IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 9, 2019, accepted November 26, 2019, date of publication December 9, 2019, date of current version January 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2019.2958336

Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography

ROAYAT ISMAIL ABDELFATAH
Electronics and Electrical Communications Engineering Department, Tanta University, Tanta 31527, Egypt
e-mail: royat_esmaeel@f-eng.tanta.edu.eg

ABSTRACT In this paper, a novel scheme for secure and real time image transmission is introduced. The scheme uses a block-based elliptic curve (BBEC) public key encryption as a first stage of encryption so it solves the key distribution and management problem of symmetric key encryption in an efficient method. Then the security of first stage BBEC encryption is enhanced through a second stage of encryption which XOR the BBEC first stage output with a pseudo random sequence generated by a new designed multi chaotic pseudo random generator STH. It merges Sine, Ten and Henon maps (STH) and so it has five secret control parameters which increase the key space and hence the scheme security against brute force attacks. Both the key of the first stage BBEC image encryption and the control parameters of the second stage STH depend on two parts: EC Diffie-Hellman shared secret key and the input plain image itself which provides a good randomness and achieves a strong resistance against chosen plaintext attacks. After the two stages of encryption, the encrypted image is digitally signed in an efficient method to achieve integrity, authentication and non-repudiation. The results prove that the proposed scheme is more secure and faster than some other recent EC based schemes. It has low correlation, huge key space; key-dependent pixel value replacement and can resist statistical, differential and noise attacks.

INDEX TERMS Image encryption, digital signature, EC cryptography, chaotic maps.

I. INTRODUCTION

Due to the wide usage of images as in the Internet, its content protection has become an urgent issue. So recently, researchers have introduced many schemes for image encryption [1]–[5]. These algorithms include two types of encryption; symmetric key and public key [6]. The information is encrypted and decrypted with the same in the symmetric key. Symmetric encryption algorithms are fast and efficient especially for large amounts of data as images [7]–[11]. However, key management and distribution is a big disadvantage in this type of encryption. The key has to be securely distributed in the network and so it may intercepted by attackers during transmission. Also, when the number of users increases, the number of keys will increase dramatically, which represents a burden on the network. The asymmetric key (Public Key Encryption-PKE) overcomes these problems as it uses two different keys; one public key for encryption called public key and another private one for decryption called private key. It is hard to derive the private key from the public one. So there is no need for secret key exchange so it overcomes the key distribution problem and it is more secure as the private key isn't transmitted to anyone. It also can provide digital signature service which can't be achieved with symmetric key. Digital signature provides message integrity, authentication and nonrepudiation.

The most common mathematical hard problems used in PKE are integer factorization and discrete logarithm. These two hard problems are used in RSA and DSA algorithms respectively. In 1985, Miller [12] and Koblitz [13] introduced a new public key cryptography called elliptic curve (EC) which improves the efficiency of various techniques. Actually, cryptographers have found that they can achieve computational efficiency in performance and higher security with very low key-size compared to other algorithms. There is no sub exponential algorithm for solving the discrete logarithm

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

problem on a properly chosen elliptic curve which makes the ECC more attractive. So ECC uses smaller parameters compared with other competitive algorithms, but with equivalent levels of security. This makes ECC has the advantage of faster computations, and smaller processing power, storage space and bandwidth. EC Diffie-Hellman key agreement scheme is widely used in many applications. It is used to exchange a shared secret key that can be used for symmetric key encryption as DES and AES. Many schemes for image encryption based on ECC are proposed. In [14], a color image encryption using EC and discrete chaotic map is provided, where the keys and parameters are obtained by using ECC while the chaotic is used for image scrambling. In [15], EC Diffie-Hellman and DNA based encryption is proposed. In this scheme, the original image is converted into DNA codes then addition is done, and the finally ECDHE is used to obtain the cipher image. Results claimed that this scheme has large key space and good resistance against attacks. EC-variant of ElGamal encryption is introduced in [16] and it has been used for image encryption in many schemes. In [17], EC-ElGamal and chaotic systems based image encryption is proposed, where compression, encryption by cat map and the EC-ElGamal encryption is applied sequentially. It achieves better security compared with other schemes. A similar scheme is presented in [18] for image encryption using a new additive homomorphism in the EC-ElGamal encryption. In [19], an improved ElGamal encryption which encrypts a group of pixels at the same time is applied to medical image which makes it more efficient. In [20], a color image encryption and digital signature scheme using EC-ElGamal algorithm is proposed. This scheme depends on pixel grouping to achieve faster encryption but unfortunately it still consumes many EC point multiplications. In [21], a chaotic system and EC-ElGamal based image encryption scheme is proposed. Firstly, the initial values of the chaotic map are generated using SHA-512, then crossover and EC-ElGamal encryption is used. Finally, the DNA encoding is used to obtain cipher image. The results prove that the scheme has high security and it is robust against attacks but it still consume more time than other image encryption schemes.

Chaotic maps are dynamical systems with high ergodicity and sensitivity to control parameter and initial conditions. Any slight change in the initial conditions causes a remarkable deviation. This initial conditions sensitivity increases the randomness. Encryption schemes based on chaos use initial conditions as a cryptographic key. Many chaos-based schemes have been proposed for image encryption such as Logistic map [22], the Arnold cat map [23], Chebyshev map [24], Tent map [1], Lorenz system [25], the hyper chaotic system [26], the spatiotemporal chaotic system [3] and the memristive chaotic system [27].....ect.

This paper proposes an improved image encryption and digital signature scheme which has the following advantages: the encryption consists of two stages (a) the first stage key depends not only on EC Diffie-Hellman key but also on the input plain image itself and so it has more randomization and more resistance against statistical and differential attacks. (b) The security of the scheme is more enhanced by adding a second stage of encryption with a new designed triple chaotic pseudo random generator that merges three different chaotic: Sine, Ten and Henon maps (STH). This triple combination has more advantages than the simple single chaotic system (henon map, sin map, ten map,....) such as larger parameter space, high randomization and many chaotic sequences. So it is hard to prophesy the chaotic series generated by it. Also the control parameters of SHT are made secret and depend on the input plain image itself, so it is more secure against known-plaintext attack and chosen-plaintext attack. (c) The scheme is time efficient due to two reasons: firstly, it has a less number of EC point multiplications; which is the most time consuming operation; compared to many recent EC based image encryption schemes and secondly, it uses EC group of pixels point multiplication instead of single pixel EC point multiplication. This matter achieves computational time saving. The results and security analysis of the scheme are introduced to prove its advantages.

The remainder of the paper is organized as following: Section II provides the preliminary studies. Section III introduces the proposed scheme. In Section IV, the simulation results are introduced. Section V gives the security performance. Finally, conclusions and future work are given in Section IV.

II. PRELIMINARIES

A. CHAOTIC SYSTEM

Chaotic maps are highly sensitive to initial values and control parameters. Any slight change in the initial conditions causes a remarkable deviation. This sensitivity strongly limits the prediction ability. Encryption schemes based on chaos use initial conditions as a cryptographic key. The chaotic maps include one-dimensional and high dimensional chaotic maps. The one-dimensional map commonly has one variable and little parameters. The one dimension maps as Sine Map (*SM*) and Tent map (*TM*), indicated as:

Sine map:

$$SM\ (n+1) = r \times [\sin(pi \times SM\ (n))] \tag{1}$$

Tent map:

$$TM\ (n+1) = r \times |1 - 2TM\ (n)| \tag{2}$$

and one-dimension decomposition Henon Map (*HM*):

$$HM\ (n+1) = 1 - uHM\ (n)^2 + \beta HM\ (n-1) \tag{3}$$

Now the proposed STH will be considered.

1) PROPOSED MULTI CHAOTIC MAP (STH)

In the proposed scheme, the Sine map and Tent map are combined with Henon map as shown in Fig. 1 to get new one dimensional chaotic system with simple structure and more variables, parameters and more random behaviour than single one dimensional map. The Mathematical function of the

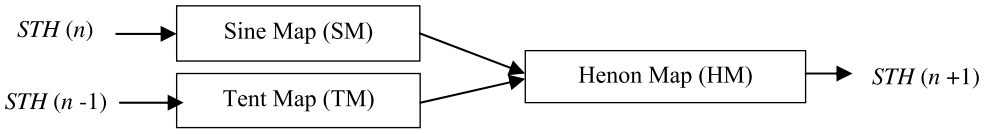

FIGURE 1. The proposed triple chaotic map (STH).

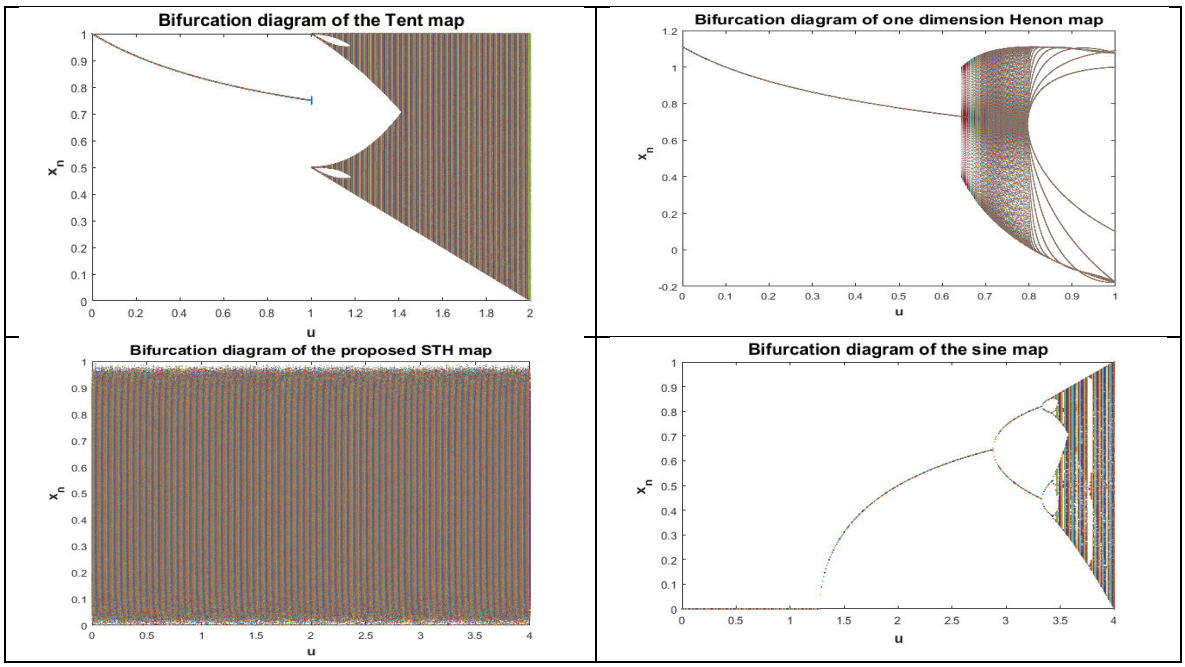

FIGURE 2. Bifurcation diagram comparison.

proposed *Sine –Tent Henon Map* is described as following:

$$STH\ (n+1) = |u - 10 \times sin^2(pi \times STH\ (n)) + (\beta \times r \times |1 - 2STH(n-1)|)\ | \quad (4)$$

where u, β, r is the chaotic system parameter and $STH(1)$, $STH(0)$ are initial values.

2) STATISTICAL TESTS AND CHAOTIC BEHAVIOR OF THE PROPOSED (STH) MAP

The randomness of the proposed STH map is tested by the NIST test suit which consists of 16 statistical tests. These tests are defining if the generated sequence is random or not. The basic dependence within these tests is on the probability value (p-value). The p -value is compared by the significance level α which is the threshold between rejection and non-rejection region. In NIST the significant level equal 0.01. For p-value less than 0.01 this means that the sequence is not random and reject and for p-value greater than 0.01 this means that the sequence is random and accepted. 10^6 bit binary sequence obtained from the proposed STH is tested by SP800-22 with 10^3 iterations and the results are given in Table 1.

The chaotic behavior of the proposed map is evaluated with The Lyapunov exponent and bifurcation analysis. The performance of the proposed STH map is compared with that of Tent, Sine and Henon maps which are used as basic maps in STH. The bifurcation diagrams of the basic maps and the proposed map are shown in Fig. 2. From this figure, it is clear that the proposed STH generates a highly chaotic sequence x_n which is uniformly distributed for $u \in (0, 4)$, while the basic maps are not uniformly distributed and chaotic in only certain intervals of u.

The Lyapunov Exponent (LE) is another metric which can be used to evaluate the performance of chaotic map. LE measures the chaotic sensitivity to the initial values. Negative values of LE mean stable system, while positive values refer to exponential divergence from the initial value. The higher the maximum LE, the higher the chaotic behavior of a map is. The LE of the proposed STH, Logistic and Sine chaotic maps is shown in Fig. 3. It is clear that the LE of STH is positive for all values of $u \in (0, 4)$, while the other chaos has negative values and so not chaotic for some intervals of u. So the sequence generated by the proposed STH is more chaotic.

B. ELLIPTIC CURVE CRYPTOGRAPGY (ECC)

Let F_p denotes the finite field of modulo of a large prime p. An elliptic curve E over the finite field F_p is defined via

$$Y^2 = X^3 + aX + b\ mod\ p \quad (5)$$

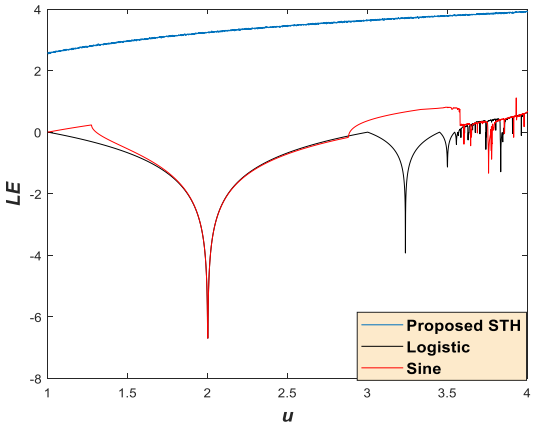

FIGURE 3. Lyapunov exponent (LE) comparisons.

where a and b satisfies:

$$4a^3 + 27b^2 \; mod \; p \neq 0 \tag{6}$$

A base point P of the elliptic curve E with order n should satisfy $N.\ P = O$, where N is the order of the base point P and O is a point at infinity of E. The points of elliptic curve $Ep\ (a, b)$ together with a point O at infinity form an addition cyclic group G_p with order p). The equation above is what is called *Weierstrass normal form for elliptic curves* as shown in Fig.4.

EC includes four operations:

1) EC POINT ADDITION

For any two points $P(x_1, y_1) \neq Q(x_2, y_2)$ on an elliptic curve, If a line is drawn through P and Q, this line will intersect the elliptic curve at a third point $R(x_3, y_3)$. Then the addition of P and Q is reflection of this point about x-axis. It is calculated using following equations:

$$P\,(x_1, y_1) + Q\,(x_2, y_2) = R\,(x_3, y_3) \tag{7}$$

$$x_3 = (\lambda_2 - x_1 - x_2) \; mod \; p \tag{8}$$

$$y_3 = (\lambda\,(x_1 - x_3) - y_1) \; mod \; p \tag{9}$$

$$\text{where } \lambda = (y_2 - y_1)/(x_2 - x_1) \; mod \; \text{p} \tag{10}$$

2) EC POINT SUBTRACTION

Point subtraction is shown in Fig. 2 (b) according to the following equation:

$$P\,(x_1, y_1) - Q\,(x_2, y_2) = P\,(x_1, y_1) + Q\,(x_2, -y_2) \tag{11}$$

3) EC POINT MULTIPLICATION

Multiplication is repeated addition of the base coordinate point. Many algorithms have been developed to perform point multiplication swiftly: $k.P = P + P + P + \cdots + k$ times.

The security of the EC-based schemes depends on the hardness of the EC Discrete Logarithm Problem (EC-DLP) which is defined as following:

Given a point Q on the EC of elliptic curve E_p(a, b), *such that* $Q = k.\ P$ *and k is a random integer and P is a base point. Finding the discrete logarithm of Q with respect to a publicly known base P is infeasible* [28].

TABLE 1. NIST randomness tests of the proposed (STH) binary output.

Test	P-value	Result
Monobit frequency	0.5054	Passed
Block frequency	0.7887	Passed
Runs	0.2032	Passed
Longest-run-of-ones in a block	0.9099	Passed
Binary matrix rank	0.8996	Passed
Discrete Fourier transform (spectral)	0.7480	Passed
Non-overlapping template matching	0.10354	Passed
Overlapping template matching	0.8895	Passed
Maurer's universal statistical	0.71516	Passed
Linear complexity	0.4668	Passed
Serial test	{ 0.042202, 0.14222 }	Passed
Approximate entropy	0.4644	Passed
Cumulative sums	0.6829	Passed
Random excursion	{ 0.7912 , 0.6683 , 98105 , 0.6996 , 0.5947 , 0.3343 , 0.3098,0.1511 }	Passed
Random excursion variant	{ 0.3585, 0.3191 , 0.4458 , 0.5756, 0.6759 , 0.8984 , 0.73, 0.6559, 0.6642 , 0.3853, 0.2837 , 0.3942, 0.7775 , 0.9807, 0.9883 , 0.8357 , 0.5584 , 0.5946}	Passed
Cumulative sums test reverse	0.3014	Passed
LempelZiv compression	0.7533	Passed

EC Diffie Hellman key exchange protocol can be used for secret key exchange between two parties (sender and receiver) as following:

Both the sender and receiver will generate public key and corresponding private key as following:

1. The sender selects a random integer $v_s < p - 1$, keeps it secret, computes:
$$Z_s = v_s.\ P \tag{12}$$
then sends it to the receiver. v_s is the sender's private key while Z_s is his/her public key.
2. The same for the receiver who selects a random integer $v_r < p - 1$, keeps it secret, computes:
$$Z_r = v_r.\ P \tag{13}$$
then sends it to the sender. v_r is the receiver's private key while Z_r is his/her public key.
3. Both the sender and the receiver compute the ECDH shared secret key as following: The sender computes
$$Z_{sr} = v_s.\ Z_r = v_s.\ v_r.\ P \tag{14}$$
and the receiver computes
$$Z_{sr} = v_r.\ Z_s = v_r.\ v_s.\ P \tag{15}$$

It is computationally hard to find Z_{sr} given the public keys Z_s or Z_r as this requires solving the ECDLP to obtain the private key v_s *or* v_r which is computationally infeasible.

III. PROPOSED SCHEME

The proposed scheme consists of two stages both of them use an ECDH shared secret key and another input plain image dependant key. This combination of keys increases the randomness and the security against different type of attack.

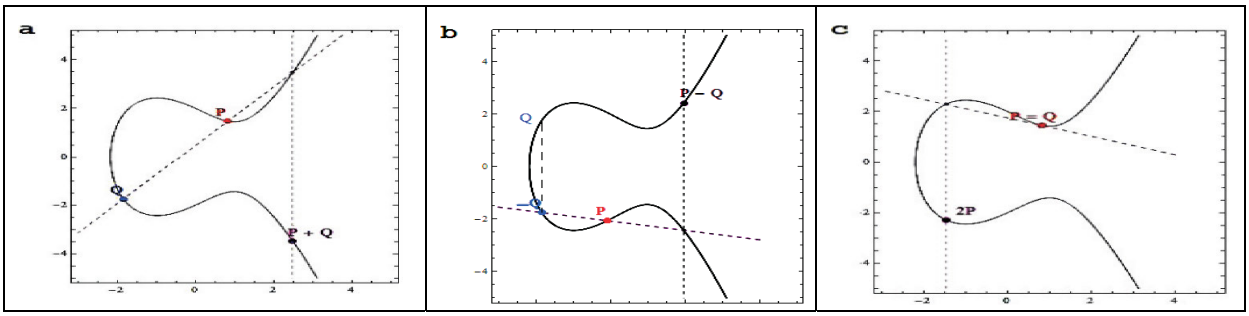

FIGURE 4. (a) Point addition: (b) Point subtraction: (c) Point doubling.

A. Ec SETUP AND KEY GENERATION

The domain parameters (p, a, b, P, n) for the elliptic curve as in Eqn. (5) are selected. Both the sender and receiver generate their public and private key as in Eqns. (12) and (13) then they share a secret key Z_{sr} as in Eqn. (14) and Eqn. (15).

B. IMAGE DIVIDING INTO BLOCKS (PIXELS GROUPING)

The image consists of pixels with value from 0-255. To increase the speed of encryption, the EC operation is applied to a group of pixels instead of individual pixel. The number of pixels that can be grouped (N) depends on the EC prime parameter p. The larger the parameter p of the EC, the more pixels can be grouped. For example for $p = 128$ bit, the number of pixels that can be grouped $N = 16$, for $p = 256$ bit, $N = 32$, for $p = 512$, N = 64. For each group of pixels, combine and concatenate the binary pixel values into one big integer, which represents an element of the prime field F_p of the EC [29].

C. IMAGE ENCRYPTION

If the sender has a RGB plain image m and wants to send it encrypted and signed with the proposed scheme, he will do the following:

1. Use the hash function SHA-256 to compute the hash value h of the plain image m:

$$h = SHA_{256}(m) \tag{16}$$

2. Compute the EC point:

$$e = h.P = (x_e, y_e) \tag{17}$$

$$\text{and } h_e = SHA_{256}\,(x_e \oplus y_e) \tag{18}$$

3. Compute the key K_E for first stage of encryption from the EC point addition of the two points e and the shared secret key Z_{sr}:

$$K_E = e + Z_{sr} = (x_E, y_E) \tag{19}$$

$$\text{and } H = SHA_{256}(x_E \oplus y_E) \tag{20}$$

H will be used as the key of the second stage of encryption which is divided into "8-bit" blocks as in Eqn. (21) and the initial values of the proposed triple chaotic STH are obtained by Eqns. (22) and (23).

$$H = h_1, h_2, h_3, \ldots\ldots h_{32} \tag{21}$$

$$STH\,(0) = STH'\,(0) + \left(\frac{h_1 + h_2 + h_3 + \ldots\ldots h_{16}}{256}\right) \tag{22}$$

$$STH\,(1) = STH'\,(1) + \left(\frac{h_{17} + h_{18} + h_{19} + \ldots\ldots h_{32}}{256}\right) \tag{23}$$

4. Decompose the RGB image (three channels color image of size (M × N × 3) into three separate channels (Red R, Green G, Blue B) or three images each of size (M × N) (if the image is gray-scale, it is directly applied to the first stage of encryption without decomposition). For each image (R, G, B), the encryption is done in two stages as following.

1) FIRST STAGE

a. Group the pixels and convert each group into one big integer < p.
b. Form one pair from each two successive big integers and store it as a point m_p.
c. Perform EC point addition of K_E with each point m_p and store it as points I_c then bring it down again into pixel values ranging from 0-255 and reshape it as a $(1 \times MN)$ vector S_1.

2) SECOND STAGE

a. Use the proposed triple chaotic STH to generate a pseudorandom sequence PR of length MN.
b. Perform XOR operation of the first stage output S_1 and the pseudorandom sequence PR to obtain a vector C of length MN.

$$C = S_1 \oplus PR \tag{24}$$

c. Reshape C as a matrix $(M \times N)$ to obtain the encrypted image.

5. After applying the two stages of encryption to the three channels R, G and B and obtain C_R, C_G and C_B, recompose them to obtain the RGB encrypted image C_{RGB}.

D. IMAGE DIGITAL SIGNATURE

In the proposed scheme the digital signature is applied to the encrypted image C_{RGB} instead of the plain image. This has an advantage at the receiver, the signature verification is done before image decryption and if it failed, the encrypted image will be rejected without decryption. This matter save time and hence achieves faster processing. The encrypted image C_{RGB} is signed as following:

1. Compute R the hash function SHA-256 for the concatenation (||) of the hash value of the encrypted image C_{RGB} and of the hash value h_e computed in Eqn.(18),:

$$R = SHA_{256}(SHA_{256}(C_{RGB})||h_e) \tag{25}$$

2. Use the hash value h of the plain image m that computed in Eqn. (16) and the sender's private key v_s to compute U as following:

$$U = \left(\frac{h}{v_s} - R\right) mod\ p \tag{26}$$

The signature is the pair (R, U) which is sent with the encrypted image C_{RGB} to the receiver. The total process of encryption and digital signature is shown in Fig. 5. At the receiver: Upon receiving the encrypted image C_{RGB} and its signature R and U, the receiver firstly verifies the signature then decrypts the encrypted image as following:

E. DIGITAL SIGNATURE VERIFICATION

The receiver does the following:

1. Compute

$$(U + R).Z_s = e' \tag{27}$$

From Eqn. (12) and Eqn. (26)

$$e' = \frac{h}{v_s}.v_s.P = h.P = (x_e', y_e')$$
$$\text{and } h_e' = SHA_{256}\,(x_e' \oplus y_e') \tag{28}$$

2. Compute

$$R' = SHA_{256}\,(SHA_{256}\,(C_{RGB})\,||h_e') \tag{29}$$

3. Check if

$$R' = R \tag{30}$$

4. Accept the encrypted image C_{RGB} if Eqn. (30) is satisfied then decrypt it. Otherwise, reject it without decryption.

As noted here, the signature verification requires only one EC point multiplication which makes the process faster than other schemes as in [20].

1) CIPHER IMAGE DECRYPTION

1) Compute the decryption key K_E' as the EC point addition of the two points $e'$and the shared Diffie Hellman secret key Z_{sr}:

$$K_E = e' + Z_{sr} = (x_E', y_E') \tag{31}$$

$$\text{and } H' = SHA_{256}(x_E' \oplus y_E') \tag{32}$$

H' which has the same value as H will be used as a secret key for the second stage of decryption which is divided into 8-bit blocks as in Eqn. (21) and the initial values of the proposed triple chaotic STH are obtained at the receiver as in Eqns. (22) and (23).

2. Decompose the encrypted image C_{RGB} into three separate channels (C_R, C_G and C_B) or three images each of size (M × N). For each image (C_R, C_G and C_B), the decryption is done in two stage as following:

2) FIRST STAGE

a. Read the encrypted image as pixels ranging from 0-255 and reshape it as a $(1 \times MN)$ vector S_d.
b. Use the proposed triple chaotic STH to generate a pseudorandom sequence PR of length MN.
c. Perform XOR operation of the S_d and the pseudorandom sequence PR to obtain a vector C_d of length MN.

$$C_d = S_d \oplus PR \tag{33}$$

d. Reshape C_d as a matrix $(M \times N)$ to obtain the image C_2.

3) SECOND STAGE

a. Group the pixels of C_2 and convert each group into a big integer.
b. Form a pair from each two successive big integers and store it as m_c.
c. Perform point subtraction of K_E' from each value of m_c and store it as I_m which is the second stage output decrypted image.
d. Bring down I_m to pixel values ranging from 0-255 and reshape it as a (M × N) matrix to obtain the original plain image.

IV. SIMULATION RESULTS

The laptop used is Intel(R) Core(TM) i5-6200UCPU@ 2.30GHz, 4GB RAM, Windows 10 (64-bit), Mathematica version 11. For prime p of size 128-bit, 256-bit and 512-bit, prime fields of those bit sizes and other elliptic curve parameters are respectively chosen from some standard elliptic curves given by ECC Brain pool [30].

The EC parameters that we choose for 256-bit class are as follows:

$$p = 76884956397045344220809746629001649093037950$$
$$2009430552037356014450315161977 51;$$

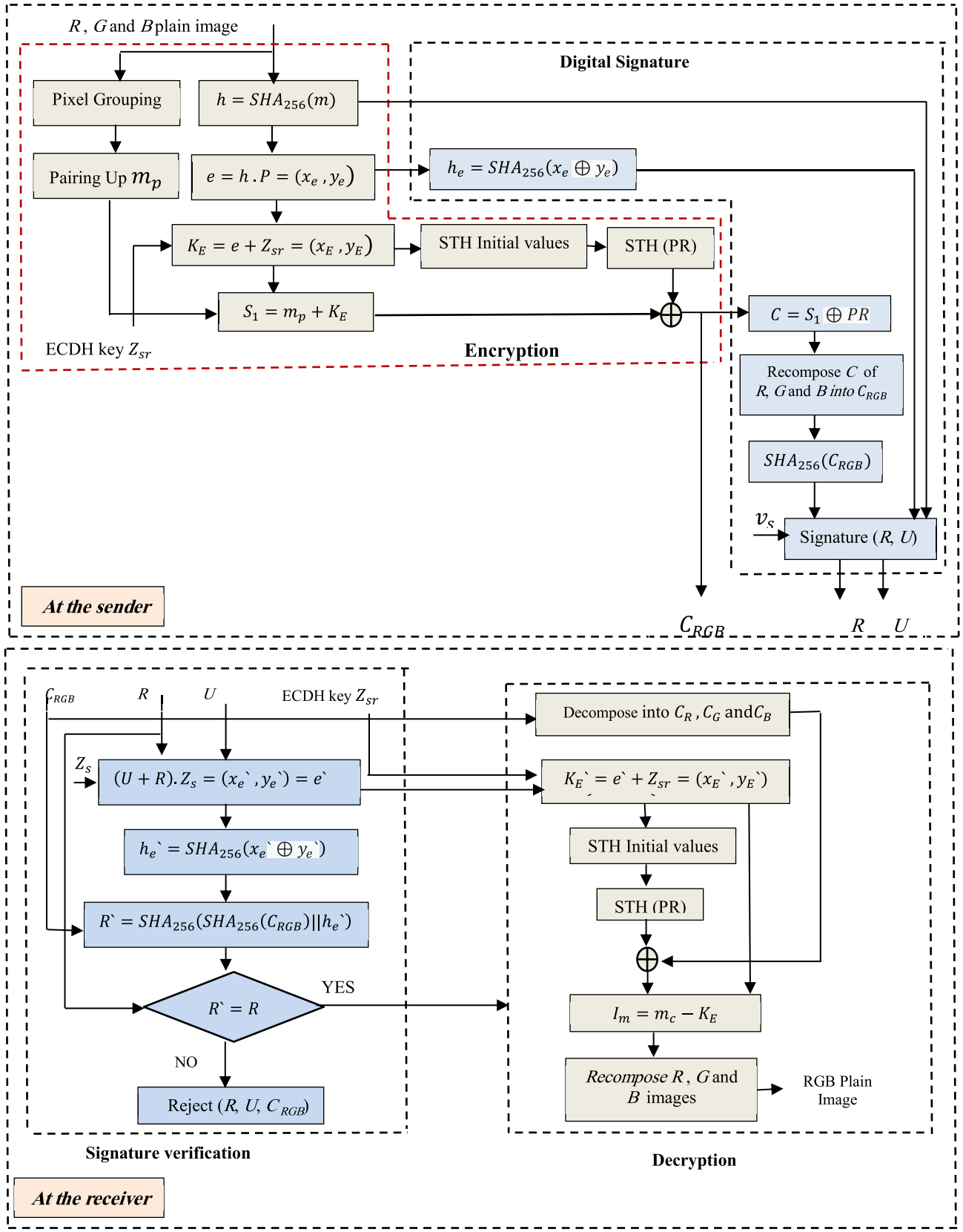

FIGURE 5. Block diagram of the proposed scheme.

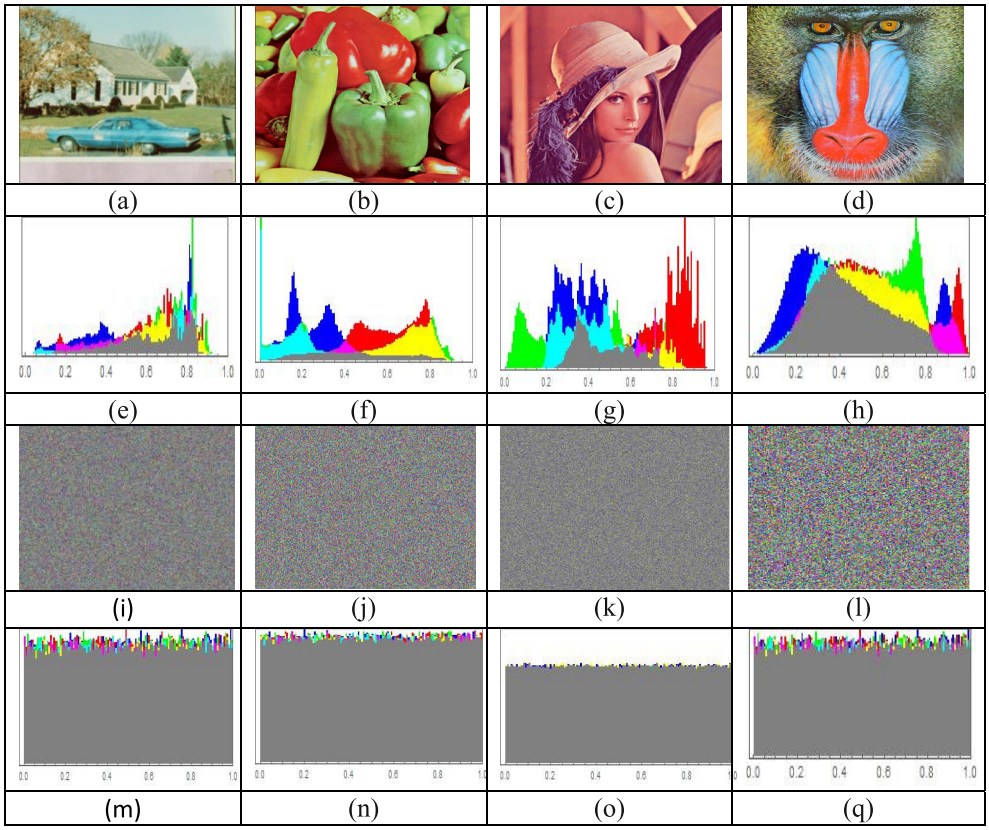

FIGURE 6. Simulation results for RGB images: a House; b Pepper; c Lena; d Baboon images; e-h Histogram of (a)-(d); i-l Cipher images of (a)-(d); m-p Histograms of (i)-(l).

$$a = 566981876053261100436272283961783460771206145394752141093868281887638841399 93;$$

$$b = 175772324973218388410756977897945202629504260589230845670468523006333254389 02;$$

$$P = \{6324372974956233335529224355031297033477817557105472658709538162362714411 4786, 3821861509375352389312227796403081038758540553977260258155783188748571799 7975\};$$

The proposed scheme can be applied to either RGB color images or Gray scale images. Firstly, it is applied to ''Baboon'', ''Peppers'', ''Lena'', and ''House'' RGB images. Secondly, it is applied to gray scale images of ''Lena'', ''Barbara'', Peppers'', ''Baboon'' and House '' with the size of 512×512 The results are given in Fig.6 and Fig.7. It is noted that the scheme converts the original images into a nearly random encrypted images.

V. SECURITY ANALYSIS

The resistance to all kinds of known attacks [31]–[35] is a measure of the goodness of an encryption scheme.

The security of the proposed scheme will be evaluated through the discussion of histogram, entropy, correlation coefficient, NPCR, UACI, MSE, avalanche effect, key space properties, noise attack, known-plaintext attack and chosen-plaintext attack analysis.

A. HISTOGRAM

Histogram is an image identification property which defines the distribution of image pixel intensities as shown in Fig.6 e-h for RGB images and Fig.7 f-j for gray scale images. These figures show that the proposed scheme makes the distribution nearly uniform or fairly flat. So it can defense against statistical attacks.

There is another measure for the uniform histogram distribution, it is the variance. It measures the scatter between the histogram and its mean values. For an image, it is defined as following:

$$Var\ (X) = \frac{1}{m^2} \sum_{i=1}^{m} \sum_{j=1}^{m} \frac{1}{2} (x\ (i) - x\ (j))^2 \qquad (34)$$

where $X = [x_0, x_1 \ldots\ldots\ldots, x_{255}]$ is a vector of the histogram values, $x\ (i)$ and $x\ (j)$ are the pixel values of the gray value i and j respectively. The smaller the variance, the more uniform the histogram is. Table 2 shows the variance of the tested images. It is noted that the variance values of the images after encryption are much smaller than the values before encryption. Also it is noted that the variance values of the encrypted images by the proposed scheme is smaller than the other schemes as in [21] as shown in Table 3. This means

TABLE 2. The variance of the proposed scheme.

Image	Lena		Barbara		Peppers		Baboon		Car	
	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher	Plain	Cipher
Variance	634734	871	383694	990.7	482617	1076.6	752398	880.2	1422410	971.4

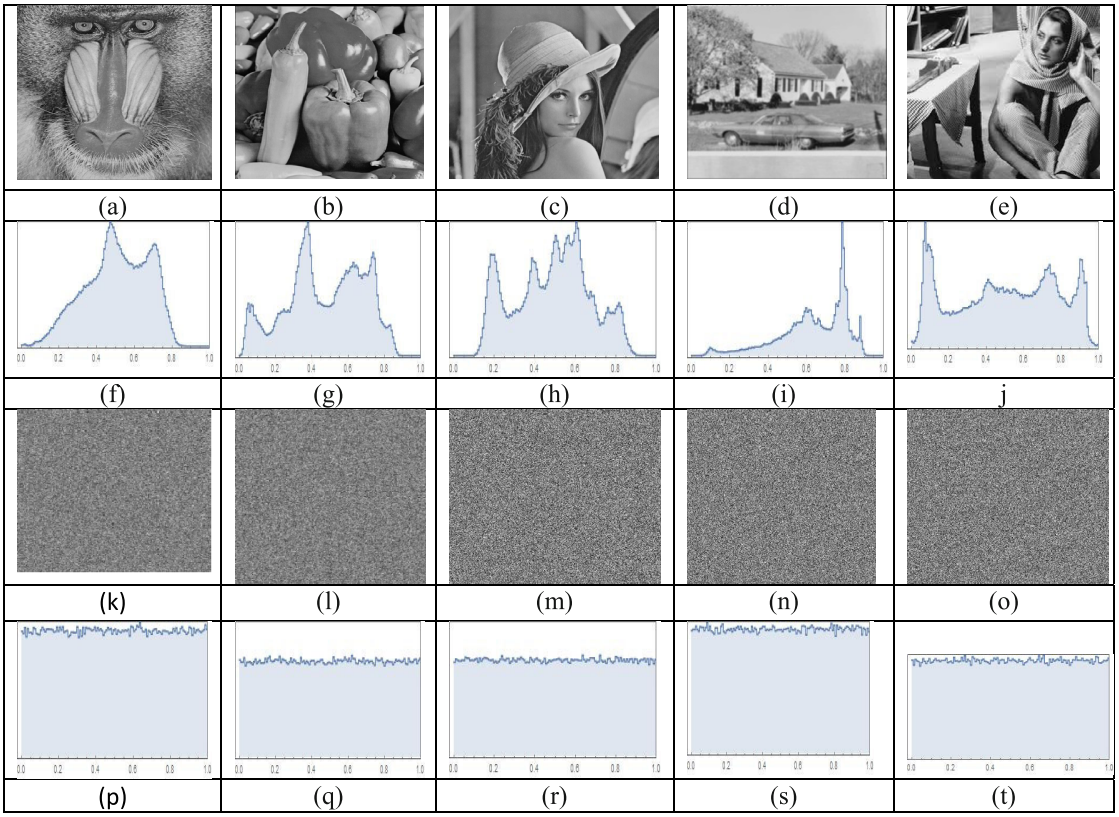

FIGURE 7. Simulation results for gray scale images: a Baboon; b Pepper; c Lena; d House e. Barbara images; f-j Histogram of (a)-(e); k-o Cipher images of (a)-(e); p-t Histograms of (k)-(o).

TABLE 3. The variance comparison.

Image	Lena	Barbara	Baboon
Ours	871	990.7	880.2
Ref.[21]	980	1013.2	1008.3

that the proposed scheme has a stronger resistance against statistical attacks.

B. CORRELATION COEFFICIENT

In fact, a plain image has high pixels correlation which has to be broken in the cipher image by a good encryption scheme to defense against statistical attack.

If N pairs of an image adjacent pixels of values as (x_i, y_i), $i = 1, 2, \ldots, N$ are randomly selected. The correlation coefficients between $x = \{x_i\}$ and $y = \{y_i\}$ is given by the equation:

$$\frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(y_i - E(y))^2}} \tag{35}$$

where, $E(x)$ is the expected value of x.

In the proposed scheme, N = 4096 pairs of adjacent pixels are randomly chosen in the horizontal, vertical, and diagonal directions of both the plain image and its corresponding cipher image. A comparison of the computed correlation coefficients of RGB tested images with that of the other recent schemes as [15] and [20] is shown in Table 4, while Table 5 shows a comparison of the computed correlation coefficients of gray scale tested images with the other recent schemes as [21] and [14], [36]–[39]. From Table 4 and Table 5, it is obvious that the plain images correlation coefficients are close to 1, while that for the cipher images are close to 0 and. So the pixels are uncorrelated in the cipher images and so the proposed scheme can strongly defense against attacks.

Fig. 8 shows horizontal, vertical, and diagonal directions correlation of Fig.6-(a) "House" image and its cipher image in Fig.6-(i).

C. ENTROPY

The entropy of an image is a good measure of its pixel randomness and it is defined as:

$$H = \sum_{I=0}^{L} p(i) \log_2 p(i) \tag{36}$$

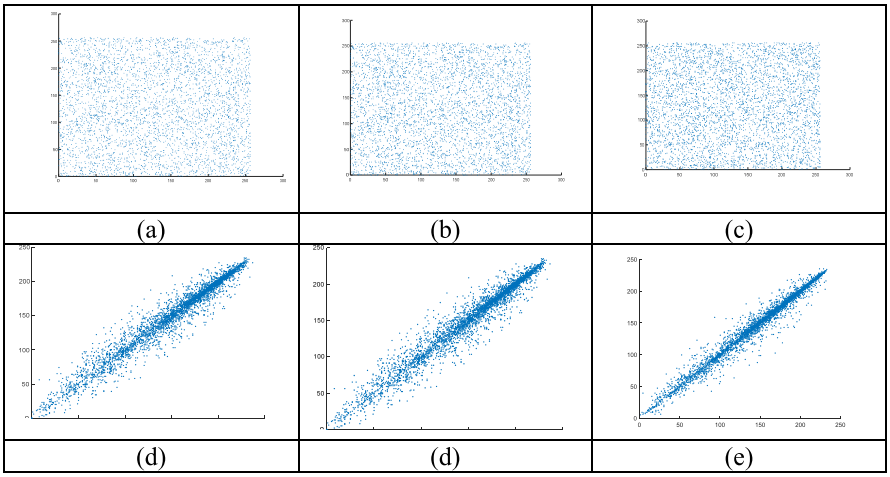

FIGURE 8. Correlation of adjacent pixels in "House" image along (a) Plain image horizontal direction; (b) Plain image vertical direction; (c) Plain image diagonal direction; (d) Cipher image horizontal direction; (e) Cipher image vertical direction; (f) Cipher image diagonal direction.

TABLE 4. Correlation coefficient of the proposed scheme for RGB tested images.

Algorithm	Image	Component	Correlation Coefficients					
			Horizontal		Vertical		Diagonal	
			Plain	Cipher	Plain	Cipher	Plain	Cipher
Ours	House	Red	0.9862	0.001	0.9714	0.00008	0.9845	0.001
		Green	0.9853	- 0.004	0.9691	- 0.0015	0.9833	- 0.0004
		Blue	0.9894	- 0.0025	0.9788	0.0016	0.9890	0.0001
	Baboon	Red	0.9011	0.0015	0.8829	0.0064	0.9351	0.0001
		Green	0.7957	- 0.0015	0.7510	-0.0005	0.8404	- 0.0034
		Blue	0.8915	0.0038	0.8510	0.0014	0.9023	0.003
	Lena	Red	0.9959	-0.0015	0.9886	0.0006	0.9931	-0.0009
		Green	0.9944	-0.0015	0.9847	-0.00076	0.9906	-0.0014
		Blue	0.9876	0.0014	0.9707	-0.00004	0.9810	0.0001
Ref. [20]	House	Red	0.9467	- 0.0067	0.9310	0.0004	0.8987	0.0147
		Green	0.9203	0.0177	0.9120	0.0175	0.8502	-0.0025
		Blue	0.9686	- 0.0153	0.9526	- 0.0001	0.9271	-0.0207
Ref. [15]	Baboon	Red	0.9280	0.0186	0.8650	- 0.006	0.8538	-0.0013
		Green	0.8625	0.0066	0.7697	0.0164	0.7256	0.0092
		Blue	0.9087	0.0067	0.8859	0.0012	0.8427	0.0172
	Lena	Red	0.9326	0.0035	0.9624	- 0.004	0.907	- 0.0410
		Green	0.9222	- 0.0097	0.9546	0.0053	0.8804	- 0.0085
		Blue	0.8938	0.0185	0.9343	0.0106	0.8634	- 0.017

where, L is the number of the image grayscale levels, and $p(i)$ is the probability of the gray value i occurrence. The maximum entropy is 8 for a true random image. The closer the cipher image entropy to this value the stronger encryption scheme is.

Table 6 indicates the entropy values of the tested RGB encrypted images compared with the scheme in [20] and the entropy values of the tested gray scale image compared with the scheme in [21]. From this table, the entropy values of the encrypted images are close to 8, and bigger than the other schemes. So the cipher image has a good resistance against the entropy analysis attack.

D. KEY SPACE

The set of all the keys which are used for image encryption is defined as the key space. It can be evaluated by using two measurements: the number of keys and the key sensitivity.

1) THE NUMBER OF KEYS ANALYSIS

For a robust encryption scheme, the key space has to be big enough to stand against the brute force attack. In the proposed scheme, the keys are the initial values Z'_0, Z'_1 and the parameter u, β, r. SHA-256 is used for computing Z'_0, Z'_1. If the computation precision is around 2^{52} as in [40] then the key space is $2^{256} \times (2^{52} \times 2^{52} \times 2^{52} \times 2^{52} \times 2^{52})$. There is another key which is the shared secret Diffie –Hellman key Z_{sr}. This key can be discovered only with the knowledge of the receiver' private key v_r or the sender's private key v_s. The EC prime parameter p is chosen to be 256 bits. So, the total key space for the proposed encryption scheme equals

$$2^{256} \times (2^{52} \times 2^{52} \times 2^{52} \times 2^{52} \times 2^{52}) \times 2^{256} = 2^{772}.$$

This value is extremely large if compared with other schemes as in Table 7. So the proposed scheme has a strong defense against brute force attack.

TABLE 5. Correlation coefficient of the proposed scheme for gray scale tested images.

Algorithm	Image	Horizontal		Vertical		Diagonal	
		Plain	Cipher	Plain	Cipher	Plain	Cipher
Ours	Lena	0.9868	0.0019	0.9590	-0.0006	0.9717	-0.0014
	Barbara	0.9876	-0.00007	0.9704	-0.0022	0.9812	0.0007
	Peppers	0.9831	-0.0023	0.9658	-0.0013	0.9808	0.0012
	Baboon	0.754	-0.0004	0.7195	-0.0027	0.8635	0.0004
	House	0.9867	-0.0003	0.9713	0.0033	0.9841	-0.0017
Ref. [21]	Lena	0.9858	0.0019	0.9801	-0.0024	0.9669	-0.0011
	Barbara	0.9689	0.0024	0.8956	0.0031	0.8536	-0.0013
	Peppers	0.9807	-0.0028	0.9752	0.0039	0.9636	-.00024
	Baboon	0.7251	0.0024	0.8558	0.0011	0.6920	-0.0008
	House	0.8942	-0.0003	0.8936	0.0014	0.8401	0.0024
Ref. [14]	Lena	0.9325	0.0074	0.9139	-0.0094	0.9469	-0.0054
Ref. [36]	Lena	0.9771	0.0925	0.9631	0.0430	0.9469	-0.0054
Ref. [37]	Lena	0.9503	-0.0226	0.9755	0.0041	0.9275	0.0368
Ref. [38]	Peppers	0.9295	0.0048	0.9294	0.0062	0.8771	0.0030
Ref. [39]	Baboon	0.7508	-0.0061	0.8562	0.0130	0.7153	0.0017

TABLE 6. Entropy analysis.

	Cipher Image	Ref. [20]	Ours
RGB	Baboon	7.99884	7.9991
	Pepper	7.99963	7.9998
	Lena	7.99986	7.9999
	Cipher Ima	Ref. [21]	Ours
Gray Scale	Lena	7.9993	7.9994
	Barbara	7.9993	7.9994
	Baboon	7.9993	7.9994
	House	7.9993	7.9994

TABLE 7. Key space analysis.

	Ref [15]	Ref [20]	Ref[21]	Ours
Key space size	2^{145}	2^{512}	2^{564}	2^{772}

2) KEY SENSITIVITY

A good image encryption scheme should have high sensitivity to all keys. This sensitivity can be measured with two methods. One is a tiny change in the key value has to provide a totally different cipher image. The other is that with a tiny change in the decryption key value the recovery of the plain image will be impossible [2]. In the proposed scheme, the correct keys are used for encrypting "House" image in Fig. 9 (a) to obtain the cipher image shown in Fig. 9 (b). Then a tiny modification in the keys values is done as listed in Table 8. The new cipher images are shown in Fig. 9(c)-(j). The differences between cipher images in the two cases are shown in Fig. 9 (k)-(r). These differences are huge, which proves that the proposed scheme has high sensitivity to the initial keys and so it has a strong defense against the brute force and statistical attacks.

E. DIFFUSION ANALYSIS

A good diffusion performance [41] is a measure of the strength of an encryption scheme. A good diffusion means a strong dependency of cipher image pixels on the plain image pixels. Differential attack is used to assess the diffusion performance. It is a type of chosen-plaintext attack [42]. The differential attack resistance is evaluated by the cipher images differences comparison, i.e. a plain image one bit change should provide a totally different cipher image. The sensitivity can be measured by the number of pixels change rate (NPCR) and unified average changing intensity (UACI). These two values are defined as:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \tag{37}$$

TABLE 8. Key sensitivity analysis.

Proposed method	Correct key	Modified key	Figure of modified key
Sender`s private key	v_s	$v_s + 1$	Fig.9 (c)
Receiver`s private key	v_r	$v_r + 1$	Fig.9 (d)
STH initial value Z_0'	Z_0'	Z_0'+ 0.1	Fig.9 (e)
STH initial value Z_1'	Z_1'	Z_1'+ 0.01	Fig.9 (f)
The control parameter u	u	u+ 0.1	Fig.9 (g)
The control parameter β	β	$\beta + 0.1$	Fig.9 (h)
The control parameter r	r	$r + 0.01$	Fig.9 (i)
The hash value h	h	$h + 1$	Fig.9 (j)

TABLE 9. NPCR and UACI comparison.

Algorithm	Image	Lena	Baboon	Barbara	Peppers	House
Ours	NPCR (%)	99.62	99.61	99.60	99.61	99.61
	UACI (%)	33.48	33.46	33.44	33.55	33.52
Ref. [21]	NPCR (%)	99.61	99.61	99.57	99.61	99.62
	UACI (%)	33.46	33.49	33.42	33.48	33.50

TABLE 10. "LENA" image NPCR and UACI comparison.

Algorithm	Ours	Ref.[21]	Ref.[43]	Ref. [44]	Ref. [45]	Ref. [46]
NPCR (%)	99.6204	99.6113	99.61	99.59	99.60	99.6094
UACI (%)	33.4898	33.4682	33.32	33.41	33.44	33.4635

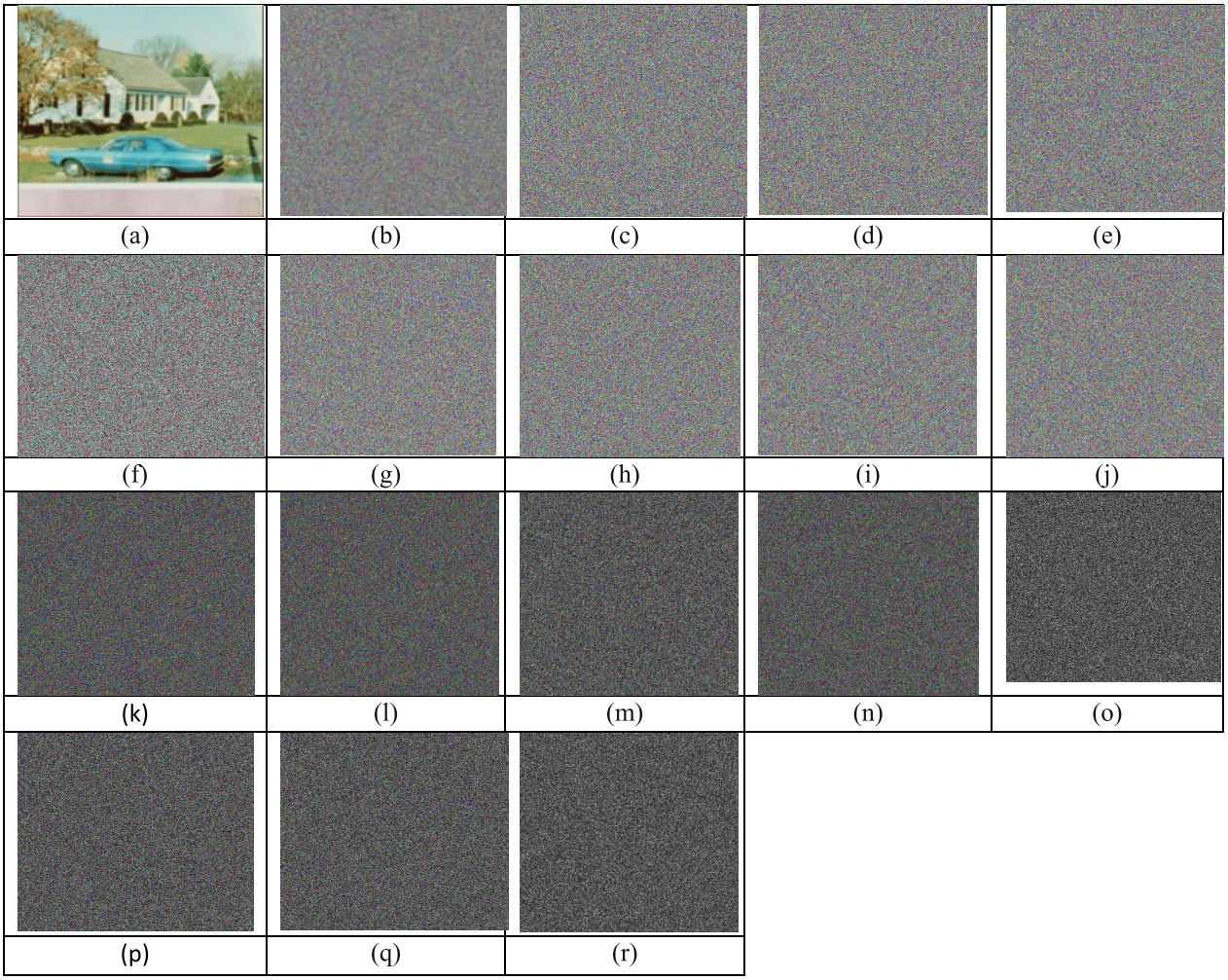

FIGURE 9. The key sensitivity analysis. (a) "House" plain image; (b) Encrypted image with original keys; (c)-(j) Encrypted images with modified keys. (k)-(r) The differences between (b) and (c)-(j).

$$UACI = \frac{1}{M \times N} \frac{\sum_{i,j} |C_1(i,j) - C_2(i,j)|}{L} \times 100\% \quad (38)$$

where $C_1(i,j)$ and $C_2(i,j)$ are the values of the pixels in the position (i, j) of the two cipher –images C_1 and C_2 respectively; L is the number of gray levels. $D(i,j)$ is given as:

$$D(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j) \\ 1, & otherwise \end{cases} \quad (39)$$

The theoretical values of NPCR and UACI are 99.61% and 33.46%, respectively. As the values of NPCR and UACI for an encryption scheme increase above these theoretical values, the encryption scheme will be better and more secure. For the proposed scheme, the value of a randomly chosen pixel is modified. Then the cipher image of the original image C_1 and the cipher image of the modified image C_2 are used to compute NPCR and UACI for different images and listed it in Table 9 compared with Ref. [21]. Comparison of the obtained values of NPCR and UACI for "Lena" image with other schemes is given in Table 10. It is noted that the obtained values of the NPCR and UACI are very close to the expected values irrespective of the chosen pixel position. Also, it is observed that the proposed scheme has lager NPCR and UACI compared to other schemes, and so better resistance against the differential attack.

TABLE 11. The avalanche and MSE values of the tested images.

Image	One bit change in image		One bit change in key	
	Avalanche (%)	MSE (dB)	Avalanche (%)	MSE (dB)
Lena	50.0419	40.3920	50.0310	40.3818
Barbara	50.0753	40.3836	50.0217	40.3759
Peppers	50.0265	40.3956	50.0192	40.3658
Baboon	50.0824	40.3821	50.0294	40.3854
House	50.0311	40.3858	50.0633	40.3939

F. AVALANCHE EFFECT ANAYSIS

Avalanche effect (AE) can be measured by the effect of making a little change in the plain image or the key on the cipher image [47]. The standard AE that if a change of one bit in the plain image is made, it has to make a change in the cipher image not less than 50% [48]. The same effect can be

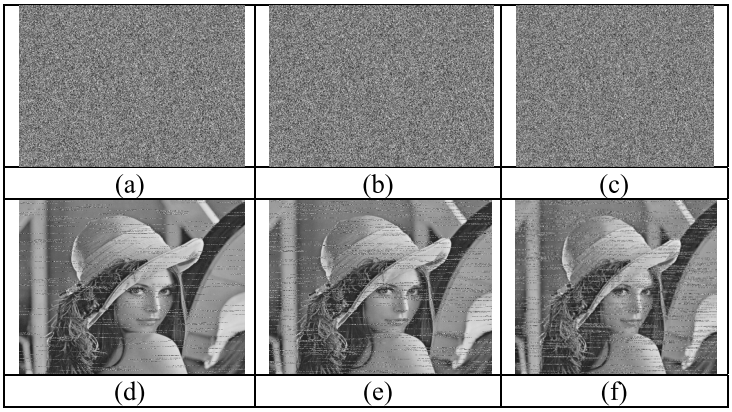

FIGURE 10. (a)-(c) Encrypted images with 10%, 20%, and 30% density salt and pepper noise; (d)-(f) the corresponding decrypted images of (a)-(c).

TABLE 12. The entropy of "All black" and "All white" images.

Image		Entropy	Correlation coefficient		
			Horizontal	Vertical	Diagonal
All black	Plain	0	-	-	-
	Cipher	7.9993	0.0016	0.0035	- 0.0021
All white	Plain	0	-	-	-
	Cipher	7.9993	- 0.001	0.0039	- 0.00042

TABLE 13. Total execution time (in sec.) comparison of the RGB tested images.

Scheme	Image	Size	Encryption	Decryption	Signing	Verification	Total
Ours	Lena	1024×1024	2.73	2.75	2.87	0.05	8.4
	Baboon	512×512	0.68	0.71	0.8	0.05	2.24
	Peppers	256×256	0.23	0.25	0.22	0.04	0.74
Ref.[20]	Lena	1024×1024	2.47	1.58	4.37	4.48	12.9
	Baboon	512×512	0.79	0.60	1.39	1.37	4.15
	Peppers	256×256	0.29	0.30	0.48	0.44	1.51

measured by the mean square error (MSE) which represents the squared error accumulated between two images. MSE is given by:

$$MSE = \frac{1}{W \times H} \sum_{i,j} (IC_1(i,j) - IC_2(i,j))^2 \qquad (40)$$

where $IC_1(i,j)$ and $IC_2(i,j)$ are the two cipher images pixel intensity at the index (i,j) with a one bit different plain image. Generally, when MSE $\geq$30 dB, the cipher images difference is clear [49]. The one bit modification should be in both the key and the plain image. For the proposed scheme, avalanche effect and MSE of one bit plain image and key change are shown in Table 11. It is obvious that the obtained values are larger than the standard irrespective of the position of the one bit change in the plain image or in the keys. This is evidence that the proposed scheme has a good avalanche effect.

G. NOISE ATTACK ANALYSIS

The encrypted image is exposed to noise during transmission in a noisy channel. The strength of an image encryption algorithm is measured by noise resistance and the ability of receiver to recognize the image after decoding it. The proposed scheme is tested by adding a 10%, 20% and 30% density salt and pepper noise to the encrypted image of "Lena" as in Fig.10. A 0.0003, 0.0005 and 0.0007 intensity Gaussian noise is added to the encrypted image in Fig.11. From these figures, it is clear that the proposed scheme is strongly robust against the noise attack.

H. KNOWN-PLAINTEXT AND CHOSEN- PLAINTEXT ATTACKS ANALYSIS

There are four types of conventional attacks: ciphertext-only attack, known-plaintext attack, chosen-plaintext attack, and chosen-ciphertext attack. Among these four types of attack, chosen-plaintext attack is the most powerful one [50] as if an image encryption scheme can defense against this type of attack; it can defense against the other three types [51]–[53]. In the proposed scheme the initial values of the proposed multi chaotic pseudorandom generator STH depend on the input plain image, so the cipher image depends strongly on the plain image. This provides a strong defense against known-plaintext attack and chosen-plaintext attack. An attacker can carry out the chosen-plaintext- attack by encrypting a special image then try to discover the secret

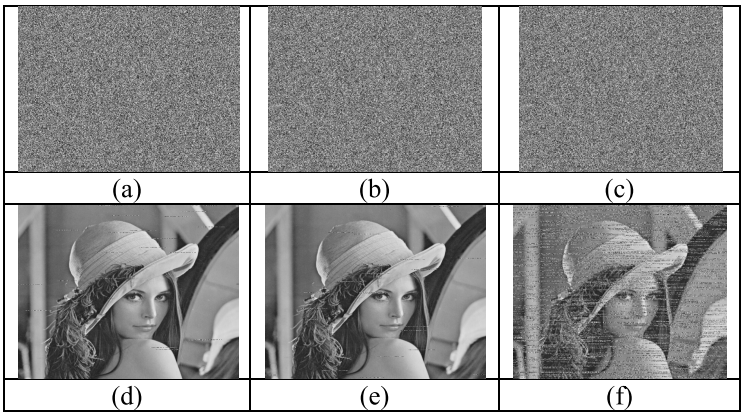

FIGURE 11. (a)-(c) Encrypted images with Gaussian noise of zero mean and variance of 0.0003; 0.0005, and 0.0007 respectively; (d)-(f) the corresponding decrypted images of (a)-(c).

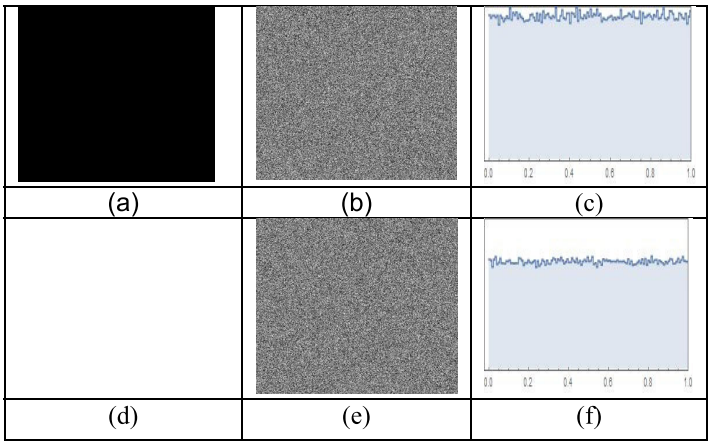

FIGURE 12. (a) All black image; (b) encrypted image of (a); (c) the histogram of (b); (d) all white image; (e) encrypted image of (d); (f) the histogram of (e).

key [1]. In the proposed scheme, two special images are chosen: all black and all white images of size 512×512 to be encrypted. The results are shown in Fig. 12 and the entropies and correlation coefficients are listed in Table 12. These results show the uniformity of the encrypted images histograms. Also, it is clear that the encrypted images entropies are close to 8, and the correlation coefficients are close to 0. This means that the attacker cannot derive any useful information about the key from the encrypted image, so the proposed scheme is strong against known-plaintext attack and chosen-plaintext attack.

I. COMPLEXITY ANALYSIS

A good encryption and digital signature scheme needs to have a fast speed and low computation complexity. The proposed scheme is time efficient as it has a less number of EC point multiplications; which is the most time consuming operation; compared to many recent EC based image encryption schemes and also it is based on pixels grouping EC operation to reduce the number of computations compared to single pixel operation. Table 13 shows a comparison of the execution time of encryption, decryption, digital signature and digital signature verification for the tested RGB images with different image size, while Table 14 shows the encryption execution time comparisons of different size gray scale images with other recent schemes. From Table 13, it is deduced that the proposed scheme achieves time saving of 51%, 46% and 34.9% for RGB image of sizes 256×256, 512×512 and 1024×1024 respectively compared to Ref. [20].

TABLE 14. Encryption time (in sec.) comparison of the gray-scale tested images.

Image size	128×128	256×256	512×512
Ours	0.06	0.23	0.68
Ref.[20]	0.351779	1.170844	4.73389
Ref. [54]	0.2934	1.4483	-
Ref. [55]	0.3796	0.498021	0.938217
Ref. [56]	3.2543	5.55679	8.97439
Ref. [57]	2.17	7.73	31.59
Ref. [58]	-	1.2615	-
Ref. [59]	-	1.44	5.41

The encryption time savings of the proposed scheme applied to different size gray scale images are listed in Table 15. As the EC point multiplication is the most time consuming operation, a comparison of the number of EC

TABLE 15. Encryption time saving (%) of the proposed scheme.

Image size	Time saving (%) to:	Ref. [20]	Ref. [54]	Ref. [55]	Ref[56]	Ref. [57]	Ref[58]	Ref. [59]
128×128		82.9%	79.55%	84.19%	98.15%	97.23%	-	-
256×256		80.35%	84.12%	53.82%	95.86%	97%	81.77%	84%
512×512		85.63%	-	27.52%	89%	97.85%	-	87.43%

TABLE 16. Number of EC point multiplication comparison.

	No. of EC point multiplication					
Scheme	Encryption	Decryption	Signature	Verification	Total	Service provided
Ours	1	1	-	1	3	Encryption & Signature
Ref. [20]	2	1	1	2	6	Encryption & Signature
Ref. [21]	2	1	NO	NO	3	Only Encryption

point multiplication of the proposed scheme and the schemes in Ref. [20] and Ref. [21] is given in Table [16]. From these comparisons, it is obvious that the proposed scheme has less number of operations and hence less computational time than the other schemes. So the proposed scheme is very suitable for real time image communications.

VI. CONCLUSION

In this paper, an efficient image encryption and digital signature scheme is introduced. The scheme consists of two stages of encryption. A block-based elliptic curve (BBEC) public key encryption is used for the first stage and so it solves the key distribution and management problem of symmetric key encryption in a very efficient method. The second stage is an XOR operation of the BBEC first stage output with a pseudo random sequence generated by a new designed multi chaotic pseudo random generator STH. This STH merges Sine, Ten and Henon maps (STH) and has five secret control parameters which increases the key space and hence the scheme security. A combined key of EC Diffie-Hellman shared secret key and the input plain image itself is used for both the first BBEC and the second stages. This matter achieves a good randomness and makes the scheme more resistant against chosen plaintext attacks. Also, the encrypted image is digitally signed in an efficient method to achieve integrity, authentication and non-repudiation. Based on the results, the proposed scheme is more secure and has faster encryption and digital signature compared to some other recent EC based schemes. It has low correlation, huge key space; key-dependent pixel value replacement and can resist statistical, differential and noise attacks. In the future work, and due to the proposed scheme advantages, it may be applied to multimedia such as audio and video with more performance improvement.

REFERENCES

[1] Y. Luo, L. Cao, S. Qiu, L. Hui, J. Harkin, and J. Liu, "A chaotic map control-based and the plain image-related cryptosystem," *Nonlinear Dyn.*, vol. 83, no. 4, pp. 2293–2310, Mar. 2016.

[2] Y. Luo and M. Du, "A self-adapting image encryption algorithm based on spatiotemporal chaos and ergodic matrix," *Chin. Phys. Rev. B*, vol. 22, no. 8, pp. 316–324, 2013.

[3] Y. Luo, M. Du, and J. Liu, "A symmetrical image encryption scheme in wavelet and time domain," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 20, no. 2, pp. 447–460, Feb. 2015.

[4] Y. Luo, R. Zhou, J. Liu, C. Yi, and X. Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dyn.*, vol. 93, no. 3, pp. 1165–1181, Aug. 2018.

[5] Y. Luo, R. Zhou, J. Liu, S. Qiu, and C. Yi, "An efficient and self-adapting color-image encryption algorithm based on chaos and interactions among multiple layers," *Multimedia Tools Appl.*, vol. 77, no. 20, pp. 26191–26217, Oct. 2018.

[6] G. J. Simmons, "Symmetric and asymmetric encryption," *ACM Comput. Surv.*, vol. 11, no. 4, pp. 305–330, 1979.

[7] L. Huang, S. Cai, X. Xiong, and M. Xiao, "On symmetric color image encryption system with permutation-diffusion simultaneous operation," *Opt. Lasers Eng.*, vol. 115, pp. 7–20, Apr. 2019.

[8] Z. Hua, Y. Zhou, and H. Huang, "Cosine-transform-based chaotic system for image encryption," *Inf. Sci.*, vol. 480, no. 1, pp. 403–419, Apr. 2019.

[9] Y. Luo, S. Tang, X. Qin, L. Cao, F. Jiang, and J. Liu, "A double image encryption scheme based on amplitude-phase encoding and discrete complex random transformation," *IEEE Access*, vol. 6, pp. 77740–77753, 2018.

[10] Y. Luo, R. Zhou, J. Liu, S.-H. Qiu, and Y. Cao, "A novel image encryption scheme based on kepler's third law and random Hadamard transform," *Chin. Phys. B*, vol. 26, no. 12, pp. 146–159, 2017.

[11] C. Zhu and K. Sun, "Cryptanalyzing and improving a novel color image encryption algorithm using RT-enhanced chaotic tent maps," *IEEE Access*, vol. 6, pp. 18759–18770, 2018.

[12] M. Miller, "Uses of elliptic curves in cryptography," in *Advances in Cryptography—Crypto*. Berlin, Germany: Springer-Verlag, 1986, pp. 417–426.

[13] N. Koblitiz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–208, 1987.

[14] Z. Liu, T. Xia, and J. Wang, "Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem," *Chin. Phys. B*, vol. 27, no. 3, pp. 1–16, 2018.

[15] 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.

[16] N. Koblitz, *A Course Number Theory Cryptography*. New York, NY, USA: Springer, 1987.

[17] 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.

[18] L. Li, A. A. A. El-Latif, and X. Niu, "Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images," *Signal Process.*, vol. 92, no. 4, pp. 1069–1078, Apr. 2012.

[19] L. D. Singh and K. M. Singh, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.

[20] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Comput. Sci.*, vol. 54, pp. 472–481, Jan. 2015.

[21] Y. Luo, X. Ouyang, J. Liu, and L. CAO, "An image encryption method based on elliptic curve elgamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019, doi: 10.1109/ACCESS.2019.2906052.

[22] H. Huang and S. Yang, "Colour image encryption based on logistic mapping and double random-phase encoding," *IET Image Process.*, vol. 11, no. 4, pp. 211–216, Apr. 2017.

[23] G. Ye and K.-W. Wong, "An efficient chaotic image encryption algorithm based on a generalized Arnold map," *Nonlinear Dyn.*, vol. 69, no. 4, pp. 2079–2087, Sep. 2012.
[24] X. Huang, "Image encryption algorithm using chaotic Chebyshev generator," *Nonlinear Dyn.*, vol. 67, no. 4, pp. 2411–2417, 2012.
[25] X.-Y. Wang, L. Yang, R. Liu, and A. Kadir, "A chaotic image encryption algorithm based on perceptron model," *Nonlinear Dyn.*, vol. 62, no. 3, pp. 615–621, 2010.
[26] X. Wang and H.-L. Zhang, "A novel image encryption algorithm based on genetic recombination and hyper-chaotic systems," *Nonlinear Dyn.*, vol. 83, nos. 1–2, pp. 333–346, 2016.
[27] X. Chai, Z. H. Gan, L. Yang, M.-H. Zhang, and Y.-R. Chen, "A novel color image encryption algorithm based on genetic recombination and the four-dimensional memristive hyperchaotic system," *Chin. Phys. B*, vol. 25, no. 10, pp. 76–88, Aug. 2016.
[28] *Elliptic-Curve Cryptography*, Wikipedia, San Francisco, CA, USA, Jun. 2019.
[29] D. M. S. Bandara, Y. Lei, and Y. Luo, "Fingerprint image encryption using a 2D chaotic map and elliptic curve cryptography," *World Acad. Sci., Eng. Technol. Int. J. Comput. Inf. Eng.*, vol. 12, no. 10, pp. 871–878, 2018.
[30] *ECC Brainpool Standard Curves and Curve Generation V.1.0*, TeleTrusT, Berlin, Germany, Oct. 2005.
[31] S. Mazloom and A. M. Eftekhari-Moghadam, "Color image encryption based on coupled nonlinear chaotic map," *J. Chaos Solitons Fractals*, vol. 42, pp. 1745–1754, Nov. 2009.
[32] C. K. Huang, C. W. Liao, S. L. Hsu, and Y. C. Jeng, "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *J. Telecommun. Syst.*, to be published, doi: 10.1007/s11235-011-9461-0.
[33] A. Akhshani, S. Behnia, A. Akhavan, H. A. Hassan, and Z. Hassan, "A novel scheme for image encryption based on 2D piecewise chaotic maps," *J. Opt. Commun.*, vol. 283, pp. 3259–3266 Sep. 2010.
[34] F. Sun, S. Liu, Z. Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map," *Chaos, Solitons Fract.*, vol. 38, no. 3, pp. 631–640, 2008.
[35] S. Behnia, A. Akhshani, S. Ahadpour, H. Mahmodi, and A. Akhavan, "A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps," *Phys. Lett. A*, vol. 366, no. 4, pp. 391–396, 2007.
[36] G.-D. Ye, X.-L. Huang, L. Y. Zhang, and Z.-X. Wang, "A self-cited pixel summation based image encryption algorithm," *Chin. Phys. B*, vol. 26, no. 1, pp. 131–138, 2017.
[37] L. Xu, X. Gou, Z. Li, and J. Li, "A novel chaotic image encryption algorithm using block scrambling and dynamic index based diffusion," *Opt. Lasers Eng.*, vol. 91, pp. 41–52, Apr. 2017.
[38] D.-D. Liu, W. Zhang, H. Yu, and Z.-L. Zhu, "An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion," *Signal Process.*, vol. 151, pp. 130–143, Oct. 2018.
[39] X. Chai, Z. Gan, K. Yang, Y. Chen, and X. Liu, "An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations," *Signal Process., Image Commun.*, vol. 52, pp. 6–19, Mar. 2017.
[40] D. Lambic, "Cryptanalyzing a novel pseudorandom number generator based on pseudo randomly enhanced logistic map," *Nonlinear Dyn.*, vol. 89, no. 3, pp. 2255–2257, Aug. 2017.
[41] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, Oct. 1949.
[42] X. Wang, X. Zhu, X. Wu, and Y. Zhang, "Image encryption algorithm based on multiple mixed hash functions and cyclic shift," *Opt. Lasers Eng.*, vol. 107, no. 1, pp. 370–379, Aug. 2017.
[43] S. Sun, "Chaotic image encryption scheme using two-by-two deoxyribonucleic acid complementary rules," *Opt. Eng.*, vol. 56, no. 11, 2017, Art. no. 116117.
[44] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.
[45] G. Ye, "A block image encryption algorithm based on wave transmission and chaotic systems," *Nonlinear Dyn.*, vol. 75, no. 3, pp. 417–427, Feb. 2014.
[46] Z. Yong, "The unified image encryption algorithm based on chaos and cubic S-Box," *Inf. Sci.*, vol. 450, pp. 361–377, Jun. 2018.
[47] A. Jawad and A. Fawad, "Efficiency analysis and security evaluation of image encryption schemes," *Int. J. Video Image Process. Netw. Secur.*, vol. 12, no. 4, pp. 18–31, 2012.
[48] X.-J. Tong, M. Zhang, Z. Wang, and J. Ma, "A joint color image encryption and compression scheme based on hyper-chaotic system," *Nonlinear Dyn.*, vol. 84, no. 4, pp. 2333–2356, 2016.
[49] L. Zhu, W. Li, L. Liao, and H. Li, "A novel image scrambling algorithm for digital watermarking based on chaotic sequences," *Int. J. Comput. Sci. Netw. Secur.*, vol. 6, no. 8B, pp. 125–130, Aug. 2006.
[50] X. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, no. 4, pp. 1101–1108, Apr. 2012.
[51] C. Zhu, G. Wang, and K. Sun, "Improved cryptanalysis and enhancements of an image encryption scheme using combined 1D chaotic maps," *Entropy*, vol. 20, no. 11, p. 843, Nov. 2018.
[52] C. Li, D. Lin, B. Feng, J. Lü, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.
[53] C. Zhu, G. Wang, and K. Sun, "Cryptanalysis and improvement on an image encryption algorithm design using a novel chaos based S-box," *Symmetry*, vol. 10, no. 9, p. 399, Sep. 2018.
[54] S. Zhu and C. Zhu, "Image encryption algorithm with an avalanche effect based on a six-dimensional discrete chaotic system," *Multimedia Tools Appl.*, vol. 77, no. 21, pp. 29119–29142, Nov. 2018.
[55] S. Zhu, C. Zhu, and W. Wang, "A novel image compression-encryption scheme based on chaos and compression sensing," *IEEE Access*, vol. 6, pp. 67095–67107, 2018.
[56] J. Chen, Z. Yu, Q. Lin, F. Chong, and L. Xu, "Exploiting chaos-based compressed sensing and cryptographic algorithm for image encryption and compression," *Opt. Laser Technol.*, vol. 99, pp. 238–248, Feb. 2017.
[57] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and DNA complementary rules," *Multimedia Tools Appl.*, vol. 74, no. 13, pp. 4655–4677, Jul. 2015.
[58] 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.
[59] R. I. Abdelfatah, "A new fast double-chaotic based image encryption scheme," in *Multimedia Tools and Applications*. Cham, Switzerland: Springer, 2019, doi: 10.1007/s11042-019-08234-4.

ROAYAT ISMAIL ABDELFATAH received the B.Sc. degree in electronics and electrical with the Communications Engineering Department, Tanta University, Egypt, in 2000, and the M.Sc. and Ph.D. degrees from Tanta University, in 2005 and 2011, respectively. Her M.Sc. is dedicated in encryption techniques and its applications. The Ph.D. is devoted to introduce new encryption, digital signature, signcryption, and hash functions algorithms for securing digital data over communication networks.