Received March 13, 2020, accepted March 19, 2020, date of publication March 23, 2020, date of current version April 1, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2982567

Hybrid Cryptosystem Based on Pseudo Chaos of Novel Fractional Order Map and Elliptic Curves

ABDULRAHMAN AL-KHEDHAIRI[1], AMR ELSONBATY[2,3], ABDELALIM A. ELSADANY[2,4], AND ESAM A. A. HAGRAS[5]

[1]Department of Statistics and Operations Researches, College of Science, King Saud University, Riyadh 11451, Saudi Arabia
[2]Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj 11942, Saudi Arabia
[3]Department of Mathematics and Engineering Physics, Faculty of Engineering, Mansoura University, Mansoura 35516, Egypt
[4]Department of Basic Science, Faculty of Computers and Informatics, Suez Canal University, Ismailia 41522, Egypt
[5]Communication and Computer Department, Faculty of Engineering, Delta University for Science and Technology, Mansoura 11152, Egypt

Corresponding author: Amr Elsonbaty (sonbaty2010@gmail.com)

This project was supported by the Deanship of Scientific Research at Prince Sattam Bin Abdulaziz University under the research project #2019/01/10295.

ABSTRACT Securing transmission of information between legitimate transmitter and receiver sides is a great challenge for mathematicians, computer scientists and engineers in recent years. This paper aims at achieving three goals. The first of them is to introduce a novel fractional order two dimensional (2D) map having very complex chaotic behavior and distinct large positive values of Lyapunov exponents over wide range of parameters, compared with other 2D maps in literature. Secondly, a new reliable secure encryption scheme combining the associated chaotic pseudo-orbits of the proposed map with the advantages of elliptic curves in public key cryptography is suggested, for first time, and applied to colored images. The hybrid scheme is capable to confirm reliable secret keys exchange in addition to highly obscure and hide transmitted information messages. Finally, a thorough mathematical analysis of security performance and evaluation of encryption scheme immunity against all possible attacks are carried out and proved its efficiency and robustness.

INDEX TERMS Chaos-based cryptography, chaotic maps, discrete fractional calculus, elliptic curves, pseudo-orbits.

I. INTRODUCTION

The last three decades have witnessed a great technological revolution which successfully reshapes our life. For example, advanced digital communication systems, personal computers, smart phones, digital cameras, internet, among others, play a crucial role in every one's daily life. The necessity for securing crucial information data transmitted between two entities and preventing the leakage or snoop of any critical information are inevitable challenge for mathematicians, computer scientists, and engineers.

The fascinating properties of chaotic dynamics, such as high sensitivity to initial conditions and parameters, noise like behavior, wideband spectrum, the possibility of being generated through utilizing very fast nonlinear laser dynamics and the possibility of attaining synchronization between transmitter and receiver, render chaotic dynamical systems a perfect choice in several modern applications including chaotic radars [1], chaotic LIDAR [2], chaos based encryption systems [3]–[5] and ultra-fast physical random number generators [6]–[9]. More specifically, chaotic dynamics have the ability to mask information signals in both frequency and time domains. Furthermore, they can be employed in different ways so as to encrypt various forms of information messages in both software and hardware layers, see for example [10]–[17] and references therein.

Chaos based communications systems have also attracted considerable interest in recent years. For example, a proposed chaotic constellation transformation technique in orthogonal frequency-division multiple access-based passive optical networks (OFDM-PON) is examined theoretically and experimentally in [18], where it has shown physical-layer security enhancement and reliable 18.86 Gb/s encrypted signal transmission over 25 Km single mode optical fiber. In [19], an optimum block dividing scheme combined with two-dimensional adjusted logistic sine map and dynamic key assignment technique is employed for further security improvement in OFDM-PON. Security enhancement for OFDM-PON using

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

three-dimensional Brownian motion and chaos in cell [20] and also using chaos encryption and DNA encoding [21] are demonstrated.

However, the very recent studies concerned with security performance of chaos based secure communication systems reveal that two factors must be considered with a great attention in building chaos based encryption systems [22]–[24]. In particular, the high complexity and dimensionality of chaos employed in these systems in addition to effective prohibition of any internal information of the chaos based encryption system from being attained from the transmitted chaotic signal by any illegal intruders are required. Few techniques have been proposed to improve chaotic dynamics and security performance of some specific chaos based cryptosystems [10], [23], [24]. For example, the presence of time delay signature in outputs of chaotic of laser systems having delayed optical feedback was regarded as a major security deficiency which has been treated in [19], [20]. Indeed, optical chaos sources that feature good suppression of time delay signature [10], [23] as well as the high-dimensional entangled photons systems [25]–[27] can serve as fast physical random number generators [9]. Such sources of physical randomness are essentially important in wide area of applications in the modern technology era.

Block image encryption scheme was proposed in [28] to treat the periodicity problems in cat map and therefor resist chosen plain text attack. More specifically, the combined Arnold cat map and dynamic random growth technique is used in the way that the secret key is dependent on plain images.

Also, in order to address the problems of long time permutation processing and poor permutation performance of traditional permutation algorithm, like Arnold, Baker and cyclic shift permutation schemes, the recent advances in the field of image encryption involve achieving efficient fast encryption in real-time systems that run for both distributed and parallel computing environments [29]. Also, the Boolean networks and matrix semi-tensor product technique are adopted in a new chaos-based image encryption system with good security characteristics [30].

On the other hand, elliptic curve cryptography has proved itself as a popular effective public key cryptography technique [31], [32]. Elliptic curves cryptography reduces the lengths of safe secret key, required for top secret documents, by approximately 90 % compared with other public key encryption techniques such as Rivest–Shamir–Adleman (RSA), Diffie–Hellman key exchange (DH), and El-Gamal. Also, it is energy efficient with very fast computations speed, memory savings and best fitting for small apparatuses.

Recently, there are few trials initiated in order to incorporate the advantages of chaos based cryptography with those of elliptic curve cryptography in a robust image encryption scheme [17], [33], [34]. Although the proposed schemes successfully possess the ability to resist some of different security attacks, there are major deficiencies occur in these works. For example, the chaos generators employed in these systems usually produce relatively weak chaos (with small values of positive Lyapunov exponents) or apply chaotic perturbations in encryption through a way which renders it more vulnerable to security attacks. Also, the joining scheme which maximizes the security performance of the hybrid (chaos/elliptic curve) cryptosystem is unclear. Furthermore, the possible occurrence of unwanted signature that may reveal the internal structure of cryptosystem in encrypted transmitted signals should be taken into account. This creates motivations for scientists, from different disciplines, to do their best efforts to treat the aforementioned issues via building new hybrid crypto- systems.

Moreover, several works have highlighted the issue of chaotic behavior degradation and suppression in simple one dimensional chaotic maps, such as logistic map or tent map [35]–[37]. The reason for this degradation is due to the finite precision impacts [35], [37]. Different strategies can be applied in order to offer appropriate solutions to chaos suppression problem via utilizing more accurate finite precision calculations or transition between chaotic outputs of different chaotic systems [35]. However, there still exist some other factors which render the realization of robust and efficient encryption algorithms a difficult work. As an example, the 1D chaotic maps based cryptosystem typically have small key space as a result of single used value of initial conditions.

The generalization of the ordinary differential and integral calculus to non-integer order calculus is called the fractional calculus (FC) [38]. Recently, FC has proved itself as useful tool for applications in many fields of research such as biomedicine, nonlinear electronic circuits, chaos based cryptography and image encryption [39]–[50]. The specific field of discrete fractional calculus (DFC) is a hot topic which develops rapidly in recent years. In fact, several new mathematical topics related to the discretization of the Riemann-Liouville and the Caputo operators have been studied such as the initial value problem in DFC [51], the variational approach to the fractional discrete model [52], the properties of the discrete forms of Riemann-Liouville and the Caputo operators [53], and the Laplace transform in discrete fractional calculus [54]. Furthermore, chaotic discrete fractional dynamical systems were examined in Refs. [55]–[57] and they proved their efficiency in some modern chaos base encryption scheme [58]–[62].

This paper is an attempt to face this challenge. The key problems which motivate this work are summarized below:

Firstly, the vast majority of chaos based cryptography systems are based on chaos generators having time series outputs with low degree of complexity. The largest Lyapunov exponent, as a measure for strength of chaotic dynamics, typically takes values less than 3 in most of these chaotic systems. So, can we introduce a new chaotic map that can successfully achieve larger values maximum Lyapunov exponents (MLEs), greater than 20, for example?

Secondly, the chaotic output of the proposed new map is to be employed implicitly in an efficient encryption scheme by adopting the corresponding pseudo orbit and therefore increase its effectiveness.

Finally, elliptic curves as a technique for public secret key transmission are well known by its superiority over other similar technique such as RSA, DH, El-Gamal,…etc. So, can we combine the advantages of this technique with the noise-like behavior of the new improvised chaotic map to devise a superior cryptosystem?

The key advantages of the proposed encryption scheme compared with other schemes in literature, such as schemes which use one-time keys, bit-level permutation, cellular automata, etc., see [63]–[66] and reference therein, are: (a) Distinctive large values of Lyapunov exponents (LEs), see for example one-time keys image encryption scheme [63] and spatial bit-level permutation [64] where the maximum LEs of employed piecewise linear chaotic map and Chen chaotic system are less than three. (b) The pseudo-chaotic encrypting sequence is extracted from two mathematically equivalent but computationally nonequivalent systems. This overcomes the possible degradation of statistical features in encrypting sequence in systems which apply chaotic outputs directly [67]. (c) The proposed system combines the advantages of robust and efficient EC key exchange with those of pseudo-chaotic orbits. In particular, the proposed scheme can be further improved in future work to easily include the more advanced supersingular isogeny ECKE and therefore can withstand the risks of quantum computers era. (d) The secret keys of the proposed encryption scheme are not fixed. They are depending on plain images and the time moment of their arrival. This implies that if the same plain image is applied multiple times, different secret keys will generated for encryption process.

Our proposed technique extends the idea of [28] by incorporating the advantages of the reliable ECKE, high complex novel chaotic map, and finally time varying and plain image dependent secret keys. Moreover, the pseudo chaotic sequence is used in permutation–diffusion processes, rather than direct application of conventional generated chaotic sequence, which increases the effectiveness of scheme, utilizes finite precision error and overcomes the degradation in statistical features of chaotic sequence due to finite precision computations on computers [67].

The paper is organized as follows. Some preliminaries and mathematical concepts are introduced in Section II followed by the proposed fractional order 2D chaotic map and its associate dynamical properties in Section III. The proposed hybrid cryptosystem is presented for the case of colored images as input data in Section IV. Simulation results and security analysis of the scheme are performed in Section V to verify its superiority then the discussion of results is concluded in Section VI.

II. PRELIMINARIES

Discrete fractional calculus was introduced to efficiently incorporate and capture the memory effects in nonlinear discrete time systems [68]–[70]. Dynamical behaviors and applications of fractional difference models, on an arbitrary time scale, were investigated in the last decade where delta difference equation was utilized [70]–[72]. Assume that a sequence $\rho(n)$ is given and the isolated time scale $\aleph_a$ is represented in terms of real valued constant τ i.e. $\{\tau, \tau+1, \tau+2, \ldots,\}$ such that $\rho : \aleph_\tau \rightarrow R$. Also, the difference operator is denoted by Δ, where $\Delta\rho(n) = \rho(n+1) - \rho(n)$. Then we summarize some key results and definitions of discrete fractional calculus as follows.

Definition 1: For $\alpha > 0$, the order α fractional sum is given by [70]

$$\Delta_\tau^{-\alpha}\rho(t) = \frac{1}{\Gamma(\alpha)} \sum_{m=\tau}^{t-\alpha} \frac{\Gamma(t-m)}{\Gamma(t-m-\alpha+1)} \rho(m), \quad t \in \aleph_{\tau+\alpha}.$$

Definition 2: The order α Caputo-like delta difference is defined by [71]:

$$\begin{aligned} {}^{C}\Delta_\tau^{\alpha}\rho(t) &= \Delta_\tau^{-(n-\alpha)}\Delta^n\rho(t) \\ &= \frac{1}{\Gamma(n-\alpha)} \sum_{m=\tau}^{t-(n-\alpha)} \frac{\Gamma(\text{t-m})}{\Gamma(t-m-n+\alpha+1)} \Delta^n\rho(m), \\ & t \in \aleph_{\tau+n-\alpha}, \quad n = \lfloor\alpha\rfloor + 1. \end{aligned}$$

Definition 3: The delta fractional difference equation of order α is represented by [72]:

$${}^{C}\Delta_\tau^{\alpha}\rho(t) = f(t+\alpha-1, \rho(t+\alpha-1)),$$

and the equivalent discrete fractional integral is given by

$$\begin{aligned} y(l) = \rho_0(t) + \frac{1}{\Gamma(\alpha)} \sum_{m=\tau+n-\alpha}^{t-\alpha} \frac{\Gamma(t-m)}{\Gamma(t-m-\alpha+1)} \\ \times f(m+\alpha-1, \rho(m+\alpha-1)), \quad t \in \aleph_{\tau+n}. \end{aligned}$$

Note that the initial iteration in this case is expressed as

$$\rho_0(t) = \sum_{k=0}^{n-1} \frac{\Gamma(t-\tau+1)}{k!\Gamma(t-\tau-k+1)} \Delta^k\rho(\tau).$$

Now, we review some key points related to elliptic curves. Elliptic curves were firstly utilized in cryptography by Neal Koblitz and Victor Miller [31], [32].

Definition 4: For a prime field $F_p, p \neq 2, 3$, assume that $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$. Then, any elliptic curve E defined over F_p is represented by

$$E : y^2 \equiv x^3 + ax + b \,(mod\ p).$$

The group of points (x, y) which satisfying the equation of elliptic curve E, along with a point O at infinity, are referred to as elliptic curve group $E(F_p)$. The basic operations on elliptic curves are addition and doubling of points. In addition, the multiplication by a scalar is carried out by combining addition and doubling operations. In particular, given two elliptic curve points $P = (x_1, y_1), Q = (x_2, y_2)$, and a positive integer k, then the addition of P and Q are defined by

$$P + Q = (x_3, y_3),$$

where $x_3 \equiv (\gamma^2 - x_1 - x_2)\, mod\ p$,

$y_3 \equiv (\gamma\,(x_1 - x_3) - y_1)\, mod\ p$ and

$$\gamma = \frac{y_2 - y_1}{x_2 - x_1}, \quad P \neq Q,$$
$$\gamma = \frac{3x_1^2 + a}{2y_1}, \quad P = Q.$$

For the case where $x_1 = x_2 (mod\ p), y_1 + y_2 = 0\,(mod\ p)$, then $P + Q = O$.

The scalar multiplication is defined by

$$kP = P + P + P + \ldots + P\,(k\ times)\,.$$

Given two points M and N on an elliptic curve E, then it is computationally very hard to find the value of k which achieves $Q = kP$. This problem is referred to as Elliptic Curve Discrete Logarithm Problem (ECDLP) which is computationally very hard problem to solve provided that the recommended values for parameters suggested by National institute of Standards (NIST) are used.

III. THE PROPOSED FRACTIONAL ORDER 2D CHAOTIC MAP

Inspired by excellent characteristics of lemniscate chaotic map [73], the proposed chaotic map is inherited from lemniscate map [73] as a seed. In particular, three identical lemniscate chaotic maps are cascaded in the way that the output of third stage is fed back as input to the first stage. Figure 1 elucidates how new map was formulated from three identical lemniscate chaotic maps. It is important to notice that the proposed structure of the map is not restricted to only three cascaded maps but it can be extended to general n-stages setup. More specifically, it is observed that the values positive Lyapunov exponents in new map increase linearly with the number of cascaded seed maps. Nevertheless, the forms of resulting new maps become more and more complicated when the number of cascaded seed maps increase. Therefore, if four or five cascaded maps are employed to form new map then the MLEs will be further increases whilst more computations costs are demanded for the highly intricate developed map. In the present work we establish the proposed map with three maps to achieve the balance between complexity of computations and the improved dynamics of the map.

The proposed model is presented in two forms, namely, integer order form and fractional order form as follows.

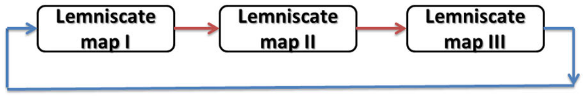


FIGURE 1. Construction of the proposed chaotic map from three lemniscate chaotic maps.

Integer order form

$$x(n+1) = \frac{\mathrm{Cos}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(n)]\mathrm{Sin}[2^r x(n)]}{1+\mathrm{Sin}[2^r x(n)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(n)]\mathrm{Sin}[2^r x(n)]}{1+\mathrm{Sin}[2^r x(n)]^2}\right]^2},$$
$$y(n+1) = \frac{2\sqrt{2}\mathrm{Cos}\left[\frac{2^r\mathrm{Cos}[2^r y(n)]}{1+\mathrm{Sin}[2^r y(n)]^2}\right]\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(n)]}{1+\mathrm{Sin}[2^r y(n)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(n)]}{1+\mathrm{Sin}[2^r y(n)]^2}\right]^2}. \quad (1)$$

Caputo-like delta fractional difference form of order α

$$^C\Delta_\tau^\alpha x\,(t) + x(t-1+\alpha) = \frac{\mathrm{Cos}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(t-1+\alpha)]\mathrm{Sin}[2^r x(t-1+\alpha)]}{1+\mathrm{Sin}[2^r x(t-1+\alpha)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(t-1+\alpha)]\mathrm{Sin}[2^r x(t-1+\alpha)]}{1+\mathrm{Sin}[2^r x(t-1+\alpha)]^2}\right]^2},$$
$$^C\Delta_\tau^\alpha \mathrm{y}\,(\mathrm{t}) + \mathrm{y}\,(t-1+\alpha) = \frac{2\sqrt{2}\mathrm{Cos}\left[\frac{2^r\mathrm{Cos}[2^r \mathrm{y}(t-1+\alpha)]}{1+\mathrm{Sin}[2^r \mathrm{y}(t-1+\alpha)]^2}\right]\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r \mathrm{y}(t-1+\alpha)]}{1+\mathrm{Sin}[2^r \mathrm{y}(t-1+\alpha)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r \mathrm{y}(t-1+\alpha)]}{1+\mathrm{Sin}[2^r \mathrm{y}(t-1+\alpha)]^2}\right]^2}, \quad (2)$$

where fractional order satisfies $0 < \alpha < 1$ and parameter r is positive.

Hence, we get the following equivalent integral form (3), as shown at the bottom of this page.

A. DYNAMICAL BEHAVIORS OF THE NOVEL CHAOTIC MAP

In this subsection, the interesting nonlinear dynamics exhibited by new chaotic map are investigated through time series plots, phase portraits, bifurcation diagrams and maximum Lyapunov exponent plot. It will be shown that the proposed system has distinguished large positive value of maximal Lyapunov exponent and very wide range of parameter r at which the map exhibit complex chaotic behavior.

$$x\,(n) = x\,(0) + \frac{1}{\Gamma\,(\alpha)}\sum_{j=1}^{n}\frac{\Gamma\,(n-j+\alpha)}{\Gamma\,(n-j+1)}\times\left(\frac{\mathrm{Cos}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(j-1)]\mathrm{Sin}[2^r x(j-1)]}{1+\mathrm{Sin}[2^r x(j-1)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(j-1)]\mathrm{Sin}[2^r x(j-1)]}{1+\mathrm{Sin}[2^r x(j-1)]^2}\right]^2} - x\,(j-1)\right),$$
$$y\,(n) = \mathrm{y}\,(0) + \frac{1}{\Gamma\,(\alpha)}\sum_{j=1}^{n}\frac{\Gamma\,(n-j+\alpha)}{\Gamma\,(n-j+1)}\times\left(\frac{2\sqrt{2}\mathrm{Cos}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]^2} - y\,(j-1)\right) \quad (3)$$

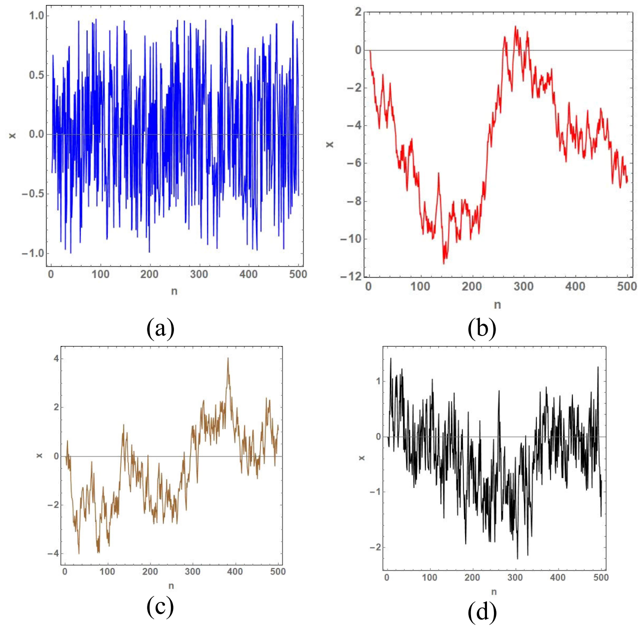


FIGURE 2. Time series of x output of new chaotic map at $r = 10$ and (a) $\alpha = 1$, (b) $\alpha = 0.95$, (c) $\alpha = 0.75$, (d) $\alpha = 0.5$.

Moreover, incorporating memory influences, via fractional order difference operator, has the advantage of increasing the number of parameters in the model and hence enlarging the secret key space for encryption process. Also, the coexistence of stable chaotic multiple attractors are observed in fractional order case.

Firstly, the value of r is fixed and the time series plots of the output of proposed map are depicted in Fig.2 at different values fractional order α. It is found that a significant influence is induced by fractional difference which appears through the obvious modulation of conventional chaotic signal produced by integer order map. Also, chaotic fluctuations are observed for wide range of fractional order α.

The next step is to thoroughly examine the integer order case via obtaining x-y phase portraits at different values of parameter r. It is shown that the new map undergoes a sequence of period-doublings in a small range of r $(0 < r < 1)$. The occurrence of chaotic dynamics is therefore observed for wide range of r values. Examples of phase portraits generated by new map (1) are illustrated in Fig.3. Furthermore, bifurcation diagram and spectra of Lyapunov exponents (LE) are utilized to give a broad view of the dynamics of new map (1) versus r and to confirm the existence of chaotic output for wide range of this parameter. The LE spectra are obtained to quantify the degree of complexity and sensitivity to initial conditions [18] in the proposed chaotic map. Figure 4 shows LE spectra of the chaotic map (1) and shows that both LEs have distinguished large positive values which confirm the occurrence of complicated behavior in the proposed map. From Fig.4, it can be demonstrated that compared with other conventional chaotic maps, like Logistic, Henon, Sine, Zaslavisky, etc., the proposed map has a distinguished large value of MLE that is increasing with r.

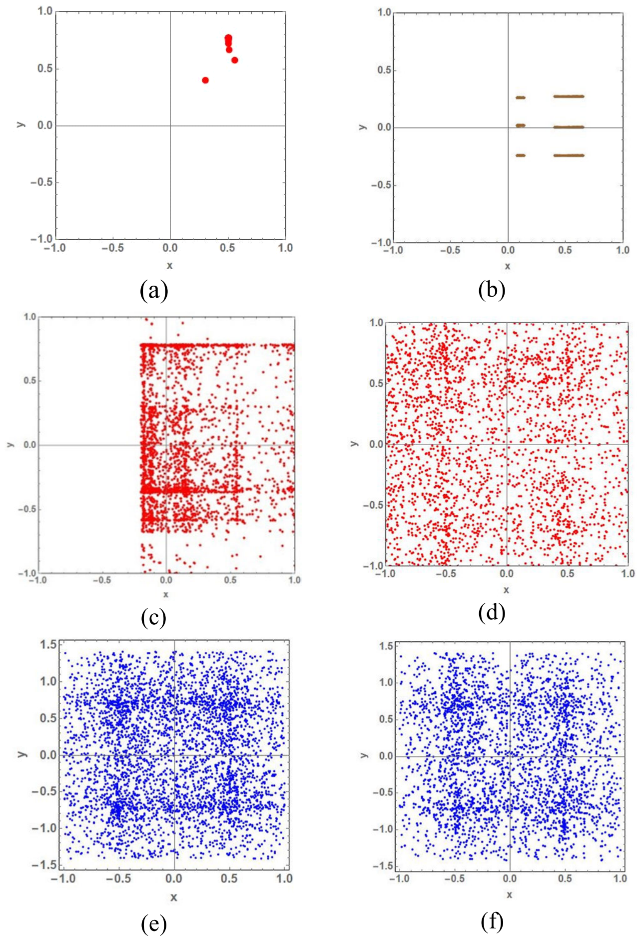


FIGURE 3. Phase portraits of integer order chaotic map (1) obtained at (a) $r = 0.3$, (b) $r = 0.8$, (c) $r = 1$, (d) $r = 4$, (e) $r = 12$, and finally (f) $r = 19$.

Finally, the case of proposed Caputo-like delta fractional difference map (3) is scrutinized where some results are presented in Fig.5. In Fig.5, the value of r is fixed at 10 and the value of fractional order is varied so as to inspect the changes in system dynamics; see Fig.5 (a-c). The first and foremost important observation here is that the orbits starting from distinct initial positions will subsequently converge to different coexisting chaotic attractors in phase space. These simultaneously occurring attractors is colored by red, blue, brown and black in Fig.5. Changing the value of r, the same phenomenon is observed; see for example Fig.5 (d). Bifurcation diagrams in terms of parameters α and r verify that complex dynamics persist over a broad range of α and r, see Fig.5 (e-f). The aforementioned characteristics of new Caputo-like fractional difference map (3) render it preferable in chaos based cryptography applications.

IV. THE PROPOSED HYBRID CRYPTOSYSTEM

A. INPUT

Plain image of size $h \times v$ pixels. There are three values associated to each pixel such that they they are corresponding to degrees of colors red, green and blue. For a pixel in position (i, j), denote by $P_r(i, j)$, $P_g(i, j)$, and $P_b(i, j)$ the

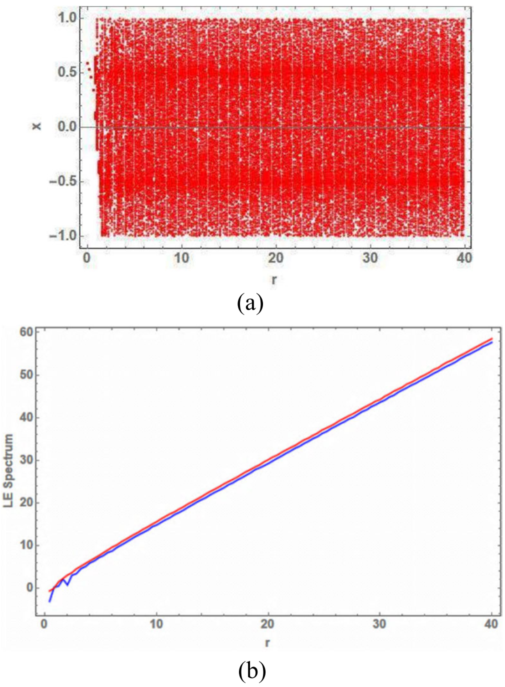


FIGURE 4. Bifurcation diagram of state variable x and LE spectrum evaluated for new chaotic map (1) versus parameter r.

red, green, and blue pixel values, respectively, which range from 0 to 255. The internal clock of transmitter is initiated when the encryption session starts.

B. PUBLIC KEYS

Group generator and parameters of one of the standard elliptic curves suggested by NIST in USA. For example, in the following simulations we consider the P-192 curve groups in the form

$$y^2 = x^3 - 3x + b,$$

with

$$\begin{aligned} G = \{&602\,046\,282\,375\,688\,656\,758\,213\,480\,587\\ &526\,111\,916\,698\,976\,636\,884\,684\,818,\\ &174\,050\,332\,293\,622\,031\,404\,857\,552\,280\\ &219\,410\,364\,023\,488\,927\,386\,650\,641\},\\ b = &\,2\,455\,155\,546\,008\,943\,817\,740\,293\,915\,197\\ &451\,784\,769\,108\,058\,161\,191\,238\,065,\\ q = &\,277\,101\,735\,386\,680\,763\,835\,789\\ &423\,207\,666\,416\,083\,908\,700\,34\,961\,279, \end{aligned}$$

refer to group generation, parameter of the curve and modulus of finite field, respectively.

C. SECRET KEYS

- **(a)** The initial values of parameters r and α in the proposed chaotic map, namely, r_0 and α_0.
- **(b)** Private key at the sender side i.e. k_s.
- **(c)** Private key at the receiver side i.e. k_R.

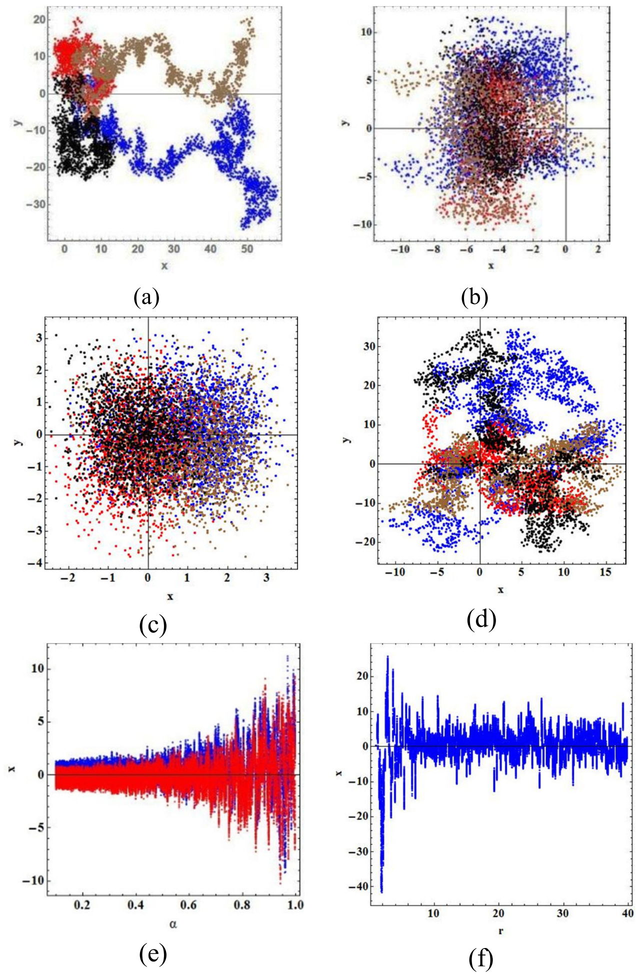


FIGURE 5. The phase portraits of proposed map (3) are shown in (a)-(e) for (a) $r = 10$ and $\alpha = 0.95$, (b) $r = 10$ and $\alpha = 0.75$, (c) $r = 10$ and $\alpha = 0.5$, (d) $r = 20$ and $\alpha = 0.95$. The bifurcation diagrams versus α and r in (e) and (f), respectively.

- **(d)** The two initial conditions of proposed chaotic map.
- **(e)** A set of arbitrary m-perturbation values denoted by $\{p_1, p_2, \ldots, p_m\}$.
- **(f)** An arbitrary real number μ.

D. ENCRYPTION/DECRYPTION PROCESS

1) Employ the following two mathematically equivalent forms of new map (3)

$$x(n) = x(0) + \frac{1}{\Gamma(\alpha)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\alpha)}{\Gamma(n-j+1)} \times \left(\frac{\mathrm{Cos}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(j-1)]\mathrm{Sin}[2^r x(j-1)]}{1+\mathrm{Sin}[2^r x(j-1)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(j-1)]\mathrm{Sin}[2^r x(j-1)]}{1+\mathrm{Sin}[2^r x(j-1)]^2}\right]^2} - x(j-1) \right),$$

$$y(n) = y(0) + \frac{1}{\Gamma(\alpha)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\alpha)}{\Gamma(n-j+1)} \times \left(\frac{2\sqrt{2}\mathrm{Cos}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]^2} - y(j-1) \right), \quad (4)$$

and (5), as shown at the bottom of this page, which can be considered as two interval extension of the map (3). In spite of being mathematically equivalent, the restrictions of floating point representation implies that two pseudo orbits emanate from systems (4) and (5) will diverge exponentially. For a review on analysis of interval extensions and the lower bound error theorem, see Refs [74], [75].

2) Compute the following three image-dependent perturbation values

$$c_t = \frac{\mu}{(h \times v)^2} \sum_{i=1}^{h} \sum_{j=1}^{v} P_t(i,j),$$

where $t = r, g, b$ and μ is an arbitrary real number.

3) The reading T of internal clock in transmitter part is used to further update the values of c_t such that

$$\hat{c}_t = c_t + \varepsilon(T+1),$$

where $\varepsilon \ll 1$ has an arbitrary random value. The value of ε is selected randomly for each new encryption session.

4) Update the values of parameters and initial conditions as follows, where hat is omitted for brevity

$$r = r_0 + c_r, \quad \alpha = \alpha_0 + c_b, \; x_0 = x_{init} + c_b,$$
$$y_0 = y_{init} + c_g.$$

5) Using the updated values of parameters and initial conditions, simulate the two systems (4) and (5), which represent two natural interval extensions of original new map, such that each system is iterated $3 \times h + h \times v$ times for state variable x and $3 \times v + h \times v$ times for state variable y. Note that a sufficient initial transient number of iterations, say q iterations, should be discarded firstly so as to neglect any transient dynamics.

6) The perturbation values denoted by $\{p_1, p_2, \ldots, p_m\}$ are added to the output time series by the following way: For $n = 1 : 1000$ $X_{n,1} = x_{n,1} + p_1$, $Y_{n,1} = y_{n,1} + p_1$, $X_{n,2} = x_{n,2} + p_1$, $Y_{n,2} = y_{n,2} + p_1$, For $n = 1001 : 2000$ $X_{n,1} = x_{n,1} + p_2$, $Y_{n,1} = y_{n,1} + p_2$, $X_{n,2} = x_{n,2} + p_2$, $Y_{n,2} = y_{n,2} + p_2$, and so on.

7) The module one operation is applied to the perturbed time series such that

$$X_{n,1} = mod\left(X_{n,1}, 1\right), \quad Y_{n,1} = mod\left(Y_{n,1}, 1\right),$$
$$X_{n,2} = mod\left(X_{n,2}, 1\right),$$
$$Y_{n,2} = mod\left(Y_{n,2}, 1\right).$$

8) The lower bound error for each state variable is then evaluated by

$$(e_{lx})_i = \frac{X_{i,1} - X_{i,2}}{2}, \quad (e_{ly})_i = \frac{Y_{i,1} - Y_{i,2}}{2}.$$

Figure 6 shows examples for lower bound errors obtained for different values of r.

Therefore, the minimum values of e_{lx} and e_{ly} series are found and used to compute the following two encrypting sequences

For the first $3h$ values of e_{lx}:

$$Enc_x = mod\left(IntegerPart\left[\frac{e_{lx}}{\min(e_{lx})} \times 10^{15}\right], h\right).$$

For the first $3v$ values of e_{ly}:

$$Enc_y = mod\left(IntegerPart\left[\frac{e_{ly}}{\min(e_{ly})} \times 10^{15}\right], v\right).$$

For the remaining values of e_{lx} and e_{ly}

$$Enc_x = mod\left(IntegerPart\left[\frac{e_{lx}}{\min(e_{lx})} \times 10^{15}\right], 256\right),$$
$$Enc_y = mod\left(IntegerPart\left[\frac{e_{ly}}{\min(e_{ly})} \times 10^{15}\right], 256\right).$$

$$x(n) = x(0) + \left(\frac{1}{\Gamma(\alpha)} \sum_{j=1}^{n} \frac{2\sqrt{2}\Gamma(n-j+\alpha)}{\Gamma(n-j+1)} \times \frac{\mathrm{Cos}\left[\frac{2^r\mathrm{Cos}[2^r x(j-1)]\mathrm{Sin}[2^r x(j-1)]}{1+\mathrm{Sin}[2^r x(j-1)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^{\frac{3}{2}+r}\mathrm{Cos}[2^r x(j-1)]\mathrm{Sin}[2^r x(j-1)]}{1+\mathrm{Sin}[2^r x(j-1)]^2}\right]^2} - \frac{1}{\Gamma(\alpha)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\alpha)}{\Gamma(n-j+1)} \times x(j-1) \right),$$

$$y(n) = y(0) + \left(\frac{1}{\Gamma(\alpha)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\alpha)}{\Gamma(n-j+1)} \times \frac{\mathrm{Cos}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]}{1+\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]^2} \times \frac{\mathrm{Sin}\left[\frac{2^r\mathrm{Cos}[2^r y(j-1)]}{1+\mathrm{Sin}[2^r y(j-1)]^2}\right]}{1/2\sqrt{2}} - \frac{1}{\Gamma(\alpha)} \sum_{j=1}^{n} \frac{\Gamma(n-j+\alpha)}{\Gamma(n-j+1)} \times y(j-1) \right) \quad (5)$$

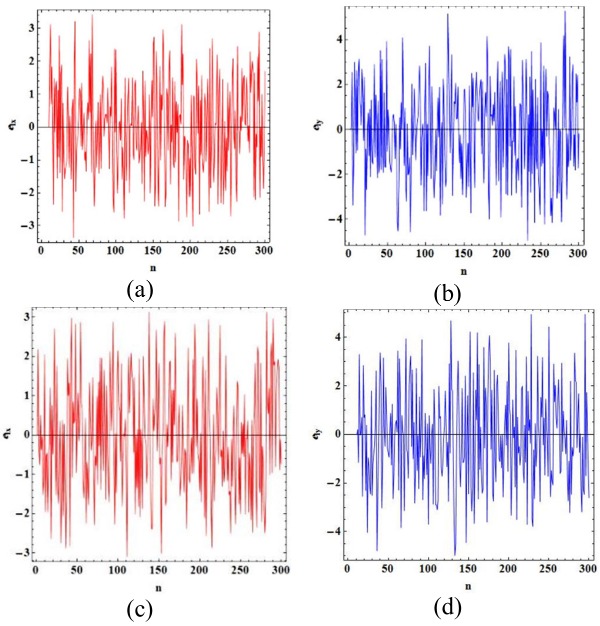


FIGURE 6. Lower bound errors of state variables x and y of system (2) obtained when (a,b) $r = 12$ and (c,d) $r = 19$.

9) The average chaotic time series can be calculated from the following equation

$$Enc_{av} = mod\left(IntegerPart\left[\frac{X_1 + X_2 + Y_1 + Y_2}{4} \times 10^{15}\right], 256\right).$$

10) The first $3h$ components of Enc_x and the first $3v$ components of Enc_y are separated and arranged in an ascending order, after deleting any possible repeating values, to form the following six confusion vectors: $S_R^r = Enc_x(1:h)$, $S_G^r = Enc_x(h+1:2h)$, $S_B^r = Enc_x(2h+1:3h)$, $S_R^c = Enc_y(1:v)$, $S_G^c = Enc_y(v+1:2v)$, and $S_B^c = Enc_y(2v+1:3v)$.
11) The rows of plain image pixel matrix are scrambled in the way that red component values of pixels are permuted according to S_R^r whereas green and blue components follow S_G^r and S_B^r orders, respectively. Similarly, the columns of plain image pixel matrix are scrambled by using S_t^c, $t = R, G, B$.
12) The permuted plain image is reshaped in a new formed three vectors such that each of which has length of $h \times v$ elements corresponding to pixel intensity of a specific colour e.g. red or green or blue.
13) The bitwise XOR operations between the aforementioned three vectors, namely, V_R, V_G and V_B, and three encrypting sequence Enc_x, Enc_y and Enc_{av} are carried out in order to obtain the three ciphered components of encrypted image i.e.

$$(V_R)_{enc} = V_R \oplus Enc_x, \quad (V_G)_{enc} = V_G \oplus Enc_y,$$
$$\text{and } (V_B)_{enc} = V_B \oplus Enc_{av}.$$

14) The transmitted side publishes $[k_s]G$ whereas the receiver side publishes $[k_R]G$. Subsequently, the two sides agree on a shared symmetric key $[k_s]([k_R]G) = [k_R]([k_s]G)$. This is known as Diffie-Hellman analogy of elliptic curve key exchange.
15) The three image-dependent perturbation values c_t in addition to preselected m perturbation values and integer number μ are ciphered using the agreed symmetric key. In particular, El-Gamal scheme for encryption with elliptic curve can be efficiently employed [76].
16) Utilizing the shared secret keys, identical chaotic maps and the same setting for precision of numerical representation at receiver side, the three encrypting sequence Enc_x, Enc_y and Enc_{av} can be regenerated successfully.
17) The transmitted three ciphered vectors are decrypted at receiver side via repeating the bitwise XOR operations of step (10) but with the encrypted vectors.
18) Finally, the plain image can be recovered by reshaping the deciphered vectors into original matrix associated with the plain image.

V. NUMERICAL RESULTS AND SECURITY PERFORMANCE

In this part, the proposed chaotic pseudo-orbit-based encryption algorithm is applied to some samples of colored images. The robustness of the presented scheme against main possible types of attacks, such as statistical attacks, differential attacks, and brute-force attacks, is examined.

Numerical simulations are carried out for $r = 20$, $\alpha = 0.95$, $\mu = 0.1100587139$, and the other perturbation values are selected randomly from the interval (0,1). Using Intel Core i7-8550U CPU @ 1.8GHz and 16 GB RAM, the execution times of the proposed encryption algorithm for 256×256 and 512×512 colored images are 292 ms and 1.2 s, respectively. Figure 7 (a) shows the original plain baboon image, encrypted baboon image and decrypted baboon image. The image histograms for separate red, green and blue components within the pixels of each image are depicted in Fig.7 (b). Similarly, Fig.8 and Fig.9 depict the results of encryption scheme when it is applied to pepper and Egyptian pyramids images. From these figures, it is seen that distribution of pixels intensities in cipher images is flat and makes uniform distribution which makes the cipher images invulnerable to statistical attacks.

The variance of histogram is employed to quantify the uniformity of ciphered images. In particular, the lower value of variances indicates the higher uniformity of ciphered images [77]. The variance of histogram is defined for red, green and blue, respectively colors by [77]:

$$\sigma_R = \frac{1}{2 \times 256^2} \sum_{i=1}^{256} \sum_{j=1}^{256} (H_i^R - H_j^R)^2,$$
$$\sigma_G = \frac{1}{2 \times 256^2} \sum_{i=1}^{256} \sum_{j=1}^{256} (H_i^G - H_j^G)^2,$$
$$\sigma_B = \frac{1}{2 \times 256^2} \sum_{i=1}^{256} \sum_{j=1}^{256} (H_i^B - H_j^B)^2,$$

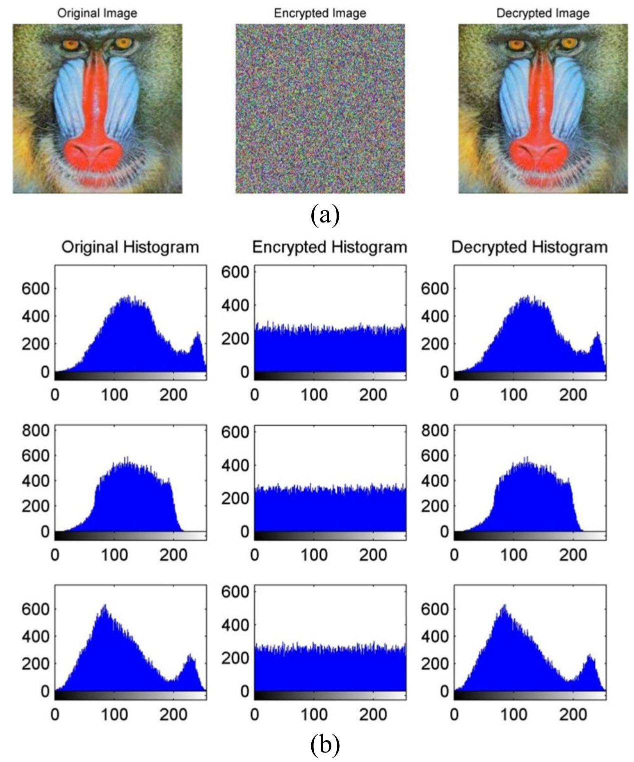


FIGURE 7. The original, encrypted and decrypted baboon images are presented in (a) while their associated image histograms for each color component are shown in (b) such that the top, middle and bottom rows are corresponding to red, green and blue components, respectively.

TABLE 1. The variance of histogram values.

Image	σ_R	σ_G	σ_B
Plain Baboon Cipher Baboon	2.93×10^4 287.945	1.051×10^5 289.55	2.681×10^5 287.289
Plain Pepper Cipher Pepper	4.766×10^4 215.469	3.994×10^4 309.566	2.332×10^5 234.266
Plain Pyramids Cipher Pyramids	3.06×10^4 296.882	1.599×10^5 202.273	2.602×10^5 265.251

where H_i^S denotes number of pixels having i values for color component S such that $S = G, B, R$. Table 1 shows the variance of histogram values for each image and each color component.

A. SECRET KEYS ANALYSIS

The proposed novel encryption scheme has two initial conditions, two interior chaotic system parameters, i.e. r and α, three plain image dependent perturbation values and sixty five perturbation values for generated time series (for the case of 256×256 size images). Assuming that the double-precision binary floating-point IEEE 754 format is employed. Hence, the key space size of our scheme is equal to 2^{3816} excluding the parameters related to elliptic curve key exchange step. It is known that the minimum key space necessary to resist brute-force attacks is 2^{100} [78], [79]. Thus, the proposed encryption scheme has a sufficiently very large key space to render any brute force attack useless.

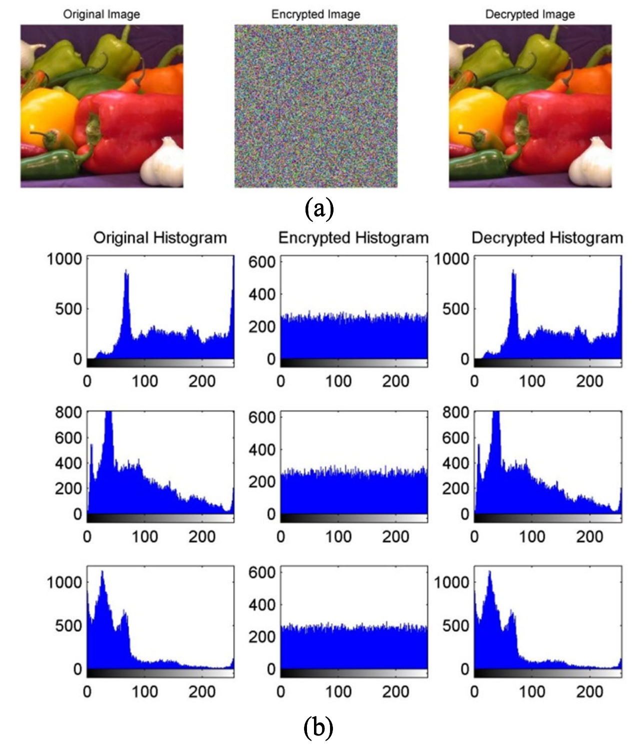


FIGURE 8. Similar to Fig.7 but for pepper image.

B. CORRELATION ANALYSIS

The tiny values for correlation coefficients in cipher images, between neighboring pixels in all directions i.e. in horizontal, vertical and diagonal directions, are necessary for a good encryption system so as to resist statistical attacks. Given two vectors x and y of specific color component in adjacent pixels, then the correlation coefficient ρ_{xy} corresponding to them is computed from the following as follows:

$$\rho_{xy} = \frac{Cov(x, y)}{D_x D_y},$$
$$E_x = \frac{1}{N}\sum\nolimits_{i=1}^{N} x_i, \quad D_x = \frac{1}{N}\sum\nolimits_{i=1}^{N} (x_i - E(X))^2,$$
$$Cov(x, y) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)),$$

where x_i and y_i are the color values of selected two neighboring pixels in the image. More specifically, a random sample of 1000 pairs of adjacent pixels is considered for each of red, green and blue color components in both of plain and cipher images.

Figure 10 depicts the correlations of adjacent pixels in original and encrypted images. Moreover, Table 2 shows the values of correlation coefficients of plain and cipher images

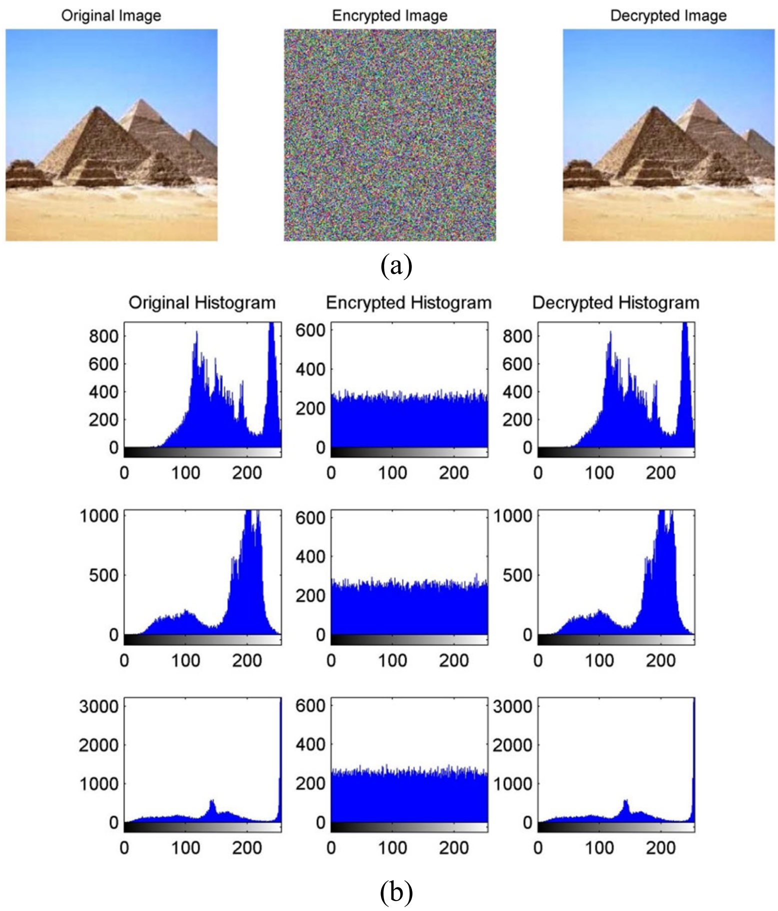


FIGURE 9. Similar to Fig.8 but for Egyptian pyramids image.

where it indicates the suppression made in values of coefficients of correlation in cipher images.

C. KEY SENSITIVITY ANALYSIS

The high sensitive to teeny alternations in the secret keys is another major requirement for an efficient encryption scheme. By adding a perturbation value of 10^{-14} to one of secret keys of our cryptosystem and then employing the generated chaotic pseudo orbit to decrypt the cipher image, the sensitivity to mismatch in parameters can be examined. For example, the value of r is increased by 10^{-14} and the decrypted baboon, pepper and pyramids images are illustrated in Fig.11. It is obvious that the slight difference in r cannot successfully decrypt the cipher images and also similar conclusions are acquired regarding other secret keys in the system.

It is crucial to quantify the sensitivity to mismatch in parameters [80]. Table 3 illustrates the original value of one of the secret keys which is used in encryption process, the percentage of relative error or mismatch in secret key's value used for decryption, and the percentage of difference between the resulting two deciphered images for each color component value.

D. INFORMATION ENTROPY ANALYSIS

The information entropy is considered as a measure for amount of randomness and uncertainty in cipher image. In particular, the higher value of information entropy of an encrypted image the high randomness it has. The entropy in bits for an input source of information is defined as [81]

$$H(m) = -\sum_{i=0}^{2^N-1} p(m_i) log_2 p(m_i)$$

where m is the input variable and $p_{(m_i)}$ denotes the probability of symbol m_i. The optimum value of information entropy in a given cipher image is to be very near to eight. The values of information entropy of the cipher-images which result from our encryption scheme are illustrated in Table 4 where it is obvious that these values are very close to 8 which emphasizes the reliability of the suggested scheme.

E. DIFFERENTIAL ATTACK ANALYSIS

Effective image cryptosystem must be also very sensitive to very small and negligible variations in plain image as well as secret keys of the scheme. This means that any tiny perturbations applied to the input plain image produce a significant change in the output cipher image and thus the encryption technique is more robust to possible differential attacks.

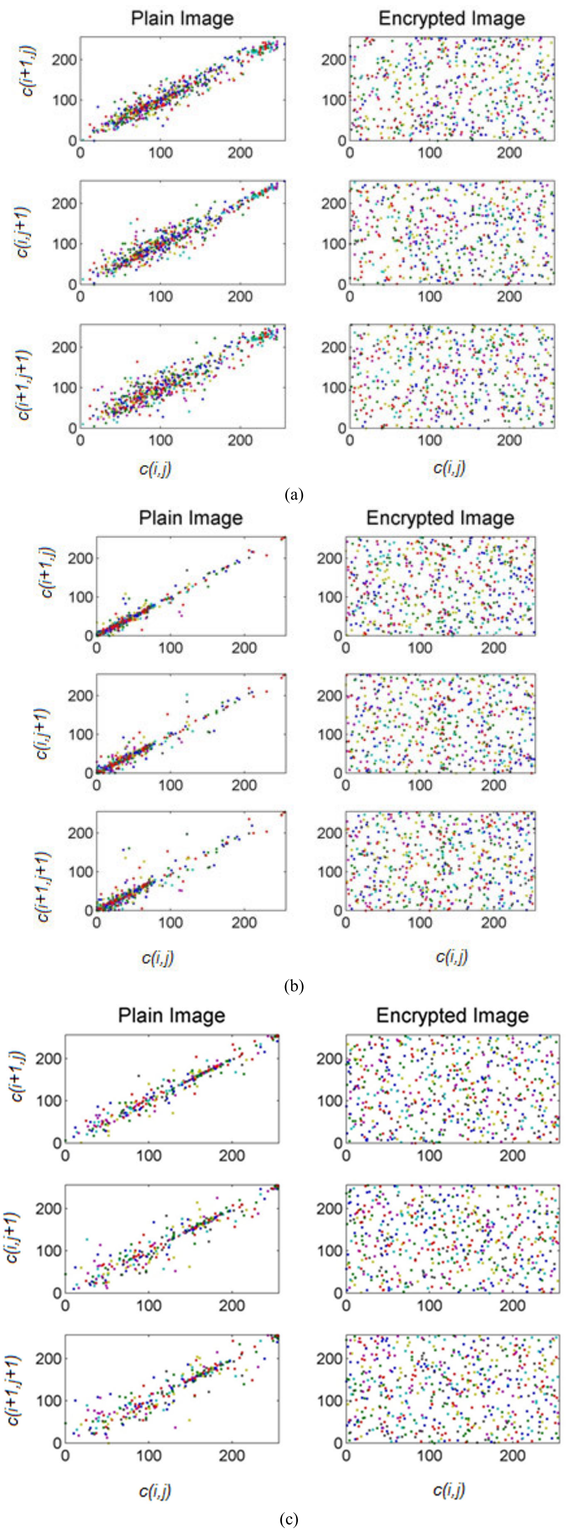


FIGURE 10. Correlation between adjacent pixels in horizontal (first row), vertical (second row) and diagonal (third row) directions for (a) baboon image, (b) pepper image and (c) pyramids image. The left column is associated to plain images while the right column is associated to cipher images.

TABLE 2. Correlation coefficients of plain and ciphered images for each color component.

Image	Correlation Coefficients (Red color)		
	H	V	D
Baboon	0.9608, 0.0018	0.9479 0.0047	0.9243 0.00167
Pepper	0.9917 0.0038	0.9875 0.0012	0.9788 0.00156
Pyramids	0.9803 0.0049	0.9596 0.00296	0.9503 0.0065

Image	Correlation Coefficients (Green color)		
	H	V	D
Baboon	0.9372 0.00452	0.9162 0.0087	0.8795 0.00424
Pepper	0.9871 0.0057	0.9821 0.0079	0.9663 0.00522
Pyramids	0.9802 0.00419	0.9601 0.0060	0.9501 0.00632

Image	Correlation Coefficients (Blue color)		
	H	V	D
Baboon	0.9640 0.00770	0.9543 0.00207	0.9326 0.00114
Pepper	0.9799	0.9711	0.9459
	0.00536	0.00213	0.00697
Pyramids	0.9907 0.0034	0.9815 0.00371	0.9768 0.0010

TABLE 3. Quantification of sensitivity to mismatch in parameters.

Image	Secret key	Mismatch (%)	Difference (%)
Baboon	$r = 20$	0.00001	G: 99.63 R:99.62 B: 99.66
Baboon	$x_0 = 0.5$	0.00001	G: 99.64 R:99.63 B:99.66
Baboon	$y_0 = 0.5$	0.00001	G:99.64 R:99.61 B:99.67
Pepper	$r = 20$	0.00001	G: 99.65 R: 99.63 B: 99.66
Pepper	$x_0 = 0.5$	0.00001	G: 99.61 R: 99.68 B: 99.65
Pepper	$y_0 = 0.5$	0.00001	G: 99.61 R: 99.67 B: 99.60
Pyramids	$r = 20$	0.00001	G: 99.59 R: 99.57 B: 99.52
Pyramids	$x_0 = 0.5$	0.00001	G: 99.66 R: 99.65 B: 99.68
Pyramids	$y_0 = 0.5$	0.00001	G: 99.63 R: 99.68 B: 99.66

Two well-known quantities are utilized to quantify the sensitivity to changes in the original image. The first one is the number of pixels change rate (NPCR) which can be defined as the percentage of different pixels between two cipher images when their original images differ in one pixel only. The unified average changing intensity (UACI) is the second

TABLE 4. Information entropy in encrypted images.

Image	Information entropy (Red-Green-Blue)		
Baboon	7.9968	7.9976	7.9967
Pepper	7.9968	7.9966	7.9978
Pyramids	7.9972	7.9973	7.9975

TABLE 5. NPCR and UACI for baboon, pepper and pyramids cipher images.

Image	NPCR (%)	UACI (%)
Baboon	99.6368 99.6170 99.6241	33.5321 33.5252 33.5275
Pepper	99.6536 99.6170 99.6307	33.4601 33.4826 33.5002
Pyramids	99.6367 99.6298 99.6322	33.4574 33.4571 33.4576

quantity which evaluates the average differences intensity between two cipher images for only one pixel change in their corresponding original images.

Suppose that C_1 and C_2 are two cipher images associated with two plain images which have only one pixel difference. Let $C_1(i,j)$ and $C_2(i,j)$ denote the values of one of color components in pixel at position (i,j) of the two images C_1 and C_2, respectively. Thus, the NPCR is defined by [82]

$$NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} D(i,j)}{M * N} \times 100\%,$$

where $D(i,j)$ is an array of the same size as the cipher image but with the next components

$$D(i,j) = \begin{cases} 1 & \text{if } C_1(i,j) \neq C_2(i,j) \\ 0 & \text{if } C_1(i,j) = C_2(i,j). \end{cases}$$

The second test, i.e. UACI, is defined as

$$\text{UACI} = \frac{1}{M \times N} \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} |C_1(i,j) - C_2(i,j)|}{2^n - 1} \times 100\%.$$

Table 5 gives the values of NPCR and UACI when one pixel value difference between two plain images, in one color component, is applied. The three consecutive values correspond to red, green and blue color components.

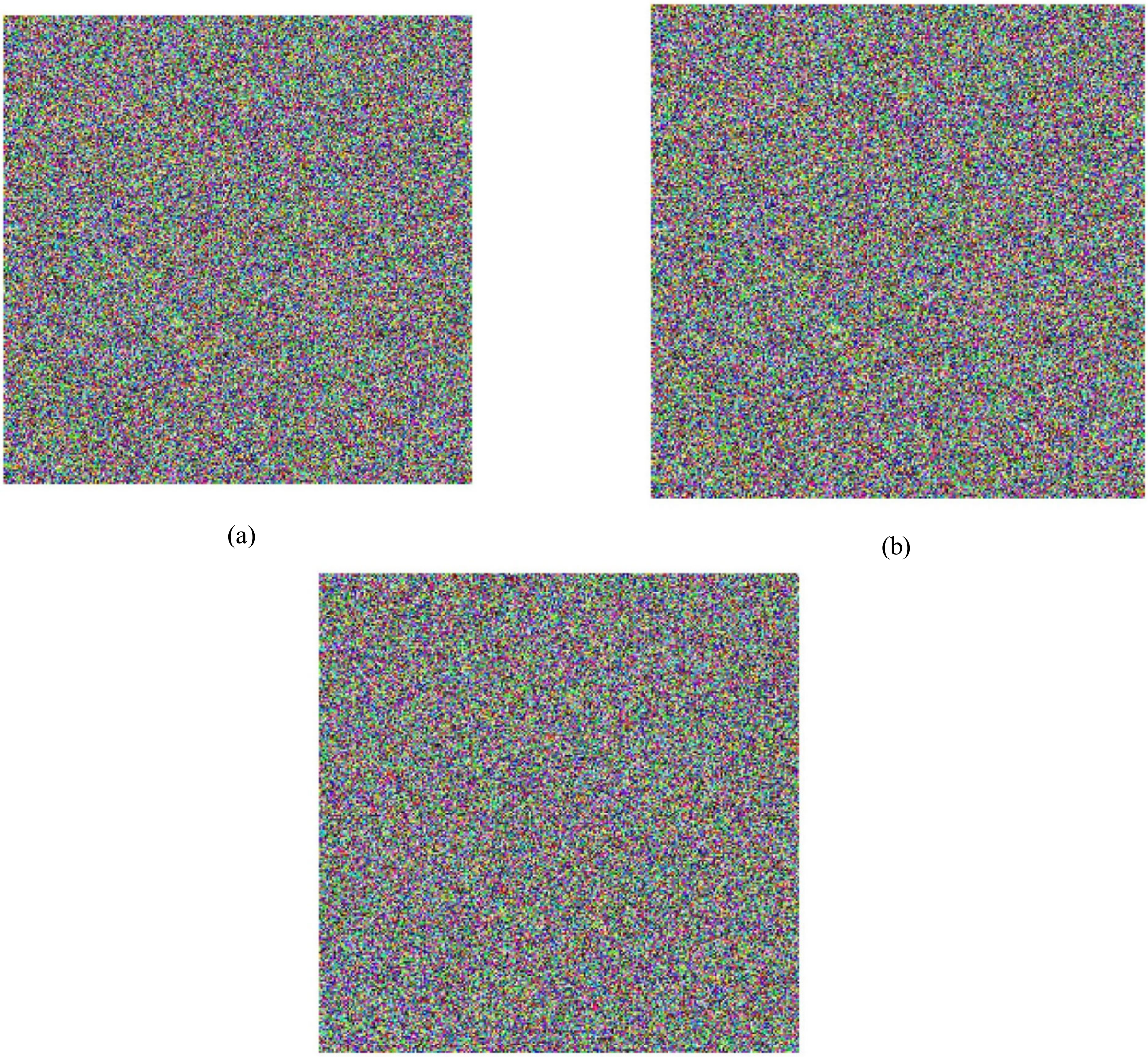
F. RESISTANCE AGAINST OTHER ATTACKS

According to Kerckhoff's principle [83], we assume that any potential eavesdropper knows the design and detailed steps of encryption process in the present encryption scheme, not including the values of secret keys. Hence, the cryptanalyst can apply one of the basic four attacks, namely, ciphertext only, known plaintext, chosen plaintext and chosen ciphertext attacks. In particular, in chosen plaintext attack, the attacker can secretly get a temporary access to the encryption machine whereas in chosen ciphertext attack, he is able to get temporary access to decryption machine. It is known that if the proposed encryption system is immune to the powerful chosen plaintext/ciphertext attacks, then it can resist the other two types [24], [84].

The proposed hybrid scheme process involves calculations of plain image-dependent parameters, time dependent parameters, acquirement of pseudo chaotic perturbing values, elliptic curve key exchange, shuffling of pixels position and bit-XORing of pixels values. The secret keys of the system control and determine the output of each stage of encryption so that the encryption process is highly sensitive to these values. The first crucial point here is that some statistical features are extracted from plain image in order to update the secret keys of the algorithm. This implies that different cipher images are produced for different plain images even if tiny differences occur among plain images. The values of UACI and NPCR confirm this fact. Furthermore, supplying the same image to the encryption machine at different times will generate different cipher images since the secret keys depend on the time moment when the plain image is supplied to transmitter. In other words, the values of secret keys are not fixed but they are time varying and also plain image-dependent. Moreover, the permutation and diffusion stages are not depending explicitly on the output of one chaos generator system but rely on the lower bound error between outputs of two interval extensions. As a result, the proposed hybrid technique can resist known-plaintext and chosen-plaintext attacks [24], [84].

Regarding to the above discussion, it is crucial to note that if the attacker gets the values of some plain-pixels and their corresponding cipher-pixels, i.e. via applying known-plaintext attack, he cannot attain any further information regarding the values of secret keys. Indeed, both of the time varying secret keys and pseudo chaotic sequences confirm this result even if all values of pixels in the plain image are set to zeros, or any pre-specified values, which may cause a degenerate security performance in other encryption systems, see [85]–[87]. Similarly, if the attacker utilizes chosen-ciphertext attack to provide some special forms of cipher images, such as zero cipher images, to decryption machine, it obvious that he will not able to achieve his goal due to aforementioned reasons too.

Finally, the opponent may try to reveal the values of secret keys via employing one of Baby Step, Giant Step attack or Pollard's Rho attack, rather than conventional naive attack, to overcome elliptic curve key exchange procedure [88]–[90]. Nevertheless, it is practically impossible for the attacker to fulfill his aim. The reason is that although the aforementioned attacks reduce the computational cost of integer factorization or discrete logarithmic problem, it still requires approximately $\sqrt{C_{EC}}$ operations for attacking scheme to solve this problem, where C_{EC} is the size of cyclic group of EC over a finite field. For the proposed hybrid encryption scheme, $\sqrt{C_{EC}} = 7.9228 \times 10^{28}$. In other words, it takes more than



(a) (b) (c)

FIGURE 11. Decrypted baboon, pepper and pyramids images for mismatch in parameter *r* in (a), (b) and (c), respectively.

10^{14} years to accomplish this task using Intel Core i7-8550U CPU @ 1.8GHz and 16 GB RAM.

Finally, the proposed chaos-based public key image encryption has featured several advantages over other conventional symmetric-key image cipher, whose key has been exchanged through another public-key cryptosystem such as RSA. Firstly, compared to RSA, DH, and El-Gamal, the elliptic curve scheme considerably reduces adequate length of secret keys required for top secret documents [76] as shown in the Table 6. This implies that elliptic curve-based scheme has low computations' complexity, high performance and low capacity requirements. Secondly, the proposed scheme can be further improved in future work to involve supersingular isogeny elliptic curve key exchange and therefore establish a powerful a post-quantum cryptographic algorithm that can resist quantum algorithms running on quantum computers.

TABLE 6. Recommendations for Secret key lengths.

Key Performance	RSA (bits)	DH/ Elgamal (bits)	EC (bits)
Provides absolutely minimum security	1776	1776	192
Guarantees minimum security	2432	2432	224
Adequate except top secret plain-data	3248	3248	256
Adequate for top secret plain-data	15424	15424	512

Thirdly, the proposed scheme also utilizes the enhanced statistical features of noise-like pseudo chaotic orbits by adopting finite precision errors and it efficiently employs time varying and plain image dependent secret keys.

TABLE 7. Comparisons with some recent state-of-the-art chaos-based image encryption schemes.

Paper	MLE	Entropy	UACI	NPCR	MCC	Key Space	ECKE
Present work (2 rounds)	**Up to: 59**	**7.997**	**99.79**	**33.47**	**0.0087**	2^{3816}	**Yes**
Ref. [91] (2 rounds)	**2**	**7.903**	**99.81**	**33.48**	**0.0191**	**N.A.**	**No**
Ref. [92]	**2**	**7.997**	**99.61**	**33.42**	**0.0131**	**N.A.**	**No**
Ref. [93]	**N.A.**	**7.991**	**99.61**	**33.45**	**0.0082**	2^{187}	**No**
Ref. [94]	**6.756**	**7.998**	**99.61**	**33.40**	**0.0143**	**N.A.**	**No**

VI. DISCUSSION AND CONCLUSION

A reliable framework to design a superior hybrid encryption system with enhanced characteristics is proposed. The first advantage of the encryption system is its dependence on a novel 2D fractional discrete chaotic map with large value of positive Lyapunov exponents which extend over wide range of parameters. Compared with conventional 2D maps that were employed in similar schemes, the proposed map has distinguished preferable characteristics including the coexistence of multiple chaotic attractors and positive values of Lyapunov exponent greater than 30. The presented scheme has also the advantages of indirectly implementing chaotic time series in encryption process. In particular, the pseudo orbits which are obtained from any two interval extension of the proposed chaotic map are utilized in order to increase complexity of encryption process with relatively low computational cost.

Furthermore, the proposed encryption technique adopts robust elliptic curve key exchange with recommended arguments of NIST to achieve efficient secure transmission of secret keys between sender and receiver sides. Also, the generations of noise-like encrypting signal is made highly dependent on moment of transmission and on any perturbations occur in information message. To best of authors' knowledge, this is the first attempt to design encryption scheme that incorporates chaotic pseudo orbits and elliptic curve key exchange. Numerical simulations are accomplished on different colored images and confirm the efficiency of suggested hybrid scheme against possible statistical, brute-force, chosen plaintext/ciphertext attacks and differential attacks.

Finally, comparisons with key results of some recent state-of-the-art chaos-based image encryption schemes are summarized in in the Table 7. Here, MCC denotes maximum correlation coefficients found in cipher pepper and baboon images while the mean values of other security measurements for three color components are given in the table. It is obvious that the proposed encryption scheme has comparable performance results but with distinguished large value of MLE and more extended key space.

The future work can involve adopting high dimensional chaotic maps in single or in network configurations. Also, the very fast and ultra wide-band chaotic laser systems can be employed in similar yet more efficient hybrid schemes combining supersingular isogeny elliptic curve key exchange and thus establishing a powerful a post-quantum cryptographic algorithm that can resist quantum algorithms running on quantum computers.

ACKNOWLEDGMENT

The authors would like to thank anonymous Reviewers and Editor for handling this article and providing their helpful comments which significantly improved the scientific contents, readability, and clarity of the work.

REFERENCES

[1] F.-Y. Lin and J.-M. Liu, "Chaotic radar using nonlinear laser dynamics," *IEEE J. Quantum Electron.*, vol. 40, no. 6, pp. 815–820, Jun. 2004.
[2] F.-Y. Lin and J.-M. Liu, "Chaotic lidar," *IEEE J. Quantum Electron*, vol. 10, no. 5, pp. 991–997, Sep./Oct. 2004.
[3] V. Annovazzi-Lodi, G. Aromataris, and M. Benedetti, "Multi-user private transmission with chaotic lasers," *IEEE J. Quantum Electron.*, vol. 48, no. 8, pp. 1095–1101, Aug. 2012.
[4] T. Deng, G. Q. Xia, and Z. M. Wu, "Broadband chaos synchronization and communication based on mutually coupled VCSELs subject to a bandwidth-enhanced chaotic signal injection," *Nonlinear Dyn.*, vol. 76, no. 1, pp. 399–407, Apr. 2014.
[5] Z. Kang, J. Sun, L. Ma, Y. Qi, and S. Jian, "Multimode synchronization of chaotic semiconductor ring laser and its potential in chaos communication," *IEEE J. Quantum Electron.*, vol. 50, no. 3, pp. 148–157, Mar. 2014.
[6] A. Uchida, K. Amano, M. Inoue, K. Hirano, S. Naito, H. Someya, I. Oowada, T. Kurashige, M. Shiki, S. Yoshimori, K. Yoshimura, and P. Davis, "Fast physical random bit generation with chaotic semiconductor lasers," *Nature Photon.*, vol. 2, no. 12, pp. 728–732, Dec. 2008.
[7] Y. Akizawa, "Fast Random Number Generation With Bandwidth-Enhanced Chaotic Semiconductor Lasers at 8 × 50 Gb/s," *IEEE Photon. Technol. Lett.*, vol. 24, no. 12, pp. 1042–1044, Jun. 2012.
[8] R. Sakuraba, K. Iwakawa, K. Kanno, and A. Uchida, "Tb/s physical random bit generation with bandwidth-enhanced chaos in three-cascaded semiconductor lasers," *Opt. Express*, vol. 23, no. 2, pp. 1470–1490, Jan. 2015.
[9] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "Numerical analysis of ultrafast physical random number generator using dual-channel optical chaos," *Opt. Eng.*, vol. 55, no. 9, Sep. 2016, Art. no. 094105.
[10] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "Simultaneous suppression of time-delay signature in intensity and phase of dual-channel chaos communication," *IEEE J. Quantum Electron.*, vol. 51, no. 9, pp. 1–9, Sep. 2015.
[11] Z. Hua, Y. Zhou, C.-M. Pun, and C. L. P. Chen, "2D sine logistic modulation map for image encryption," *Inf. Sci.*, vol. 297, pp. 80–94, Mar. 2015.
[12] 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.
[13] L. Chen, B. Ma, X. Zhao, and S. Wang, "Differential cryptanalysis of a novel image encryption algorithm based on chaos and line map," *Nonlinear Dyn.*, vol. 87, no. 3, pp. 1797–1807, Feb. 2017.
[14] Y. Li, C. Wang, and H. Chen, "A hyper-chaos-based image encryption algorithm using pixel-level permutation and bit-level permutation," *Opt. Lasers Eng.*, vol. 90, pp. 238–246, Mar. 2017.
[15] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new beta chaotic maps," *Opt. Lasers Eng.*, vol. 96, pp. 39–49, Sep. 2017.
[16] A. A. Elsadany, A. M. Yousef, and A. Elsonbaty, "Further analytical bifurcation analysis and applications of coupled logistic maps," *Appl. Math. Comput.*, vol. 338, pp. 314–336, Dec. 2018.
[17] Z. Liu and T. Xia, "Novel two dimensional fractional-order discrete chaotic map and its application to image encryption," *Appl. Comput. Informat.*, vol. 14, no. 2, pp. 177–185, Jul. 2018.

[18] W. Zhang, C. Zhang, C. Chen, and K. Qiu, "Experimental demonstration of security-enhanced OFDMA-PON using chaotic constellation transformation and pilot-aided secure key agreement," *J. Lightw. Technol.*, vol. 35, no. 9, pp. 1524–1530, May 1, 2017.

[19] T. Wu, C. Zhang, H. Wei, and K. Qiu, "PAPR and security in OFDM-PON via optimum block dividing with dynamic key and 2D-LASM," *Opt. Express*, vol. 27, no. 20, pp. 27946–27960, Sep. 2019.

[20] T. Wu, C. Zhang, C. Chen, H. Hou, H. Wei, S. Hu, and K. Qiu, "Security enhancement for OFDM-PON using Brownian motion and chaos in cell," *Opt. Express*, vol. 26, no. 18, p. 22857, Sep. 2018.

[21] C. Zhang, W. Zhang, C. Chen, X. He, and K. Qiu, "Physical-enhanced secure strategy for OFDMA-PON using chaos and deoxyribonucleic acid encoding," *J. Lightw. Technol.*, vol. 36, no. 9, pp. 1706–1712, May 1, 2018.

[22] Z. Lin, G. Wang, X. Wang, S. Yu, and J. Lü, "Security performance analysis of a chaotic stream cipher," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1003–1017, Oct. 2018.

[23] A. Elsonbaty, S. F. Hegazy, and S. S. A. Obayya, "Simultaneous concealment of time delay signature in chaotic nanolaser with hybrid feedback," *Opt. Lasers Eng.*, vol. 107, pp. 342–351, Aug. 2018.

[24] G. Ye, C. Pan, X. Huang, and Q. Mei, "An efficient pixel-level chaotic image encryption algorithm," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 745–756, Oct. 2018.

[25] S. F. Hegazy and S. S. A. Obayya, "Tunable spatial–spectral phase compensation of type-I (ooe) hyperentangled photons," *J. Opt. Soc. Amer. B, Opt. Phys.*, vol. 32, no. 3, pp. 445–450, 2015.

[26] S. F. Hegazy, S. S. A. Obayya, and B. E. A. Saleh, "Orthogonal quasi-phase-matched superlattice for generation of hyperentangled photons," *Sci. Rep.*, vol. 7, no. 1, p. 4169, Dec. 2017.

[27] S. F. Hegazy, Y. A. Badr, and S. S. A. Obayya, "Relative-phase and time-delay maps all over the emission cone of hyperentangled photon source," *Opt. Eng.*, vol. 56, no. 2, Feb. 2017, Art. no. 026114.

[28] X. Wang, L. Liu, and Y. Zhang, "A novel chaotic block image encryption algorithm based on dynamic random growth technique," *Opt. Lasers Eng.*, vol. 66, pp. 10–18, Mar. 2015.

[29] X. Wanga, L. Feng, and H. Zhao, "Fast image encryption algorithm based on parallel computing system," *Inf. Sci.*, vol. 486, pp. 340–358, Jun. 2019.

[30] 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.

[31] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.

[32] D. Hankerson, A. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography*. New York, NY, USA: Springer-Verlag, 2004.

[33] A. A. Abd 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, Feb. 2013.

[34] D. S. Laiphrakpam and M. S. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field," *Multimedia Tools Appl.*, vol. 77, no. 7, pp. 8629–8652, Apr. 2018.

[35] S. Li, G. Chen, and X. Mou, "On the dynamical degradation of digital piecewise linear chaotic maps," *Int. J. Bifurcation Chaos*, vol. 15, no. 10, pp. 3119–3151, Oct. 2005.

[36] L.-C. Cao, Y.-L. Luo, S.-H. Qiu, and J.-X. Liu, "A perturbation method to the tent map based on Lyapunov exponent and its application," *Chin. Phys. B*, vol. 24, no. 10, Oct. 2015, Art. no. 100501.

[37] C. Li, T. Xie, Q. Liu, and G. Cheng, "Cryptanalyzing image encryption using chaotic logistic map," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 1545–1551, Oct. 2014.

[38] K. S. Miller and B. Ross, *An Introduction to the Fractional Calculus and Fractional Differential Equations*. New York, NY, USA: Wiley, 1993.

[39] E. Ahmed and A. Hashish, "On modelling the immune system as a complex system," *Theory Biosci.*, vol. 124, nos. 3–4, pp. 413–418, Mar. 2006.

[40] Y. Zhou, K. Panetta, and S. Agaian, "Image encryption using binary key-images," in *Proc. IEEE Int. Conf. Syst., Man Cybern.*, Oct. 2009, pp. 4569–4574.

[41] Y. Zhou, K. Panetta, and S. Agaian, "Image encryption based on edge information," *Int. Soc. Opt. Photon.*, vol. 7256, Jan. 2009, Art. no. 725603.

[42] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft Comput.*, vol. 12, no. 5, pp. 1457–1466, May 2012.

[43] Y. Zhou, K. Panetta, S. Agaian, and C. L. P. Chen, "(n, k, p)-Gray code for image systems," *IEEE Trans. Cybern.*, vol. 43, no. 2, pp. 515–529, Apr. 2013.

[44] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[45] A. Belazi, A. A. Abd El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[46] S. Toughi, M. H. Fathi, and Y. A. Sekhavat, "An image encryption scheme based on elliptic curve pseudo random and advanced encryption system," *Signal Process.*, vol. 141, pp. 217–227, Dec. 2017.

[47] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017.

[48] G. Ye and X. Huang, "An efficient symmetric image encryption algorithm based on an intertwining logistic map," *Neurocomputing*, vol. 251, pp. 45–53, Aug. 2017.

[49] S. M. Salman and A. A. Elsadany, "On the bifurcation of Marotto's map and its application in image encryption," *J. Comput. Appl. Math.*, vol. 328, pp. 177–196, Jan. 2018.

[50] J. S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimensional Syst. Signal Process.*, vol. 30, no. 2, pp. 943–961, Apr. 2019.

[51] F. M. Atici and P. W. Eloe, "Initial value problems in discrete fractional calculus," *Proc. Amer. Math. Soc.*, vol. 137, no. 3, pp. 981–989, Sep. 2008.

[52] F. M. Atıcı and S. Şengüel, "Modeling with fractional difference equations," *J. Math. Anal. Appl.*, vol. 369, pp. 1–9, Sep. 2010.

[53] T. Abdeljawad, "On Riemann and Caputo fractional differences," *Comput. Math. Appl.*, vol. 62, no. 3, pp. 1602–1611, Aug. 2011.

[54] T. Abdeljawad and D. Baleanu, "Fractional differences and integration by parts," *J. Comput. Anal. Appl.*, vol. 13, no. 3, pp. 574–582, 2011.

[55] M. T. Holm, "The laplace transform in discrete fractional calculus," *Comput. Math. Appl.*, vol. 62, no. 3, pp. 1591–1601, Aug. 2011.

[56] G.-C. Wu, D. Baleanu, and S.-D. Zeng, "Discrete chaos in fractional sine and standard maps," *Phys. Lett. A*, vol. 378, nos. 5–6, pp. 484–487, Jan. 2014.

[57] G.-C. Wu and D. Baleanu, "Discrete fractional logistic map and its chaos," *Nonlinear Dyn.*, vol. 75, nos. 1–2, pp. 283–287, Jan. 2014.

[58] 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, Mar. 2018, Art. no. 030502.

[59] M. Alawida, A. Samsudin, and J. S. Teh, "Enhancing unimodal digital chaotic maps through hybridisation," *Nonlinear Dyn.*, vol. 96, no. 1, pp. 601–613, Apr. 2019.

[60] G.-C. Wu, Z.-G. Deng, D. Baleanu, and D.-Q. Zeng, "New variable-order fractional chaotic systems for fast image encryption," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 29, no. 8, Aug. 2019, Art. no. 083103.

[61] S. M. Ismail, L. A. Said, A. G. Radwan, A. H. Madian, and M. F. Abu-ElYazeed, "A novel image encryption system merging fractional-order edge detection and generalized chaotic maps," *Signal Process.*, vol. 167, Feb. 2020, Art. no. 107280.

[62] M. H. Annaby, H. A. Ayad, M. A. Rushdi, and E. A. Nehary, "Difference operators and generalized discrete fractional transforms in signal and image processing," *Signal Process.*, vol. 151, pp. 1–18, Oct. 2018.

[63] H. Liu and X. Wang, "Color image encryption based on one-time keys and robust chaotic maps," *Comput. Math. Appl.*, vol. 59, no. 10, pp. 3320–3327, May 2010.

[64] H. Liu and X. Wang, "Color image encryption using spatial bit-level permutation and high-dimension chaotic system," *Opt. Commun.*, vol. 284, nos. 16–17, pp. 3895–3903, Aug. 2011.

[65] X. Wang and D. Luan, "A novel image encryption algorithm using chaos and reversible cellular automata," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 18, no. 11, pp. 3075–3085, Nov. 2013.

[66] 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, Nov. 2010.

[67] E. G. Nepomuceno, L. G. Nardo, J. Arias-Garcia, D. N. Butusov, and A. Tutueva, "Image encryption based on the pseudo-orbits from 1D chaotic map," *Chaos, Interdiscipl. J. Nonlinear Sci.*, vol. 29, no. 6, Jun. 2019, Art. no. 061101.

[68] F. M. Atici and P. W. Eloe, "A transform method in discrete fractional calculus," *Int. J. Difference Equ.*, vol. 2, no. 2, pp. 165–176, 2007.

[69] G.-C. Wu and D. Baleanu, "Chaos synchronization of the discrete fractional logistic map," *Signal Process.*, vol. 102, pp. 96–99, Sep. 2014.

[70] C.-C. Tseng and S.-L. Lee, "Closed-form designs of digital fractional order butterworth filters using discrete transforms," *Signal Process.*, vol. 137, pp. 80–97, Aug. 2017.
[71] A. Ouannas, A.-A. Khennaoui, Z. Odibat, V.-T. Pham, and G. Grassi, "On the dynamics, control and synchronization of fractional-order Ikeda map," *Chaos, Solitons Fractals*, vol. 123, pp. 108–115, Jun. 2019.
[72] A.-A. Khennaoui, A. Ouannas, S. Bendoukha, G. Grassi, X. Wang, and V.-T. Pham, "Generalized and inverse generalized synchronization of fractional-order discrete-time chaotic systems with non-identical dimensions," *Adv. Difference Equ.*, vol. 2018, no. 1, p. 303, Dec. 2018.
[73] D. A. Cristina and B. Radu, *A Novel Pseudo-Random Bit Generator Based on a New Couple of Chaotic Systems* (Economic Sciences Series), vol. 11. Constanţa, Romania: Ovidius Univ. Constanta, 2011, pp. 553–558.
[74] E. G. Nepomuceno, S. A. M. Martins, G. F. V. Amaral, and R. Riveret, "On the lower bound error for discrete maps using associative property," *Syst. Sci. Control Eng.*, vol. 5, no. 1, pp. 462–473, Jan. 2017.
[75] R. E. Moore and R. B. Kearfott, *Introduction to Interval Analysis*, vol. 110. Philadelphia, PA, USA: SIAM, 2009.
[76] J. Teeriaho, "Elliptic Curve Cryptography with Mathematica," in *Proc. 7th Int. Arctic Seminar*, Rovaniemi, Finland: Lapland Univ. of Applied Sciences, 2018.
[77] Z. Ying-Qian and W. Xing-Yuan, "A symmetric image encryption algorithm based on mixed linear–nonlinear coupled map lattice," *Inf. Sci.*, vol. 273, pp. 329–351, Jul. 2014.
[78] B. Norouzi and S. Mirzakuchaki, "A fast color image encryption algorithm based on hyper-chaotic systems," *Nonlinear Dyn.*, vol. 78, no. 2, pp. 995–1015, Oct. 2014.
[79] T. Hu, Y. Liu, L.-H. Gong, and C.-J. Ouyang, "An image encryption scheme combining chaos with cycle operation for DNA sequences," *Nonlinear Dyn.*, vol. 87, no. 1, pp. 51–66, Jan. 2017.
[80] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft Comput.*, vol. 26, pp. 10–20, Jan. 2015.
[81] 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.
[82] Y. Wu, J. P. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption," *Cyber J. Multidisciplinary J. Sci. Technol.*, vol. 2, pp. 31–38, Apr. 2011.
[83] N. K. Pareek, V. Patidar, and K. K. Sud, "Cryptography using multiple one-dimensional chaotic maps," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 10, pp. 715–723, Oct. 2005.
[84] X. Y. Wang, L. Teng, and X. Qin, "A novel colour image encryption algorithm based on chaos," *Signal Process.*, vol. 92, pp. 1101–1108, Apr. 2012.
[85] Z. Lin, S. Yu, X. Feng, and J. Lü, "Cryptanalysis of a chaotic stream cipher and its improved scheme," *Int. J. Bifurcation Chaos*, vol. 28, no. 7, Jun. 2018, Art. no. 1850086.
[86] D. Xiao, X. Liao, and P. Wei, "Analysis and improvement of a chaos-based image encryption algorithm," *Chaos, Solitons Fractals*, vol. 40, no. 5, pp. 2191–2199, Jun. 2009.
[87] C. Li, D. Lin, B. Feng, J. Lu, and F. Hao, "Cryptanalysis of a chaotic image encryption algorithm based on information entropy," *IEEE Access*, vol. 6, pp. 75834–75842, 2018.
[88] M. S. Khoirom, D. S. Laiphrakpam, and T. Themrichon, "Cryptanalysis of multimedia encryption using elliptic curve cryptography," *Optik*, vol. 168, pp. 370–375, Sep. 2018.
[89] D. Shanks, "Class number, a theory of factorization, and genera," in *Proc. Sympos. Pure Math.*, vol. 20. New York, NY, USA: Stony Brook Univ., 1969, pp. 415–440.
[90] J. M. Pollard, "Monte Carlo methods for index computation (*modp*)," *Math. Comput.*, vol. 32, no. 143, pp. 918–924, Jul. 1978.
[91] M. Alawida, J. S. Teh, A. Samsudin, and W. H. Alshoura, "An image encryption scheme based on hybridizing digital chaos and finite state machine," *Signal Process.*, vol. 164, pp. 249–266, Nov. 2019.
[92] 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.
[93] Y.-Q. Zhang, Y. He, P. Li, and X.-Y. Wang, "A new color image encryption scheme based on 2DNLCML system and genetic operations," *Opt. Lasers Eng.*, vol. 128, May 2020, Art. no. 106040.
[94] M. Zhou and C. Wang, "A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks," *Signal Process.*, vol. 171, Jun. 2020, Art. no. 107484.

ABDULRAHMAN AL-KHEDHAIRI received the B.Sc. degree in operation research and statistics from King Saud University, Saudi Arabia, in 1995, the M.Sc. degree in operation research from Lancaster University, U.K., in 2000, and the Ph.D. degree in statistics and mathematics from Birmingham University, U.K., in 2004.

He works as an Associate Professor with the Department of Statistics and Operations Researches, College of Science, King Saud University, Saudi Arabia. His current research interests include operation research, applied mathematical modeling, game theory, and dynamical systems.

AMR ELSONBATY received the B.Sc. degree in electronics and communications engineering, the M.Sc. degree in engineering mathematics, and the Ph.D. degree in engineering mathematics from Mansoura University, Egypt, in 2006, 2011, and 2015, respectively.

He was formerly a Postdoctoral Researcher with the Center for Photonics and Smart Materials, Zewail City of Science and Technology, from 2015 to 2018. He is currently an Assistant Professor with the Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia, and with the Faculty of Engineering, Mansoura University. His current research interests include nonlinear dynamics of electronic circuits, bifurcation theory, chaos control and synchronization, chaos generation utilizing lasers, and chaotic optical communication systems.

ABDELALIM A. ELSADANY received the B.Sc. degree in mathematics, and the M.Sc. and Ph.D. degrees in applied mathematics from Mansoura University, Egypt, in 1996, 2002, and 2007, respectively.

He was an Assistant Professor of applied mathematics with the Faculty of Computers and Informatics, Suez Canal University, Egypt, from 2011 to 2016, where he has been an Associate Professor, since October 2016. Since then, he has been an Associate Professor with the Department of Mathematics, College of Science and Humanities in Al-Kharj, Prince Sattam Bin Abdulaziz University, Al-Kharj, Saudi Arabia. His current research interests are in the areas of applied mathematics, economic dynamics, mathematical biology, chaos, nonlinear dynamical systems, and fractional calculus.

ESAM A. A. HAGRAS received the B.Sc. degree in electrical engineering from Alexandria University, Egypt, in 1994, the M.Sc. degree in electrical engineering from Mansoura University, Egypt, in 2001, and the Ph.D. degree in electrical engineering from Alexandria University, in 2008.

He was the Head of the Electronics and Communication Research Center, Armed Forces, Cairo, Egypt, from 2100 to 2017. He is currently an Assistant Professor with the Communications and Computer Department, Faculty of Engineering, Delta University for Science and Technology, Mansoura, Egypt. His current research interests include data protection in digital communication systems and developments of new encryption algorithms.