Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

NEW HIDING TECHNIQUE IN DIGITAL SIGNATURE BASED ON ZIGZAG TRANSFORM AND CHAOTIC MAPS

NADA E. EL-MELIGY
Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha, Egypt.
Email: nadaelmeligy@bhit.bu.edu.eg

WAGEDA I. EL-SOBKY*
Department of Basic Engineering Sciences, Benha Engineering Faculty, Benha University, Benha, Egypt.
*Corresponding Author Email: wageda.alsobky@bhit.bu.edu.eg

ASHRAF S. MOHRA
Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha, Egypt.
Email: amohra@bhit.bu.edu.eg

ASHRAF Y. HASSAN
Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha, Egypt.
Email: ashraf.fahmy@bhit.bu.edu.eg

TAMER O. DIAB
Electrical Engineering Department, Benha Faculty of Engineering, Benha University, Benha, Egypt.
Email: tamer.almarsafawy@bhit.bu.edu.eg

Abstract

This paper presents a novel approach to digital signature by integrating the ElGamal or Schnorr digital signature algorithms, chaotic systems, and scanning techniques. Briefly, ZZBCRP is a zigzag transformation that is used firstly to construct a permuted transaction, which technique starts from any random position and intersects in both directions, which is more complex than zigzag transform techniques. Then using ElGamal or Schnorr signature schemes based on chaotic maps. This modification aims to make private key and random number dependent on discrete chaotic maps. Even if the private key chosen is small, it is easy by using the huge amount of points in chaotic maps 2-D or 3-D to extract strong and unique key. This change complicates the relationship between the private key, public key and the transaction signature. A two-dimensional trigonometric discrete chaotic map is used that integrated Logistic-sine-cosine maps, and a three-dimensional hyperchaotic map (3-D SCC) which are based on a sine map. Our performance analysis shows that compared to schemes; this scheme not only improves the level of efficiency but also assures safety. The performance analysis shows that our scheme is not only more efficient compared to other related systems, but also safer.

Keywords: Digital Signature, Scanning Technique, Cryptocurrency, Chaotic Map.

1. INTRODUCTION

Digital signature is the backbone of every electronic transaction in today's world. The world trade relies tremendously on the digital signature; so many additional properties are needed. Applications include electronic mail, office automation, and blockchain [1], [2]. A digital signature is a cryptography implementation, used as an alternative to a real signature, which is used to ensure the authenticity and integrity of a message. Digital signature schemes are constructed by using asymmetric cryptographic algorithms.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

The ElGamal signature scheme is a digital signature scheme that relies on the difficulty of calculating discrete logarithms. It was described by Taher ElGamal in 1984[3] [4]. In this algorithm, each user must be had a private and public key. The private Key is used to sign the transaction and the public key is used to check if this transaction is manipulated or not. Schnorr digital signature was described by Claus Schnorr from the development of the ElGamal signature [5]. This algorithms also depend on discrete logarithm problem and has many advantage: high security, This schema has tight and strong security proof such as the results in [6] have demonstrated the security of the Schnorr schema in the Random Oracle model and has high performance, Schnorr's scheme is considered to be the most efficient signature scheme among the ElGamal signature scheme family.

At this time, there is a strong development in the blockchain and digital currencies in electronic transactions over the internet, so the ElGamal and Schnorr digital signatures are very interested in seeking applications in those systems.

One of the significant difficult issues in the classical digital signature is that the signature of the message might be longer than or as long as the message that sign. The cryptographic hash functions are used to deal with this problem [7]. A hash function converts a message of arbitrary length into a fixed length called a message digest. Hash function should satisfy some conditions to be useful in cryptographic works:

- Preimage resistance: means that when knowing the output (message digest h (m)), it is impossible to guess the original message (m).
- Strong collision resistance: meaning that infeasible to find two different message has the same message digest;
- Calculate the message digest should be very quickly.

In recent years, chaotic systems have been widely used for the development of robust cryptographic algorithms [8], [9]. These systems have proven their ability to build very robust defenses against various types of attacks. Furthermore, the systems provide a good balance between efficiency, speed, and security, making it the best candidate for secure digital signature [10]. Chaotic system has nonlinear characteristics such as unpredictability and non-prediodcity that generated by highly sensitive to the parameters and initial states. The security of chaotic digital signature schemes depends on the complexity of the applied chaotic system. Its properties, such as the widely distributed of the chaotic sequences, which make it difficult to accurately predict long term, and being sensitive to parameters.

An algorithm called the zigzag scan rearranges a two-dimensional matrix to reduce the correlation between the matrix's members. It is used for scanning in Zigzag manner. This method is used to weaken the strength of the relationship between the original plaintext which is represented by matrix 8x8, which leads to a strong cryptography algorithm [11], [12].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

Our contributions propose a new digital signature scheme with new properties suitable for work organization. We integrated a zigzag scanning method and chaotic maps with El-Gamal and schnorr digital signature to improve the security against any attacks.

The rest of paper is organized as follows: section 2 shows El-Gamal and schnorr digital signature, zigzag scanning and used of chaotic systems. In section 3 presents the new digital signature in detail. Testing and security analysis is drawn in section 4. Finally in section 5, concludes the paper.

2. DIGITAL SIGNATURES

Using the digital signature is becoming more and more necessary to assure the validity and integrity of digital documents and messages [13]–[15]. More organizations are switching from physical documents to digital ones to perform daily transactions. Digital signatures must be provided the following terms:

1. Integrity: the transaction content has not been changed since it was signed by digital signature;
2. Validity: confirm that signer is signed the transaction;
3. The signer cannot deny that signed on the transaction.

The digital signature scheme works as shown in Figure 1 as follows:

1. Hash function takes the message regardless of its size and produces the fixed message digest;
2. The message digest is encrypted by using standard cryptography, and that is called digital signature;
3. To check the signature’s authenticity and integrity, the verifier must be decrypted the digital signature by using the same cryptography scheme;
4. Calculate the hash of the message;
5. The results of steps (3) and (4) are compared.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

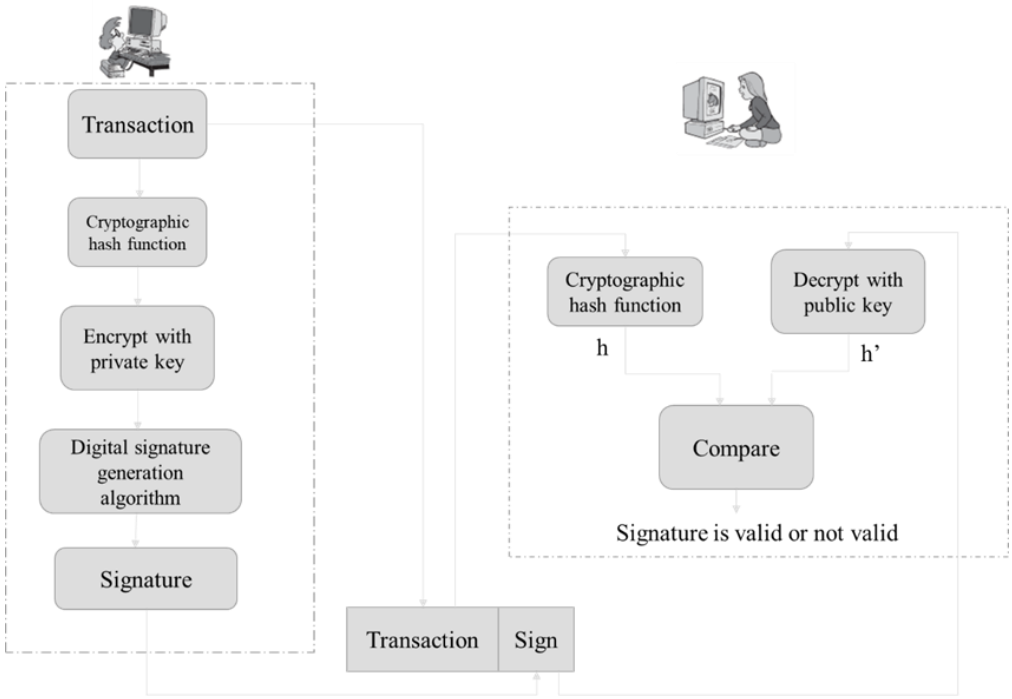


Figure 1: Digital signature

2.1. El-Gamal digital signature

El-Gamal digital signature is a powerful and practical signature scheme. El Gamal's security based on the difficulty of computing the discrete logarithm of large prime numbers. The discrete logarithm problem is a particularly difficult problem in mathematics because it mainly depends on the conditions to get all the possible solutions to it. Therefore, breaking this encryption system is almost impossible or takes a very long time. The main advantage of El-Gamal digital signature is that the same message gives different digital signatures each time it is signed [3], [16], [17].

It works as El-Gamal encryption, the global elements are (p) a large prime number and (α) a primitive root of p. User A generates public key from private key as follows:

- Select a private key SA , in which 1< SA < p-1;
- Calculate public key YA= α^{SA} mod p.

User A signs the message (M) as follows:

- Compute the hash m=H(M);
- Select a random number K_A in which 1 ≤ K_A ≤ p-1 and gcd(K_A,p-1)=1;
- Calculate S1= α^{KA} mod p;
- Calculate S2= K_A^{-1}(m- S_A * S1) mod p-1;
- The signature of message M consists of (S1, S2).

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

The signature can be verified by user B as follows:

- Calculate V1= α^m mod p;
- Calculate V2= $(Y_A)^{S1} (S1)^{S2}$ mod p;
- If V1 and V2 are equal, then the signature is valid.

2.2. Schnorr digital signature

The Schnorr digital signature depends on the discrete logarithms as El-Gamal signature scheme. This is a digital signature scheme known for its simplicity and was one of the first to have its security based on the insolvability of a given discrete logarithm problem. This is efficient and produces short signatures. The main work of signature generation is message-independent and can be performed during processor idle time [18], [19].

The global elements are (p) a prime number and (q) is a prime factor of (p-1). User A generates public key from private key as follows:

- Select an integer a, in which a^q=1 mod p;
- Select a private key s, such that 1 < S_A <q;
- Calculate public key Y_A= a ^{SA} mod p.

User A signs the message (M) as follows:

- Select a random integer r, in which 0< K_A < q;
- Calculate X= a ^{KA} mod p;
- X is concatenated with the message and hash the result S1=H(X ||M);
- Calculate S2= (K_A -(S_A *S1)) mod q;
- The signature of message M consists of (S1, S2).

The signature can be verified by user B as follows:

- Calculate V1= $(Y_A)^{S1}$ $(a)^{S2}$ mod p;
- Calculate V2=H(V1 || M);
- If S1 and V2 are equal, then the signature is valid.

3. CHAOTIC MAPS

In designing chaotic systems, it is classified into two categories of dynamic systems depended on their dimensionality: 1-D and n-D (n ≥ 2) dynamic systems [20]–[23].

- 1-D chaotic has some advantage such as low processing time, low computational complexity, easy design and simple structure;
- n-D has better performance than a one-dimensional map. High-dimensional maps are difficult to implement and computationally expensive, but their sequences can

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

be used in many areas, such as designing cryptographic algorithms that are unbreakable.

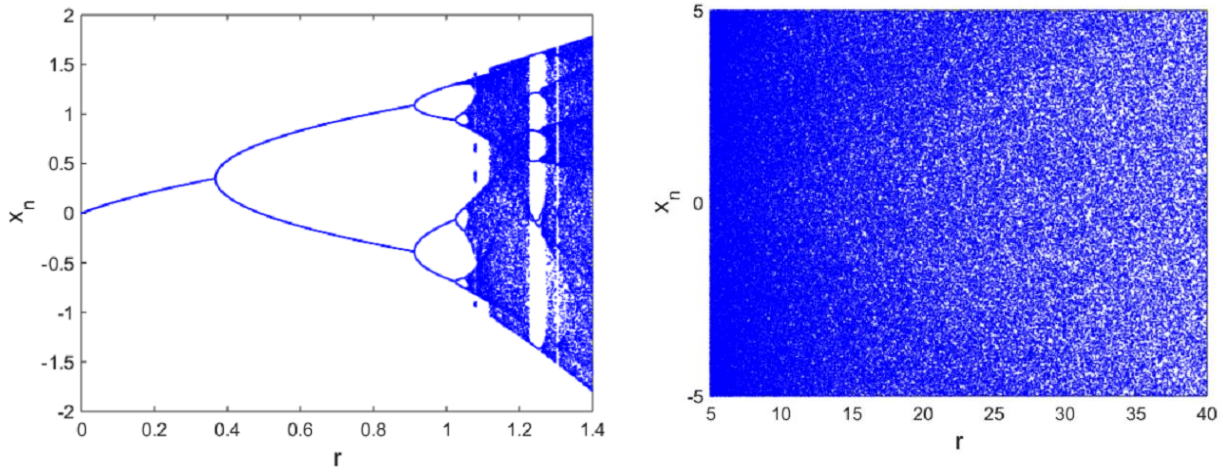
The bifurcation diagram and Lyapunov exponent are a high indicator to verify the dynamic chaotic state. The bifurcation diagram is used to provide a full view of chaotic behavior and also to indicate the chaotic parameter range. When Lyapunov exponent has large positive values, the sensitively is high and the divergence rate [24]–[27].

3.1 2D TRIGONOMETRIC MAP

2-D trigonometric is a new chaotic map with complex chaotic behavior compared to other 2-D chaotic map[28]. The proposed map is composed as defined in formula 1. The map is chaotic for r ∈ [0 ; 1000] ,ω = 100π, and x_0 = 1.5, y_0 = 0.5.

$$\begin{cases} x_{n+1} = \sin(\omega x_n) - r sin(\omega y_n) \\ y_{n+1} = \cos(\omega x_n) \end{cases}, \quad (1)$$

Hénon map dynamics transition from periodic behavior to chaotic behavior, intertwined with the periodicity of chaotic dynamics as shown in Figure 2(a). Given this parameter, a perturbation can change the system from chaotic to periodic dynamics. This type of dynamics is undesirable in real applications where the system works only in chaotic windows. To solve this problem, a triangular map with an aperiodic bifurcation diagram is used, as shown in the Figure 2(b).

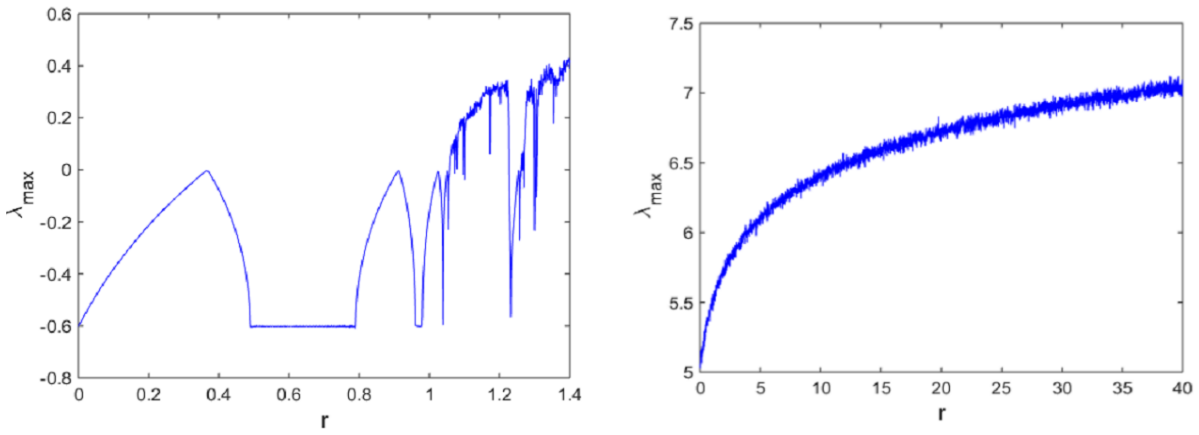


(**a**) (**b**)

Figure 2: Bifurcation plot: (a) Hénon map; (b) Trigonometric map

The highest Lyapunov exponent of Hénon map and trigonometric is computed as shown in figure 3. The highest Lyapunov exponent of the trigonometric map is always positive and get more substantial, therefore, close trajectories diverge faster.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408



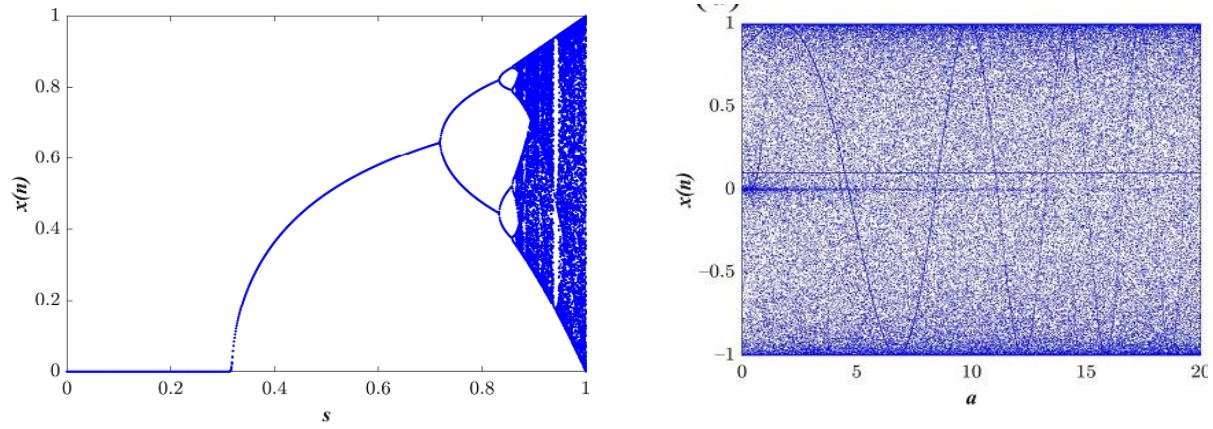
(**a**) (**b**)

Figure 3: Highest Lyapunov exponent of (a) 2-D Trigonometric map, (b)Hénon map

3.2 3D SCC chaotic map

This chaotic system is inspired from sine map, the one-domension sine chaos map is defined as follows:

$$x_{i+1} = S\sin(\pi x_i), \tag{2}$$



(**a**) (**b**)

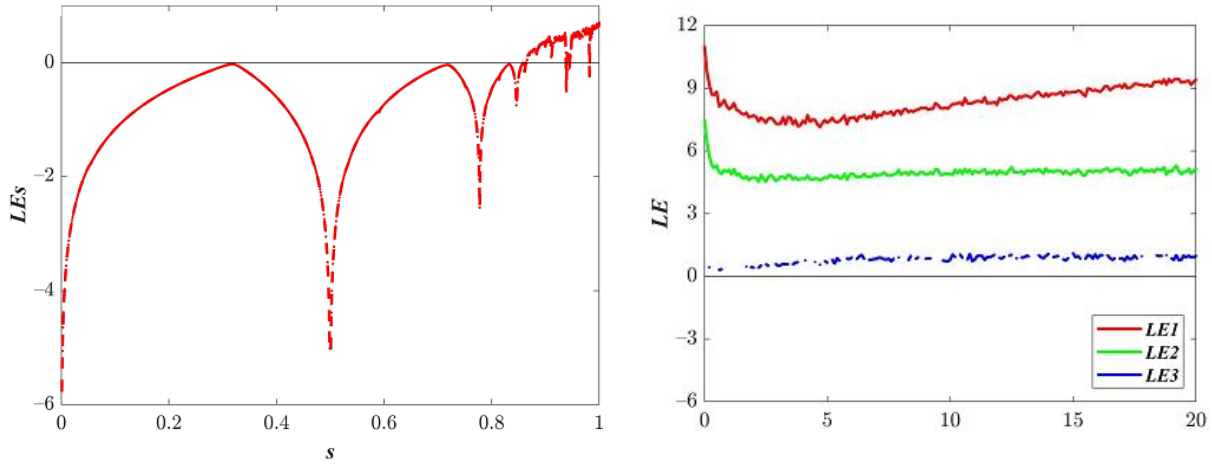
Figure 4: Bifurcation plot (a) sine map with xϵ [0, 1] and s ϵ [0.87,1], (b) 3-D SCC map with (x0, y0, z0) = (0.1, 0.1, 0.1), h=3, a ∈ [0, 20] b = 2 and c = 2

The parameter of xϵ [0, 1] and s ϵ [0.87,1] as shown in figure 4(a)[29]. In order to increase frequency diversity, cos functions added as two- dimensions as formula (3). The control parameters of this system are a,b,c,h where h ϵ [1,10], a,b,c ϵ [0,10^7] and x,y,z ϵ [-1,1].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

With its high sensitivity, infinite parameter range and high complexity, 3-D SCC exhibits desirable chaotic properties as shown in figure 4(b)[30].

$$x_{i+1}=[(ax_i+\frac{y_i^2}{x_iz_i+\epsilon})^h],$$
$$y_{i+1}=[(by_i+\frac{z_i^2}{x_iy_i+\epsilon})^h], \quad (3)$$
$$z_{i+1}=[(cz_i+\frac{x_i^2}{y_iz_i+\epsilon})^h]$$



(**a**) (**b**)

Figure 5: Lyapunov exponent of (a) sine map with xϵ [0, 1] and s ϵ [0.87,1], (b)3-D SCC map with (x0, y0, z0) = (0.1, 0.1, 0.1), h=3, a ∈ [0, 20] b = 2 and c = 2.

The most important characteristic of this type of chaotic is that with increases the LE value, The three LE values are all positive for all possible parameters as shown in figure 5(b), and that uncommon in other types of chaotic maps. That indicates that a chaotic map has good robustness and a high chaotic degree.

4. ZIGZAG SCANNING TECHNIQUE

In order to decrease the tight relationships between transaction bytes and increase the entropy value, the byte positions in the input transaction are changed using the scan approach. Zigzag transformation is used to scan all elements perpendicular to the diagonal of a matrix starting from one corner to the diagonal end as shown in figure 6(a) and so it was created one-dimensional vector containing all elements as shown in figure 6(b). The zigzag method defect is that just four one dimensional vectors may be produced since the initial scan position only starts from one of the four corners which means a continuous scan of Z words has a high correlation between elements [23], [31]–[33].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

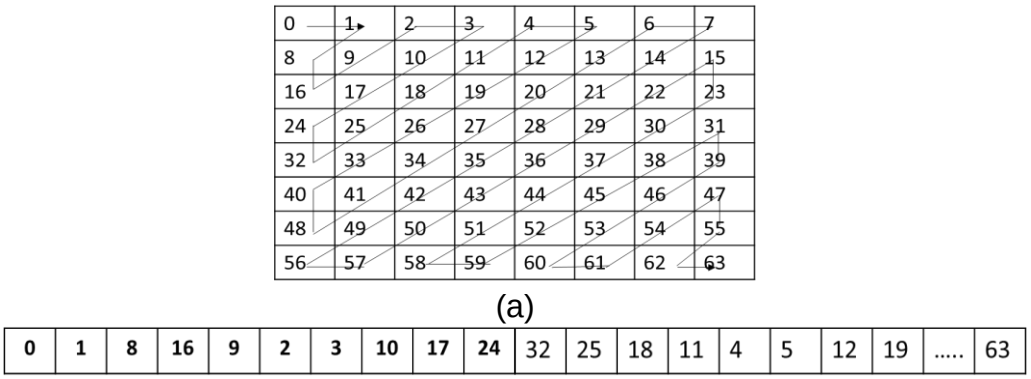


Figure 6: (a) Zigzag scan, (b) One dimensional vector

Paper [32] proposed ZZBCRP (Zigzag transform that starts at random positions and crosses bidirectionally) which solve the defect of zigzag transform by starting at any position in matrix and crosses bidirectionally. The ZZBCRP is described as follows based on selecting Z be a matrix of size n X n:

- **Step1:** choose two random number 0≤i,j≤n, where (i, j) represents the transformation's initial coordinate position;
- **Step2:** Z-scan to the higher right and the lower left corners as shown in Figure 7(a), respectively, starting from location(i,j), to produce the two vectors v1 and v2 as shown in Figure 7(b);
- **Step3:**create vector V by merging two vectors v1 and v2 as shown in Figure 7(c).

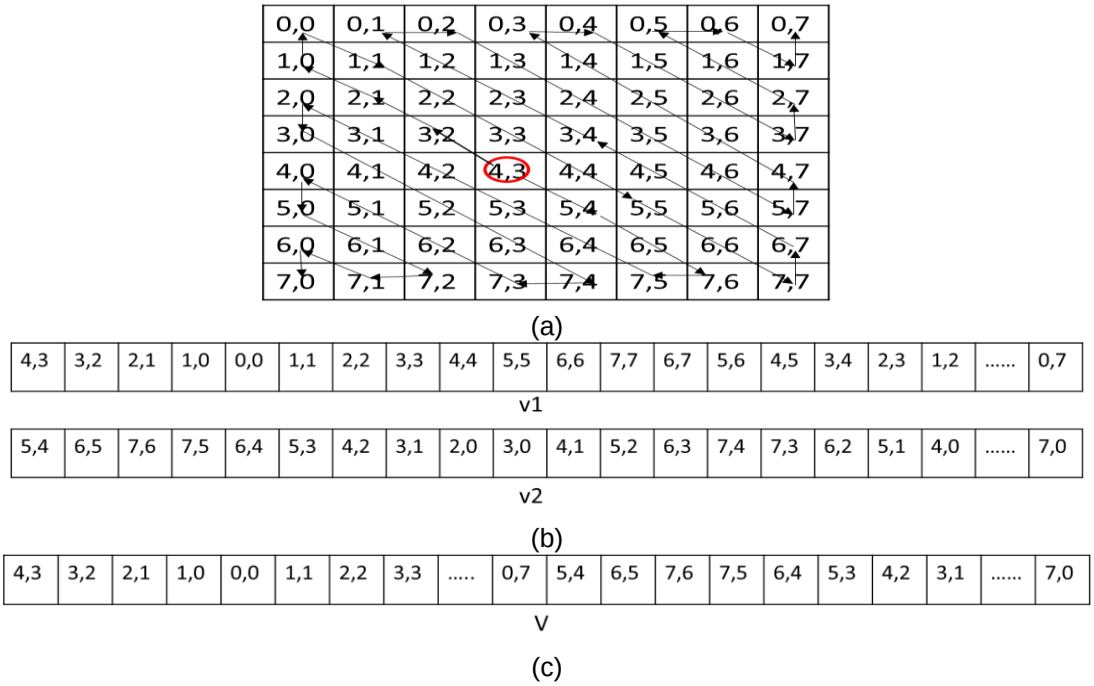


Figure 7: (a) ZZBCRP scan, (b) v1 and v2 vectors, (c) vector V

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

5. PROPOSED SCHEMES

The main objective of a proposed digital signature is generated digital signature based on a chaotic map. Each of the suggested digital signatures have a same initialization phase. The digital signature is produced as follows, as shown in Figure 8.

5.1 Initialization phase:

In this phase, the transaction is permuted by using ZZBCRP scan, and making it more complicated to rebuild.

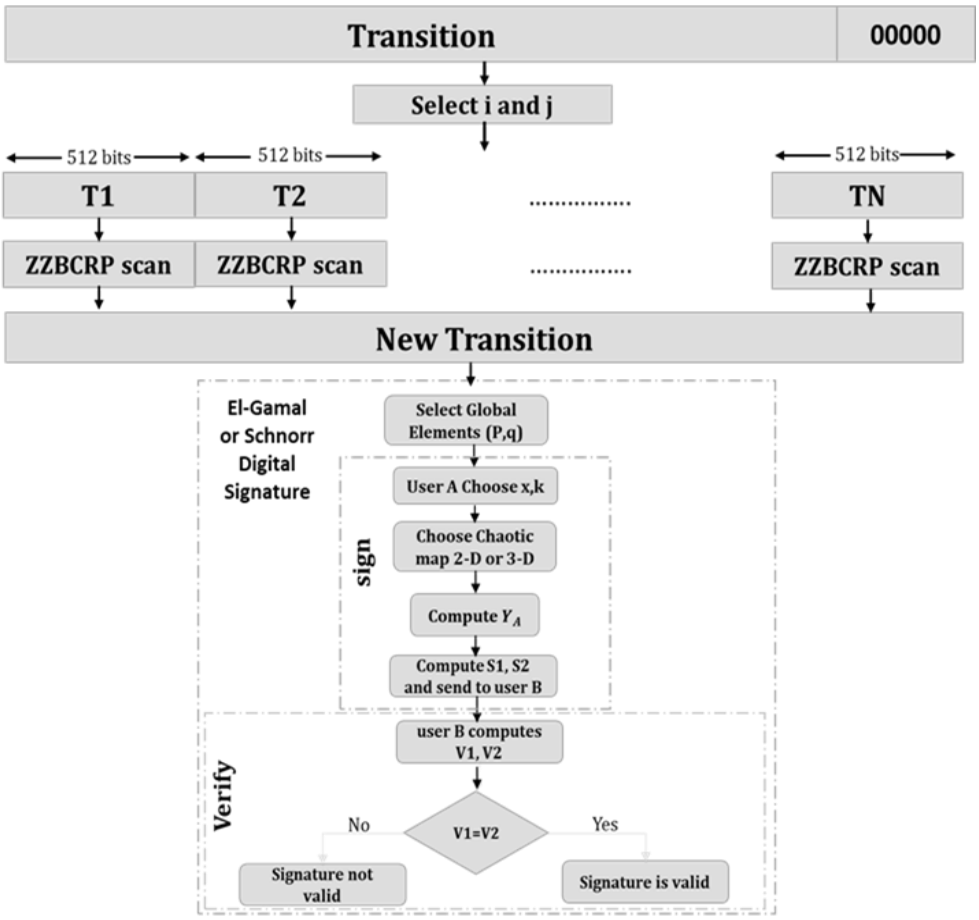


Figure 8: The proposed digital signatures

Scanning Algorithm	
Input: T (transaction), i and j(0≤ i , j≤7)	
Output: New_T	
1.	If (len(T)<(512*N)) then T=T||000..00
2.	Divide into blocks b0 …….. bN-1 each block 512 bit
3.	New_b0 ← ZZBCRP(b_0), …, New_b_{N-1} ← ZZBCRP(b_{N-1})
4.	New_T← New_b_0 ||…. || New_b_{N-1}

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

5.2 Key Generation phase:

In this phase, the signer chooses private key X and random number K (1< X,K <P-1) which is P is prime number and as shown in Chaotic map algorithm computed new private key and K.

$$Z=\begin{cases}\left(\frac{\sum_{i=0}^{n} X_i-\sum_{i=0}^{n} Y_i}{\sum_{i=0}^{n} X_i^2} * P\right) mod\ P & \sum_{i=0}^{n} X_i > \sum_{i=0}^{n} Y_i \\ \left(\frac{\sum_{i=0}^{n} Y_i-\sum_{i=0}^{n} X_i}{\sum_{i=0}^{n} Y_i^2} * P\right) mod\ p & \sum_{i=0}^{n} Y_i > \sum_{i=0}^{n} X_i\end{cases} \quad (4)$$

Chaotic map Algorithm

Input: q, X, and random number K

Output: Public key PU

1. If 2D-trigonometric chaotic map is chosen then:
   a. $X_0[0\text{-}5] \leftarrow X/512, Y \in [-1,1]$, $\omega = 100\pi$ and $r \in [0 ; 1000]$;
   b. compute $X_1, X_2, X_3, \ldots\ldots X_{N-1}$ and also $Y_1, Y_2, Y_3, \ldots\ldots Y_{N-1}$ as defined in formula 1;
   c. $X= X_0+X_1+\ldots..+X_{n-1}$ and $Y= Y_0+Y_1+\ldots..+Y_{n-1}$ (note: you choose number of iteration and range);
   d. Compute new_X as shown in formula 4.
2. else if 3D-SCC chaotic map is chosen then:
   a. $X_0[0\text{-}1] \leftarrow X/512, Y_0 \in 0.1$, $Z_0 \in 0.1$, $a \in [0, 107]$ and b = 100, c = 100 and h = 3;
   b. compute $X_1, X_2, X_3, \ldots\ldots X_{N-1}$, $Y_1, Y_2, Y_3, \ldots\ldots Y_{N-1}$ and also $Z_1, Z_2, Z_3, \ldots\ldots Z_{N-1}$ as defined in formula 3;
   c. $X= X_0+X_1+\ldots..+X_{n-1}$, $Y= Y_0+Y_1+\ldots..+Y_{n-1}$,and $Z= Z_0+Z_1+\ldots..+Z_{n-1}$ (note: you choose number of iteration and range);
   d. compute new_X as shown in formula 4

5.3 Signature Generation and verification phase

In this phase, the signer computes the public key PU and generate S1,S2 where are the signature transaction and send them to user B To verify the transaction is valid or not by computing V1 and V2.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

El-Gamal Digital signature

Input: α, q, K, X, and new_T (where q is prime number, α is primitive root of q and 1< X,K < q-1).

Output: signature is valid or not valid

1. Goto chaotic map algorithm and compute new_X from X.
2. Goto chaotic map algorithm and compute new_K from K.
3. If (gcd(new_K, q - 1) != 1) then choose another k and goto using chaotic map algorithm.
4. Public key PU= α^{new_X} mod q.
5. To sign the transaction
    a. S1= α^{new_k} mod q;
    b. U=H(new_T);
    c. S2= (new_k^{-1} (U- (S1*new_X)))mod (q-1);
    d. Compute new_X as shown in formula 4.
6. To verify the transaction
    a. U=H(new_T))q;
    b. V1=α^{U} mod q;
    c. V2= (PU^{S1})*($S1^{S2}$) mod q;
    d. if V1=V2 then signature is valid;

Schnorr Digital signature

Input: p, q, S, a, r and new_T (where p is prime number, q is prime factor of p-1, S is private key, and a is integer aq=1 mod p)

Output: signature is valid or not valid

1. Goto chaotic map algorithm and compute new_S from S.
2. Public key PU= a^{new_S} mod p
3. To sign the transaction
    a. Goto chaotic map algorithm and compute new_r from r;
    b. U= a^{new_r} mod p;
    c. E=H(U||new_T)
    d. S= (new_r-(new_S*E))% q
4. To verify the transaction.
    a. XX= (as + PUE) mod p;
    b. EE = H(XX|| new_T);
    c. If (E=EE) then signature is valid

6. RESULTS ANALYSIS

The global elements of El-Gamal digital signature is (g, y, p) are public key where y= pow(g, x) mod p and anyone can know these values, and such in Schnorr and El-Gamal digital signature y= pow(a, x) mod p. the discrete logarithm problem must be hard to prevent anyone forge a signature, but in the proposed digital signature the secret key X is entered in chaotic map 2-D or 3-D more times and sum of some iterate Xch is the new private key so no one can know the secret key and forge a signature to any transaction.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

Table 1 shows the new value of private key based on the type of digital signature chosen and chaotic map type and its certain parameters.

Table 1: lookup table for initializing private key and k.

Map	parameters	Digital signature	Values before chaotic	Initial value of x_0	Values before chaotic
2D-Trigonometric	ω = 100π, y_0 = 0.6, r=5, N=10	El-Gamal (p =997,a=990)	PR_key= 900	0.0137	PR_key= 197
			K= 968	0.0147	K= 71
		Schnorr (p=907,q=151,a=100)	PR_key =150	0.5859	PR_key = 62
			R=130	0.5078	R=19
3D-SCC	y_0=0.1, z_0=0.1, a=2, b=2, c=2, h=3,e=0, N=10	El-Gamal (p =997,a=990)	PR_key = 900	0.0137	PR_key =338
			K=298	0.0045	K=167
		Schnorr (p=907,q=151,a=100)	PR_key = 110	0.4296	PR_key =96
			R=130	0.5078	R=47

Table 2: Key Selection Methods

Algorithm	**Select public key**
El-Gamal Digital signature	based on private key which is in range of 1 and any large prime number
Schnorr Digital signature	based on private key which is in range of 1 and any large prime number
Proposed digital signature	based on Chaotic maps 2-D or 3-D
Ref [34]	use Block cipher symmetric algorithm

Tested the accuracy of the algorithm on 100000 messages using test code written in python on Intel Core 2.6 GHz processor running Windows 10 64 bit. Table 4-8 are the results obtained when implementing the used algorithm on 10 different text data. The execution time for the modified El-Gamal and schnorr is more than the original that is because dependent on the ZZBCRP scan and discrete chaotic maps.

Table 3: Test results for 100000 message tests

Digital signature algorithm	Prime Number (p)	Execution time (ms)		
		ZZBCRP scan	Signing	verifing
El-Gamal	q=39305063412410223286956703455542737154290 4833 a=39305063412410223286956703455542737154290 4744 PR=39305063412410223286956703455542737154290 9048	-	0.34725 8	0.6738269
Schnorr	p = 662411604887801410715798647 97 q = 16560290122195035267894966199 a = 16560290122195035267894966195 PR=1656029012219503526789496 6 r = 16560290122195035267894966100	-	0.1699	0.3609
El-Gamal based on 2-D	q=39305063412410223286956703455542737154290 4833	0.4823	0.6212	0.6267

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

tigonometric map	a=39305063412410223286956703455542737154290 4744 PR=39305063412410223286956703455542737154290 9048			
El-Gamal based on 3D-SCC	q=39305063412410223286956703455542737154290 4833 a=39305063412410223286956703455542737154290 4744 PR=39305063412410223286956703455542737154290 9048	0.4664	0.7018	0.6651
Schnorr based on 2-D tigonometric map	p = 662411604887801410715798647 97 q = 165602901221950352678949661 99 a = 165602901221950352678949661 95 PR=16560290122195035267894966 r = 1656029012219503526789496610 0	0.5156	0.3745	0.3939
Schnorr based on 3D-SCC	p = 662411604887801410715798647 97 q = 165602901221950352678949661 99 a = 165602901221950352678949661 95 PR=16560290122195035267894966 r = 1656029012219503526789496610 0	0.5199	0.4991	0.3964

Table 4: Comparison between algorithms for 224 bit key length

Algorithm	Time of signature (ms)	Time of verification (ms)
El-Gamal	0.4946	1.4503
Schnorr	0.1310	0.2075
El-Gamal DS based on 2D-Trigonometric	1.3081	1.4480
El-Gamal DS based on 3D-SCC	1.3456	1.4634
Schnorr DS based on 2D-Trigonometric	0.3924	0.2609
Schnorr DS based on 3D-SCC	0.5075	0.2538
Ref [35]	3,5000	5,2200

Table 5: El-Gamal Digital signature based on 3D-SCC for 100000 msg

	Length of characters	ZZBCRP scan (ms)	Signing (ms)	Verifying (ms)
1	208	0.2634	0.6562	0.6213
2	416	0.4982	0.6938	0.6317
3	624	0.9008	0.7142	0.6576
4	823	1.1226	0.6844	0.6421
5	1040	1.1985	0.6778	0.6319
6	1248	1.4761	0.6430	0.7412
7	1456	1.5536	0.6668	0.6416
8	1660	1.9041	0.6967	0.6656
9	1868	2.0275	0.7151	0.6668
10	2076	2.1079	0.6727	0.6371

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

Table 6: Schnorr Digital signature based on 3D-SCC for 100000 msg

	Length of characters	ZZBCRP scan (ms)	Signing (ms)	Verifying (ms)
1	208	0.2680	0.4740	0.3997
2	416	0.5077	0.4761	0.3807
3	624	0.6125	0.4800	0.3849
4	823	0.8468	0.4630	0.4010
5	1040	1.0947	0.4577	0.3969
6	1248	1.2205	0.4619	0.4115
7	1456	1.4586	0.4676	0.3963
8	1660	1.5464	0.4819	0.4007
9	1868	1.8187	0.4762	0.3942
10	2076	2.0536	0.4813	0.3969

Table 7: El-Gamal Digital signature based on 2D-trigonometric for 100000 msg

	Length of characters	ZZBCRP scan (ms)	Signing (ms)	Verifying (ms)
1	206	0.2792	0.5656	0.6529
2	416	0.5018	0.5743	0.6327
3	624	0.5957	0.5567	0.6353
4	832	0.8734	0.5350	0.6461
5	1040	1.1112	0.5583	0.6273
6	1248	1.2564	0.5906	0.6554
7	1456	1.5066	0.5720	0.6413
8	1660	1.6698	0.5879	0.6603
9	1868	1.8728	0.5884	0.6553
10	2076	2.1191	0.5791	0.6520

Table 8: Schnorr Digital signature based on 2D-trigonometric for 100000 msg

	Length of characters	ZZBCRP scan (ms)	Signing (ms)	Verifying (ms)
1	208	0.2429	0.3235	0.4375
2	416	0.5316	0.3731	0.3978
3	624	0.6214	0.3685	0.3865
4	832	0.9137	0.3595	0.3936
5	1040	1.1344	0.3629	0.3992
6	1248	1.2382	0.3679	0.4094
7	1456	1.4954	0.3742	0.3827
8	1660	1.5881	0.3707	0.4051
9	1868	1.7992	0.3700	0.3878
10	2076	2.0303	0.3619	0.3892

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

7. CONCLUSIONS

The most important goal of any digital signature algorithm satisfying security. The proposed method improves the security performance by using ZZBCRP technique and different types of chaotic maps (2-D trigonometric and 3-D SCC chaotic maps). Confidentiality, authentication and integrity are also guaranteed. This paper proposes improving digital signature algorithms in two aspects: permutation of the original transaction and modification the transaction signature S1 and S2 to be depended on sensitivity to change in initial conditions and control parameters of chaotic maps. These algorithms were tested for different sizes of parameters and messages. The results of the experiments indicate that the proposed digital signature algorithms provide high security and quality of service.

References

1. A. Capponi, S. Olafsson, and H. Alsabah, Proof-of-Work Cryptocurrencies: Does Mining Technology Undermine Decentralization?, *SSRN Electron. J*., pp. 1–53, 2021, doi: 10.2139/ssrn.3869144.
2. F. Tschorsch and B. Scheuermann, Bitcoin and beyond: A technical survey on decentralized digital currencies, *IEEE Commun. Surv*. Tutorials, vol. 18, no. 3, pp. 2084–2123, 2016, doi: 10.1109/COMST.2016.2535718.
3. T. Elgamal, a Public Key Cryptosystem and a Signature based on Discrete Logarithms, *IEEE Trans. Inf. Theory*, vol. 31, pp. 10–18, 1976.
4. E. Edition, O. Systems, S. Edition, and B. D. Communications, *the William Stallings Books on Computer Data and Computer Communications*, Eighth Edition, vol. 139, no. 3. 2011.
1. Schnorr, C.P. Efficient signature generation by smart cards *J. Cryptol*., vol. 4, no. 4995082, pp. 161–174, 1991.
2. D. Pointcheval and J. Stern. Security arguments for digital signatures and blind signatures. *J. Cryptol.*, vol. 13, no. 3, pp. 361–396, 2000, doi: 10.1007/S001450010003.
3. N. E. El-Meligy, T. O. Diab, A. S. Mohra, A. Y. Hassan, and W. I. El-Sobky, a Novel Dynamic Mathematical Model Applied in Hash Function Based on DNA Algorithm and Chaotic Maps. *Mathematics*, vol. 10, no. 8, 2022, doi: 10.3390/math10081333.
4. X. Chai, Z. Gan, K. Yuan, Y. Chen, and X. Liu. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Comput. Appl.*, vol. 31, no. 1, pp. 219–237, 2019.
5. H. Nasry, A. A. Abdallah, A. K. Farhan, H. E. Ahmed, and W. I. E. Sobky. Multi Chaotic System to Generate Novel S-Box for Image Encryption. *J. Phys. Conf. Ser.*, vol. 2304, no. 1, 2022, doi: 10.1088/1742-6596/2304/1/012007.
6. S. F. Yousif, A. J. Abboud, and H. Y. Radhi. Robust Image Encryption with Scanning Technology, the El-Gamal Algorithm and Chaos Theory. *IEEE Access*, vol. 8, no. August, pp. 155184–155209, 2020, doi: 10.1109/ACCESS.2020.3019216.
7. J. Wenli, Z. Minrui, and J. Yuping. Research on digital image scrambling algorithm based on Zigzag transform. *Comput. Appl. Softw.*, vol. 26, no. 3, pp. 71–73, 2009.
8. M. Padmaa and D. Y. Venkataramani. ZIG-ZAG PVD—A nontraditional approach. *Int. J. Comput. Appl.*, vol. 5, no. 6, pp. 5–10.

ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

9. M. H. Mohamed*, W. I. El Sobky, and S. Hamdy. Elliptic Curve Digital Signature Algorithm Challenges and Development Stages. *Int. J. Innov. Technol.* Explor. Eng., vol. 10, no. 10, pp. 121–128, 2021, doi: 10.35940/ijitee.j9433.08101021.

10. W. Fang, W. Chen, W. Zhang, J. Pei, W. Gao, and G. Wang. Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *Eurasip J. Wirel. Commun.* Netw., vol. 2020, no. 1, 2020, doi: 10.1186/s13638-020-01665-w.

11. G. Babatunde, A. Elisha Okeyinka, O. Alao, B. Gbadamosi, and R. Oluwaseun Ogundokun. Application of SHA-256 in Formulation of Digital Signatures of RSA and Elgamal Cryptosystems *Oper. Res. Inf. Eng.*, vol. 1, no. 2, pp. 61–66, 2018, [Online]. Available: http://www.aascit.org/journal/orie.

12. A. M., An Organizational Signature Schemes based on ElGamal Signature. *Int. J. Appl. Inf. Syst.*, vol. 10, no. 4, pp. 6–9, 2016, doi: 10.5120/ijais2016451483.

13. R. A. Haraty, A. N. El-Kassar, and B. M. Shebaro. A comparative study of elgamal based digital signature algorithms. 2006 World Autom. Congr. WAC'06, no. August, 2006, doi: 10.1109/WAC.2006.375953.

14. Seurin and Yannick. On the Exact Security of Schnorr-Type Signatures in the Random Oracle Model. *Cryptol.* ePrint Arch. Int. Assoc. Cryptologic Res., 2023.

15. H. D. Luu. Some Variants of the Schnorr Signature Schema on the Finite Field and the Elliptic Curve. *J. Sci. Tech.*, vol. 11, no. 2, pp. 7–22, 2022, doi: 10.56651/lqdtu.jst.v11.n02.532.ict.

16. S. Mansoor, P. Sarosh, S. A. Parah, H. Ullah, M. Hijji, and K. Muhammad. Adaptive Color Image Encryption Scheme Based on Multiple Distinct Chaotic Maps and DNA Computing *Mathematics*, vol. 10, no. 12, 2022, doi: 10.3390/math10122004.

17. M. Lawnik and M. Berezowski. New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography. *Symmetry* (*Basel)*., vol. 14, no. 5, pp. 1–18, 2022, doi: 10.3390/sym14050895.

18. D. Ibrahim, K. Ahmed, M. Abdallah, and A. A. Ali. A New Chaotic-Based RGB Image Encryption Technique Using a Nonlinear Rotational 16 × 16 DNA Playfair Matrix, Cryptography, vol. 6, no. 2, 2022, doi: 10.3390/cryptography6020028.

19. K. A. Hussein, S. A. Mehdi, and S. A. Hussein, "Image Encryption Based on Parallel Algorithm via Zigzag Manner with a New Chaotic System. Xinan Jiaotong Daxue Xuebao/*Journal Southwest Jiaotong* Univ., vol. 54, no. 4, 2019, doi: 10.35741/issn.0258-2724.54.4.29.

20. M. Alawida, A. Samsudin, N. Alajarmeh, J. Sen Teh, M. Ahmad, and W. H. Alshoura. A Novel Hash Function Based on a Chaotic Sponge and DNA Sequence. IEEE Access, vol. 9, pp. 17882–17897, 2021, doi: 10.1109/ACCESS.2021.3049881.

21. F. Yang, X. An, and L. Xiong. A new discrete chaotic map application in image encryption algorithm. *Phys. Scr.*, vol. 97, no. 3, 2022, doi: 10.1088/1402-4896/ac4fd0.

22. B. Yousif, F. Khalifa, A. Makram, and A. Takieldeen. A novel image encryption/decryption scheme based on integrating multiple chaotic maps. *AIP Adv.*, vol. 10, no. 7, 2020, doi: 10.1063/5.0009225.

23. Hala Saeed, Hossam E.Ahmed, Tamer O.Diab, Hossam L.Zayed, Hany Nasry Zaky, and Wageda I.Elsobky. Evaluation of the Most Suitable Hyperchaotic Map in S-Box Design Used in Image Encryption. *International Journal of Multidisciplinary Research and Publications* (IJMRAP), Volume 5, Issue 4, pp. 176-182, 2022

24. N. Tsafack et al. A New Chaotic Map with Dynamic Analysis and Encryption Application in Internet of Health Things. *IEEE Access*, vol. 8, pp. 137731–137744, 2020, doi: 10.1109/ACCESS.2020.3010794.

25. J. Griffin. The Sine Map. no. 3, pp. 1–9, 2013.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 09-2023
DOI: 10.5281/zenodo.8379408

26. H. Zhong, G. Li, X. Xu, and X. Song, Image Encryption Algorithm Based on a Novel Wide-Range Discrete Hyperchaotic Map. *Mathematics*, vol. 10, no. 15, pp. 1–23, 2022, doi: 10.3390/math10152583.

27. X. Xu and J. Feng. Research and implementation of image encryption algorithm based on Zigzag transformation and inner product polarization vector. *Proc. IEEE Int. Conf.* Granul. Comput., pp. 556–561.

28. H. Gao and X. Wang. Chaotic Image Encryption Algorithm Based on Zigzag Transform with Bidirectional Crossover from Random Position. *IEEE Access*, vol. 9, no. Icmic, pp. 105627–105640, 2021, doi: 10.1109/ACCESS.2021.3099214.

29. M. Abbadi. A new message authentication technique using zigzag manipulation and block chaining. *Journal of Applied Sciences*, vol. 8, no. 21. pp. 3863–3870, 2008, doi: 10.3923/jas.2008.3863.3870.

30. P. Kuppuswamy. A New Efficient Digital Signature Scheme Algorithm based on Block cipher. *IOSR J. Comput. Eng.*, vol. 7, no. 1, pp. 47–52, 2012, doi: 10.9790/0661-0714752.

31. S. Kazmirchuk, A. Ilyenko, S. Ilyenko, O. Prokopenko, and Y. Mazur. The Improvement of Digital Signature Algorithm Based on Elliptic Curve Cryptography. Adv. *Intell. Syst. Comput.*, vol. 1247 AISC, no. January, pp. 327–337, 2021, doi: 10.1007/978-3-030-55506-1_30.