Computer Science and Information Systems 18(3):1057–1076 https://doi.org/10.2298/CSIS200502018K

Dynamic Fractional Chaotic Biometric Isomorphic Elliptic Curve for Partial Image Encryption

Ahmed Kamal[1], Esam A. A. Hagras[2], H. A. El-Kamchochi[3]

[1] Engineering Dept., Air Defense College, Alexandria University, Alexandria, Egypt
ahmed_kamal8030@yahoo.com
[2] Communications and Computers Department, Faculty of Engineering, Delta University for Science and Technology, Gamasa, Dakahlia, Egypt
esam.hagras@deltauniv.edu.eg
[3] Electrical Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt
helkamchouchi@hotmail.com

Abstract. In this paper, a Modular Fractional Chaotic Sine Map (MFC-SM) has been introduced to achieve high Lyapunov exponent values and completely chaotic behavior of the bifurcation diagram for high level security. The proposed MFC-SM is compared with the conventional non MFC-SM and it has an excellent chaotic analysis. In addition, the randomness test results indicate that the proposed MFC-SM shows better performance and satisfy all randomness tests. Due to the excellent chaotic properties and good randomization results for the proposed MFC-SM, it is used to be cooperated with the biometric digital identity to achieve dynamic chaotic biometric digital identity. Also, for real time image encryption, both Discrete Wavelet Transform (DWT)partial image encryption and Isomorphic Elliptic Curve (IEC)key exchange are used. In addition, the biometric digital identity is extracted from the user fingerprint image as fingerprint minutia data incorporated with the proposed MFC-SM and hence, a new Dynamic Fractional Chaotic Biometric Digital IdentityIEC (DFC-BID-IEC) has been introduced. Dynamic Fractional Chaotic Key Generator (DFC-KG) is used to control the key schedule for all encryption and decryption processing. The encryption process consists of the confusion and diffusion steps. In the confusion step, the 2D Arnold Cat Map (ACM) is used with secret parameters taken from DFC-KG. Also, the diffusion step is based on the dynamic chaotic self-invertible secret key matrix which can be generated from the proposed MFC-SM. The IEC key exchange secret parameters are generated based on Elliptic Curve Diffie–Hellman(ECDH) key exchange and the isomorphism parametre. Statistical analysis, differential analysis and key sensitivity tests are performed to estimate the security strengths of the proposed DFC-BID-IEC system. The experimental results show that the proposed algorithm is robust against common signal processing attacks and provides a high security level and high speed for image encryption application.

Keywords: Image encryption, Biometric identity, Elliptic curve cryptography, Chaotic Maps.

1. Introduction

In today's digital world, usage of images arenotably increased across the network. It became an indispensable part of our life. Also,it has become a great source of information and contains personal data. Thus, strong security and protection must be ensured using cryptography. So, a large number of researchers have introduced numerous schemes for image encryption [1-3]. These encryption techniques are employed in two ways, namely Symmetric Encryption and Asymmetric Encryption [4]. In 1985, Neal Koblitz and Victor S. Miller [5-6] introduced a new public key cryptography EC which provides a high level of security and achieve computational efficiency in performance with smaller key size compared to other cryptographic technique [7]. Most of thetraditional ciphers are not efficient in image encryption because their slow speed, the large data volume and strong correlation among image pixels. So, chaotic cryptography has been attracting more attention of large number of researchers because of their high ergodicity and sensitivity to control parameter, initial conditions and non-linearity. Definitely, many chaos-based image encryption algorithms have been proposed for image encryption such as Chebyshev map, Logistic map [12], the ACM[8], Tent map [1], sine map [9] etc. However, these maps have some weaknesses, namely, non-uniform distribution, small key space and periodicity [10]. Some proposed recently hyperd maps can overcome these imperfections and enhance security [3]. Several paradigms have been used to extract cryptography key from biometric traits. The key based on the biometric features was applied earliest in online trading for the IBM transaction security system in 1989, by using signature pen and handwriting signal processor [11]. Many schemes for image encryption based on ECC and chaotic map are proposed. In [12],an image encryption scheme based on chaotic system and EC has been proposed usesECDHfor key exchange between sender and receiver in addition, logistic map is used to generate a chaotic sequence using initial condition from elliptic curve. In [13] an algorithm for image encryption uses ECC and modified hill cipher to secure the image data. In [8] Essam et. al. introduced a selective encryption algorithm use DWT and multi-map orbit hopping chaotic encryption, the multi-chaotic logistic maps generate a hopping pattern of random numbers used to encrypt the low-low sub-band decomposition only. In [14] a chaotic tent map used to encrypt a medical image extracted by DWT-DCT. In [15] Abd El-Latif et. al. proposed a hybrid image encryption scheme based on a cyclic EC and chaotic system. An image encryption algorithm based on a secure variant of Hill cipher and three one-dimensional (1D) chaotic maps suggested in [9], this algorithm aims to encrypt pixel-by- pixel all types of images with black background or with high correlation of adjacent pixels. In[16] present based on an ordered isomorphic EC for generating a large number of distinct, mutually uncorrelated, and cryptographically injective S-boxes. In [17] an image encryption algorithm based on the H-fractal and dynamic self-invertible matrix have been proposed.

This paper proposes an improved image encryption scheme uses IECfor initial key exchange between two parties. The generated IEC secret keys used to generate the initial conditions. Using the fractional modular chaotic map and biometric key based on IEC to build key schedule that is used as a parameter generator for the system. The image is scrambled using ACM and is encrypted using self invertible matrixto attain confusion and diffusion. The initial condition for the proposed MFC-SMare taken from the key schedule. the proposed MFC-SM is used to construct the self invertible matrix.

The rest of this paper is organized as following: Section 2 provides guidelines for Manuscript Preparation. Section 3 presents the proposedDFC-BID-IEC scheme. In Section 4 the simulation results and security analysis are introduced. Finally, conclusion and future work are given in Section 5.

2. Proposed Scheme Preparation

2.1. Novel Modular Fractional Chaotic Sin Map

Discrete fractional calculuswas introduced to efficiently incorporate and capture the memory effects in nonlinear discrete time systems [18]. 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.Assume that a sequence $\rho(n)$ is given and the isolated time scale $\aleph_a$is represented in terms of real valued constant τ as $\{\tau, \tau+1, \tau+2, \dots,\}$ such that $\rho: \aleph_\tau \to \mathbb{R}$. The difference operator is denoted by Δ, where $\Delta\rho(n) = \rho(n+1) - \rho(n)$ then some of the basic definitions related to discrete fractional calculus are summarized as follows:
For $\alpha > 0$, the fractional sum of order α is given by [18]

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

the Caputo-like delta difference of order α is defined by [18]:

$${}^{C}\Delta_{\tau}^{\alpha}\rho(t) = \Delta_{\tau}^{-(n-\alpha)}\Delta^{n}\rho(t)$$

$$= \frac{1}{\Gamma(n-\alpha)}\sum_{m=\tau}^{t-(n-\alpha)}\frac{\Gamma(t-m)}{\Gamma(t-m-n+\alpha+1)}\Delta^{n}\rho \quad t \in \aleph_{\tau+n-\alpha},\ n = \lfloor\alpha\rfloor + 1 \quad (2)$$

the delta fractional difference equation of order α is represented by [18] and the equivalent discrete fractional integral is given by

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

$$\rho(t) = \rho_0(t) + \frac{1}{\Gamma(\alpha)}\sum_{m=\tau+n-\alpha}^{t-\alpha}\frac{\Gamma(t-m)}{\Gamma(t-m-\alpha+1)} \times f\big(m+\alpha-1, \rho(m+\alpha-1)\big),\ t \in \aleph_{\tau+n} \quad (3)$$

note that the initial iteration in this case is:

$$\rho_0(t) = \sum_{k=0}^{n-1}\frac{\Gamma(t-\tau+1)}{k!\,\Gamma(t-\tau-k+1)}\Delta^{k}\rho(\tau) \quad (4)$$

The *non-modular* fractional sine map with Caputo fractional order is introduced in [18], it leads to a highLyapunov exponent value, so we have to introduce some definitions about the fractional calculus. The *non-modular* fractional sine map is given by:

$$x(n) = x(0) + \frac{\mathrm{r}}{\Gamma(v)}\sum_{j=1}^{n}\frac{\Gamma(n-j+v)}{\Gamma(n-j+1)}sin(x(j-1) \quad (5)$$

the proposed new *modular* fractional sine map is given by:

$$x(n) = (x(0) + \frac{r}{\Gamma(v)} \sum_{j=1}^{n} \frac{\Gamma(n-j+v)}{\Gamma(n-j+1)} sin(x(j-1))) \ mod\ 1 \qquad (6)$$

where $'r'$ is the control parameter of non-modular and MFC-SM and $v$is the difference order. Using more than one parameter of the sine map gives high Lyapunov exponent value [19], high chaotic range and a large key space. Fig. 1 shows the Lyapunov exponent and the bifurcation diagram of the Non modular fractional chaotic sine map. Also, Fig.2 shows both the Lyapunov exponent and the bifurcation diagram of the proposed modular fractional chaotic sine map. As shown in these figures, the proposed MFC-SMhas highly Lyapunov exponent values and completely chaotic behavior of the bifurcation diagram compared with the conventional Non modular fractional chaotic sine map.

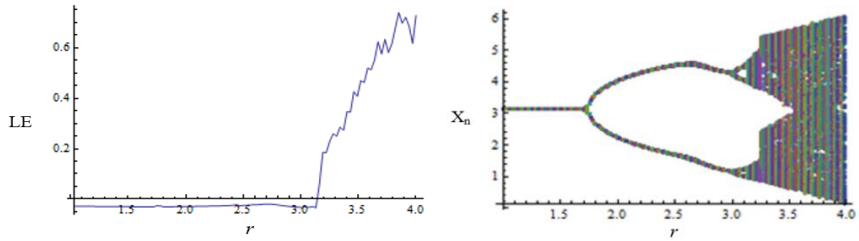

Fig. 1. Lyapunov exponents (LE) and Bifurcation diagram of the non-modular fractional order sine map.

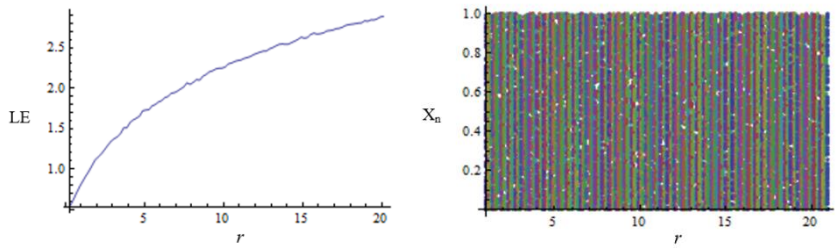

Fig. 2. Lyapunov exponents (LE) and Bifurcation diagram of the non-modular fractional order sine map.

The randomness of the proposed MFC-SM is tested by the NIST 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 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 modular fractional sine map is tested by SP800-22 [3] and the results are given in Table 1.

Table 1. NIST Randomness Tests of the Proposed MFC-SMBINARY OUTPUT.

TEST	P-VALUE	RESULT
MONOBIT FREQUENCY	0.553273	PASSED
BLOCK FREQUENCY	0.538714	PASSED
RUNS	0.596352	PASSED
LONGEST-RUN-OF-ONES IN A BLOCK	0.692018	PASSED
BINARY MATRIX RANK	0.352617	PASSED
DISCRETE FOURIER TRANSFORM (SPECTRAL)	0.438291	PASSED
NON-OVERLAPPING TEMPLATE MATCHING	0.527163	PASSED
OVERLAPPING TEMPLATE MATCHING	0.592763	PASSED
MAURER'S UNIVERSAL STATISTICAL	0.421873	PASSED
LINEAR COMPLEXITY	0.537524	PASSED
SERIAL TEST	0.437163	PASSED
APPROXIMATE ENTROPY	0.418315	PASSED
CUMULATIVE SUMS	0.468232	PASSED
RANDOM EXCURSION	0.391823	PASSED
RANDOM EXCURSION VARIANT	0.538138	PASSED
CUMULATIVE SUMS TEST REVERSE	0.387263	PASSED
LEMPEL-ZIV COMPRESSION	0.498163	PASSED

2.2. Isomorphic Elliptic Curve

An EC over prime field $F_p$is defined with the cubic equation:

$$\boldsymbol{y^2 = x^3 + ax + b \, mod \, p} \tag{7}$$

where p is a large prime number and a, b satisfies the condition$4a^2 + 27b \neq 0$, each value of $a, b \epsilon p$ gives a different EC $EC_{p,a,b}$ where p, a and b are called the EC parameters. For two ECs $E_{p,a,b}$ and $E_{p,a',b'}$ over the field F_p are said to be isomorphic if and only if there exists an integer $i \in p \setminus \{0\}$. Such that, the EC parameter (a, b) will be (a', b') for the isomorphic elliptic curve, the value of the IEC parameters (a', b') will be computed using i as following:

$$\boldsymbol{a' = ai^4 mod p, b' = bi^6 mod p} \tag{8}$$

where i is called the isomorphism parameter between $E_{p,a,b}$ and $E_{p,a',b'}$. Thus, every point $(x, y) \in E_{p,a,b}$ will be$(x', y') \in E_{p,a',b'}$ and (x', y') will be computed as

$$\boldsymbol{x' = xi^2 mod p, y' = yi^3 mod p} \tag{9}$$

It is easy to observe that isomorphism is an equivalence relation on the family of all ECs over the field F_p. It is well-known that for prime p there exists a unique finite field F_p, up to the field isomorphism, with exactly $p$elements. There are $p^2 - p$ ECs over the field F_p. The number of ECs isomorphic to a given EC over $F_p$can be computed as the following:

For a prime $p > 3$ and $a, b \in [0, p - 1]$ are two integers. The number of ECs isomorphic to the EC $E_{p,a,b}$is

- $(p - 1)/6$ if $a = 0$ and F_p has a non-zero element of group order 6.

- $(p-1)/4$ if $b = 0$ and F_p has a non-zero element of group order 4.
- $(p-1)/2$ Otherwise.

The number of elements$\#E_{F_{p,a,b}}$in EC is equal to the number of points lying on EC over F_p. Hasse's Theorem gives the bounds of total number of points on EC [20]:

$$\boldsymbol{p+1-2\sqrt{p} \leq \#E_{F_{p,a,b}} \leq p+1+2\sqrt{p}} \quad (10)$$

The order of the EC is the total number of points lies on the EC along with the point at infinity $O(x = \infty;\ y = \infty)$ denoted by $\#E$. The smallest positive integer n for which nP is equal to point at infinity O $(nP = O)$ is called order of point P such that $n \leq \#E$. Then, $P, 2P, \ldots, (n-1)P$ are distinct points on elliptic curve. For certain choice of a and b it is possible to choose a base point P of highest order $n = \#E$ [15].

For example, let $p = 37, a = -1, b = 6$ are the main EC parameters, $i = 3$ and $i = 5$ are two different isomorphism parameters. Such that, the IEC parameter for $i = 3$ computed as $a^{'} = -1 * 3^4 \ mod\ 37$ and $b^{'} = 6 * 3^6 \ mod\ 37$. thus,$(a^{'} = 30, b^{'} = 8)$ and for $i = 5$ computed as $a^{''} = -1 * 5^4 \ mod\ 37$ and $b^{''} = 6 * 5^6 \ mod\ 37$. Thus, $(a^{''} = 4,\ b^{''} = 29)$. Fig. 3 shows the difference between the points lays on the main EC and its tow isomorphic elliptic curves.

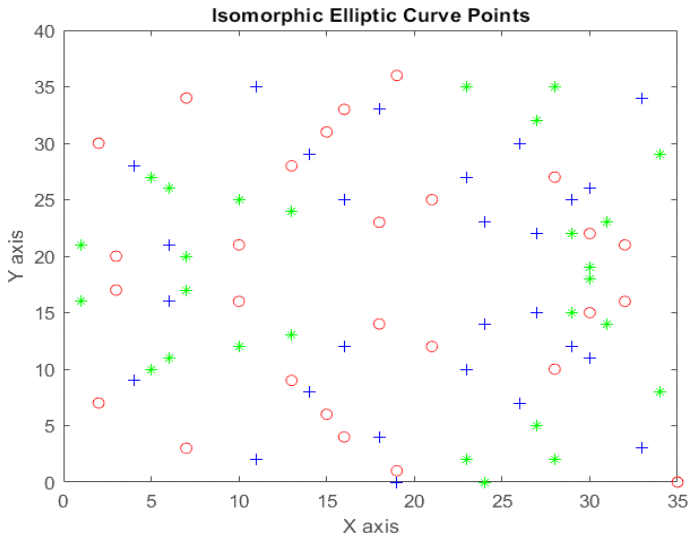

Fig. 3. The different points of the main EC represented by blue(+) and its isomorphic elliptic curves with isomorphic parameters $\boldsymbol{i = 3}$represented by red (o) and $\boldsymbol{i = 5}$ represented by green (*).

2.3. Elliptic Curve Diffie–Hellman Key Exchange

Let$G$ is a base point of an EC,P_A andP_B can be computed as

$$\boldsymbol{P_A = n_A.G,\ P_B = n_B.G} \quad (11)$$

where P_A ,P_B is the public keys of sender and receiver respectively and n_A,$n_B$is the privet keys. The shared key is computed as $n_A P_B$ and $n_B P_A$ by the sender and receiver respectively.

$$\boldsymbol{Sk = n_A P_B = n_A n_B G = n_B n_A G = n_B P_A} \tag{12}$$

2.4. Self Invertable Matrix

FirstlyHill used self-invertible matrices in his proposed encryption algorithm [17]. Hill cipher algorithm uses a matrix to convert the plain-text into cipher-text, and the key is the matrix itself. The Plaintext N is encrypted as:

$$\boldsymbol{C = K_{IM} \times N(mod m)} \tag{13}$$

where C is the Cipher text block, K_{IM} is the Self-Invertible Matrix and m is the plain-text value range (For image encryption, m = 256). K_{IM} must satisfy the criteria [21] to be an invertible matrix and the gcd($det\ [K_{IM}]\ mod m, m$) =1.

$$\boldsymbol{N = K_{IM} \times C(mod m)} \tag{14}$$

$$\boldsymbol{K_{IM} \times K_{IM}^{-1} = I} \tag{15}$$

where *I* is the identity matrix. The receiver cannot decrypt the cipher message if K_{IM} is not invertible matrix. To create $K_{IM}$to be used for encryption and decryption.

$$\boldsymbol{K_{IM} = \begin{bmatrix} K_c & I - K_c \\ I + K_c & -K_c \end{bmatrix} mod\ m} \tag{16}$$

where K_c is the Chaotic key matrix that iswanted to be self-invertible to be used for encryption and decryption.

2.5. Generation of Self-Invertible 4 × 4 Matrix

Let $K_{IM} = \begin{bmatrix} k_{11} k_{12} k_{13} k_{14} \\ k_{21} k_{22} k_{23} k_{24} \\ k_{31} k_{32} k_{33} k_{34} \\ k_{41} k_{42} k_{43} k_{44} \end{bmatrix}$be self-invertible matrixpartitioned as $\left[\begin{array}{c:c} K_{11} & K_{12} \\ \hdashline K_{21} & K_{22} \end{array}\right]$

where$K_{11} = \begin{bmatrix} k_{11} & k_{12} \\ k_{12} & k_{22} \end{bmatrix}, K_{12} = \begin{bmatrix} k_{13} & k_{14} \\ k_{23} & k_{24} \end{bmatrix}, K_{21} = \begin{bmatrix} k_{31} & k_{32} \\ k_{41} & k_{42} \end{bmatrix},\ K_{22} = \begin{bmatrix} k_{33} & k_{34} \\ k_{43} & k_{44} \end{bmatrix}$

For example, a realexample for chaotic matrix $K_{4\times 4}$taken from the output of the proposed MFC-SM Used to construct the self-invertible matrix $K_{8\times 8}$ that used to encrypt and decrypt a real part of the scrambled Lena image $N_{8\times 8}$ as explained.

Let $K_{11} = \begin{bmatrix} 72 & 1 & 53 & 27 \\ 7 & 61 & 244 & 166 \\ 179 & 228 & 124 & 145 \\ 104 & 9 & 209 & 46 \end{bmatrix},\ K_{22} = \begin{bmatrix} 184 & 255 & 203 & 229 \\ 249 & 195 & 12 & 90 \\ 77 & 28 & 132 & 111 \\ 152 & 247 & 47 & 210 \end{bmatrix}$

Take $K_{12} = I - K_{11}$ with $n = 1$. Then,

$$K_{12} = \begin{bmatrix} 185 & 255 & 203 & 229 \\ 249 & 196 & 12 & 166 \\ 77 & 28 & 133 & 111 \\ 152 & 247 & 47 & 211 \end{bmatrix}, K_{21} = \begin{bmatrix} 73 & 1 & 53 & 27 \\ 7 & 62 & 244 & 166 \\ 179 & 228 & 125 & 145 \\ 104 & 9 & 209 & 47 \end{bmatrix}$$

$$\text{So, } K_{IM} = \begin{bmatrix} 72 & 1 & 53 & 27 & 185 & 255 & 203 & 229 \\ 7 & 61 & 244 & 166 & 249 & 196 & 12 & 90 \\ 179 & 228 & 124 & 145 & 77 & 28 & 133 & 111 \\ 104 & 9 & 209 & 46 & 152 & 247 & 47 & 211 \\ 73 & 1 & 53 & 27 & 184 & 255 & 203 & 229 \\ 7 & 62 & 244 & 166 & 249 & 195 & 12 & 90 \\ 179 & 228 & 125 & 145 & 77 & 28 & 132 & 111 \\ 104 & 9 & 209 & 47 & 152 & 247 & 47 & 210 \end{bmatrix}$$

$$\text{For, } N = \begin{bmatrix} 194 & 194 & 72 & 71 & 134 & 129 & 146 & 144 \\ 195 & 194 & 71 & 71 & 134 & 128 & 146 & 144 \\ 61 & 62 & 158 & 156 & 154 & 149 & 88 & 85 \\ 62 & 62 & 157 & 157 & 154 & 149 & 87 & 85 \\ 124 & 124 & 123 & 122 & 139 & 134 & 113 & 110 \\ 126 & 126 & 120 & 117 & 137 & 137 & 108 & 110 \\ 156 & 156 & 51 & 46 & 73 & 75 & 90 & 87 \\ 154 & 154 & 44 & 44 & 71 & 72 & 87 & 89 \end{bmatrix},$$

By applying Eq.13,

$$C = \begin{bmatrix} 18 & 70 & 4 & 165 & 166 & 134 & 117 & 74 \\ 165 & 92 & 168 & 56 & 181 & 183 & 121 & 246 \\ 226 & 122 & 187 & 214 & 93 & 61 & 77 & 41 \\ 96 & 40 & 100 & 242 & 47 & 47 & 115 & 1 \\ 88 & 140 & 209 & 114 & 161 & 129 & 150 & 108 \\ 234 & 160 & 119 & 10 & 178 & 174 & 159 & 24 \\ 131 & 28 & 38 & 68 & 174 & 135 & 75 & 39 \\ 4 & 204 & 213 & 99 & 130 & 124 & 115 & 253 \end{bmatrix}$$

By applying Eq. 14,

$$N' = \begin{bmatrix} 194 & 194 & 72 & 71 & 134 & 129 & 146 & 144 \\ 195 & 194 & 71 & 71 & 134 & 128 & 146 & 144 \\ 61 & 62 & 158 & 156 & 154 & 149 & 88 & 85 \\ 62 & 62 & 157 & 157 & 154 & 149 & 87 & 85 \\ 124 & 124 & 123 & 122 & 139 & 134 & 113 & 110 \\ 126 & 126 & 120 & 117 & 137 & 137 & 108 & 110 \\ 156 & 156 & 51 & 46 & 73 & 75 & 90 & 87 \\ 154 & 154 & 44 & 44 & 71 & 72 & 87 & 89 \end{bmatrix}$$

It is distinct that there no relation between the original matrix N values and the ciphered matrix C values($N \neq C$). vice versa the encrypted matrix N' istipically the same as the original matrix ($N = N'$). This prove the robustness of the proposed scheme.

2.6. Finger Print Biometric Identity Extraction:

Fingerprint is a biometric attribute that can be captured to extract digital data using several approaches, such as block based approach to generate the feature vector [18]. This feature vector is used to generate code word which can be of any arbitrary large size and random enough to use. The process subject to some steps, feature extraction, calculation of attributes of straight lines, obscuring straight lines attributes, biometric binary string generation. Firstly, extract Minutiae points(v_k), Core point(C_p) and Delta point (D_p) from fingerprint image. Calculate straight line attributes between the points in the set v_k. Let F is the fingerprint image, divide F to a number of small blocks each size $m \times m$ pixels, where $F = s \times q$ of all blocks. Calculate straight line attributes using all the blocks by computing all straight lines from one v_k of a block as a reference block to other v_k of all adjacent blocks, calculate length and angle of each straight line, length (li) using Euclidean distance and angle (a_i) with reference to the x-axis. Let F_B represents a set of lengths and angles of straight lines for all blocks $F_B = \{(l_1, a_1), (l_2, a_2), \ldots, (l_{zb}, a_{zb})\}$ size ofF_B isz^b. Extract C_p and D_p from image$E$ by finding the block E_{lm} which contains the C_P, compute all straight lines from the C_P to all other v_k of surrounding neighborhood blocks, Let F_C denotes a set of lengths and angles of straight lines, where the size of the F_C is z^c. Similarly, the set of lengths and angles of lines represented as F_D with reference to D_p where the size of the F_D is z^d, set F_B,F_C and F_D into a single set R.

$$\boldsymbol{R = \{F_B \| F_C \| F_D\},\ z = z^b + z^c + z^d} \quad (\mathbf{17})$$

For obscuring straight lines attributes, the extracted features XOR together and converted into a binary form, merge all bits in the feature setsto generate 256 bits.

2.7. Dynamic Fractional Chaotic Key Generation (DFC-KG)

In this section, we propose a new fast and efficient system for key generation using biometric identity XOR chaotic map sequence based on a hidden IEC. It consists of two parts; the first part serving for generation of initial Secret key which generated from EC using the parameters (p, a, b, G) as in Eqn. (7). Both the sender and receiver use their own private key to share the public as in Eqn. (11) using ECDH key exchange, thus, they generate the secret key Sk as in Eqn. (13). An isomorphism parameter i will be generated using the shared base point $G(x, y)$ as in Eqn. (18). It will be used as an isomorphism parameter as in Eqn. (8) to produce the IEC.Using $i$as in Eqn. (9) the public points $P_A: (x, y)$ and $P_B: (x, y)$ that lies on the EC will be $P_A^{'}: (x^{'}, y^{'})$ and $P_B^{'}: (x^{'}, y^{'})$ lies on the IEC. Similarly, $Sk: (x, y)$will be used to get the isomorphic secret key $Sk^{'}: (x^{'}, y^{'})$.

$$\boldsymbol{i = G(x \oplus y) \mod 8 + 3} \quad (17)$$

Using point addition for the isomorphic public keys $P_A^{'}$and $P_B^{'}$ with $Sk^{'}$to get two different isomorphic secret keys $ISk_1^{'}$and $ISk_2^{'}$ as following

$$\boldsymbol{ISk_1^{'} = P_A^{'} + Sk^{'}} \quad (18)$$

$$\boldsymbol{ISk_2^{'} = P_B^{'} + Sk^{'}} \tag{19}$$

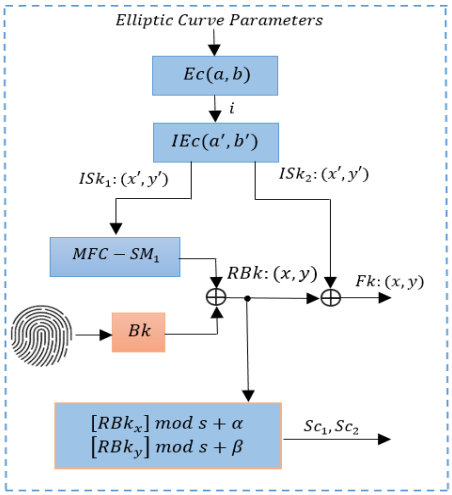

Fig.4. Proposed cryptosystem key generation.

The first $ISk_1^{'}(x,y)$ will be used as initial condition for theMFC-SM$_1$as in Eqn. (21,22) to generate a Chaotic number $R:(x,y)$. This random number XOR with the saved 256 bit Biometric key $R:(x,y)$as in Eqn. (17) to provide randomness for the biometric key. So, the output sequence is a Random Biometric key $RBk:(x,y)$which XOR with $ISk_2^{'}:(x,y)$ to generate $Fk(x,y)$ as shown in Eqn. (24) to be used as initial condition for theMFC-SM$_2$as the same in Eqn. (21,22).Eqn. (23) shows the value of $\boldsymbol{v}$.

$$\boldsymbol{x_0 = ISk_1^{'}(x) / p} \tag{20}$$

$$\boldsymbol{r = ISk_1^{'}(y)/(10 \times p)} \tag{21}$$

$$\boldsymbol{v = x + r \quad mod\ 1} \tag{23}$$

$$\boldsymbol{RBk:(x,y) = Bk:(x,y) \oplus R:(x,y)} \tag{22}$$

$$\boldsymbol{Fk:(x,y) = RBk:(x,y) \oplus ISk_2^{'}(x,y)} \tag{23}$$

The second part of key generation, the parameters used for scrambling Sc_1, Sc_2 will be generated using the $RBk:(x,y)$ according to the Eqns. (26,27).

$$\boldsymbol{Sc_1 = RBk_x mod S + \alpha} \tag{24}$$

$$\boldsymbol{Sc_2 = RBk_y\ mod\ S + \beta} \tag{25}$$

where S, α and β are integers used to eliminate the scrambling parameters. The proposed MFC-SM$_1$generates a chaotic sequence to get $K_c$which used to constructK_{IM}as in Eqn. (16). The $K_{IM}$is used for encryption and decryption. Table (2) shows the key schedule used in the whole system.

Table 2. Key Schedule

Symbol	Description	Symbol	Description
(a, b, p)	EC parameters	Sk'	Isomorphic secret key
(a', b', p)	IEC parameters	K_{IM}	InvertableKey Matrix
Sk	Initial secret key	n_A	Sender privet key
ISk_1'	First isomorphic secret key	n_B	Reciver privet key
ISk_2	Second isomorphic secret key	P_A	Sender public key
Sc_1	Scrambling parameter (1)	P_B	Reciver public key
Sc_2	Scrambling parameter (2)	P_A'	Sender isomorphic public key
i	Isomorphism parameter	P_B'	Reciver isomorphic public key

2.8. Proposed DFC-BID-IEC Scheme

The proposed encryption scheme uses ECC to share the EC parameters between two parties using ECDH to provide authenticity and confidentiality. The hidden IEC used to provide secrecy to the ECparameters and the all keys. such that, inlarge the key space. The ACMused for image confusion according to the generated scrambling parameters. The proposed MFC-$SM_2$and K_{IM} to offer randomness and chaocity for image encryption. The system provides both system and user authentication, the proposed scheme goes as follows:

2.9. Partial Image Encryption

- DWT is applied to the image $N_{M\times M}$to generate vertical LH (CV), horizontal HL(CH), diagonal HH (CD) and approximation LL (CA) matrices [14].
- The approximation LL (CA) matrix only is scrambled using ACMas [8] with the scrambling parametersSc_1, Sc_2in Eqn. (26, 27) as it holds most of the image's information. Thus, save the computational time and cost.
- The IDWT is applied to reconstruct the scrambled image$N$[22, 23].
- The initial condition for the proposed MFC-SM_2 is derived using the Fk: (x, y) using Eqn. (21, 22) for generating a chaotic sequence to construct $K_{C_{H\times H}}$ where $H = M/2$.
- Constructing the K_{IM}using the $K_C$and the identity matrix I as in Eqn. (16). WhereK_{IM} dimention is $M \times M$.
- The cipher image C is computed as in Eqn. (13).

2.10. Partial Image Decryption

- Using the decrypt Fk' as the same in Eqn. (25) to be the initial condition for the proposed MFC-$SM_2$to generate a chaotic sequenceto be used for generating$K'_{C_{N\times N}}$.
- Constructing the K'_{IM}using the$K'_C$and the identity matrix I as in Eqn. (16).
- The decipher image N' is computed as in Eqn. (14).

- Applying The DWT for the decrypted image $N^{'}$ to generate vertical LH (CV'), horizontal HL(CH'), diagonal HH (CD') and approximation LL (CA') matrices
- The approximation LL (CA') matrix is descrambled using ACMwith parameters $Sc_1^{'}$, $Sc_2^{'}$wich are generated as in Eqn. (12, 13).
- The IDWT is applied to reconstruct the descrambled image$N^{'}$.

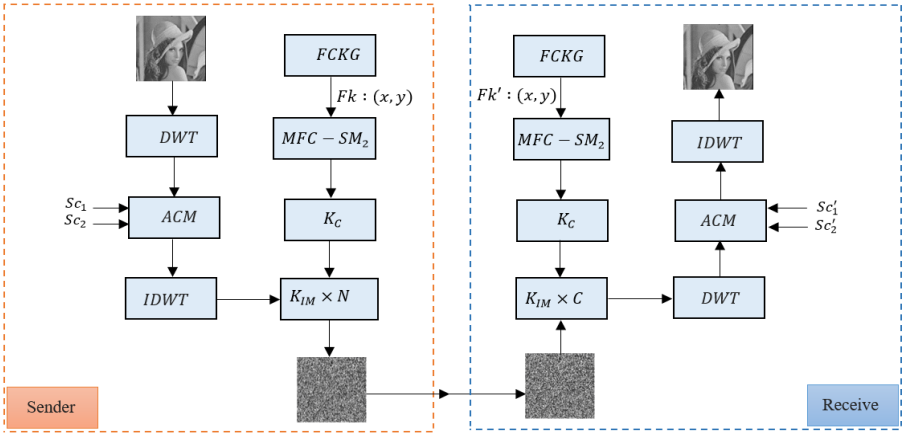

Fig. 5. Proposed partial image encryption and decryption diagram.

3. Simulation Results and Security Analysis

The laptop used is Intel(R) Core(TM) i7-4910MQ CPU@2.90GHz, 16GB RAM, Windows 10 (64-bit), MATLAB R2018b.Small parameters are used for simulation. The parameters chosen for EC $p = 113, a = -1, b = 17, G = (49,53)$. The proposed scheme will be applied on gray scale "Lena", "cameraman ", "boat", "pentagon" and "Barbara" images with size of 512×512. Fig.5 shows the result of image encryption. It is noted that the scheme converts the original images to encrypted image. The robustness of the encryption scheme is evaluated by measuring its resistance to several attacks such as known-plain text attack, cipher-text only attack, statistical attack, differential attack, and various brute-force attacks. Security analysis has been performed on the proposed scheme to be evaluated by discussing histogram, correlation coefficient, NPCR, UACI. The IEC parameters and the other output parameters of the DFC-KGthat are shown in the key schedule will be given as

Table 3. Simulation Parameters

Parameter	Value	Parameter	Value
i	7	Sk	(99, 76)
n_A	34	Sk'	(52, 78)
n_B	25	$ISk_1^{'}$	(11, 74)
P_A	(81, 27)	$ISk_2^{'}$	(97, 63)
P_B	(111, 24)	Sc_1, Sc_2	27, 92
$P_A^{'}$	(14, 108)	S, α, β	(40, 21, 60)
$P_B^{'}$	(15, 96)	Fk	(8, 62)

3.1. Histogram Analysis

Histogram plots the distribution of pixel intensities in an image. For a good encryption, the histogram of the encrypted image must be flat and uniform. So there is no information to reveal about the original image. The visual inspection for Fig. 6 shows that the histogram of the encrypted image is uniform and significantly different from the histogram of the original image. This is due to the applied confusion and diffusion in the proposed scheme. So it can defense against statistical attacks.

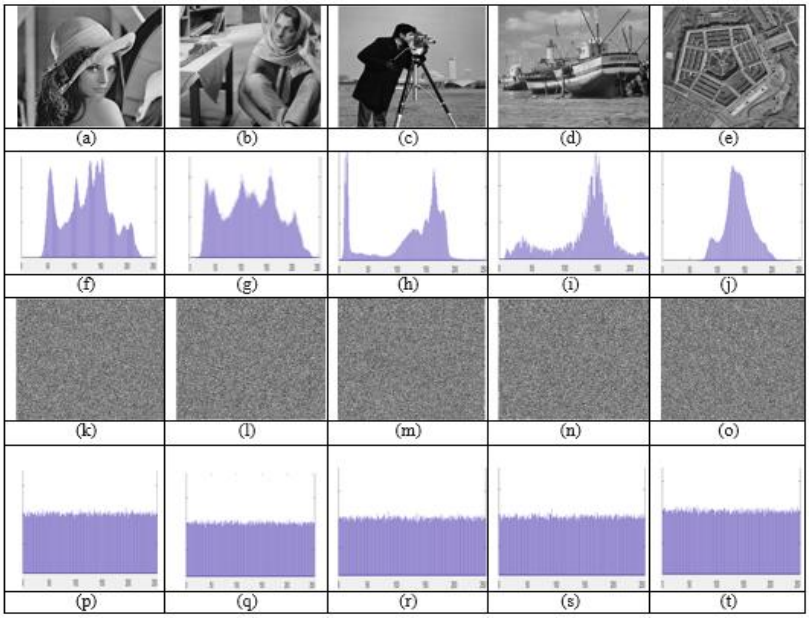

Fig. 6. Simulation results for images: a. Lena; b. Barbara; c. cameraman d. boat e. pentagon images; (f)-(j) Histogram of (a)-(e); (k)-(o) Cipher images of (a)-(e); (p)-(t) Histograms of (k)-(o).

3.2. Correlation Coefficient

In the original image each pixel is highly correlated with its adjacent pixels. A robust encryption scheme must reduce this correlation to the minimum possible value, so that it must be no correlation between adjacent pixels in vertical, horizontal and diagonal directions. Fig. 7 shows horizontal, vertical, and diagonal directions correlation of Fig.6 (a) "Lena" image and its cipher image in Fig. 6 (k). The correlation coefficient C_r between two adjacent pixels in an image is determined as in Eqn. (28), the C_r value should be almost equal to zero [15]. A comparison of the computed correlation coefficients for both the plain image and its corresponding cipher image is shown in Table (4). The comparison performed to grayscale tested images with the other recent schemes in [3, 28].

$$C_r = \frac{\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y))}{\sqrt{\sum_{i=1}^{N}(x_i - E(x))^2}\sqrt{\sum_{i=1}^{N}(yi - E(y))^2}} \quad (26)$$

Table 4. Correlation Coefficient of the Proposed Scheme for Gray Scale Tested Images.

Algorithm	Image	Horizontal		Vertical		Diagonal	
		Plain	Cipher	Plain	Cipher	Plain	Cipher
Ours	Lena	0.9741	0.0005	0.9862	0.0011	0.9619	0.0000
	Barbara	0.8954	0.0024	0.9589	0.0025	0.8830	-0.0004
	Peppers	0.9768	-0.0001	0.9792	-0.0018	0.9639	-0.0020
	Baboon	0.8665	-0.0007	0.7587	-0.0034	0.7262	0.0001
	House	0.9480	-0.0011	0.9577	-0.0025	0.9130	0.0014
Ref. [3]	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. [28]	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

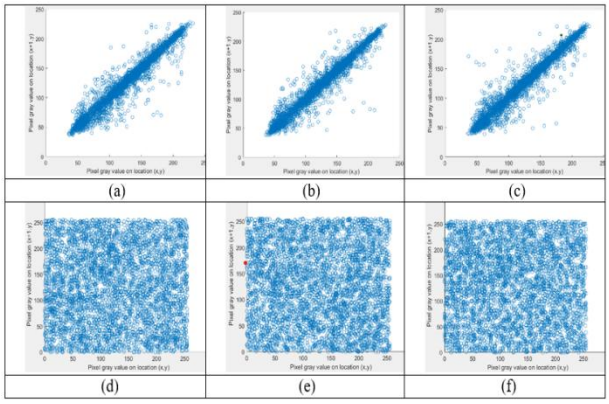

Fig. 7. Correlation of adjacent pixels in "Lena" image along (a) Plain image horizontal direction; (b) Plain image vertical direction; (c) Plain image diagonal direction; (d) Cipher image horizontal direction; (e) Cipher image vertical direction; (f) Cipher image diagonal direction.

It is clear that the correlation coefficients for the cipher images are near to zero, while for the original images are near to one. This indicates that the proposed scheme is highly resistant to statistical-based attacks.

3.3. Key Space Analysis

Key space is the set of all keys used in image encryption scheme. For efficient scheme it must be large enough to tackle the brute-force attack. It can be evaluated by measuring the key sensitivity and the number of keys.For 256-bit EC parameter used to be performed in the DFC-BID-IEC system. The key schedule shows allthe keysused in the

DFC-BID-IEC system. The total key space for the proposed encryption scheme is extremely large and it can be calculated as $2^{256} \times 2^{256} \times 2^{256} \times 2^{256} \times 2^{256} \times 2^{256} \times 2^{256} \times 2^{256} \times 2^{256} \times 2^{16} \times 2^{16} \times 2^{16} \times 2^{16} = 2^{2624}$, where, the first 256 bits are given from the EC Sk, the second and third 256 bits are from the $P_A^{'}, P_B^{'}$, the fourth , fifth and sixth 256 bits given from $(Sk, ISk_1^{'}, ISk_2^{'})$, the seventh 256 bits are given from Bk, the eighth 256 bits are the MFC-SM_1 output, the ninth 256 bits are from RBk, the tenth 256 bits are for the Fk Also, the first 16 bits are the length of the initial values of the MFC-SM_1 and the second 16 bits are the length of the MFC-SM_1 control parameter similarly, the third and the forth is for MFC-SM_2. It is obvious that the total key space for the proposed encryption scheme is extremely large because of using the IEC and this is achieved without using EC point multiplication operation. A comparison for key space with recent schemes are shown in table (5).

Table 5. Key Space Analysis

	ours	Ref [29]	Ref[28]	Ref[3]
Key space size	2^{2624}	2^{512}	2^{564}	2^{772}

3.4. Key Sensitivity Analysis

A robust cryptographic scheme should have high sensitivity to all keys. A slight change in the key should provide a totally different cipher image. Also the recovery of the plain image will be impossible with slight change in the decryption key [25]. To test the key sensitivity in the proposed scheme Fig. 6 (a, b, c, d) "pentagon", " Lena ", " Barbara " and" cameraman "images is encrypted with the correct key as shown in Fig. 8 (e, f, g, h). The cipher images are decrypted with a correct key in Fig. 8 (i, j, k, l). Another key which is just one bit different from the original key used to encrypt the original images in Fig. 8 (l, m, n, o), Fig. 8 (p, r, s, t) shows the decrypted images which are encrypted using a wrong key which is just a bit different from the original key. 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.

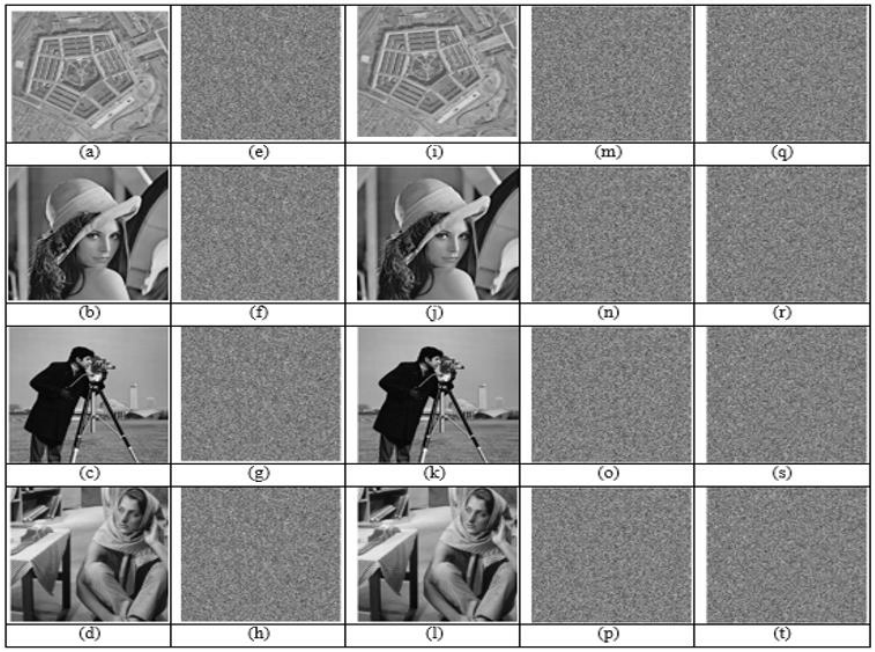

Fig. 8. The key sensitivity analysis. a. Pentagon; b. Lena; c. Barbara; d. cameraman plain images; (e)-(h) Encrypted image with original keys; (i)-(l) Decrypted images with correct key; (m)-(p) encrypted images with modified keys; (q)-(t) Decrypted images with wrong key respectively.

3.5. Differential Attack Analysis

A good diffusion performance is a measure of the strength of an image encryption scheme. It means a strong dependency of cipher image pixels on the plain image pixels. The differential attack resistance can be evaluated by comparing the differences of cipher images if the plain image one bit changed, it should provide a totally different cipher image. Number of pixels change rate (NPCR) and unified average changing intensity (UACI) are two quantitative measures used to ensure the security of an image encryption scheme against any differential attack [27].

$$\boldsymbol{NPCR} = \frac{\sum_{\mathbf{i,j}} \mathbf{D(i,j)}}{\boldsymbol{M \times N}} \times \mathbf{100}\% \tag{29}$$

$$\boldsymbol{UACI} = \frac{\mathbf{1}}{\boldsymbol{M \times N}} \frac{\sum_{i,j} |\boldsymbol{C_1}(i,j) - \boldsymbol{C_2}(i,j)|}{\mathbf{255}} \times \mathbf{100}\% \tag{27}$$

where M and N are the width and height size of the plain image respectively, $\boldsymbol{C_1}(\boldsymbol{i},\boldsymbol{j})$ and $\boldsymbol{C_2}(\boldsymbol{i},\boldsymbol{j})$ are the values of the pixels in the position $(\boldsymbol{i},\boldsymbol{j})$ of the two cipher images $\boldsymbol{C_1}$ and $\boldsymbol{C_2}$ before and after changing one bit of the plain image, $\mathbf{255}$ is the number of gray levels and $D(i,j)$ is given as:

$$D(i,j) = \begin{cases} 0, & for\ \mathrm{C}_1\ (\mathrm{i},\mathrm{j}) = \mathrm{C}_2\ (\mathrm{i},\mathrm{j}) \\ 1, & for\ \mathrm{C}_1\ (\mathrm{i},\mathrm{j}) \neq \mathrm{C}_2\ (\mathrm{i},\mathrm{j}) \end{cases} \quad (28)$$

The theoretical values of $NPCR = 99.61\%$ and $UACI = 33.46$. For better and more secure encryption scheme, the values of NPCR and UACI increase above or equal to these theoretical values. For the proposed scheme, the value of one pixel which randomly chosen is modified.Then the cipher image of the original and the modified image C_1 and C_2respectively, NPCR and UACI increase above or equal to these theoretical values. For the proposed scheme, the value of one pixel which randomly chosen is modified. Then the cipher image of the original and the modified image C_1 and C_2 respectively, NPCR and UACI are computed for the different images. The result tabulated in Table (6) and compared with Ref. [3, 28].

Table 6. NPCR AND UACI Comparison

Algorithm	Image	Lena	Baboon	Barbara	Peppers	House
Ours	NPCR (%)	99.63	99.61	99.60	99.61	99.61
	UACI (%)	33.48	33.55	33.51	33.42	33.51
Ref. [3]	NPCR (%)	99.62	99.61	99.60	99.61	99.61
	UACI (%)	33.48	33.46	33.44	33.55	33.52
Ref. [28]	NPCR (%)	99.61	99.61	99.57	99.61	99.62
	UACI (%)	33.46	33.49	33.42	33.48	33.50

3.6. Complexity Analysis

Low computation complexity and fast speed are properties of a good encryption scheme. EC point multiplicationis the most time consuming operation. The proposed scheme has a low number of EC point multiplication operation if it compared to many recent EC based image encryption schemes. A comparison with other recent schemes for encryption and decryption execution time for 256×256 and 512×512image sizes, the resultes are illustrated in Table (7). From Table (8), it is obvious that the proposed scheme has a time saving compared to other schemes. Also, it uses self-invertible matrix multiplication operation to reduce the computational time. So the proposed scheme is very efficient for real time image encryption.

Table 7. Encryption time (in sec.) comparison of the tested images

Image size	256×256	512×512
Ours	0.17685	0.2151
Ref. [3]	0.23	0.68
Ref. [29]	1.170844	4.73389
Ref. [30]	0.498021	0.938217
Ref. [31]	1.44	5.41

Table 8. Encryption time saving (%) of the proposed scheme

Image size	Time saving (%)	Ref. [29]	Ref. [30]	Ref[3]	Ref. [31]
256×256		84.89%	64.49%	23.1%	87.71%
512×512		95.45%	77.07%	68.36%	95.81%

4. Conclusion

In this paper, a new dynamic fractional chaotic biometric digital identity IEC mechanism has been proposed in order to achieve a robust partial image encryption scheme. The scheme consists of two parts of encryption. Firstly, the IEC Diffie-Hellman key exchange technique is used to solve the key distribution and management problem of symmetric key encryption. Secondly, the initial state, the biometric key and the proposed modular fraction chaotic sine map are used to build the key schedule. This condition allows the system to vary the keys every process to attain a good randomness and makes the scheme more resistant. Thus, overcome the chosen plaintext attacks. The keys generated from a combination between hidden cyclic isomorphic elliptic curve, biometric key and the proposed modular fraction chaotic sine map. The encryption and decryption process depend on scrambled plain image pixel values where scrambling is performed using Arnold's transformation. The proposed modular fraction chaotic sine map generates a chaotic sequence used to construct self-invertible matrix. From the security results, the proposed system is more efficient and has faster encryption and decryption time compared with other recent chaotic map EC based schemes. It has large key space, key-dependent pixel value replacement, low correlation 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 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.
2. 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.
3. Ro. Ismail, "Secure Image Transmission Using Chaotic Enhanced Elliptic Curve Cryptography," In: IEEE Access, vol. 7, no. 18576096,2019
4. G. J. Simmons, "Symmetric and asymmetric encryption," ACM Comput.Surv., vol. 11, no. 4, pp. 305_330, 1979.
5. M. Miller, "Uses of elliptic curves in cryptography". Advances in Cryptography Crypto '85.1986; 417-426.
6. N. Koblitiz, "Elliptic curve cryptosystems". Mathematics of computation. Vol. 48; No. 177; 1987; 203-208.
7. Ar. kumar,S.S.Tyagi, Man. Rana, Ne. Aggarwal, Pa. Bhadana, A Comparative Study of Public Key Cryptosystem based on ECC and RSA, Int. Journal on Com. Sci. and Eng., Vol. 3 No. 5 May 2011
8. Esam A. A. A. Hagras,"Selective Image Encryption Based on Multi-Level 2D-DWT and Multi-Map Chaotic System,"Int. Journal of Net. Security, vol. 9, no. 4, 2010.

9. M. Essaid, I. Akharraz, A. Saaidi and A. Mouhib, "Image encryption scheme based on a new secure variant of Hill cipher and 1D chaotic maps", Jou. of Inf. Sec. and Applications no.47 pp.173–187, 2019.
10. Arr. D., Alv. G, Fer. V., On the inadequacy of the logistic map for cryptographic applications., arXiv: 0805.4355, 2008.
11. D. G. Abraham, G. M. Dolan, G. P. Double and J. V. Stevens, "Transaction Security System", IBM Systems Journal, vol. 30, no. 2, pp. 206-229,2011.
12. Dol. Si. Laiphrakpam, Man. Si. Khumanthem, "A robust image encryption scheme based on chaotic system and elliptic curve over finite field"Springer Science Business Media, Multimed Tools Appl (2018) 77:8629–8652.
13. M. Bakr, M. A. Mok., A. Ta., "Modified Elliptic Curve Cryptography in Wireless Sensor Networks Security", 978-1-5386-9239-4/18, IEEE, 2018.
14. Y. Liu., J. Li., J. Liu, J.Che., J. Liu., L. Wang and X. Bai., "Robust Encrypted Watermarking for Medical Images Based on DWT-DCT and Tent Mapping in Encrypted Domain",X. Sun et al. (Eds.): ICAIS 2019, LNCS 11633, pp. 584–596, 2019.
15. Ah. A. Abd El-Latif, X. Niua, "A hybrid chaotic system and cyclic elliptic curve for image encryption", Int. J. Electron. Commun. (AEÜ) 67 (2013) 136– 143, 2013.
16. N. A. Azam, U. Hayat, I. Ullah, "An Injective S-Box Design Scheme over an Ordered Isomorphic Elliptic Curve and Its Characterization", Sec. and Com. Net.,Vol. 2018, A. ID 3421725, pp. 9, 2018.
17. X. Zhang, L.Wang, Y. Niu , G. Cui and S. Geng, " Image Encryption Algorithm Based on the H-Fractal and Dynamic Self-Invertible Matrix, Com. Int.andNeu. Vo. 2019, A. ID 9524080, pp. 12, 2019.
18. Guo-Cheng We, DumitruBaleana, Sheng-Da Zang, "Discrete chaos in fractional sine and standard maps," Physics letter A, 378, pp 484-487, 2014.
19. G. Jak. and K. P. Sub., "Discrete Lyapunov exponent and differential cryptanalysis," IEEE Trans. Circu. Syst. II, vol. 54, no. 6, pp. 499–501, Jun. 2007.
20. S. Turner, D. Brown, K. Yiu, R. Housley, and T. Polk, "Elliptic Curve Cryptography Subject Public Key Information," RFC Editor RFC5480, 2009.
21. D. H. Ou, W. Sun, and B. Lin, "A novel image encryption scheme with the capability of checking integrity based on inverse matrix," Journal of Graphics, vol. 33, no. 2, pp. 89–92, 2012.
22. Zheng, P., Huang, J.: Discrete wavelet transform and data expansion reduction in homomorphic encrypted domain. IEEE Trans. Image Process. 22, 2455–2468 (2013).
23. Y. a. Liu, J. Li, J. Liu, J. Cheng, J. Liu, L. Wang, and X. Bai, " Robust Encrypted Watermarking for Medical Images Based on DWT-DCT and Tent Mapping in Encrypted Domain", X. Sun et al. (Eds.): ICAIS 2019, LNCS 11633, pp. 584–596, 2019.
24. G. Panchal, D. Samanta, "A Novel Approach to Fingerprint Biometric-Based Cryptographic Key Generation and its Applications to Storage Security", Computers and Electrical Engineering 0 0 0 (2018) 1–18.
25. R. K. Kodali and Prof. N.V. Sarma, "ECC implementing using Koblitz's Encoding", Dep. of Ele. and Comm. Engineering, Nat. Ins. of Technology, Warangal.

26. T. Dhanashree, S. V. Rakesh and S. K. Premnath "An Approach for Security of Images over Elliptical Curve Cryptography and Digital Signature", Int. Jou. of Com. Applications, vol. 153, no. 11, 2016.
27. Y. Wu, J.P. Noonan, S. Agaian, " NPCR and UACI randomness tests for image encryption", J. Sel. Areas Telecommun. 4 (1) (2011) 31–38.
28. Y. Luo, X. Ouyang, J. Liu and L. CAO, " An Image Encryption Method Based on Elliptic Curve Elgamal Encryption and Chaotic Systems", vol. 7, ,IEEE Access ,2019.DOI 10.1109/ACCESS.2019.
29. L. D. Singh and Kh. M. Singh, "Image Encryption using Elliptic Curve Cryptography", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), Procedia Computer Science 54 (2015) 472 – 481, Elsevier.
30. 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.
31. R. I. Abdelfatah, "A new fast double-chaotic based image encryption scheme", Multimedia Tools Appl., Springer Science+Business Media, LLC, part of Springer Nature 2019.

Ahmed Kamal, received the B.Sc. degree in Electrical Engineering from Alexandria University, Egypt in 2007, the M.Sc. degree in Electrical Engineering from Alexandria University, in 2021. He is currently a teaching assistant in communication science branch in the Air Defense College, Alexandria University. His current research interests include data protection in digital communication systems and developments of new encryption algorithms.

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 has been Head of Electronics & Communication Research Center, Armed Forces, Cairo, Egypt from 2010 to 2017. He is currently an Assistant Professor with Communications and Computer Department, Faculty of Engineering, Delta University for Science and Technology, Gamasa, Mansoura, Dakahlia, Egypt. His current research interests include data protection in digital communication systems and developments of new encryption algorithms.

H. A. El-Kamchochi Professor with Electrical Department, Faculty of Engineering, Alexandria University, Alexandria, Egypt. His current research interests include data protection in digital communication systems and developments of new encryption algorithms. https://dblp.org/pid/12/1592.html

Received: May 02, 2020; Accepted: February 17, 2021.