IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 17 November 2022, accepted 8 December 2022, date of publication 16 December 2022,
date of current version 19 January 2023.

Digital Object Identifier 10.1109/ACCESS.2022.3230096

RESEARCH ARTICLE

An Integrated Image Encryption Scheme Based on Elliptic Curve

IJAZ KHALID[1], TARIQ SHAH[1], SAYED M. ELDIN[2], DAWOOD SHAH[1], MUHAMMAD ASIF[3], AND IMRAN SADDIQUE[4]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad 45320, Pakistan
[2]Center of Research, Faculty of Engineering, Future University in Egypt, New Cairo 11835, Egypt
[3]Department of Mathematics, University of Management and Technology, Sialkot 51310, Pakistan
[4]Department of Mathematics, University of Management and Technology, Lahore 54770, Pakistan

Corresponding author: Muhammad Asif (muhammad.asif@math.qau.edu.pk)

This work was supported in part by the Research Center of the Future University in Egypt, 2022.

ABSTRACT Due to the extensive demand for digital images across all fields, the security of multimedia data over insecure networks is a challenging task. The majority of the existing modern encryption schemes are merely developed that ensure the confidentiality of the image data. This manuscript presents a new image encryption scheme that ensures confidentiality, user authentications, and secure key sharing among the communicating parties. Initially, the users share a secret parameter using Diffie-Hellman over the elliptic curve and pass it through SHA-256. Afterwards, the proposed scheme uses the first 128-bits for the confidentiality of the data, while the remaining 128-bits are for authentication. In the encryption algorithm, the confusion module is achieved by affine power affine transformation. At the same time, the diffusion module is attained through highly nonlinear sequences, which are generated through the elliptic curve. Experimental testing and the latest available security tools are used to verify the effectiveness of the proposed algorithm. The simulation findings and the comparison of the proposed scheme with the existing image encryption techniques reveal that the suggested scheme offers a sufficient degree of security. Furthermore, the outcome of the simulation results divulges several advantages of the proposed scheme, including a large key space, resistance to differential attacks, high efficiency, and strong statistical performance.

INDEX TERMS Image encryption, S-box, elliptic curve cryptography, affine power transformation.

I. INTRODUCTION

The transmission of multimedia information, such as digital images, audio data, and video, via various networks significantly increased due to the rapid development in network evolution. However, mostly the data transmission procedures occurred through unsecured networks. Therefore, there is a chance that information might be lost, intercepted (i.e., copied and distributed illegally), and can be altered maliciously [1], [2], [3], [4]. Over the internet, the digital image is an essential source for data communication. For instance, in the medical field, images are used for visualizing different analyses and diagnoses. These analyses are transmitted in the form of images. The patients use these images and get consultations from medical specialists anywhere around the globe. So, in this case, integrity and confidentiality violation are very dangerous for the patients. Similarly, a secure image transmission technique over the open network is also required for criminal investigations. The government domain needs to ensure the secrecy and integrity of the data in order to avoid injustice. So, the security of digital image data has become a growing source of worry. Due to the inherent properties of the digital image, high correlation among the adjacent pixels and the quantity of data, the standard cryptographic techniques such as data encryption standard (DES) and advanced encryption standard (AES) algorithms are not suitable for digital image encryption. Therefore, various cryptographic techniques are presented in the literature for secure multimedia data over the open network. The properties of a nonlinear dynamical system, sensitivity to initial conditions, ergodicity,

The associate editor coordinating the review of this manuscript and approving it for publication was Yilun Shang.

mixed characteristics, convenient algorithmic description, and high complexity are beneficial for cryptographic applications. Since hyperchaotic maps produce more randomness than chaotic systems, therefore these are more suited for image encryption applications. Different scholars have presented numerous schemes based on hyperchaotic systems. In [7], a four-dimensional (4D) hyperchaotic algorithm is suggested. In the recommended work, the scheme creates key stream and controls parameters that are used to shift rows and columns of the image. In [8], suggested a 2D compound homogeneous hyperchaotic system that performed permutation of pixels. However, the proposed work is vulnerable to chosen plaintext attacks [9]. To address this flaw, plaintext was correlated with the stream of the chaotic key in the generation of the final encryption key. The stream derived from the hyperchaotic sequences improved the security against the chosen-plaintext attack [10]. Elliptic Curve Cryptography (ECC), which is based on algebraic geometry, is a cryptographic technique for power-constrained devices. ECC has recently been used for image encryption applications. RGB image encryption based on ECC is investigated in [13]. The presented scheme utilized DNA encoding and decoding for RGB image encryption and decryption followed by elliptic curve Diffie Hellman. The algorithm presented in [14], employed a cyclic group of an elliptic curve with the combination of chaos. Consequently, it increased the key space of the suggested scheme. Similarly, the image encryption based on chaos with the elliptic curve ElGamal is presented in [15]. The suggested work compressed the plain images and enhanced the complexity of the 4-D cat map. Subsequently, the encryption is executed by EC-based asymmetric encryption. Likewise, the author designed a hybrid multilayered mathematical model for colour image encryption presented in [5]. In [26], Bellare and Rogaway introduced a hybrid cryptographic architecture named Elliptic Curve Integrated Encryption Scheme (ECIES). The ECIES is a pair of key-derivation functions, a symmetric key encryption algorithm, and a MAC algorithm. Since the message is sometimes difficult to encode in the points of the curve, so challenging to encrypt; contrastingly, one can easily encrypt any message using a symmetric-key scheme of ECIES. This is a significant advantage of ECIES over the Massey-Omura and ElGamal public-key approaches [26]. In [27], the author presented a technique for medical image encryption based on the improved version of ECIES. In the suggested work, the author identified some flaws and weaknesses in the EC Hill-Cipher-based image encryption and improved the security parameter using IECIES. However, the computational complexity of the suggested scheme is slightly increased due to the serval time of scalar multiplication of the curve points.

In view of the shortcomings above, we proposed a novel integrated image encryption algorithm. The proposed scheme consists of a secure key exchange protocol, hash algorithm, and symmetric key algorithm. The exchange protocol is used for the communication of secret keys among the communicating parties. The hash function is used for data integrity, and the symmetric algorithm is used for data confidentiality. The confusion and diffusion module of the symmetric encryption is achieved by using simple operations that provide optimum security with less computational effort. Furthermore, the security performance of the scheme is thoroughly analyzed using the available tools. The resultant output demonstrates the scheme's efficiency compared to the existing scheme.

The remaining manuscript is organized as follows: The basic notation of EC is provided under Section II of this work. A detailed description of E-ECIES introduces in section III. Sections IV, V and VI, evaluate the nonlinear component and the simulation results of proposed symmetric encryption and their analysis for RGB images. The manuscript is concluded in section VII.

II. PRELIMINARIES

ECC is an asymmetric or public key method based on the algebraic structure of elliptic curves. Koblitz and Miller [28], [29] introduced its application in cryptography in 1985. The ECC offers a comparable level of security to traditional asymmetric cryptosystems like RSA but with noticeably reduced key sizes. This section consists of essential preliminaries and their related results presented in Washington and Galbraith [26]. An elliptic curve over a finite field $\mathrm{F_q}$ is defined as.

$$\mathbb{E}_{\mathcal{F}_q}^{\mathrm{a,b}} = \{\infty\} \cup \Big\{(x, y) : x, y \in \mathcal{F}_q \times \mathcal{F}_q : \Upsilon^2 \\ = x^3 + ax + b \; mod \; q\Big\} \tag{1}$$

where both a and b are the parameters of EC, with the condition that is $4a^3 + 27b^2 \neq 0$. Otherwise, the EC is said to be singular. All the points $\mathbb{E}_{\mathcal{F}_q}^{\mathrm{a,b}}$, that has a specific sort of addition law from an abelian group with the neutral element ∞, called the point of infinity.

A. ELLIPTIC CURVE ARITHMETIC OPERATION

The following mathematical equation governs an elliptic curve over a finite field. Let $P_1 = (x_1, y_1)$ and $Q_1 = (x_2, y_2)$ are the two points of the elliptic curve such that $P_1 \neq Q_1$, then the addition of P_1 and Q_1 compute using the following mathematical formula.

$$R = P_1 + Q_1 = (x_3, y_3) \tag{2}$$

where, $x_3 = \varsigma^2 - x_1 - y_1 \; mod \; p \; y_3$

$$x_3 = \varsigma\,(x_1 - x_3) - y_1 \; mod \; q \tag{3}$$

$$\varsigma = \frac{y_2 - y_1}{x_2 - x_1} \; mod \; p \tag{4}$$

If P_1 and Q_1 are the same points ($That \; is$, $P_1 = Q_1$) then the point doubling calculation is defined as:

$$2Q = (x_3', y_3') \tag{5}$$

where,

$$x_3' = \xi^2 - 2x_1 \, mod \, p,$$
$$y_3' = \xi \left(x_1 - x_3'\right) - y_1 \, mod \, q \tag{6}$$
$$\xi = \frac{3x^2 - a}{2\Upsilon} \, mod \, q \tag{7}$$

In addition to scalar point multiplication, multiple point addition is carried out.

$$MQ_1 = Q_1 + Q_1 + Q_1 \ldots .M \ times \tag{8}$$

The following Hass's inequality theorem calculates the cardinality of points on the EC.

B. THEOREM 1

Let $\mathbb{E}_p^{a,b}$ over finite field $\mathcal{F}_q$. Then the cardinality (order) of $\mathbb{E}_q^{a,b}$ should be satisfy

$$q + 1 - 2\sqrt{q} \leq \mathbb{E}_q^{a,b} \leq q + 1 + 2\sqrt{q} \tag{9}$$

C. ELLIPTIC CURVE DISCRETE LOGARITHM PROBLEM(ECDLP)

Let $\mathbb{E}_q^{\mathrm{a,b}}$ be the elliptic curve over the finite prime field $\mathcal{F}_q$, where p is prime and a, b $\in \mathcal{F}_q$. The discrete logarithm problem for an elliptic curve is defined as given a point Q_1, and Q_2 on $\mathbb{E}_q^{\mathrm{a,b}}$, to find the positive integer M, if it exists, such that $Q_2 = MQ_1$ [31].

D. SECURE HASH ALGORITHM

A category of hash functions is called Secure Hash Algorithms (SHA). It was made public by the National Institute of Standards and Technology (NIST). Applications of SHA are predominantly located in integrity security services [30]. One of the well-known SHA algorithms is SHA-256, which generates message digests with 256-bit lengths. The proposed algorithm generates the Hash of key of 256-bit between users A and B. The first 128-bit is utilized for encryption, while the 128-bit length key is used for authentication.

III. ENHANCED ELLIPTIC CURVE INTEGRATED ENCRYPTION SCHEME (E-ECIES)

The E-ECIES is used to improve the secret parameter in the negotiation phase. The improvement is made by adding the initialization vector IV to prevent repeated data encryption. The initialization vector makes it harder for the hacker to detect patterns and break encryption using a dictionary attack. Furthermore, the IV must be known by user B in order to decrypt the cipher image. There are numerous techniques to make the IV accessible to user B in order to aid in decryption. However, the IV would be agreed upon prior to communication in our suggested algorithm for user's A and B. Moreover, the symmetric key is extracted using secure SHA-256. The detailed process of the E-ECIES is summarized in the below subsection. Let user A want to send a plain image M of size $\mathcal{U} \times \mathcal{V}$ to user B over the insecure channel. At the initial step of the protocol user, B first creates his public key by choosing the elliptic curve over the finite field $\mathcal{F}_q$ such that the discrete log problem for $EC(\mathcal{F}_q)$ is difficult, and he picks a point p on EC that is generally of big prime of order $\mathcal{N}$. He then calculates the public key $P^B = \mathfrak{m}p$ using a secret number $\mathfrak{m}$. The public key parameter of user B is $\{F_q, EC, N, p, P^B)$, while the private key of user B is $\mathfrak{m}$. The following steps are computed to transmit the data between user A and user B.

A. USER A COMPUTATION

- Choose a secret key $n^A \in [1, q-1]$.
- Computed the public key $P^A = n^A \mathbb{G}$ with timestamp $\mathcal{T}_O^A$.
- Compute the $P_1^A = n^A P^B$.
- Create a random initialization vector $\mathbb{V}$ with the increment of the prime number for every block of message.
- Compute the Hash and extract the symmetric key; the mathematical description of the hash function is given below.

$$Hash\left(P^A\,(x \oplus y)\,, P_1^A, V\right) = H_1 = K_1||K_2$$

- Compute the proposed symmetric key encryption function with K_1

$$C = Enc_{K_1}(M) \text{ and } T = (C, K_2)$$

- Send $< H_1, P^A, \mathcal{T}_O^A, \mathcal{T} >$ to user B.

B. USER B COMPUTATION

In response to receiving the message from user A, the user B generates a new timestamp $\mathcal{T}_O^B$, and follows these steps:

- The user B verifies $|\mathcal{T}_O{}^B - \mathcal{T}_O^A| \leq t$. If the condition does not hold, user B aborts, or else he sustained. The duration of t is a short, predetermined time.
- User B computes $P_1^A = \mathfrak{m}P^A$ using the knowledge of private key m.
- Calculate the $Hash(P_1^A, P^A\,(x \oplus y)\,, \mathbb{V})) = H_2$. If $H_2 \neq H_1$, when it does not hold, he passes over the session. Otherwise, B continues the remaining steps of the protocol.
- Generate the symmetric key $H_2 = K_1||K_2$.
- Computes $H_2\,(C, K_2) = T_1$. If $\mathcal{T}_1 \neq \mathcal{T}$, user B rejects the cipher image; otherwise, continue the protocol steps.
- Calculate the plan-image $M = Dec_{K_1}(C)$, where Dec_{K_1}, is a symmetric key decryption function. As a part of user B computation, the second last step involves authentication, which is an essential aspect.

C. PROPOSED SYMMETRIC KEY ENCRYPTION

In this section, we proposed a new symmetric key encryption algorithm based on E-ECIES. The symmetric key encryption algorithm encapsulates the following steps to perform image encryption. Initially, the scheme uses secure SHA-256 to generate the key using the following mathematical formula.

$$Hash\left(P^A\,(x \oplus y)\,, P_1^A, \mathbb{V}\right) = \mathcal{K}_1||\mathcal{K}_2$$

where $\mathcal{K}_1$ followed by $\mathcal{K}_2$. To perform the encryption using key $\mathcal{K}_1$ the following steps are to be done. For the

$\mathcal{K}_1 = 128bit$ is utilized for the encryption, while the $128bit$ of $\mathcal{K}_2$ are used for authentication purposes. Initially, the first four-byte $b_1b_2b_3b_4$, are utilized for the permutation of the plain image using affine mapping. The mathematical construction for the permutation of the plan image using affine mapping is defined as.

$$\mathscr{p} : \mathscr{z}_m \times \mathscr{z}_m \rightarrow \mathscr{z}_m \times \mathscr{z}_m \tag{10}$$

$$\mathscr{p}\,(\mathscr{i}, \mathscr{j}) = (\mathscr{i}', \mathscr{j}') \tag{11}$$

$$\mathscr{i}' = b_1\,(\mathscr{i}) + b_2, \quad \mathscr{j}' = b_3\,(\mathscr{j}) + b_4 \tag{12}$$

where b_1, b_3 the unit's elements are $\mathscr{z}_m$, while, b_2 and b_4, are any elements in from $\mathscr{z}_m$. The $\mathscr{i}'$ and $\mathscr{j}'$, the output of the affine transformation, which shows the permuted pixel of the image.

D. DIFFUSION PHASE BASED ON ELLIPTIC CURVE PSEUDO-RANDOM NUMBER SEQUENCES

The next six bytes $b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$ is again utilized for the permutation purpose using the elliptic curve parameter with the large prime p, which is the concatenation of the last two bytes, i.e., $\text{p} = b_{11}||b_{12}$. After the generation of points on each elliptic curve, pick the y-coordinate of the first elliptic curve, i.e., $E_1^{Y_i}$, and get the first sequence, namely $\mathcal{K}_1$, similarly, we can compute the $\mathcal{K}_2$, $\mathcal{K}_3$, sequences by choosing the y-coordinate of $E_2^{Y_i}$, $E_3^{Y_i}$, respectively. After that, pick out $\mathcal{K}_1$, and $\mathcal{K}_2$, and again permute the affine permuted image A and then bit-xor with $\mathcal{K}_1$, sequence to get A^R, where A^R, represent the red channel of a permuted image next, choose the $\mathcal{K}_2$, and $\mathcal{K}_3$ and permute the A and bit-xor with $\mathcal{K}_2$, to get A^G, where A^R, shows the permuted image green channel. Finally, get A^B, using the sequences of $\mathcal{K}_3$, and $\mathcal{K}_1$, and bit-xor with $\mathcal{K}_3$. The mathematical description of the above execution is defined as:

$$\mathcal{K}_1 = E_1^{Y_i} : \mathscr{y}^2 = x^3 + b_5x + b_6\, mod \text{ p} \tag{13}$$

$$\mathcal{K}_2 = E_2^{Y_i} : \mathscr{y}^2 = x^3 + b_7x + b_8\, mod \text{ p} \tag{14}$$

$$\mathcal{K}_3 = E_3^{Y_i} : \mathscr{y}^2 = x^3 + b_9x + b_{10}\, mod \text{ p} \tag{15}$$

where the length of each sequence is $1 \times \mathscr{mn}\ mod\ \mathscr{m}$. The pixel scrambling and diffusion of each layer of the above affine permuted image are defined in eq(15)

$$A_1^1 = A^r\,(\mathcal{K}_1, \mathcal{K}_2) \tag{16}$$

$$A^R = \mathcal{K}_1 \oplus A_1^1 \tag{17}$$

$$A_1^2 = A^g\,(\mathcal{K}_2, \mathcal{K}_3) \tag{18}$$

$$A^G = \mathcal{K}_2 \oplus A_1^2 \tag{19}$$

$$A_1^3 = A^b\,(\mathcal{K}_3, \mathcal{K}_1) \tag{20}$$

$$A^B = \mathcal{K}_3 \oplus A_1^3 \tag{21}$$

Concatenate all the above three-layer (A^R, A^G, A^B) and get the permuted image.

E. CONFUSION PHASE BASED ON AFFINE POWER AFFINE TRANSFORMATION

After that, the last four-byte $b_{13}b_{14}b_{15}b_{16}$, is utilized for the confusion phase (S-box). To construct the s-box, we use affine power affine transformation (APA) [32] using the following mathematical construction.

$$S = F_2^8 \rightarrow F_2^8 \text{ is defined by}$$

$$S = \mathcal{A} \circ \left(\text{P} \circ \mathcal{A}'\right) \tag{22}$$

Where, $\mathcal{A} = b_{13}\,(x) + b_{14}$, $\mathcal{A}' = b_{15}\,(x) + b_{16}$ are the affine surjection [33]. Where Pis still a nonlinear component, which is to be defined as:

$$P\,(x) = x^{2^n - 2}$$

For $n = 8$ the power polynomial becomes,

P (x) $=$ x^{254} is a bijective permutation using any primitive polynomial in $GF(2^8)$. Moreover, the elements $b_{13}, b_{14}, b_{15}, b_{16} \in F_2^8$, so we can construct 2^{32} new APA S-box represented by $S_{c,d}^{a,b}$, with strong algebraic properties. The proposed APA S-box with different parameters is given in Tables 1 and 2, respectively. Furthermore, we analyzed the S-box not only by the coordinate functions but also by evaluating all the security analysis by their component function and comparing it with excellent literature [17], [18], [19], [20], [21], [22], [23], [24], [25]. The comparison analysis in table 4, shows that the proposed new APA S-box has excellent algebraic properties and affine equivalent to the AES S-box [34]. Meanwhile, the only power permutation, $P\,(x) = x^{254}$, some vulnerable properties like fixed point and opposite fixed are given in Table 3, which improve by the affine parameter chosen by the proposed symmetric key extracted from the Hash of the E-ECIES. After the substitution phase, we get a cipher image. The flow chart of the proposed E-ECIES is illustrated in Figure 1.

IV. SECURITY ANALYSIS OF THE PROPOSED SYMMETRIC KEY ENCRYPTION

This section compares our proposed symmetric encryption algorithm security and performance against the findings of several experiments in [5], [13], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], and [27]. The enhanced version is subjected to several security analyses to assess the suggested work randomization and prove its resiliency against various known attacks. We take the substitution permutation network (SPN). The permutation phase is achieved by three different kinds of elliptic curves utilized for the permutation as well, as we add the nonlinear component APA S-box for the confusion phase. In the APA S-box, the encryption is evaluated by substituting uncorrelated encrypted data for plan image data. Our suggested APA S-boxes are examined using the standard S-box evaluation criteria in the results and evaluation section, which include nonlinearity score(NLS), bit independence criterion(BIC), fixed point(FP), opposite fixed point(OFP), autocorrelation(AC) maximum cycle length (MCL), linear structure(LS), linear

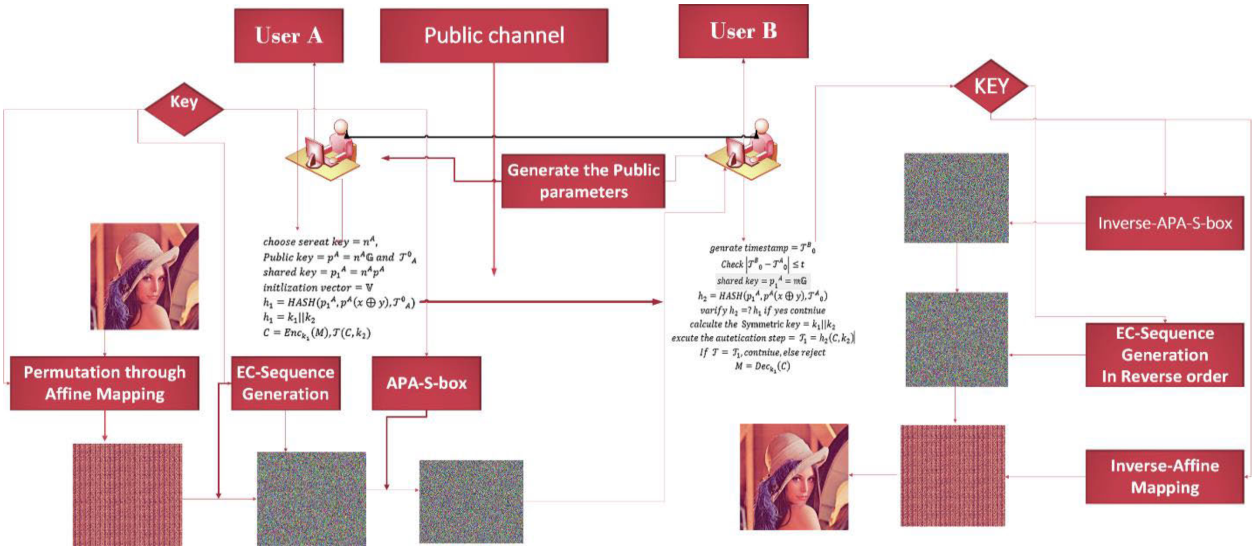

User A
Public channel
User B
Key
KEY
Generate the Public parameters
choose sereat key $= n^A$,
Public key $= p^A = n^A\mathbb{G}$ and $\mathcal{T}^0{}_A$
shared key $= p_1{}^A = n^A p^A$
initlization vector $= \mathbb{V}$
$h_1 = HASH(p_1{}^A, p^A(x \oplus y), \mathcal{T}^0{}_A)$
$h_1 = k_1 || k_2$
$C = Enc_{k_1}(M), \mathcal{T}(C, k_2)$
genrate timestamp $= \mathcal{T}^B{}_0$
Check $|\mathcal{T}^B{}_0 - \mathcal{T}^A{}_0| \leq t$
shared key $= p_1{}^A = m\mathbb{G}$
$h_2 = HASH(p_1{}^A, p^A(x \oplus y), \mathcal{T}^A{}_0)$
varify $h_2 =? h_1$ if yes contniue
calculte the Symmetric key $= k_1 || k_2$
excute the autetication step $= \mathcal{T}_1 = h_2(C, k_2)$
If $\mathcal{T} = \mathcal{T}_1$, contniue, else reject
$M = Dec_{k_1}(C)$
Permutation through Affine Mapping
EC-Sequence Generation
APA-S-box
Inverse-APA-S-box
EC-Sequence Generation In Reverse order
Inverse-Affine Mapping

FIGURE 1. Flow chart of proposed E-ECIES.

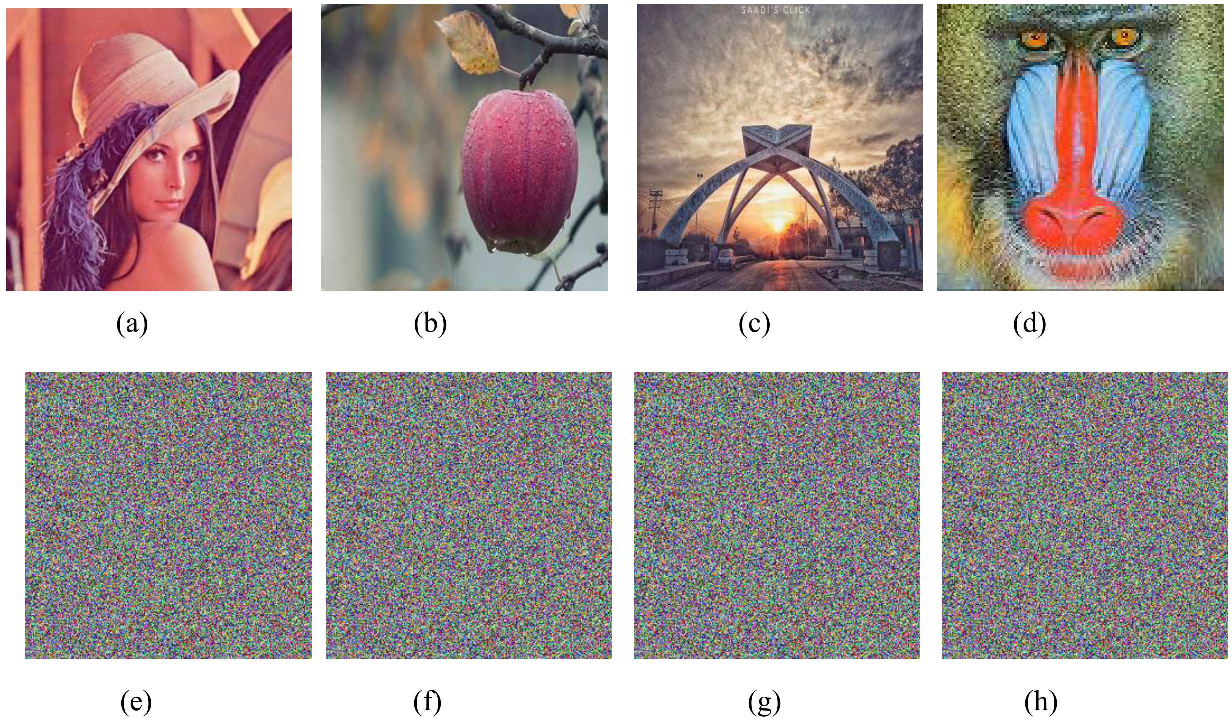


FIGURE 2. (a-d) Plain images of Lena, Apple, Babul-Quaid, Baboon (e-h) Cipher images of Lena, Apple, Apple, Babul-Quaid, Baboon.

and differential branch number(LDBN), linear approximation probability(LP), strict avalanche criterion(SAC), and differential approximation probability(DP). Moreover, in other literature [17], [18], [19], [20], [21], [22], [23], [24], [25], the S-box analysis is evaluated by their coordinate function, but the in our proposed work, we implement all the results on component functions wel; in the case of $n = 8$, we examined 2^n, Component function by their different S-box analysis. While the permutation phase evaluates the diffusion properties, including two effective tools, namely, the number of pixels change rate (NPCR) and unified average changing intensity (UACI). The portable PC with Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz is used to conduct the various evolution tests using different coloured images. Figure 2, shows the proposed symmetric encryption algorithm's plan and corresponding encrypted images.

A. NONLINEARITY SCORE

The nonlinearity score of function or S-box, $S = F_2^n \rightarrow F_2^m$ is represented by $\mathcal{NLS}(S)$ and defined by [35].

$$\mathcal{NLS}\left(S\right) = 2^{n-1} - \frac{1}{2}\left(|Walsh(u, v)|\right)$$
$$S\left(u\right) = v \quad \text{For } u \in F_2^n, v \in F_2^m \tag{23}$$

The $\mathcal{NLS}$ proposed S-box is 112, as shown in Table 4.

B. STRICT AVALANCHE CRITERIA

Webster and Tavares introduced the SAC idea. The strict avalanche criterion (SAC) is the essential component of the S-boxes. Informally, an S-box satisfies SAC if one input bit is altered. 50% of the output bits must also be changed [33]. The mathematical expression of SAC is defined in eq (24).

$$S = F_2^n \rightarrow F_2^m$$
$$S\left(x\right) + S\left(x + a\right) \text{ is balanced for all } a, wt\left(a\right) = 1. \tag{24}$$

C. BIT INDEPENDENCE CRITERION

The concept of bit-independent creation (BIC) was also developed by Webster and Tavares. For any two Boolean functions f^i, f^j, of an S-box, if the bit-xor of both functions, that is, $f^i \oplus f^j$, is highly nonlinear and satisfies the criterion of SAC. Then, when one input bit is changed, the correlation coefficient of each pair of output bits may be extremely near zero. So, by confirming that $f^i \oplus f^j(i \neq j)$ is holds, we may find out the BIC of the S-box of any two output bits that satisfy the SAC criterion [37]. Table 4, shows the performance of the new APA S-box and the comparison with excellent existing literature.

D. DIFFERENTIAL APPROXIMATION PROBABILITY

Measurement of differential uniformity is the differential approximation probability (DP) of the S-box, which is defined as

$$\mathcal{D}p^S\left(\Delta a \rightarrow \Delta b\right) = \left[\frac{\neq \{a \in x \,|\, S\left(a\right) + S(a \pm \Delta a = \Delta b)\}}{2^m}\right] \tag{25}$$

where $\Delta \boldsymbol{a}$, $\Delta \boldsymbol{b}$ is the input differential and output differential, which implies that an input differentia $\Delta \boldsymbol{a}_{\boldsymbol{i}}$ must precisely map to an output differential $\Delta \boldsymbol{b}_{\boldsymbol{i}}$ Order to guarantee a uniform chance of mapping for each i. According to the Performance indexes of the new APA, the average differential approximation probability is 0.01562. The comparisons Table 4, shows that the differential approximation probability (DP) of the new APA S-box is better than [17], [19], [20], [21], [22], and [23] and the same as with AES S-box.

E. LINEAR APPROXIMATION PROBABILITY

The linear approximation probability (LP) is the highest possible value of an event's imbalance. The mask chooses the output bits $\psi_{\boldsymbol{a}}$, have the same parity as the input bits chosen by the mask $\psi_{\boldsymbol{b}}$. The original Matsui formulation states that the linear approximation probability of a given S-box is defined as:

$$\mathcal{LP} = \max_{\psi_a \psi_b \neq 0,} \left|\frac{\neq \{a \in x \,|\, a\psi_a = s(a)\psi_b\}}{2^n} - \frac{1}{2}\right| \tag{26}$$

where x is the set of input space and 2^n, is the total number of elements in x. The input-output masks are respectively represented by $\psi_{\boldsymbol{a}}$ and $\psi_{\boldsymbol{b}}$ Them.

F. FIXED POINT

Given an S-box, $S = F_2^n \rightarrow F_2^m$, the input element $x \in F_2^n$ is said to be a fixed point (FP) if $S\left(x\right) = x$. The new APA S-box has no FP due to the affine transformation parameter chosen by the hash value of 128-bit in symmetric key encryption. In contrast, only the power permutation has 4 FP. The comparison Table 4, shows that the new-APA S-box is on top of no fixed point like the AES S-box.

G. OPPOSITE FIXED POINT

Given an S-box, $S = F_2^n \rightarrow F_2^m$, the input element $x \in F_2^n$ is said to be the opposite fixed point (OFP) if $S\left(x\right) = \bar{x}$ [6]. The new APA S-box has no OFP.

H. AUTO CORRELATION

The autocorrelation (AC) of an S-box, which is defined from, $S = F_2^n \rightarrow F_2^m$, taken concerning $o \in F_2^n$ denoted by its polarity form $\widehat{S}$, is represented by $\widehat{r_S}(o)$ and defined as:

$$\widehat{r_S}\left(o\right) = \sum_{x \in F_2^n} \left(-1\right)^{S(x)+S(x+o)}$$
$$= \sum\nolimits_{x \in F_2^n} \widehat{S}\left(x\right) + \widehat{S}(x + o) \tag{27}$$

The range of $\widehat{r_S}\left(o\right)$ is $[-2^n, 2^n]$ for all $o \in F_2^n$. For any n variable boolean function, the low value of autocorrelation is expected. The new APA S-box's auto-correlation value is 32, the same as the AES S-box.

I. DIFFERENTIAL AND LINEAR BRANCH NUMBER

Given an S-box, $S = F_2^n \rightarrow F_2^m$ The differential branch number (DBN) is represented by $\varphi_{DBN}(S)$ as defined as

$$\varphi_{DBN}\left(S\right) = min_{x,x' \in F_2^n, x \neq x'}\left(\left\{wt\left(x \oplus x'\right) + wt\left(S\left(x\right) \oplus S(x')\right)\right\}\right) \tag{28}$$

The linear branch number of the S-box is denoted by $\varphi_{LBN}\left(S\right)$, and defined as:

$$\varphi_{LBN}\left(S\right) = min_{o, \mathcal{B} \in F_2^n, \widehat{r_S}(o, \mathcal{B}) \neq 0}\left(\{wt\left(o\right) + wt(\mathcal{B})\}\right) \tag{29}$$

where $\widehat{r_S}\left(o, \mathcal{B}\right)$ shows the coefficient of autocorrelation. The suggested APA S-box the $\varphi_{DBN}\left(S\right)$ and $\varphi_{LBN}\left(S\right)$, is 2, as shown in Table 4.

TABLE 1. Proposed APA S-box $S^{3,57}_{233,154}$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	139	193	16	157	237	44	218	164	153	133	112	247	27	186	141	86
2	34	151	12	145	222	221	42	61	55	89	126	229	161	143	115	179
3	166	246	29	48	134	167	10	5	163	45	3	119	38	6	99	14
4	172	192	243	108	132	136	124	67	207	140	200	100	84	146	152	189
5	30	52	235	174	116	184	131	156	95	68	220	122	203	194	96	175
6	204	57	255	76	93	137	56	11	78	228	92	97	191	213	169	91
7	190	46	138	182	98	142	87	63	197	80	252	13	0	79	28	231
8	183	154	60	244	129	1	202	82	225	173	83	73	35	201	248	121
9	144	9	114	206	230	148	25	64	69	88	49	127	113	210	181	36
10	104	59	165	118	150	242	240	65	74	195	106	40	162	226	249	232
11	77	72	158	62	53	50	253	75	188	199	4	102	160	211	155	171
12	58	205	94	19	31	216	159	250	20	128	176	7	223	47	238	214
13	90	147	2	187	26	149	180	85	254	123	110	170	178	233	43	21
14	103	251	245	24	168	120	117	22	130	101	234	33	224	66	185	239
15	51	109	212	125	135	81	196	215	15	54	208	41	23	111	107	217
16	17	70	71	39	198	177	227	105	18	241	236	219	209	37	8	32

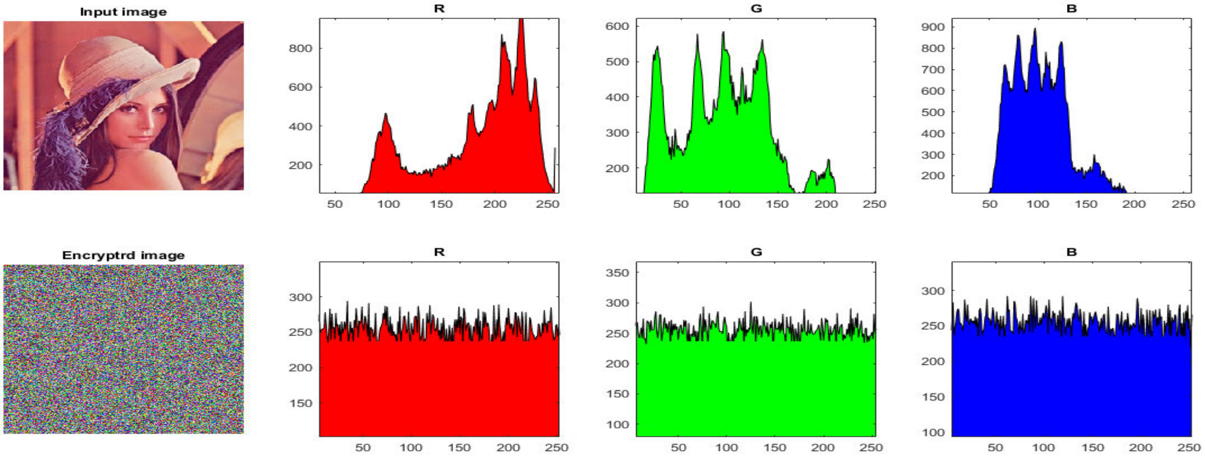


FIGURE 3. Histogram of plain image "Lena" and corresponding cipher image histogram.

J. LINEAR STRUCTURE

The linear structure of the S-box is examined for its cryptography importance. It has been noted that attacks that could be carried out far more quickly than a thorough key search can break block ciphers with linear designs [47]. Therefore, in the block cipher, the confusion phase must avoid the linear structure. The mathematical expression of the linear structure of an S-box is defined as:

$$f(x) + f(x + a) = C$$

where $f(x) \in F_2^n$ $\forall x \in F_2^n$ and for some $a \in F_2^n$ and $C \in F_2$. Then C is called the linear structure of the S-box. There are two types of linear structure invariant linear structure if $C = 0$ and the other one is a complementary linear structure if $= 1$. Table 4, shows that the proposed APA S-box has no linear structure and is suitable for cryptographic primitive.

V. SIMULATION RESULTS OF ENCRYPTION

In this section, we evaluated the simulation results of the symmetric key encryption of different standard images of Lena, Apple, Babul-Quaid, and Baboon, to examine the strength of E-ECIES. The figure 2, shows the plan images listed and corresponding to their encrypted images; from figure 2, shows that the randomization of the encryption scheme is achieved. The image obtained after the encryption process reveals its unpredictability, and it is impossible to decipher the plan image without the decryption key. As a result, from

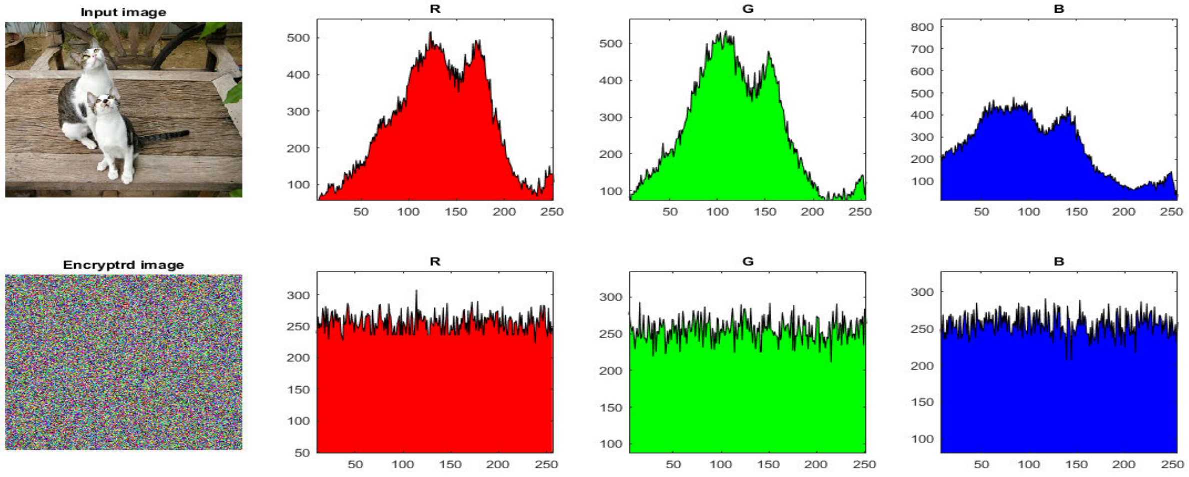


FIGURE 4. Histogram of plain image "Cat" and corresponding their Cipher image histogram.

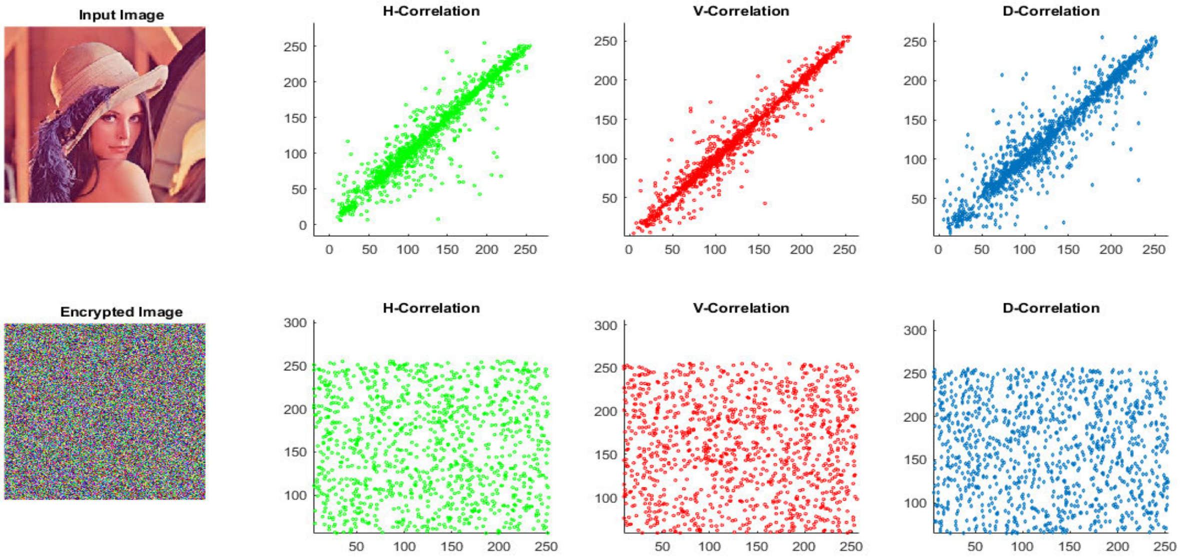


FIGURE 5. Correlation analysis multidirectional (horizontal, vertical, and diagonal) of plain image Lena and corresponding their cipher image.

the simulation analysis, we identified that the original secret information could be accurately recovered without any difference or loss, proving the usefulness and validity of the entire encryption scheme.

VI. STATISTICAL ANALYSIS

A. HISTOGRAM ANALYSIS

An image's histogram can effectively and graphically depict a digital image's distribution of grey values. When the distribution of the grey value is more even, it will be more difficult for the eavesdropper to extract information from the encrypted image through statistical attacks [6]. As such, the histogram of the encrypted image should almost be uniform while differentiating itself from the one derived from the plaintext image. Moreover, the histogram's distribution was figured out from the cipher image and is relatively uniform, reducing the association between neighbouring pixels and preventing the attackers from learning anything. Figure 3 and Figure 4, illustrate the histogram analysis of the plan images of Lena and Cat and their encrypted versions of Lena and Cat, respectively.

B. CHAI SQUARE TEST

The Chi-square test measures the amount of variation between the original sample data and the theoretical inference value of the statistical samples. Sometimes the visual representation of the histogram is not sufficient to measure the pixels of the encrypted image. So the quantitative measure of

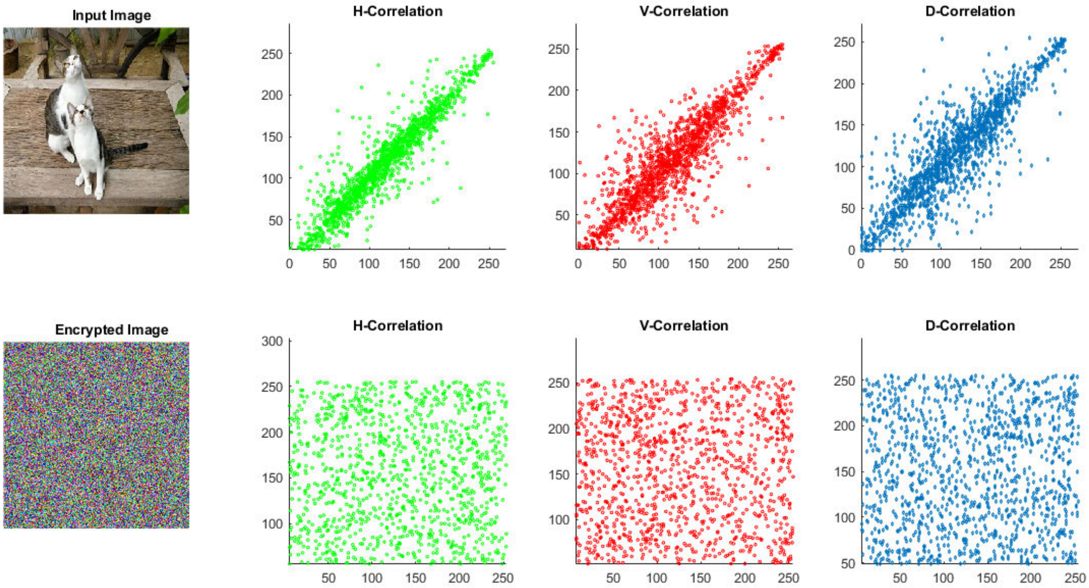


FIGURE 6. Correlation analysis multidirectional (horizontal, vertical, and diagonal) of plain image "Cat" and corresponding their cipher image.

TABLE 2. Proposed APA S-box $S_{1,54}^{2,23}$.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	24	59	252	66	99	117	237	178	198	110	36	120	206	191	6	13
2	94	71	100	195	161	115	182	61	215	223	251	97	239	159	230	3
3	18	86	185	155	85	232	108	104	248	133	218	216	174	113	227	28
4	192	43	14	214	69	210	38	116	75	184	246	145	151	47	52	154
5	211	19	42	139	173	50	70	22	186	39	77	7	129	164	181	149
6	46	250	254	225	166	234	244	5	74	224	219	125	255	127	212	188
7	170	64	222	37	180	65	143	202	54	81	21	41	136	226	10	197
8	84	107	87	118	60	167	162	190	177	29	126	240	76	91	88	153
9	137	175	83	56	49	4	12	229	228	102	33	201	247	233	189	169
10	55	1	109	217	96	236	140	15	235	11	121	157	183	141	146	45
11	205	221	106	156	158	144	220	238	8	203	16	213	93	207	148	165
12	53	67	231	27	79	90	72	25	241	98	119	138	168	101	128	89
13	150	147	31	82	204	111	193	208	187	200	2	58	160	57	131	80
14	209	40	103	132	35	194	242	34	122	105	142	249	152	92	199	32
15	134	63	44	176	163	17	48	196	112	78	253	95	179	26	73	30
16	20	9	124	62	171	172	114	23	245	135	51	130	123	0	243	68

histogram monotony, we employ the chi-square test analysis. The mathematical description of the chi-square test is as follows:

$$\mathcal{X}^2 = \sum_{i=0}^{255} \frac{(ob\,(f_i) - ex(f_0))}{ex(f_0)} \tag{30}$$

$$ex\,(f_0) = \frac{(M \times N)}{\mathcal{Q}} \tag{31}$$

where $ob\,(f_i)$ is the observed frequency, $i\,(i = o\ to\ 255)$, while $ex\,(f_0)$ is the expected frequency. The value of $\mathcal{Q}$, in our case, is 256. According to the chi-square distribution, the numerical value of the chi-square test, at the significance level of 5%, is 293.2478. The test values of the chi-square analysis of the proposed scheme is shown in Table 5, which ensures that the value of the suggested encryption scheme is not greater than 293.2478. Hence, the proposed method is to resist Statistical attacks.

C. CORRELATION ANALYSIS

In plaintext images, the coefficient correlation between two contiguous distinct pixels is typically significant, so a secure

TABLE 3. S-box-based on only power permutation p (x) = x^{254}.

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	203	212	40	232	176	252	39	106	138	76	237	20	220	81	24
2	1	82	218	11	79	225	27	169	222	216	36	92	42	249	236	62
3	125	65	25	111	56	3	66	108	223	59	210	18	211	67	101	46
4	160	28	89	32	52	140	102	146	145	33	98	74	175	54	72	195
5	141	123	15	163	41	229	230	4	109	114	135	5	136	154	97	34
6	246	209	228	47	192	199	172	83	50	132	191	202	159	137	23	240
7	221	205	187	53	91	104	57	69	71	147	206	38	94	166	143	251
8	156	26	119	242	35	70	243	44	244	51	231	200	22	73	184	124
9	179	227	152	162	173	235	90	168	129	208	61	87	186	151	239	113
10	30	215	21	194	207	214	241	201	130	6	118	134	60	133	31	120
11	43	180	122	197	64	63	148	157	150	131	254	49	247	155	100	37
12	153	116	7	219	255	88	139	248	115	126	29	45	2	158	167	84
13	80	78	193	48	14	13	58	85	161	182	142	188	16	121	224	117
14	93	8	10	68	198	177	110	77	250	112	165	189	181	183	12	17
15	95	75	174	226	178	204	196	144	190	127	103	105	185	149	19	9
16	96	170	99	234	238	253	213	107	86	128	55	245	164	217	171	233

TABLE 4. Comparison of the nonlinear component with the existing algorithm.

Algorithm	$\mathcal{NLS}$	AC	DP	LP	SAC	BIC	FP	OFP	LBN	DBN	LS
$\boldsymbol{p = x^{127}}$	112	32	0.0156	0.0625	0.4375	0.1285	4	1	2	2	0
$\boldsymbol{S^{2,23}{}_{1,54}}$	112	32	0.0156	0.0625	0.4375	0.1349	0	0	2	2	0
$\boldsymbol{S^{3,57}{}_{233,154}}$	112	32	0.0156	0.0625	0.4375	0.1285	0	0	2	2	0
Ref.[17]	86	120	0.2109	0.1640	0.2656	0.2887	2	3	2	2	0
Ref.[18]	112	32	0.0156	0.0625	0.4375	0.1299	1	0	2	2	0
Ref.[19]	94	96	0.0468	0.1328	0.3437	0.2799	1	1	2	2	0
Ref.[20]	94	88	0.0781	0.1484	0.3750	0.2863	1	0	2	2	0
Ref.[21]	94	88	0.0468	0.1328	0.3437	0.3069	1	1	2	2	0
Ref.[22]	94	88	0.0390	0.1328	0.3750	0.2511	2	1	2	2	0
Ref.[23]	94	88	0.0390	0.1328	0.3750	0.3138	1	0	2	2	0
Ref.[24]	94	96	0.0390	0.1328	0.3437	0.3282	2	1	2	2	0
Ref.[25]	94	104	0.0390	0.1328	0.3437	0.2204	0	1	2	2	0

TABLE 5. Results of chi square test.

Test Images	Test Values	Result
Lena	234.753	Success
CAT	244.543	Success
Baboon	239.741	Success
Babul-Quaid	241.459	Success
Apple	234.875	Success

and efficient encryption procedure is needed to minimize this correlation. After the encryption procedure for the plaintext image, the goal of a low coefficient correlation among the adjacent pixels should be conducted in the cipher image. The mathematical formula for the correlation analysis between two adjacent pixels is defined as [42]:

$$\mathcal{R}\left(x', y\right) = \frac{e(x' - e(x')(y - e(y))}{\sqrt{\mathcal{D}(x')\mathcal{D}(y)}} \tag{32}$$

$$e\left(x'\right) = \frac{1}{N}\sum\nolimits_{i=1:n} x'_i \tag{33}$$

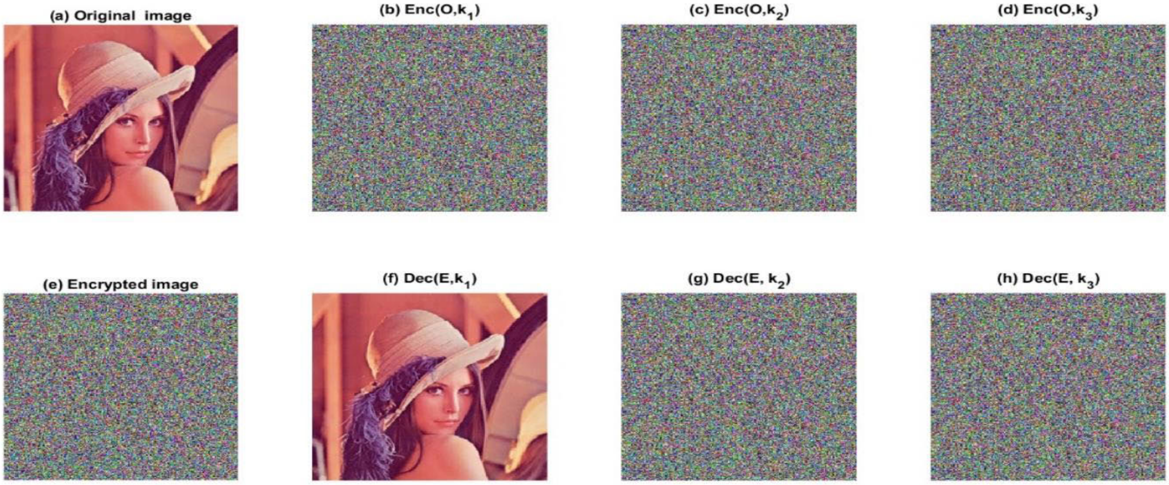


FIGURE 7. Key Sensitivity Analysis: 1st row (a) Original image (b)Encrypt with K_1 (c) Encrypt with K_2 (d) Encrypt with K_3, 2nd row (e) Encrypted image (f) decrypt with K_1 (g) decrypt with K_2 (h) decrypt with K_3.

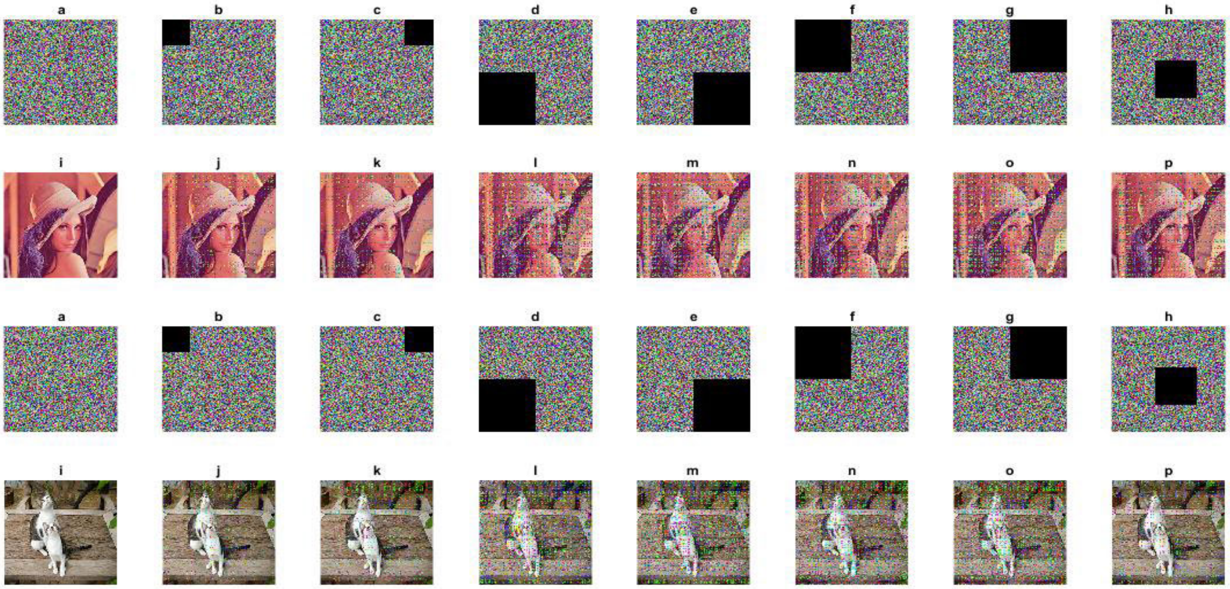


FIGURE 8. Occlusion Analysis 1st row from (a-h) "LENA" encrypted image with different rate of lose the data, 2nd row from (i-p) Cros- ponding Decrypted image of "LENA", 3rd row from(a-h) "CAT" encrypted image with different rate of lose the data 4th row from (i-p) Corresponding Decrypted image of "CAT".

$$\mathcal{D}\left(x'\right)=\frac{1}{N}\sum\nolimits_{i=1:n}(x_i-e(x_i'))^2 \tag{34}$$

where, $x'y$ are the pixels of the plan and cipher image, respectively. We choose the pixel pairings in the encrypted and plaintext image in the multidirectional: Horizontal, vertical, and diagonal directions. The above eq (32-34) mathematical formulas was used to get the coefficient correlation between the cipher image and the associated plaintext image in three directions. Table 6, displays the test results for the correlation in three directions between plaintext images and images after the encryption process. Table 6, shows that the correlation of cipher image in multidirectional is nearly close to zero, which ensures that correlation is significantly reduced. Hence, the proposed E-ECIES scheme is not vulnerable to correlation analysis.

D. GLOBAL INFORMATION ENTROPY

The global information entropy(GIE), which shows the degree of confusion in the image, is one of the key characteristics of showing the randomness of the image and evaluating the encryption method. The following equation was used to find the information entropy [27].

$$\mathbb{H}\left(m\right)=-\sum\nolimits_{i=1}^{j}\mathcal{P}(m_i)\log_2\mathcal{P}(m_i) \tag{35}$$

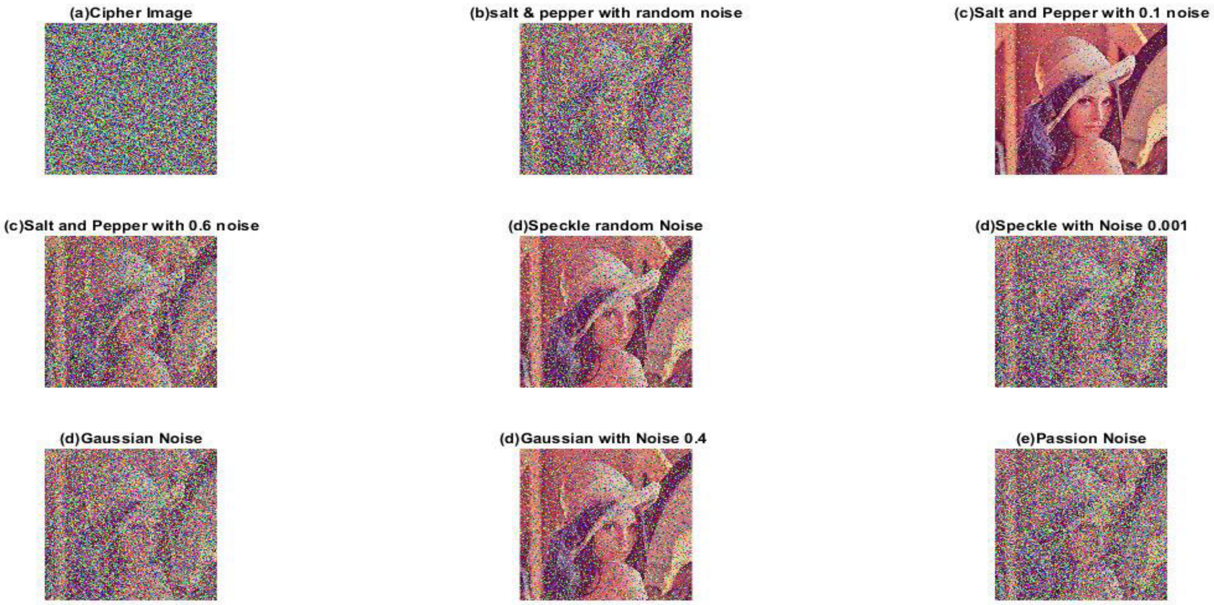

(a)Cipher Image
(b)salt & pepper with random noise
(c)Salt and Pepper with 0.1 noise
(c)Salt and Pepper with 0.6 noise
(d)Speckle random Noise
(d)Speckle with Noise 0.001
(d)Gaussian Noise
(d)Gaussian with Noise 0.4
(e)Passion Noise

FIGURE 9. Noise attacks: 1st row shows, (a) the encrypted image of "LENA" (b) salt & pepper with random noise, (c) salt & pepper with (0.1) noise. 2nd row shows, (c) salt & pepper with (0.6) noise (d) speckle with random noise (d) speckle with noise (0.001). 3rd- row shows (d) Gaussian noise (d) Gaussian with 0.4 noise, and (e) Passion noise.

TABLE 6. Correlation analysis of proposed E-ECIES.

Correlation Coefficients							
		Plan-Image			Cipher-Image		
Test-Images		H	V	D	H	V	D
Lena	R	0.9172	0.9504	0.9872	0.0009	0.0007	0.0007
	G	0.9772	0.9618	0.9682	−0.009	−0.0009	−0.0007
	B	0.9772	0.9801	0.9792	0.0017	0.0009	0.0009
CAT	R	0.9801	0.9713	0.9582	−0.0219	−0.00229	−0.0229
	G	0.8713	0.8456	0.9772	−0.00055	−0.0095	−0.0009
	B	0.9012	0.9651	0.9372	−0.0046	−0.0046	−0.0073
Baboon	R	0.9872	0.9872	0.9772	0.00021	0.0029	0.0019
	G	0.9834	0.9834	0.9802	−0.0139	−0.00169	−0.0013
	B	0.9751	0.9008	0.9917	0.0044	0.00049	0.0091
Babul-Quaid	R	0.9026	0.9326	0.9912	−0.00319	−0.00329	−0.0075
	G	0.9761	0.9861	0.9882	−0.0045	−0.0065	−0.0009
	B	0.8462	0.9562	0.9698	−0.0006	−0.0026	−0.00016
Apple	R	0.9636	0.9546	0.9792	−0.0009	−0.0129	−0.0079
	G	0.9821	0.9701	0.9887	−0.0009	−0.0085	−0.0084
	B	0.9625	0.9715	0.9917	−0.0017	−0.0016	−0.0059

where $\mathbb{H}\,(m)$, represent the value of entropy and $\mathcal{P}(m_i)$ show the probability of m_i. The theoretical result of the information entropy is 8. Much more uncertainty is visible, along with the image's increasing entropy. The more challenging it is for the attackers to extract information from the image, the closer it gets to the optimal value of 8. The entropy values of the Lena, Baboon, Babul-Quaid, Cat and Apple images and their corresponding encrypted images are shown in Table 7. Concluding from the values in the table, following encryption, the entropy for each of the above images is close to the ideal theoretical value and utterly different from the values in the corresponding plaintext image. Considering the entropy values, we conclude that the algorithm proposed here performs effectively against the statistical attacks.

E. LOCAL SHANON ENTROPY INFORMATION

Local Shannon entropy calculates the sample mean of global information entropy (GIE) over several non-overlapping and randomly selected image blocks. It overcomes some weaknesses of (GIE) because sometimes, GIE fails to find the true randomness of the image. We can define the local Shanon entropy information by the following mathematical equation:

$$\overline{\mathbb{H}_{\mathcal{k},t_{\mathcal{b}}}}(S) = \sum\nolimits_{i=1}^{\mathcal{k}} \frac{\mathbb{H}(S_i)}{\mathcal{k}} \tag{36}$$

where $S_i(i = 1 \ldots\ldots, \mathcal{k})$, are non-overlapping blocks with randomly chosen pixels $t_{\mathcal{b}}$, of the cipher image. $\mathbb{H}(S_i)$, represent the global information entropy of $S_1, S_2, S_3, \ldots\ldots\ldots, S_{\mathcal{k}}$. For the test, we select $\mathcal{k}$ images and $t_{\mathcal{b}}$ pixels and $\mathcal{k} = 64, t_{\mathcal{b}} = 1024$. The range of $\mathcal{k} = 64, t_{\mathcal{b}} = 1024$, should be from $[7.901901305 - 7.903037329]$, with a significance level of 0.05 [50]. Table 8, represents the information on local Shannon entropy, showing that the cipher images' results possess true randomness.

F. SENSITIVITY ANALYSIS

1) DIFFERENTIAL ATTACKS

The differential attack evaluates an image encryption algorithm's plaintext sensitivity [24]. Therefore, the encryption algorithm can extend this influence over the entire encryption process if we slightly alter the plain image, a desirable image. The Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are measures of the ability to withstand the differential attack and are defined as follows:

$$\mathcal{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} \mathcal{F}(i,j)}{\mathcal{M}\times\mathcal{N}} \times 100\% \tag{37}$$

$$\mathcal{UACI} = \frac{\sum_{i=1}^{m}\sum_{i=1}^{n} \left|E'(i,j) - E''(i,j)\right|}{255\times\mathcal{M}\times\mathcal{N}} \times 100\% \tag{38}$$

where $E'(i,j)$ is cipher image of the original image after the entire encryption process $E''(i,j)$ anther encrypted image after a one-bit change in plan-image, both the encrypted image put into the above two formulas to get the experimental analysis of $\mathcal{NPCR}$ and $\mathcal{UACI}$. Where, $\mathcal{F}(i,j)$ is defined as [11], [42], [27].

$$\mathcal{F}(i,j) = \begin{cases} 1, & E'(i,j) \neq E''(i,j) \\ 0, & E'(i,j) = E''(i,j) \end{cases} \tag{39}$$

Consequently, the proposed E-ECIES offers excellent resistance to the differential attack. The results $\mathcal{NPCR}$ and $\mathcal{UACI}$ measurements in this manuscript and other references are also shown in Table 9. However, the value in our algorithm for the $\mathcal{UACI}$ results is closer to the theoretical value than for any other encryption scheme. As a result, the suggested encryption method is useful and efficient for encrypting multimedia data. Moreover, we also calculated the critical value of $\mathcal{NPCR}$ and $\mathcal{UACI}$ using the following mathematical equations:

$$\begin{aligned} \mathcal{NPCR}_{a} &= \mu_{\mathcal{NPCR}} - \varphi^{-1}(a)\sigma_{\mathcal{NPCR}} \\ &= \left(F - \varphi^{-1}(a)\sqrt{\frac{F}{\mathcal{M}\times\mathcal{N}}}\Big/ F+1\right) \end{aligned} \tag{40}$$

$$\mathcal{UACI}_{a}^{+} = \mu_{\mathcal{UACI}} - \varphi^{-1}\left({}^{a}\!/_{2}\right)\sigma_{\mathcal{UACI}} \tag{41}$$

$$\mathcal{UACI}_{a}^{-} = \mu_{\mathcal{UACI}} + \varphi^{-1}\left({}^{a}\!/_{2}\right)\sigma_{\mathcal{UACI}} \tag{42}$$

where, φ^{-1} is the inverse of the cumulative distributive function(CDF) of the normal standard distribution N(0, 1), μ and σ, represent the expectation and variance of $\mathcal{NPCR}$ and $\mathcal{UACI}$ and a is the significance value of the two encrypted images E', E'', respectively. Table 10, shows the critical values of $\mathcal{NPCR}$ and $\mathcal{UACI}$ with different significance levels.

2) PSNR, NC AND SSIM

Three important sensitive analyses, Peak Signal-to-Noise Ratio (PSNR), Normalized Correlation ($\mathcal{NC}$), and Structural Similarity (SSIM), are used to measure the quality and change the values of pixels in images after decryption [43]. The following formula is used to calculate the value of PSNR

$$PSNR = 10 \times \log_{10}\frac{2^{16}-1}{\mathcal{MSE}} \tag{43}$$

where $\mathcal{MSE}$ is defined by the following equation

$$\mathcal{MSE} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(P(i,j) - E'(i,j)\right)^2}{\mathcal{M}\times\mathcal{N}} \tag{44}$$

where $P(i,j)$, $E'(i,j)$ represent the plan and encrypted receptively of dimension $\mathcal{M} \times \mathcal{N}$. The similarity degree is evaluated by the normalization correlation $\mathcal{NC}$ metric.

In addition, this result could be considered a reliable indicator of the encryption algorithms' effectiveness because two entirely unrelated images have a correlation coefficient that is almost zero. The equation is shown below the computed NC value.

$$\mathcal{NC} = \sum\nolimits_{i=1}^{m}\sum\nolimits_{j=1}^{n}\frac{\left(P(i,j) - E'(i,j)\right)}{\sum_{i=1}^{m}\sum_{j=1}^{n} P(i,j)^2} \tag{45}$$

The structural similarity between two images is evaluated using the SSIM index. This metric improves on methods like mean squared error (MSE) and conventional PSNR. On several windows of a given image, the SSIM index is calculated. As a result, the following mathematical expression provides the $SSIM$ between two windows, X and Y, of standard size $\mathcal{N}\times\mathcal{N}$.

$$SSIM\,(X,Y) = \frac{(2\mu_{x'}\mu_{y'} + \mathcal{b}_1)(2\sigma_{x'y'} + \mathcal{b}_2)}{(\mu_{x'}^2 + \mu_{y'}^2 + \mathcal{b}_1)(\sigma_{x'}^2 + \sigma_{y'}^2 + \mathcal{b}_2)} \tag{46}$$

where $\mu_{x'}$ and $\mu_{y'}$ shows the mean values of X and Y, respectively. $\sigma_{x'}$ and $\sigma_{y'}$ used for standard deviations of X and Y, respectively. The covariance of X and Y is represented by $\sigma_{x'y'}$, and to avoid the value of zero in dominators, the coefficients $\mathcal{b}_1$ and $\mathcal{b}_2$ are used in eq-(46). The comparison of the plan image with the encrypted image should have

TABLE 7. Global entropy information of proposed E-ECIES.

Coefficient of Global Entropy Information							
Test-Images	Plan-Image			Cipher-Image			
	R	G	B	R	G	B	Entropy
Lena	7.2763	7.5834	7.0160	7.9972	7.9974	7.9975	7.9991
CAT	7.7450	7.7671	7.7671	7.9972	7.9972	7.9975	7.9992
Baboon	7.6094	7.3876	7.6885	7.9972	7.9974	7.9975	7.9991
Babul-Quaid	7.7600	7.6617	7.2264	7.9973	7.9973	7.9971	7.9990
Apple	7.4513	7.4170	7.2021	7.9973	7.9973	7.9971	7.9990

TABLE 8. Local Shanon entropy information.

Test Images	$(\mathscr{k}, t_{\mathscr{b}})$	Test Values	Result
Lena	(64,1024)	7.9012	Success
CAT	(64,1024)	7.8992	Success
Baboon	(64,1024)	7.9001	Success
Babul-Quaid	(64,1024)	7.9028	Success
Apple	(64,1024)	7.8901	Success

TABLE 9. Differential analysis.

Differential Attacks								
	NPCR			UACI			Average	
	R	G	B	R	G	B	Avg NPCR	Avg UACI
Lena	99.6753	99.7531	99.6521	33.3342	33.4672	33.4192	99.6935	33.4069
CAT	99.4753	99.6521	99.6421	33.3352	33.4672	33.4192	99.5898	33.4072
Baboon	99.6753	99.6231	99.6221	33.3322	33.4442	33.4192	99.6402	33.3985
Babul-Quaid	99.6554	99.6541	99.5551	33.3352	33.4762	33.4192	99.6215	33.4102
Apple	99.6743	99.6531	99.5521	33.3372	33.4812	33.4192	99.6265	33.4125

TABLE 10. Critical values of NPCR and UACI.

Critical values of Differential Attacks							
	$\mathcal{NPCR}_{0.05} = 99.5693$, $\mathcal{NPCR}_{0.01} = 99.5527$, $\mathcal{NPCR}_{0.001} = 99.5341$			$\mathcal{UACI^{+}}_{0.05} = 33.6447$. $\mathcal{UACI^{+}}_{0.01} = 33.7016$. $\mathcal{UACI^{+}}_{0.001} = 33.7677$.			Result
	5%	1%	0.1%	5%	1%	0.1%	Success
Lena	99.6753	99.7531	99.6521	33.3342	33.4672	33.4192	Success
CAT	99.4753	99.6521	99.6421	33.3352	33.4672	33.4192	Success
Baboon	99.6753	99.6231	99.6221	33.3322	33.4442	33.4192	Success
Apple	99.6743	99.6531	99.5521	33.3372	33.4812	33.4192	Success

low *PSNR*, *NC* and *SSIM* values. Otherwise, the plan and encrypted image show the value of *SSIM* and *NC* is 1 and a high *PSNR* value. Additionally, it's important to note that the image after decryption is the same as the plan image. Table 11, shows the value of *PSNR*, *NC* and *SSIM* of the plan-images cross-ponding their encrypted images. The results in Table 11, ensure that our enhanced scheme performs well in terms of low *PSNR*, *NC* and *SSIM*. Finally, it can be concluded that the E-ECIES is secure against sensitive analysis attacks based on the *PSNR*, *NC* and *SSIM*.

3) KEY SENSITIVITY

The secret key must be highly sensitive to an encryption technique for the actual key space to match the theoretical one.

TABLE 11. PSNR, NC and SSIM values between plain and encrypted images.

Security Parameters	*PSNR Values*		*SSIM*	*NC*
	P vs E	P vs D	P vs E	P vs E
Lena	7.8298	∞	0.0021	0.6185
Baboon	7.9832	∞	0.0131	0.7135
Cat	8.8945	∞	0.0101	0.6374
Babul-Quaid	8.5095	∞	0.0041	0.6245
Apple	9.4847	∞	0.0100	0.6588

A high key sensitivity means two entirely different encrypted and decrypted outputs will arise from slightly modifying the secret key throughout the encryption and decryption procedures. We generate an original secret key K_1 utilizing the E-ECIES at random and then creating two other secret keys, $\mathcal{K}_2$ and $\mathcal{K}_3$ By modifying one bit in K_1. This process is done to determine the sensitivity of the secret keys. The original secret key K_1 and the modifying keys $\mathcal{K}_2$, $\mathcal{K}_3$ by the following expression.

$$K_1 = b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}b_{13}b_{14}b_{15}b_{16}$$
$$\mathcal{K}_2 = b_1b_2b_3b_4b_5b_6b_7\boldsymbol{b_8}b_9b_{10}b_{11}b_{12}b_{13}b_{14}b_{15}b_{16}$$
$$\mathcal{K}_3 = b_1b_2b_3b_4b_5b_6b_7b_8b_9b_{10}\boldsymbol{b_{11}}b_{12}b_{13}b_{14}b_{15}b_{16}$$

Figure 7, shows the key sensitivity analysis results attained throughout the encryption process of the E-ECIES. The 1st row of figure 7 shows the original image of Lena and three encrypted images encrypted using K_1, $\mathcal{K}_2$ and $\mathcal{K}_3$.

In the 2nd row of figure 7, only the original secret key K_1 can exactly retrieve the original image. Figure 7, illustrates how the decrypted results with just a single bit of difference between $\mathcal{K}_2$ and $\mathcal{K}_3$ they yield entirely indistinguishable results.

4) KEY SPACE ANALYSIS

The key space shall be sufficiently large to withstand a brute force attack. The number of keys employed in the permutation, diffusion and confusion processes is used to compute the key space. The proposed E-ECIES initially utilized $b_1b_2b_3b_4$ for diffusion process, after that $b_5b_6b_7b_8b_9b_{10}b_{11}b_{12}$ used for the permutation process and again utilized for diffusion, and the last four bytes $b_{13}b_{14}b_{15}b_{16}$ is for the confusing process. The total number of key spaces is 2^{128} which is larger than 2^{80} and enough for brute force attacks. Moreover, the security of E-ECIES is based on the discreet logarithm problem at the initial stage of key sharing. Hence, the proposed work has a comparatively large key space.

G. ROBUSTNESS ANALYSIS

1) OCCLUSION ANALYSIS

Decryption operations for encrypted images delivered across communication channels may be ineffective due to data loss [43]. In this case, the ciphered images are subjected to a loss operation known as an occlusion attack to examine the enhanced encryption scheme noise tolerance. Figure 8 shows the encrypted colour image with data loss rates of 50% from the right and left from the top and below. Similarly, 25% were left and right and from top to bottom. As shown in figure 8, after the decryption, the loss rate of 50% and 25% in an encrypted image, the corresponding decrypted image keeps most of the visual data from the original image. Consequently, it ensures that the E-ECIES is effective and resists occlusion attacks.

2) NOISE ATTACKS

This section examines how a cryptosystem responds to noise during encryption and decryption. Some noise is always present when digital images are broadcast across communication channels. Most of the encrypted digital images are affected by different noises, and therefore, to investigate the proposed E-ECIECS, we must check the noise analysis of the proposed encryption scheme and ensure that the suggested work is noise resistant in such a manner that the digital image after decryption algorithm must be understandable for the receiver sides. So, to evaluate the E-ECIECS, the encrypted image is anticipated by different kinds of noise with different densities, namely: Gaussian, Salt, speckle, Poisson, and Pepper Noise. Major sources of Gaussian, Salt and Pepper, and other noise appear in remote sensing images during acquisition, including Poor illumination, high temperatures, inadequate transmission, and other factors that can all lead to sensor noise, such as electronic circuit noise [43].

3) GAUSSIAN NOISE

The normal distribution, which is also referred to as the Gaussian distribution, has a probability distribution function (PDF) equal to that of Gaussian noise. Additive white Gaussian noise(AWGN) is the most popular name for this type of noise [43]. The proper definition of Gaussian noise is noise with a Gaussian amplitude distribution. The following mathematical expression describes the Gaussian distribution of this kind of noise

$$\mathcal{F}(g) = \frac{1}{\sqrt{2\pi\sigma^2}} - e^{(g-m)^2/2\sigma^2} \tag{47}$$

where in eq-(47), σ represents the standard deviation, g, m shows the average and gray level of the function. For a random variable $\mathcal{S}$ of the gaussian, the PDF is expressed by the following equation.

$$\mathcal{PG}(\mathcal{S}) = \frac{1}{\sqrt{2\pi\sigma}} - e^{(\mathcal{S}-u)^2 / 2\sigma^2} \tag{48}$$

where u and σ represent the mean and standard deviation. The simulation results of the Lena encrypted image with the addition of gaussian noise to the decrypted image of Lena in figure 9 are still readable for the receiver side.

4) SALT AND PEPPER

Intensity spikes, often known as salt and pepper noise, are an impulsive form of noise. Generally, data transmission failures are what cause this. Each usually has a chance of less than 0.1. The image has a "salt and pepper" appearance because the contaminated pixels are alternately assigned to the minimum or maximum value. The impairment of pixel elements in-camera sensors is the primary cause of the salt and pepper noise [43]. The encryption image of the suggested technique, Lena, with the addition of Salt and Pepper noise, is shown in figure 9, along with the matching decrypted images that remain readable after the decryption procedure. By The following expression, compute the *PDF* for the bipolar impulse noise model

$$\mathcal{PI}\,(\mathcal{S}) = \begin{cases} \mathcal{P}_{a} & for\ \mathcal{S} = a \\ \mathcal{P}_{b} & for\ \mathcal{S} \neq a \\ 0 & otherwise \end{cases} \tag{49}$$

5) SPECKLE NOISE

A grayscale image's pixels can be affected by speckle noise, a multiplicative noise. It mainly appears in images with low brightness levels, such as MRI and Synthetic Aperture Radar (SAR) images. Before further image processing, such as object detection, picture segmentation, edge detection, etc., image enhancement is essential to reduce speckle noise [45]. Figure 9, shows the encrypted images, Lena of the proposed algorithm, with the addition of Poisson noise and corresponding decrypted images, which are still understandable after the decryption algorithm

6) POISSON NOISE

A random temporal distribution may be used to treat individual photon detections as separate, discrete occurrences. Thus, photon counting is a standard Poisson process. The discrete probability distribution describes the number of photons recorded by a specific sensor element across time intervals using the following mathematical formula.

$$\mathcal{P}ro\,(\mathcal{N} = \mathcal{K}) = \frac{e^{-\gamma\tau}(\gamma\tau)^{\mathcal{K}}}{\mathcal{K}!} \tag{50}$$

This is a standard Poisson distribution with a rate parameter $\gamma\tau$ that equates to the anticipated incidence photon count, where γ, the expected number of photons per unit of time, is proportional to the incident scene irradiance [46]. Photon noise is the term for the uncertainty that this distribution encapsulates. Photon noise offers a lower bound on the measurement error of light since it derives from the nature of the signal itself. Any measurement would be prone to photon noise even under perfect imaging circumstances, devoid of any additional sensor-based noise sources of noise (such as read noise). Figure 9, shows the encrypted images, Lena of the proposed algorithm, with the addition of Poisson noise and corresponding decrypted images, which are still understandable after the decryption algorithm. As a result, the proposed E-ECIES are secure against poison noise.

H. COMPUTATIONAL COMPLEXITY AND RUNNING TIME

The asymptotic complexity theoretically approximates the execution time of an algorithm. In general, the asymptotic complexity is denoted by big oh O. This subsection presented the proposed algorithm's asymptotic complexity and running encryption time. We have theoretically analyzed the proposed scheme's encryption and decryption procedure and skipped the preprocessing for secret key exchange. Since the proposed scheme is a substitution permutation network, in the substitution module, each byte is substituted in constant time $O(1)$. So, the complexity of the overall substitution module is $O(M \times N)$ for the image of the dimension of $(M \times N)$. Moreover, the complexity of addition and multiplication modulo n is $log(n)$ and $log(n)^2$, respectively, and the permutation module is an affine transformation that consists of addition and multiplication modulo n. So, the complexity of the permutation module is $Mlog(M) \times Nlog(N)$. So, the complexity of the overall algorithm is $M \log M^2 \times N \log N^2$. Additionally, we evaluate the proposed E_ECIES running time using Matlab R2021a. The following specifications apply to the experimental environments: Windows 10 operating system, Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM. The proposed method takes 0.2230/sec to encrypt the standard image Lena of dimension 256 × 256. Comparing the computational complexity and running time of the proposed E-ECIES with other existing excellent algorithms is shown in Table 12. The suggested encryption scheme performed better results compared to the [36], [38], [39], and [41] but was less effective than [40]. For evaluating encryption time, we also utilized different images of the same dimensions, 256 × 256. The results are displayed in Table 12.

I. COMPARATIVE ANALYSIS AND DISCUSSION

In this subsection, we will compare our proposed encryption algorithm with other existing cryptosystems based on EC and chose-based mathematical structures [7], [12], [23], [48], [49], [50], [16], [18], [19], [20], [27], [43]. The comparative analysis and discussion are based on some state-of-the-art differential and statistical analysis mentioned in Table 13. We have tested all of these metrics on a standard digital image Lena based on the proposed encryption algorithm. Image encryption techniques based on chaos, presented in [48], [49], [50], and [51], are complex, have high memory requirements, and are difficult to implement on modern devices. The

TABLE 12. Computational complexity and running time with other algorithms.

Methode	Running time	Computational Complexity	Experimental Environment
Proposed (256*256) 1. Lena 2. Baboon 3. Cat 4. Apple	0.2230/sec	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
	0.2130/sec	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
	0.2240/sec	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
	0.2250/sec	$O(M\log M^2 \times N\log N^2)$	Matlab R2021a,CPU @ 2.60GHz 2.80 GHz and 8 GB of RAM.
Ref[36]	0.340/sec	$O(7MN + 3M\log\frac{MN}{3} + 3M + 3N)$	Matlab R2017b, CPU 2.3 GHz, 8 GB memory
Ref[38]	1.320/sec	$O(25MN)$	Matlab R2009a, CPU 2.5 GHz, 4 GB memory
Ref[39]	0.6212/*sec*	$O(18MN + 2M\log\frac{MN}{2})$	Matlab R2012b, CPU 2.6 GHz, 2 GB memory
Ref[40]	0.1179/*sec*	–	Matlab R2017, CPU 2.70 GHz, 8 GB memory
Ref[41]	0.38/*sec*	–	Mathematica Version 11, CPU 1.80 GHz,1.992 MHz, 8 GB memory

TABLE 13. Comparative analysis.

Security parameters	Sensitivity analysis				Statistical analysis			
	NPCR	UACI	PSNR		H.Cor	V.Cor	D.Cor	Entropy
Scheme			P vs E	P vs D				
Proposed	99.6935	33.4069	7.8298	∞	0.0009	0.0007	0.0007	7.9991
Ref [7]	99.5693	33.2824	-	-	-0.0009	0.0008	0.0021	7.9972
Ref [12]	99.6155	33.4274	-	-	-0.0036	0.00262	0.00123	7.9995
Ref [5]	99.7100	33.3600	8.65	∞	-0.0483	-0.0703	-0.0534	7.9995
Ref [16]	99.3300	33.1400	-	-	0.0030	0.0050	-0.0020	7.9900
Ref [18]	-	-	-	-	0.0081	0.0182	0.0065	7.9022
Ref [19]	99.5911	33.3765	-	-	-0.0006	-0.0009	-0.0005	7.9994
Ref [20]	99.976	33.5872			-0.0005	-0.0003	0.0001	7.9993
Ref [43]	99.6541	33.4615	4.5789	-	0.0001	0.0005	0.0015	7.9993
Ref [48]	99.6090	33.4630	-	-	- 0.0002	- 0.0070	0.0005	7.9980
Ref [49]	99.6	33.45	9.2645	-	- 0.0003	- 0.0007	- 0.0001	7.9977
Ref [50]	99.6418	33.558	-	-	-0.0024	-0.0012	0.0011	7.9990
Ref [51]	99.6053	33.4621	7.8616	∞	0.0018	-0.0042	0.0041	7.9991

scheme presented [43] is based on the fusion of improved ECIES and chaotic equations, namely the Hyper chaotic Lorenz generator (HCLG) and Arnold cat map (ACT).

The HCLG was utilized for the confusion module, which is unsuitable and involves more mathematical operations. They also did not properly describe the analysis of the confusion phase. Moreover, the Cat map was utilized for the matrix multiplication, which is more expensive. While in the suggested encryption scheme, the confusion module is achieved by the nonlinear component (S-box) followed by the APA transformation. As a result, obtaining the confusion by the proposed scheme is less time-consuming than integrating the confusion and diffusion, which requires more fusion of EC and chaotic operation. Furthermore, the following bullet points give a detailed comparison of the proposed symmetric encryption algorithm with the existing excellent literature.

- According to Table 13, the proposed cryptosystem outperforms in the differential analysis compared to other chaotic and EC-based encryption techniques presented in [7], [12], [19], [48], [49], [50], and [51] and below from [20].
- The Entropy information of the proposed encryption is nearly close to the ideal value and shows better results from [16], [18], [48], [49], and [50] and nearly below the [7], [19], [20], [43] and equal to the [51].
- According to the correlation analysis, the results of the horizontal, vertical and diagonal of the proposed symmetric encryption scheme are nearly close to the ideal value, which makes sure that the suggested encryption

scheme would perform better and be resistant to statistical attacks as compared to other chaotic and elliptic curve-based encryption schemes [5], [7], [12], [18], [43], [48], [50], [51] and less from the [19], [20], and [49].
- The PSNR values of the encrypted versus plan image and plain versus the decrypted image of the proposed symmetric encryption are 7.8536 and ∞, respectively, show better results than other cryptographic algorithms presented in [49] and [51] and somehow below from the [5] and [43].

Based on the comparative analysis of Table 13, we can see that the proposed symmetric cryptosystem testing findings have shown better outcomes than recent chaotic and EC-based encryption techniques and give robust security and high resistance against state-of-art cryptanalysis.

VII. CONCLUSION

In this research, we proposed an elliptic curve integrated encryption scheme (ECIES) to secure RGB images. In the initial module, the suggested approach of the symmetric encryption scheme achieves the aim of diffusion using the first twelve bytes of the symmetric key of 128-bits. The confusion module is accomplished by the affine power affine transformation followed by the last four bytes of the symmetric key. A comparison of the proposed encryption scheme with the existing algorithm is presented in Table 13. From the table, we can observe that the statistical and sensitivity analysis of the proposed algorithm offers excellent security and can withstand common attacks. In light of the results in Table 13, our approach may be utilized for secure image transmission and is more valuable when sending RGB images to several recipients.

ACKNOWLEDGMENT

This work was partially funded by the research center of the Future University in Egypt, 2022. We are very thankful to Future University Egypt for funding.

REFERENCES

[1] L. Liu, Z. Zhang, and R. Chen, "Cryptanalysis and improvement in a plaintext-related image encryption scheme based on hyper chaos," *IEEE Access*, vol. 7, pp. 126450–126463, 2019.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[3] F. Ö. Çatak and A. F. Mustacoglu, "CPP-ELM: Cryptographically privacy-preserving extreme learning machine for cloud systems," *Int. J. Comput. Intell. Syst.*, vol. 11, no. 1, p. 33, 2018.

[4] F. O. Catak, I. Aydin, O. Elezaj, and S. Yildirim-Yayilgan, "Practical implementation of privacy preserving clustering methods using a partially homomorphic encryption algorithm," *Electronics*, vol. 9, no. 2, p. 229, Jan. 2020.

[5] N. Sasikaladevi, K. Geetha, K. Sriharshini, and M. D. Aruna, "H^3-hybrid multilayered hyper chaotic hyper elliptic curve based image encryption system," *Opt. Laser Technol.*, vol. 127, Jul. 2020, Art. no. 106173.

[6] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.

[7] L.-L. Huang, S.-M. Wang, and J.-H. Xiang, "A tweak-cube color image encryption scheme jointly manipulated by chaos and hyper-chaos," *Appl. Sci.*, vol. 9, no. 22, p. 4854, Nov. 2019.

[8] H. Zhu, X. Zhang, H. Yu, C. Zhao, and Z. Zhu, "An image encryption algorithm based on compound homogeneous hyper-chaotic system," *Nonlinear Dyn.*, vol. 89, no. 1, pp. 61–79, Jul. 2017.

[9] M. Li, K. Zhou, H. Ren, and H. Fan, "Cryptanalysis of permutation–diffusion-based lightweight chaotic image encryption scheme using CPA," *Appl. Sci.*, vol. 9, no. 3, p. 494, Jan. 2019.

[10] C. Zhu, "A novel image encryption scheme based on improved hyperchaotic sequences," *Opt. Commun.*, vol. 285, no. 1, pp. 29–37, 2012.

[11] W. Liu, K. Sun, and C. Zhu, "A fast image encryption algorithm based on chaotic map," *Opt. Lasers Eng.*, vol. 84, pp. 26–36, Sep. 2016.

[12] M. Zarebnia, H. Pakmanesh, and R. Parvaz, "A fast multiple-image encryption algorithm based on hybrid chaotic systems for gray scale images," *Optik*, vol. 179, pp. 761–773, Feb. 2019.

[13] M. Kumar, A. Iqbal, and P. Kumar, "A new RGB image encryption algorithm based on DNA encoding and elliptic curve Diffie–Hellman cryptography," *Signal Process.*, vol. 125, pp. 187–202, Aug. 2016.

[14] A. A. A. El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-Int. J. Electron. Commun.*, vol. 67, no. 2, pp. 136–143, 2013.

[15] J. Wu, X. Liao, and B. Yang, "Color image encryption based on chaotic systems and elliptic curve ElGamal scheme," *Signal Process.*, vol. 141, pp. 109–124, Dec. 2017.

[16] S. Farwa, N. Bibi, and N. Muhammad, "An efficient image encryption scheme using Fresnelet transform and elliptic curve based scrambling," *Multimedia Tools Appl.*, vol. 79, nos. 37–38, pp. 28225–28238, Oct. 2020.

[17] M. Khan and Z. Asghar, "A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S_8 permutation," *Neural Comput. Appl.*, vol. 29, no. 4, pp. 993–999, Feb. 2018.

[18] N. A. Azam, U. Hayat, and M. Ayub, "A substitution box generator, its analysis, and applications in image encryption," *Signal Process.*, vol. 187, Oct. 2021, Art. no. 108144.

[19] U. Hayat, I. Ullah, N. A. Azam, and S. Azhar, "A novel image encryption scheme based on elliptic curves over finite rings," *Entropy*, vol. 24, no. 5, p. 571, Apr. 2022.

[20] M. I. Haider, A. Ali, D. Shah, and T. Shah, "Block cipher's nonlinear component design by elliptic curves: An image encryption application," *Multimedia Tools Appl.*, vol. 80, no. 3, pp. 4693–4718, Jan. 2021.

[21] A. Javeed, T. Shah, and A. Ullah, "Construction of non-linear component of block cipher by means of chaotic dynamical system and symmetric group," *Wireless Pers. Commun.*, vol. 112, no. 1, pp. 467–480, May 2020.

[22] N. Siddiqui, A. Naseer, and M. Ehatisham-ul-Haq, "A novel scheme of substitution-box design based on modified PASCAL's triangle and elliptic curve," *Wireless Pers. Commun.*, vol. 116, no. 4, pp. 3015–3030, Feb. 2021.

[23] F. Masood, J. Masood, L. Zhang, S. S. Jamal, W. Boulila, S. U. Rehman, and J. Ahmad, "A new color image encryption technique using DNA computing and Chaos-based substitution box," *Soft Comput.*, vol. 26, no. 16, pp. 1–17, 2021.

[24] F. Artuğer and F. Özkaynak, "An effective method to improve nonlinearity value of substitution boxes based on random selection," *Inf. Sci.*, vol. 576, pp. 577–588, Oct. 2021.

[25] D. Lambić, "A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design," *Nonlinear Dyn.*, vol. 100, no. 1, pp. 699–711, 2020.

[26] M. Abdalla, M. Bellare, and P. Rogaway, "The Oracle Diffie–Hellman assumptions and an analysis of DHIES," in *Proc. Cryptographers' Track RSA Conf.* Berlin, Germany: Springer, Apr. 2001, pp. 143–158.

[27] M. Benssalah, Y. Rhaskali, and K. Drouiche, "An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography," *Multimedia Tools Appl.*, vol. 80, no. 2, pp. 2081–2107, Jan. 2021.

[28] N. Koblitz, A. Menezes, and S. Vanstone, "The state of elliptic curve cryptography," *Designs, Codes Cryptogr.*, vol. 19, nos. 2–3, pp. 173–193, Mar. 2000.

[29] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Aug. 1985, pp. 417–426.

[30] R. Guesmi, M. A. B. Farah, A. Kachouri, and M. Samet, "A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2," *Nonlinear Dyn.*, vol. 83, no. 3, pp. 1123–1136, Feb. 2016.

[31] S. D. Galbraith and P. Gaudry, "Recent progress on the elliptic curve discrete logarithm problem," *Des., Codes Cryptogr.*, vol. 78, no. 1, pp. 51–72, Jan. 2016.

[32] L. Cui and Y. Cao, "A new S-box structure named affine-power-affine," *Int. J. Innov. Comput., Inf. Control*, vol. 3, no. 3, pp. 751–759, Jun. 2007.

[33] P. P. Mar and K. M. Latt, "New analysis methods on strict avalanche criterion of S-boxes," *World Acad. Sci., Eng. Technol.*, vol. 48, nos. 150–154, p. 25, 2008.

[34] J. Daemen and V. Rijmen, "Reijndael: The advanced encryption standard," *J. Softw. Tools Prof. Programmer*, vol. 26, no. 3, pp. 137–139, 2001.

[35] C. Carlet and C. Ding, "Nonlinearities of S-boxes," *Finite Fields Appl.*, vol. 13, no. 1, pp. 121–135, Jan. 2007.

[36] Q. Lai, H. Zhang, P. D. K. Kuate, G. Xu, and X. W. Zhao, "Analysis and implementation of no-equilibrium chaotic system with application in image encryption," *Appl. Intell.*, vol. 2022, pp. 1–24, Jan. 2022.

[37] M. Matsui, "Linear cryptanalysis method for DES cipher," in *Proc. Workshop Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, May 1993, pp. 386–397.

[38] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[39] M. Alawida, A. Samsudin, J. S. Teh, and R. S. Alkhawaldeh, "A new hybrid digital chaotic system with applications in image encryption," *Signal Process.*, vol. 160, pp. 45–58, Jul. 2019.

[40] X. Wang and S. Gao, "Image encryption algorithm for synchronously updating Boolean networks based on matrix semi-tensor product theory," *Inf. Sci.*, vol. 507, pp. 16–36, Jan. 2020.

[41] B. Jasra and A. H. Moon, "Color image encryption and authentication using dynamic DNA encoding and hyper chaotic system," *Expert Syst. Appl.*, vol. 206, Nov. 2022, Art. no. 117861.

[42] H. Liang, G. Zhang, W. Hou, P. Huang, B. Liu, and S. Li, "A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography," *Appl. Sci.*, vol. 11, no. 12, p. 5691, Jun. 2021.

[43] N. Bhosale, R. Manza, and K. V. Kale, "Analysis of effect of Gaussian, salt and pepper noise removal from noisy remote sensing images," in *Proc. 2nd Int. Conf. Emerg. Res. Comput., Inf., Commun. Appl.* Amsterdam, The Netherlands: Elsevier, Aug. 2014, pp. 1–15.

[44] P. Arulpandy and M. T. Pricilla, "Speckle noise reduction and image segmentation based on a modified mean filter," *Comput. Assist. Methods Eng. Sci.*, vol. 27, no. 4, pp. 221–239, 2020.

[45] S. W. Hasinoff, "Photon, Poisson noise," in *Computer Vision: A Reference Guide*, vol. 4, 2014.

[46] C. K. Wu and D. Feng, *Boolean Functions and Their Applications in Cryptography*. Berlin, Germany: Springer, 2016.

[47] A. Girdhar, H. Kapur, and V. Kumar, "A novel grayscale image encryption approach based on chaotic maps and image blocks," *Appl. Phys. B, Lasers Opt.*, vol. 127, no. 3, pp. 1–12, Mar. 2021.

[48] S. Zhou, X. Wang, Y. Zhang, B. Ge, M. Wang, and S. Gao, "A novel image encryption cryptosystem based on true random numbers and chaotic systems," *Multimedia Syst.*, vol. 28, pp. 95–112, May 2021.

[49] C. M. Kumar, R. Vidhya, and M. Brindha, "An efficient chaos-based image encryption algorithm using enhanced thorp shuffle and chaotic convolution function," *Appl. Intell.*, vol. 52, no. 3, pp. 2556–2585, 2022.

[50] Z. Bashir, M. G. A. Malik, M. Hussain, and N. Iqbal, "Multiple RGB images encryption algorithm based on elliptic curve, improved Diffie Hellman protocol," *Multimedia Tools Appl.*, vol. 81, no. 3, pp. 3867–3897, Jan. 2022.

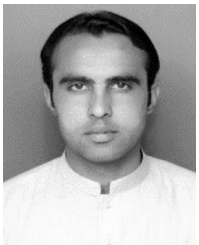
[51] Z. E. Dawahdeh, S. N. Yaakob, and R. R. B. Othman, "A new image encryption technique combining elliptic curve cryptosystem with Hill cipher," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 30, no. 3, pp. 349–355, Jul. 2018.

[52] Y. Wu, Y. Zhou, G. Saveriades, S. Agaian, J. P. Noonan, and P. Natarajan, "Local Shannon entropy measure with statistical tests for image randomness," *Inf. Sci.*, vol. 222, pp. 323–342, Feb. 2013.

IJAZ KHALID is currently a Ph.D. Research Scholar with the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. He has been working on an elliptic curve cryptography, since 2018.

TARIQ SHAH received the Ph.D. degree in mathematics from the University of Bucharest, Romania, in 2000. He is currently a Professor with the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include commutative algebra, non-associative algebra, error-correcting codes, and cryptography.

SAYED M. ELDIN is currently with the Faculty of Engineering and Technology, Future University, in Egypt, on leave from Cairo University after nearly 30 years of service at the Faculty of Engineering, Cairo University. He was the Dean of the Faculty of Engineering, Cairo University, where he achieved many unique signs of progress in both academia and research on the impact of emerging technologies in electrical engineering. He was a PI of several nationally and internationally funded projects. He has many publications in highly refereed international journals and specialized conferences in the applications of artificial intelligence on protection of electrical power networks. He is in the editorial boards of several international journals.



DAWOOD SHAH received the M.Phil. and Ph.D. degrees in mathematics from the Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan. His research interests include coding theory and cryptography.

MUHAMMAD ASIF received the Ph.D. degree in mathematics from Quaid-i-Azam University, Islamabad, Pakistan, in 2020. He is currently an Assistant Professor with the Department of Mathematics University of Management and Technology, Sialkot, Pakistan. His research interests include large scale of coding theory, cryptography, information theory, and fuzzy algebra.

IMRAN SADDIQUE is working as a Full Professor with the University of Management and Technology, Lahore, Pakistan. He is a reviewer of several well-known SCI and ESCI journals. His research interests include artificial intelligence, fuzzy algebra and soft sets, fuzzy fluid dynamics, fluid mechanics, lubrication theory, soliton theory, and graph theory.