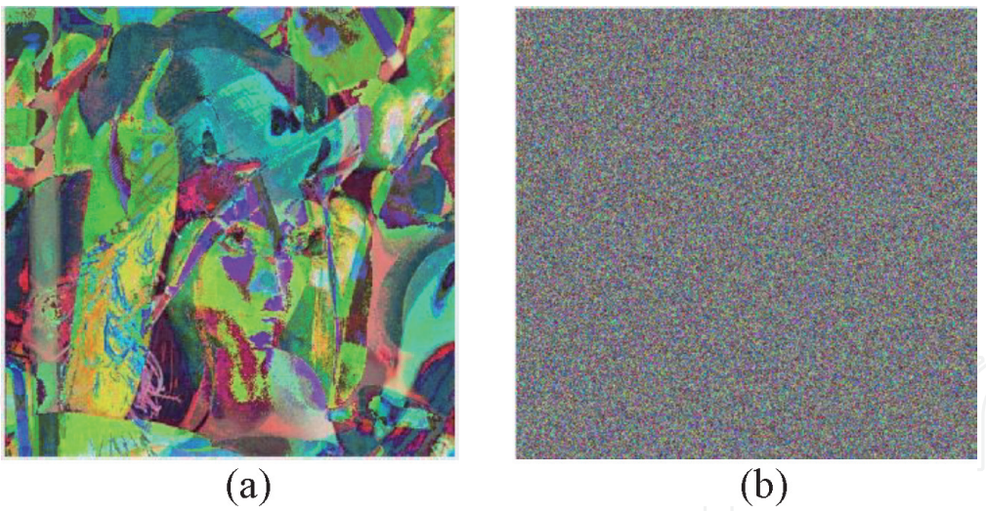


Figure 7.
Plain text analysis: (a) is the P1Xor P2, (b) is the C1 Xor C2.

P1 and P2 are the plain Lena and Pepper images, while, C1 and C2 are their corresponding encrypted images, respectively. **Figure 7** shows that the XOR of encrypted image and clear image are not equal, i.e., the proposed cryptosystem algorithm resists chosen plain text attack.

4.6 Security key analysis

An improved cryptographic model must have a large key size space. Because the suggested model employs a stream cipher encryption technique, the random generation period should be long. In order to guarantee the safety of the propound model, 128- bit AES is utilized that results in a large enough key space versus the brute force attack (requires 2^{128} states to crack the key). The random generator employed in the suggested model is acquired from the elliptic Curve cryptosystem ECC, where its randomness is justified by the NIST. In the encryption step, the value of G (x, y) is modified at the debut of the encryption because the curve is changed. This result a dramatic modification in the created randoms and IV.

4.7 Key sensitivity analysis

An enhanced encryption model should be greatly sensitive to key changes. Similarly, the suggested model must be resistant to the Brute-force attack obtained by large key space. For the Elliptic Curve Cryptosystem, we have employed a 256 key size and for the AES, we have selected the use of 128 bits key size which are big

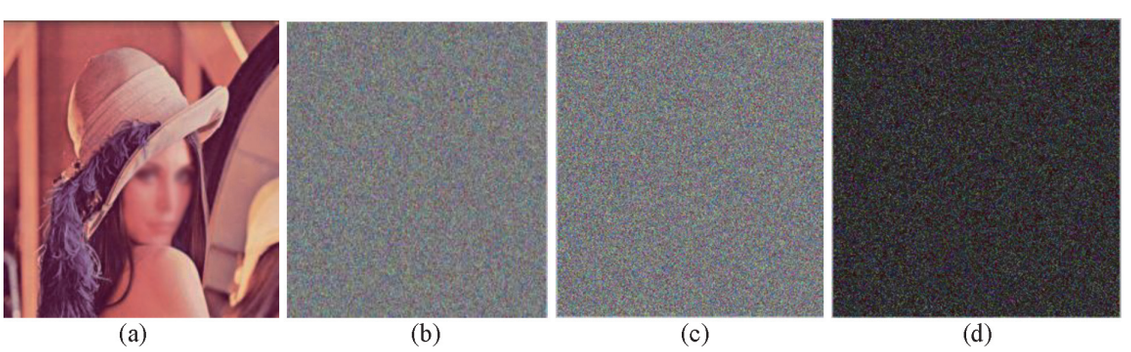


Figure 8.
Test of the key encryption sensitivity: (a) plain image Lena 512 × 512 (b) cipher image by the main key (c) cipher image by the modified key (d) encryption with the key difference between the two keys.

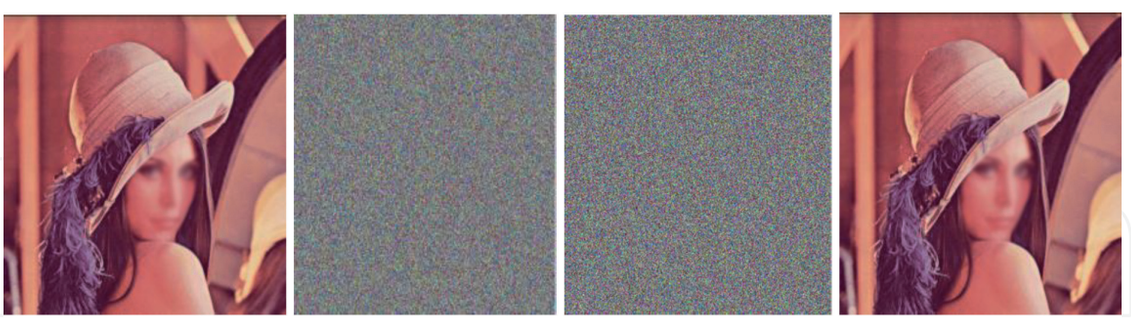
enough to resist versus attacks. To check the encryption process, the plain image is encrypted by three various keys: the first is the main key, the second is the same key with a small change in one bit and the last is a variance between the two keys. The finding of three different ciphered images are presented in **Figure 8**. Similarly, the ciphered image is decrypted by two keys: one is the original key and the other is the modified key. The changed key does not allow retrieval of the clear image as seen in **Figure 9**. As result, the suggested model is greatly sensitive to the key changes.

4.8 Time complexity

In real-time image processing, the execution time is a major constraint. In a software implementation, the speed of execution mainly depends on CPU performance. The proposed algorithm is implemented using the Matlab R2017a software running on a personal computer with CPU Intel Core-i7–3770 3.4 GHz frequency. The time consumption is evaluated where α was dynamic initiated based on image size. **Table 4** gives findings obtained by our hybrid model compared to original AES and ECC.

4.9 Discussion

Through security analysis, it is shown that the histogram of the ciphered picture has uniform distribution and the correlation between pixels is decreased. The entropy value of Lena's standard image is 7.99951 (close to the ideal value). The suggested cryptographic model has an efficient encryption effect and a big secret keyspace. Further, findings prove that the proposed model can resist versus noise with various intensity and differential attacks. The execution time of the proposed scheme is executed with some images with different sizes. We note that our algorithm requires much less calculation time than the standard AES and ECC algorithms.



(a) (b) (c) (d)

Figure 9.
Test of the key decryption sensitivity: (a) original image Lena 512 × 512 × 3 (b) cipher image by the right key (c) decryption by 1-bit key change (d) decryption with the right key.

Encryption Model (s)	128×128	256×256	215×215	1024×1024
AES	0.64	1.320	2.987	5.315
ECC	22.215	40.320	87.120	-
Proposed Model	0.32	0.615	1.197	2.157

Table 4.
Running time of proposed model for different image sizes.

DOI: http://dx.doi.org/10.5772/intechopen.95511

5. Conclusion and future work

A novel technique for image encryption was suggested in this paper. The procedure of encryption is performed using cooperation between Elliptic Curve Cryptography (ECC) and the Advanced Encryption Standard (AES). In this hybrid scheme, we have proposed to take the benefits of the Elliptic Curve Random Generator to generate a sequence of arbitrary numbers based on the curve. Then, the AES is performed to these sequences using arbitrary keys for image encryption. Security analysis over this model proved that it is resistant to known attacks. The histogram, correlation of adjacent pixels, and entropy of the encrypted image were computed and findings were hopeful. The optimal keyspace that can be used for encryption is 256-bit ECC and 128-bit AES key. As continuity to this work, we propose cooperation between Elliptic Curve Digital Signature (ECDSA) and AES cryptosystem. This prototype will be applied in large images and video signals.

Author details

Amal Hafsa[1*], Mohamed Gafsi[1], Jihene Malek[1,2] and Mohsen Machhout[1]

1 Electronics and Micro-Electronics Laboratory, University of Monastir, Monastir, Tunisia

2 Department of Electronics, Sousse University, Higher Institute of Applied Sciences and Technology, Sousse, Tunisia

*Address all correspondence to: hafsaamal12@gmail.com

References

[1] C. JunLi, Q. Dinghu, Y. Haifeng, Z. Hao, M. Nie, Email encryption system based on hybrid AES and ECC, in: Wireless Mobile and Computing (CCWMC 2011), IET International Communication Conference on, IET, 2011, pp. 347–350.

[2] A. R. Ganesh, P. N. Manikandan, S. P. Sethu, R. Sundararajan, K. Pargunarajan, An improved AES-ECC hybrid encryption scheme for secure communication in cooperative diversity based wireless sensor networks, in: Recent Trends in Information Technology (ICRTIT), 2011 International Conference on, IEEE, 2011, pp. 1209–1214

[3] H.T,Mohd BJ, A. Itradat, AN. Quttoum, Performance and information security evaluation with firewalls. Int J Secur Appl 7(6):355–372. https://doi.org/10.14257/ijsia.2013.7.6.36.

[4] H. T, S. Ullah, B.J. Mohd, KS. Balagani, An enhanced WLAN security system with FPGA.IEEE Syst J 11(4): 2536–2545. https://doi.org/10.1109/JSYST.2015.2424702.2017.

[5] A.M. Atteya, AH. Madian, A hybrid Chaos-AES encryption algorithm and its implementation based on FPGA,2014, New Circ Syst IEEE 217–220. https://doi.org/10.1109/NEWCAS.2014.6934022.

[6] K. Shankar, P. Eswaran, An efficient image encryption technique based on optimized key generation in ecc using genetic algorithm, in: Artificial Intelligence and Evolutionary Computations in Engineering Systems, Springer, 2016, pp. 705–714.

[7] A. A. A. El-Latif, X. Niu, A hybrid chaotic system and cyclic elliptic curve for image encryption, AEU-International Journal of Electronics and Communications 67 (2) (2013) 136–143.

[8] H. Liu, Y. Liu, Cryptanalyzing an image encryption scheme based on hybrid chaotic system and cyclic elliptic curve, Optics & Laser Technology 56 (2014) 15–19.

[9] F. Rannou, Numerical study of discrete plane area-preserving mappings, Astronomy and Astrophysics 31 (1974) 289.

[10] Fips, N (2009). Announcing the advanced encryption standard, AES. Technol. Lab. Natl.2001, Inst. Stand. Vol., pp. 8–12.

[11] V. Miller, “Use of Elliptic Curves in Cryptography,” Advances in Cryptology – CRYPTO’85, vol. LNCS 218, pp. 417–426, 1986.

[12] N. Koblitz, “Elliptic curve cryptosystems,” Mathematics of Computation, vol. 48, no. 177, pp. 203–203, Jan. 1987.

[13] Montgomery, P. (2010) ‘Speeding the Pollard and elliptic curve methods of factorization’, Mathematics of Computation, Vol. 48, 243–264.

[14] A.Hafsa; A. Sghaier; M. Zeghid; J. Malek; M. Machhout,(2020), An improved co-designed AES-ECC cryptosystem for secure data transmission, International Journal of Information and Computer Security, Vol.13 No.1, pp.118–140.

[15] Tanja Lange, A note on López-Dahab coordinates. Source DBLP, January 2004.

[16] Shuo Chen; Rui Wang; XiaoFeng Wang & Kehuan Zhang (May 2010). "Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow" (PDF). Microsoft Research. IEEE Symposium on Security & Privacy 2010.

[17] Kocher, Paul (1996). "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems". Advances in Cryptology — CRYPTO '96.Advances in Cryptology—CRYPTO'96. Lecture Notes in Computer Science. 1109. pp. 104–113. doi:10.1007/3–540-68697-5_9. ISBN 978–3–540-61512-5. Retrieved 14 April 2014.

[18] Recommendation for random number generation using deterministic random bit generators, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-90Ar1.pdf.

[19] D. J. Bernstein, T. Lange, R. Niederhagen, Dual ec: A standardized back door, in: The New Codebreakers, Springer, 2016, pp. 256–281.

[20] Z. Lin, J. Liu, J. Lian, Y. Ma, X. Zhang (2019), A novel fast image encryption algorithm for embedded systems, Multimedia Tools and Applications 78:20511–20531 https://doi.org/10.1007/s11042-018-6824-5.

[21] A. A. A. El-Latif, X. Niu, (2013), A hybrid chaotic system and cyclic elliptic curve for image encryption, AEU-International Journal of Electronics and Communications 67 (2) 136–143.

[22] Y. Bentoutou, EL.H.Bensikadour,N. Taleb,N.Bounoua,(2019),An Improved Image Encryption Algorithm for Satelite Application, *Advances in Space Research*, elseiver, Doi:https://doi.org/10.1016/j.asr.2019.09.027.

[23] Sundararaman Rajagopalan, Sivaraman Rethinam, Sridevi Arumugham, Har Narayan Upadhyay, John Bosco Balaguru Rayappan Rengarajan Amirtharajan, "Networked hardware assisted key image and chaotic attractors for secure RGB image communication», Multimedia Tools Appl (2018) 77:23449–23482 https://doi.org/10.1007/s11042-017-5566-0.