Defence Science Journal, Vol. 74, No. 6, November 2024, pp. 893-903, DOI : 10.14429/dsj.74.19877
© 2024, DESIDOC

Fuzzy Soft Set-Based Identification of Best Chaotic System for Security Applications

Meenakshi Agarwal[#,*], Arvind[$], Chaman Arya[!], and Ram Ratan[!]

[#]*Department of Mathematics, University of Delhi, Delhi – 110 007, India*
[$]*Department of Mathematics, Hansraj College, University of Delhi, Delhi – 110 007, India*
[!]*DRDO-Scientific Analysis Group, Delhi - 110 054, India*
[*]*E-mail: ameenakshi68.ma@gmail.com*

ABSTRACT

Identifying the most suitable chaotic system from a pool of options to embed in a cipher system is crucial for ensuring the security of sensitive information. Selecting the wrong chaotic system can have serious repercussions on data security. This paper proposes an identification methodology that uses fuzzy soft set criteria to identify the best chaotic system. The methodology quantifies the graphical representation of chaotic system attributes. Then it uses these quantifications to make decisions based on score values computed from the fuzzy soft set, fuzzy soft matrix, and dominancy matrix. Simulation results demonstrate that this methodology allows for the accurate identification of the most suitable chaotic system without any uncertainty. Moreover, it may also help identify weaker chaotic systems and improve them to meet the desired level of security.

Keywords: Information security; Cryptography; Chaotic system; Chaotic characteristics; System identification

1. INTRODUCTION

With the advancements in science and technology, accessing and exchanging information has become convenient for users over current computer and communication networks. Securing vital digital data is one of the major issues faced by users in the digital world. An encryption system plays an important role in information security to prevent critical information from being unauthorized. The encryption algorithm of an encryption system transforms vital plane data into cipher data which does not show any intelligible information. Such ciphered data is kept in storage media or communicated securely over a channel from sender to receiver. The data to be secured by an encryption system may be speech, text, video, image, map, and multimedia. An encryption system is designed by applying appropriate cryptographic design principles, which are based on the concepts of information security which deal with the privacy, confidentiality, authenticity, and non-repudiation of information[1-2]. The security strength of an encryption system depends on the difficulties of cracking its encryption algorithm apart from other security measures such as access control, integrity, key management, emergency erasure, tamper detection, and response mechanisms. Within the cutting-edge time of advanced innovations, communication, and computer systems if a user does not have the appropriate encryption systems and enough security measures, an adversary may get access to sensitive data and misuse it. The utilisation of encryption systems is expanding continuously because of their major part in endless security applications in defense services, banking, telemedicine, and indeed within the entertainment industries. Conventional encryption methods do not seem more suitable for encrypting certain data types such as images and videos and for encrypting such data, researchers have suggested new based on chaotic theory and quantum theory[3-4].

Chaos is a common objective phenomenon found in nature which is required in chaotic cipher systems. The characteristics of chaos make chaotic theory very useful in various scientific fields including cryptography. The chaotic maps are categorised as One-Dimensional (1D) or High-Dimensional (HD) based on state variables[5-7]. The 1D chaotic maps are not so secure as compared to the HD chaotic maps having better chaotic performance but they have complex structures. The Hybrid chaotic systems consist of multiple chaotic maps to achieve high chaotic characteristics values and randomness. Chaos-based cipher systems provide good security strength depending on the structure of encryption algorithms and the characteristics of chaotic maps employed[8-11]. Numerous developers are providing chaos-based cipher systems to the customers and everybody is claiming that their systems attain high security to sensitive information. It has been found that due to some flaws in the embedded chaotic map, some of the encryption algorithms that were claimed to be secure are insecure, and ciphered data can be analysed to gain meaningful information about the key, algorithm, and data[12-17]. Before acquiring a chaos-based cipher system, it is an essential task for users to gather the specifics of security parameters and select the chaotic system that best meets their needs in terms of security.

The inherent difficulties are often immense in the selection of a chaotic system. There are no simple and precise quantitative measures that enable an automatic decision, a chaotic system is better than others. A chaotic system consists

Received : 06 February 2024, Revised : 23 July 2024
Accepted : 12 September 2024, Online published : 25 November 2024

of numerous attributes and sub-attributes. The attribute values of a chaotic system that appear in graphical form are quantified by measuring the proportionate area covered in the graphs of chaotic characteristics. When numerous attributes are present and ambiguous situations are arrived then choosing the best becomes complex and challenging. To better handle this issue, researchers have presented different decision-making methodologies. Various multi-criteria decision-making techniques have been documented by researchers[18-19] including the forced decision matrix approach[18], the analytic hierarchy process[18], the Delphi method[18], and the decision matrix approach[18]. These techniques rely on the judgment of experts and are useful when quantitative measures about the systems are accessible.

A pattern recognition-based identification approach can be applied to find an appropriate chaotic system. Various decision-making methods are reported. A classical method cannot be used to handle the complexity of vagueness and to arrive at the right decision. For making the right decision in complex and ambiguous situations the fuzzy set-based approaches are found more suitable[20]. The study built a game model for production decisions related to new energy vehicles and traditional fuel vehicles under a dual credit policy[18-19]. Decision-making models in agriculture are reviewed which targets the potential of mathematical model-based decision making[20]. Roy*, et al.* studied soft set theory and found its applications in decision-making problems[21]. The validity of the Roy–Maji method is discussed and its limitations are found[22]. The study considers the selection of light machine guns as a multiple-criteria decision-making problem[23]. The techniques[18-23] utilising multi-decision criteria based on a decision matrix are applicable when quantitative data about the systems is available. The recognition methods from imprecise data involving fuzzy soft sets are reported[20-22,24-26] for finding the best decision. The fuzzy soft set theory[22,27-29] developed is being used in many different areas. A method under an interval-valued intuitionistic fuzzy environment is reported by linear programming[30]. A fuzzy decision approach based on an opinion score matrix is reported to solve multi-criteria decision problems that require experts' intervention[31]. Fuzzy soft sets were used by Kirişci[32] to help in decision-making in medical applications. They are utilized to help energy planners to utilize resources for sustainable development[33]. A fuzzy soft set-based group decision procedure is developed to solve multi-attribute group decision-making with linguistic Z-numbers[34].

The soft set theory has yielded valuable insights into how decisions are made and applied in different situations. Since the soft set handles the binary case, but to handle the non-binary case, the soft set needs to express itself in fuzzy form. Many researchers have studied fuzzy soft sets, and shown their applications in decision-making problems[3,23,35-38]. It is seen that methods[22,38] are failing to arrive at the correct decisions. These methods use dominancy values and general scoring alone to decide the option. The use of dominancy values as well as scoring values provides the results correctly without ambiguity and stuck the decision[39].

This paper presents a fuzzy soft set decision criterion-based identification methodology to find the best chaotic system among several chaotic systems. The fuzzy soft sets, fuzzy soft matrix, Σ-fuzzy set, dominance matrix, and score matrix are all used in the suggested methodology. As the approaches, using either score values or dominancy values, do not give correct options, the method suggested using both values provides an accurate decision for more extensive data. Simulation study and observations on catered data for attributes and sub-attributes demonstrate the identification results correctly. The attributes used in the methodology are computed appropriately by the algorithm discussed in the paper.

1.1 Highlights

- Identification methodology finds the best chaotic system among several systems using multivariable fuzzy soft decision criteria
- Computed attribute values quantitatively for chaotic characteristics represented graphically by measuring proportionate regions covered in the figures
- Decision is obtained based on the score values computed from the fuzzy soft set, fuzzy soft matrix, and dominancy matrix
- Methodology performs well for several chaotic systems and provides the best suitable systems without mistakes
- The methodology can be extended for various cryptographic and hardware security measures to find the best system.

2. FUZZY SOFT SETS AND CHAOTIC CIPHER SYSTEM

The section presents a brief introduction to a chaotic cipher system and the definitions of fuzzy soft sets utilized in our decision methodology. We extract the fuzzy soft set definitions from several relevant papers[39-41].

2.1 Chaotic Cipher System

A chaotic cipher system[40] is a software/hardware unit that uses chaotic functions and cryptography to secure vital information. It utilizes a Random Number Generator (RNG) based on different approaches such as shift registers, non-linear functions, and chaotic maps. The input/output, RNG, and encryption/decryption modules are the main components of a cipher system. The RNG may be pseudo or true depending on deterministic and non-deterministic nature. The RNG module creates arbitrary bits when a call is started by a sender. The key planning module receives these bits and produces initial bits. These initial bits are utilized to initialize the encryption algorithm module. After initializing with specific initial bits for each message, the stream cipher-based encryption algorithm module generates a key sequence that is added bit-by-bit using the *XOR* operation with an input message coming from the input module to deliver the encrypted message. The output module sends the encrypted message via secure communication protocols to the recipient where encrypted data is decrypted to get a plain message. To protect the chaotic cipher system from cryptanalytic attacks, the embedded chaotic system should be carefully developed and examined for its cryptographic strength. The chaotic function employed plays an important role in achieving the security strength of chaotic cipher systems. The mathematical and statistical robustness of the embedded chaotic system are essential measures for a secure encryption system. The goal of an attacker is to extract the details of the algorithm, keys, sequences, and message. Even with unlimited computational power and encrypted data, a chaotic cipher system should not leak any information by the Shannon criteria. Security solely depends on the keys and not on obscuring cryptographic algorithms by Kerckhoff's criteria, which means that everything about the algorithm aside from the keys is available to the public. Thus, the security strength of a chaotic cipher system is based on the embedded chaotic system which is further based on its attributes each of which is dependent on the sub-attributes.

2.2 Fuzzy Soft Sets

This paper denotes U as an initial universal set and E as the set of possible parameters which are attributes, characteristics, or properties of the objects in U. The set of all subsets of U will be denoted by $P(U)$, and $A \subseteq B$ is the choice attribute set.

Fuzzy set[18] is given by $A = \{\mu_A(x) \mid x \in U, \mu_A(x) \in [0,1]\}$ where, $\mu_A : U \to [0,1]$ is the membership function of A, which describes the membership degree of each element x to the fuzzy set A. The closer $\mu_A(x)$ is to 1, the more likely x belongs to A.

Soft Set[21] A pair (F, A) is a soft set over U, where F is a mapping given by $F : A \to P(U)$. In other words, a soft set over U is a parametrised family of subsets of the universe U. For $a \in A, F(a)$ is called the set of a- approximate elements of the soft set (F, A).

Fuzzy soft set[21] Let $\gamma_A(e)$ be a fuzzy set over U for all $e \in E$. A fuzzy soft set Γ_A over U is a set defined by a function γ_A representing a mapping $\gamma_A : E \to F(U)$ such that $\gamma_A(e) = \varnothing$ if $e \notin A$. Here, γ_A is called the fuzzy approximate function of the fuzzy soft set Γ_A and the value $\gamma_A(e)$ is a fuzzy set called e- element of the fuzzy soft set for all $e \in E$. Thus, a fuzzy soft set Γ_A over U can be represented by the set of ordered pairs $\Gamma_A = \{(e, \gamma_A(e)) : e \in E, \gamma_A(e) \in F(U)\}$. Since $\gamma_A(e) \in F(U), \mu_{\gamma_A(e)} : U \to [0,1]$ is a membership function of the fuzzy set $\gamma_A(e)$ for every $e \in E$. Therefore, A fuzzy soft set can also be represented as

$$\Gamma_A = \{(e, \mu_{\gamma_A(e)}(u)) : e \in E, u \in U, \gamma_A(e) \in F(U)\} \tag{1}$$

Characteristic function and Fuzzy soft matrix[28] Let Γ_A be a fuzzy soft set over U. Then a subset of $U \times E$ is uniquely expressed by $R_A = \{u \times e \mid e \in A, \mu_{\gamma_A(e)}(u) > 0\}$, this is a relation of Γ_A. The characteristic function of R_A is defined as $\chi_A : U \times E \to [0,1]$ and it is given by

$$\chi_A(u,e) = \begin{Bmatrix} \mu_{A(e)}(u), if (u,e) \in R_A \\ 0, otherwise \end{Bmatrix} \tag{2}$$

If $U = \{u_1, u_2, \ldots, u_m\}$, $E = \{e_1, e_2, \ldots, e_n\}$, $A \subseteq E$ and $A_{i,j} = \chi_{R_A}(u_i, e_j), i = 1,2,\ldots,m,$ $j = 1,2,\ldots,n$ then fuzzy soft matric is given by:

$$[A_{i,j}]_{m \times n} = \begin{pmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mn} \end{pmatrix} \tag{3}$$

This fuzzy soft matrix is of size $m \times n$ of fuzzy soft set Γ_A over U. The fuzzy set Γ_A is uniquely characterised by the matrix $[A_{i,j}]_{m \times n}$. Accordingly, we can identify any fuzzy soft set by its fuzzy soft matrix.

Dominancy matrix[39,41] is created by comparing the parametric values of the objects, and d_{ik} defines each entry where,

$$d_{ik} = \#\{j : A_{ij} \geq A_{kj}\}, i,k \in \{1,2,\ldots,m\}, j = \{1,2,\ldots,n\} \tag{4}$$

Σ-Fuzzy set[39] A Σ-Fuzzy set corresponding to the fuzzy soft set $\Gamma_A \in FS(U)$ (set of fuzzy soft sets over U) is denoted by γ_{Γ_A} and defined by:

$$\gamma_{\Gamma_A} = \{u / \mu_{\gamma_{\Gamma_A}} \mid u \in U\} \tag{5}$$

Membership function[18] $\mu_{\gamma_{\Gamma_A}} : U \to [0,1]$ is defined by $\mu_{\gamma_{\Gamma_A}} = \frac{1}{|A|}\sum_{e \in A} f_e(u), u \in U$. Here, $f_e(u) = \min_{u \in U}(AV(e), \mu_{\gamma_A(e)}(u))$ for each $e \in A$ and $AV : U \to [0,1]$ is given as $AV(e) = \max_{u \in U}(\mu_{\gamma_A(e)}(u))$.

3. ATTRIBUTES VALUES FOR CHAOTIC AND RANDOMNESS CHARACTERISTICS

This section discusses the computing of attribute values for chaotic and randomness characteristics. These values are computed by quantifying graphical details of various chaotic characteristics[42-46]. Thus, minimizing human intervention in the automatic decision process. The precision in computing the attribute values is taken of the order of degree 4 (up to 4 decimal digits).

3.1 Values for Chaotic Attributes

The first attribute set, we consider stands for chaotic characteristics in which phase diagram, sensitivity, Lyapunov exponent spectrum, bifurcation diagram, entropy, 0-1 test, and variability represent its sub-attributes.

3.1.1 Phase Diagram

It shows the movement path of a dynamical system's outputs obtained by plotting a x_n v/s x_{n+1} graph. It reflects the randomness of a chaotic map. For a cryptographically useful map, the trajectory never closes or repeats. Moreover, a chaotic map occupying larger distribution areas exhibits higher ergodicity and randomness. The sub-attribute is measured by finding the proportion of the phase plane occupied by the phase diagram. For this, a sequence of length n is generated and the phase diagram is plotted. Since each term of the chaotic sequence takes a value from the interval (0,1). Therefore, the phase diagram lies in the rectangle (0,1)×(0,1). In the figure, the rectangle is divided into $n \times n$ grids of equal area. A matrix C of order $N \times N$ is generated whose elements correspond to $n \times n$ grids. The entries are either 0 or 1. It is 1 if any one point of the trajectory lies in the corresponding grid and if, not even a single point lies in the grid, then the corresponding entry is taken 0. A counter is run on a total number of elements of C which takes an increment for every non-zero entry of C. The final counter value is divided by n^2 to find the proportion of the phase space occupied by the phase diagram. For illustration, the phase value attribute for the phase diagram given in Fig. 1(a) obtained is 0.0007 for a chaotic sequence of 1000 terms generated by a logistic map with control parameter $r = 3.9$.

3.1.2 Sensitivity

It is the property that shows the dissimilarity and deviating trajectories for a small change in control parameters and seed values. A good chaotic system exhibits high sensitivity concerning small changes in its control parameters. A chaotic map should be highly sensitive concerning its control parameter and initial value. To find the coefficient of key sensitivity of a chaotic system, we choose a control parameter value K1 and change only one decimal digit of K1 to get K2 and use them to generate chaotic sequences $\{x(i)\}$ and $\{x^{'}(i)\}$ of the desired length n. The difference profiles of these two sequences are considered to present the sensitivity. The sequence $\{z(i) = \{x(i) - x^{'}(i)\}\}_{i=1}^{n}$ lies in the interval [-1,1]. To calculate the sub-attribute value, the interval is divided into n sub-intervals of equal length. An array, C, of order $1\times n$ is generated. Out of n terms of $z(i)$ If m are lying in the j^{th} sub-interval then $C(j)=m$. A counter is run on the total number of elements of C which takes an increment for every non-zero entry of C. The final counter value is divided by n to evaluate the proportion of the interval [-1,1] occupied by the sequence $\{z(i)\}_{i=1}^{n}$. For illustration, the sensitivity attribute value computed is 0.599 for the logistic map. The difference profile $\{x(i) - x^{'}(i)\}$ of two sequences generated from a logistic map varying in the interval [-1,1] is obtained. The difference profile is evaluated by change in the least significant digit of the value of the control parameter, i.e., r=3.9 and r=3.91 shown in Fig 1(b). The sensitivity attribute value obtained is 0.599.

3.1.3 Bifurcation

The bifurcation diagram is obtained by plotting chaotic map outputs against the control parameter. It shows the relation between values of changing parameters and the solutions to the system. The point where bifurcation appears indicates the chaotic behavior of the system at this point. The areas of control parameters with dense points show good chaotic behavior and the areas of control parameters with solid lines and blank zones show their non-chaotic property. From the bifurcation diagram, one can observe how the map behaves for different values of the control parameter. For illustration, we evaluate the sub-attribute value of logistic map output. Fig 1(c) shows the bifurcation results for $r\in$ [0, 1]. It is found that only 37 % of the area [0,4] x [0,1] is occupied by the bifurcation diagram of the logistic map which gives us 0.37 as a sub-attribute value.

3.1.4 Lyapunov Exponent

It is a measure of the chaotic behavior of a chaotic map $f(x)$. The following Eqn. gives it.

$$\lambda = \lim_{n\to\infty} \frac{1}{n} \left(\sum_{i=1}^{n} \log | f'[x_i] |\right)$$

where, $f'(x)$ represents the derivative of $f(x)$. The chaotic behaviour of a map is indicated by a positive LE value. A higher positive LE value indicates a faster divergence of the output's trajectory and higher chaoticity of the chaotic map whereas negative LE indicates converging trajectories. A strong chaotic map should have a higher LE for a good system. For illustration, the LE attribute value computed is 0.125 for the logistic map. This map has a positive Lyapunov exponent when r is in range [3.5,4] as can be seen from Fig 1(d).

3.1.5 Entropy

The Entropy $H(S)$ of a random binary sequence S is given by the following Eqn.,

$$H(S) = -\sum_{i=0}^{N-1} p(s_i) \log_2 p(s_i)$$

where, $p(s_i)$ is the possibility of the symbol s_i appearing with N number of symbols. The value of $H(S)$ lies between 0-1. The ideal entropy value is 1. In this way, we calculate the entropy sub-attribute which equals $H(S)$ for a chaotic sequence S. The entropy measure for the chaotic sequence generated from the logistic map by taking the control parameter as 3.9 is 0.9815. So, the entropy sub-attribute value is 0.9815.

3.1.6 0-1 Test

It is a measure to study chaotic characteristics[43-44]. This test evaluates the system from generated sequences each of length N. For sequences $D(N)_{n=1,2,\ldots,N}$, we find K by the following equation

$$K = \frac{\log M(n)}{\log n} \quad \text{where.}$$

$$M(n) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} [p(i+n) - p(i)]^2 + [s(i+n) - s(i)]^2,$$

$$p(n) = \sum_{i=1}^{n} D(i)\cos(ic), \quad s(n) = \sum_{i=1}^{n} D(i)\sin(ic).$$

Here, c is a real value constant $\in (\frac{\pi}{5}, \frac{4\pi}{5})$. We say the system is chaotic if $K \approx 1$ and non-chaotic for $K \approx 0$. The relative range in which a chaotic sequence passes the 0-1 test represents its sub-attribute value. For illustration, the 0-1 test attribute value for the logistic map is computed and it is found to be 0 Since $g(K)$ never takes a value greater than 0.99 as can be seen from Fig 1(e).

3.1.7 Variability

In chaotic cryptosystems, the chaotic parameters also play the role of key. Variability refers to the sum of widths of chaotic parameters of a chaotic system, i.e., the length of all control parameter intervals, where the motion exhibited by the system is chaotic, are added to compute the variability of a system.

The variability sub-attribute value for a system C_i with variability m_i is equal to m_i/k. However, if $m_i > k$ for some i, then the sub-attribute value for the system C_i is defined to be 1. Here, k denotes a large number that symbolizes enough variability to resist brute-force attack. In this paper, we take k=100. As an example, the logistic map is chaotic for $r \in [3,4]$ which gives us variability equal to 4-3=1. The variability sub-attribute value, therefore, is equal to 1/100=0.01.

3.2 Values for Randomness Attributes

The randomness of the output of the chaotic map is tested using the NIST test suite[45-46]. Chaotic randomness attribute

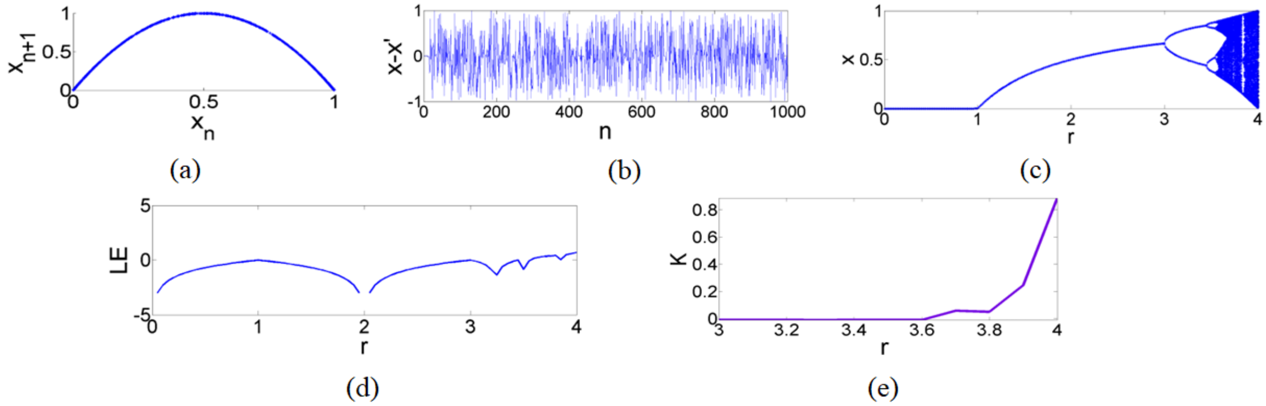

Figure 1. Dynamics of logistic map, (a) Trajectory; (b) Difference profile for sensitivity test; (c) Bifurcation diagram; (d) Lyapunov exponent; and (e) 0-1 test.

Table 1. Statistical test results for chaotic sequences

Name of test	*p_value*	Sub-attribute value
Frequency test	0.0519	1
Frequency within a block test	0.4073	1
Runs test	0.0294	1
Longest run of ones in a block test	0.7593	1
Binary matrix rank test	0.0243	1
Non-overlapping template matching test	0.6964	1
Overlapping template matching test	0.9684	1
Maurer's universal test	0.2766	1
Linear complexity test	0.7895	1
Serial test	0.0188, 0.1964	1
Approximate entropy test	0.5750	1
Cumulative sums (cusum) test	0.0617, 0.0743	1
Random excursions test	0.8328, 0.6746, 0.7320, 0.3020, 0.4651, 0.8546, 0.9819, 0.0244	1
Random excursions variant test	0.1778, 0.1881, 0.2261, 0.1882, 0.2192 0.4417, 0.4075, 0.2897, 0.5451, 0.3221 0.2995, 0.5715, 0.7030	1

has 14 sub-attributes i.e., a set of 14 tests that must be passed by the data if it is random. The *p_value* is computed for the input sequence of length N for each test. A sequence that has a *p_value* higher than the significant level α, pass a test else fail. For a significance value of α=0.01, one would expect 1 sequence to fail out of 100 sequences. The sub-attribute value for a test is taken to be 1 if the test is passed by chaotic sequence else it is taken to be 0. There are the 14 sub-attributes of chaotic randomness attribute corresponding to fourteen different tests namely: frequency test, run test, longest run of ones in a block test, binary matrix rank test, non-overlapping template matching test, overlapping template matching test, Maurer universal test, linear complexity test, serial test, approximate entropy test, cumulative sums (Cusum) test, random excursions test, and random excursions variation test. As an illustration, these 14 tests are performed on the chaotic map[45]. The results of randomness tests are given in Table 1 which shows that the *p_value* for different tests are quite higher than the value of α=0.01 for chaotic sequences and hence the generated sequence passes all the tests. Also, the chaotic map should have all sub-attribute values equal to 1.

4. IDENTIFICATION METHODOLOGY

Let $U=\{CHS_1,CHS_2,\ldots,CHS_m\}$ be the set of given chaotic systems, and let $E=\{E_1,E_2,\ldots E_n\}$ be the set of attributes for a security system on which the best system is to be identified. The knowledge representation for all systems is taken as $S=(U,E)$. Each attribute has $E_{k,k=1,2,\ldots n}$ sub-attributes.

Let $\gamma_{E_K}: E_k \to F(U)$ represent a mapping from the set of sub-attributes E_k to the set of fuzzy sets $F(U)$ over U. For each $k=1,2,...,n, \Gamma_{E_K}$ are fuzzy soft sets over U. The number of sub-attribute parameters in E_k are n_k, and A is the fuzzy soft matrix corresponding to the fuzzy soft set Γ_{E_k}. Each sub-attribute value here denotes how much better it is over other systems and domains of attributes when $V_{E_k}=[0,1]$. Let $E_k=\{e_k^j \mid j=1,2,...,n_k\}$ where $e_k^j: U \to V_{E_k}, k=1,2,...,n$, the membership function of a fuzzy set $\gamma_{E_k}(e_k^j)$ is defined as

$$\mu_{\gamma_{E_k}(e_k^j)}(CHS_i)=e_k^j(CHS_i),\quad i=1,2,...,m,\quad j=1,2,...,n_k,\quad k=1,2,...,n.$$

For $E_{n_k n_l}=E_k \Lambda E_l$, a new attribute set $E_{n_k n_l}$ is now created from the sets E_k and E_l. The number of attribute parameters in $E_{n_k n_l}$ is $n_k * n_l$. Then, $\Gamma_{E_{n_k n_l}}$ is a fuzzy soft set over U and the corresponding soft matrix is:

$[E_{i,j}]_{m\times(n_k\times n_l)}=\min\{[A_{i,j}]_{m\times n_k},[B_{i,r}]_{m\times n_l}\}$, i=1,2,…,m, j=1,2,…,n_k, r=1,2,…,n_l, k=1,2,…,n-1, nl=1,2,…,n. The fuzzy soft

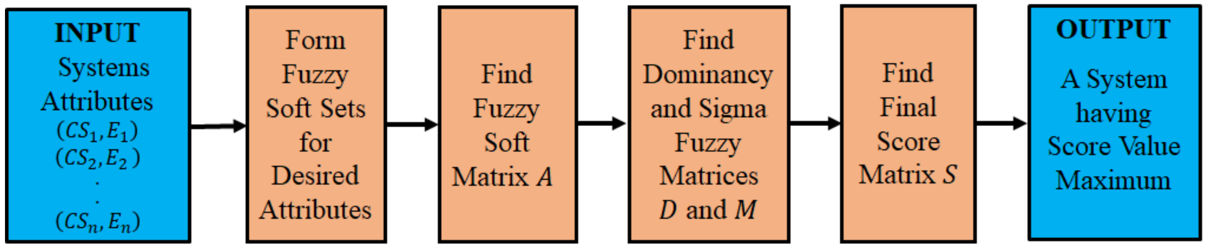

Figure 2. Block diagram of identification methodology.

matrices $[A_{i,j}]_{m\times n_k}$ and $[B_{i,r}]_{m\times n_l}$ corresponds to fuzzy soft sets Γ_{E_k} and Γ_{E_l} respectively. Likewise, the attribute set can also be created by combining all the sub-attribute sets $E_1, E_2, \ldots, E_n$. The combined attribute set is therefore given by the formula $E_{n_1n_2\ldots n_n} = \Lambda_{k=1}^{n} E_k$. The number of attribute parameters is $n_1 \times n_2 \times \ldots \times n_n$. $[E_{i,j}]_{m\times(n_1\times n_2\times\ldots\times n_n)}$ is a fuzzy soft set, and its fuzzy soft matrix is $\Gamma_{E_{n_1n_2\ldots n_n}}$.

The block diagram of identification methodology shown in Fig. 2 works in two different ways (i) at the attribute level and (ii) sub-attribute level to identify the best one. The presented methodology is inspired by the methodology already introduced in Study[47]. At the attributes level, the methodology takes the following steps.

- Form fuzzy soft sets concerning desired attributes $\Gamma_{E_{n_1n_2\ldots n_n}}$ using Eqn. (1).
- find fuzzy soft matrix $A = [E_{i,j}]_{m\times(n_1\times n_2\times\ldots\times n_n)}$ using Eqn. (2).
- Find dominancy matrix $D_{m\times n}$ using Eqn. (3)
- Find Σ-fuzzy set using Eqn. (4) and corresponding final score matrix $M_{m\times 1}$ using Eqn. (5).
- Find the final score matrix $S=D\times M$ using Eqn. (6).
- Find a decision that corresponds to $S_{m\times 1}$ (Select m for which the decision score is maximum).

5. RESULTS AND FINDINGS

In identification, one can take any number of chaotic systems and the desired number of attributes and sub-attributes for identifying problems to select the best system among available different such systems to meet the requirement. We consider a set of systems, $U=\{CHS_1, CHS_2, \ldots, CHS_{10}\}$ where elements $CHS_1, CHS_2, \ldots, CHS_{10}$ indicate ten chaotic systems. Let the attribute set $E=\{E_1, E_2\}$ represents the chaoticity of a chaotic map (E_1), the randomness of a chaotic sequence E_2. Let the following are the sub-attributes of each attribute:

- E_1= {Phase diagram (e_1^1), Sensitivity (e_2^1), Bifurcation (e_3^1), Lyapunov exponent spectrum (e_4^1), Entropy (e_5^1), 0-1 test (e_6^1), Variability (e_7^1) },
- E_2={Frequency (Monobit) Test (e_1^2), Frequency Test within a Block (e_2^2), Runs Test (e_3^2), Test for the Longest Run of Ones in a Block (e_4^2), Binary Matrix Rank Test (e_5^2), Non-overlapping Template Matching Test (e_6^2), Overlapping Template Matching Test (e_7^2), Maurer's Universal Statistical Test (e_8^2), Linear Complexity Test (e_9^2), Serial Test (e_{10}^2), Approximate Entropy Test (e_{11}^2), Cumulative Sums (Cusum) Test (e_{12}^2), Random Excursions Test (e_{13}^2), Random Excursions Variant Test (e_{14}^2)}.

We consider the following ten recently reported hybrid chaotic systems with the above attribute set to demonstrate the identification methodology to find the best among these:

BZCL[48] system (CHS_1) consists of a control sequence generator logistic map and two chaotic sequence generators tent and sine maps given by following:

$$f_1(Y_n) = L(Y_n) = rY_n(1-Y_n), q_n = \begin{Bmatrix} 1, f_1(Y_n) < 0.5 \\ 0, f_1(Y_n) \geq 0.5 \end{Bmatrix},$$

$$X_{n+1} = F(X_n, q_n) = \begin{Bmatrix} f_2(X_n), q_n = 0 \\ f_3(X_n), q_n = 1 \end{Bmatrix}$$

$$f_2(X_n) = T(X_n) = \begin{Bmatrix} uX_n, X_n < 0.5 \\ u(1-X_n), X_n \geq 0.5 \end{Bmatrix}, f_3(X_n) = S(X_n) = a\sin(\pi X_n)$$

where, $X_n \in (0,1)$ are state variables of the system and u,r,a are three control parameters of the system.

- PTM[3] system (CHS_2) is expressed by a mathematical model given by the following:

$$X_{n+} = \frac{u}{4}\sin\left(\frac{\pi}{k}X_n\right)\cos\left(\frac{\pi}{k}X_n\right)$$

where $X_n \in (0,1)$ are state variables of the system and $u \in [2.5410, 5.180]$ and $k \in (0, 2.558)$ are two control parameters of the system.

- FFF[49] system (CHS_3) is composed of three chaotic functions: logistic map $(f: x_n \to x_{n+1})$, tent map $(g: y_n \to y_{n+1})$ and sin map $(h: z_n \to z_{n+1})$ and it is given by the following:

  $x_{n+1}=(r^{10}h(x_n)o(g(x_n))o(f(x_n)))\mathrm{mod}1$ where, $0 \leq r < 4$ and o stands for composition function.

- ZLGYM[50] system (CHS_4) is a non-linear combination of three different 1D chaotic maps given by the following:

$$x_{n+1} = \begin{Bmatrix} \mathrm{mod}(a\sin(\pi\mu\ x_n) + \gamma\mu\ x_n(1-\mu\ x_n), 1), 0 < x_n \leq 0.5 \\ \mathrm{mod}(a\sin(\pi\mu\ (1-x_n)) + \gamma\mu\ (1-x_n)(1-\mu\ (1-x_n)), 1), 0.5 < x_n \leq 1 \end{Bmatrix}$$

  where, $\mu \in [0.5, 0.9], \gamma \in [1, 1.9]$ and $a \in [0.975, 0.995]$ are the control parameters.

- PHBM[51] system (CHS_5) is a nonlinear mixture of three different chaotic maps, i.e., Logistic map, Tent map, and Sine map described by the following:

  $x_{n+1}=Logistic(Tent(SINE(x_n)))\mathrm{mod}1$ where $X_n \in (0,1)$ are state variables.

- MARCS[45] (CHS_6) is a hybrid system that utilizes modified versions of three chaotic maps, logistic map, sine map, and exponential map as $a_{i+1}=\mathrm{mod}(r_{ai}(1-a_i),1)$,$b_{i+1}=\mathrm{mod}(s \sin(\pi b_i),1)$ and $c_{i+1} = \mathrm{mod}(t^{c_i},1)$ respectively and these are combined through the following:

x_{i+1}=mod($2^d(a_ib_i+b_ic_i+a_ic_i+x_i)$,1) where, $x_n \in (0,1)$ are state variables of the system and r,s,t and $d \in (0,60]$ are four control parameters of the system.

- ZBC[52] (CHS_7) combines the Logistic and Tent maps as given by the following:

$$x_{n+1} = \begin{Bmatrix} \text{mod}(rx_n(1-x_n) + \dfrac{(4-r)}{2}x_n, 1), x_n < 0.5 \\ \text{mod}(rx_n(1-x_n) + \dfrac{(4-r)}{2}(1-x_n), 1), x_n \geq 0.5 \end{Bmatrix}$$

where, $x_n \in (0,1)$ are state variables of the system and r is a control parameter of the system.

- AAKE[53] (CHS_8) combines the Logistic, Sine, and Tent maps given by following:

$$x_{n+1} = \begin{Bmatrix} rx_n(1-x_n)(1-|\,cx_n - 0.5c\,| + \mu\ x_n), x_n < 0.5 \\ \text{mod}(r\sin(\pi x_n)(1-|\,cx_n - 0.5c\,| + \mu\ (1-x_n)), 1), x_n \geq 0.5 \end{Bmatrix}$$

where, $x_n \in (0,1)$ are state variables of the system and r, μ and c are the control parameters of the system.

- DYCWE[54] (CHS_9) is an extension of a 1D Tent map with multiple parameters given by the following:

$$x_{n+1} = \begin{Bmatrix} \dfrac{10}{7}x_n(1-\alpha\,|\cos(\lambda_1)| - \alpha\,|\sin(\lambda_2)| - \alpha\,|\,\text{a}\tan(\lambda_3)\,|), x_n < 0.7 \\ \dfrac{10}{3}(1-x_n)(1-\alpha\,|\cos(\lambda_4)| - \alpha\,|\sin(\lambda_5)| - \alpha\,|\,\text{a}\tan(\lambda_6)\,|), x_n \geq 0.7 \end{Bmatrix}$$

where, $\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6 \in \mathbb{R}$ and $\alpha \in [10^{-4}, 10^{-2}]$ are the control parameters.

- MZBKK[55] (CHS_{10}) combines the characteristics of Tent and Sine maps. it is mathematically represented as follows:

$$x_{n+1} = \begin{Bmatrix} \text{mod}(4\sin(2\pi r x_n) + x_n, 1), 0 < x_n < 0.5 \\ \text{mod}(4\sin(2\pi r x_n) + 1 - x_n, 1), 0.5 \leq x_n < 1 \end{Bmatrix}$$

where, $x_n \in (0,1)$ are state variables of the system and r is a control parameter of the system.

The methodology of identification and computing procedures to find the attributes values are simulated in MATLAB programming. The values corresponding to each attribute set for different chaotic systems mentioned above in terms of the Fuzzy soft set computed are given as follows:

Γ_{E_1} =

$\{e_1^1, \{CHS_1/0.06, CHS_2/0.04, CHS_3/0.63, CHS_4/0.04, CHS_5/0.09, CHS_6/0.63,$
$CHS_7/0.0008, CHS_8/0.0008, CHS_9/0.0008, CHS_{10}/0.0008\};$
$e_2^1, \{CHS_1/0.73, CHS_2/0.61, CHS_3/0.67, CHS_4/0.7, CHS_5/0.63, CHS_6/1,$
$CHS_7/0.614, CHS_8/0.588, CHS_9/1, CHS_{10}/0.562\};$
$e_3^1, \{CHS_1/0.8, CHS_2/0.57, CHS_3/0.65, CHS_4/0.01, CHS_5/0.9, CHS_6/1,$
$CHS_7/0.2231, CHS_8/0.0022, CHS_9/0.2585, CHS_{10}/0.5456\};$
$e_4^1, \{CHS_1/0.87, CHS_2/0.5, CHS_3/0.73, CHS_4/0.19, CHS_5/0.89, CHS_6/1,$
$CHS_7/0.975, CHS_8/1, CHS_9/0.9995, CHS_{10}/1\};$
$e_5^1, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/0.86, CHS_5/0.99, CHS_6/1,$
$CHS_7/0.9999, CHS_8/0.9985, CHS_9/0.9999, CHS_{10}/0.9651\};$
$e_6^1, \{CHS_1/0.44, CHS_2/0.32, CHS_3/0.7, CHS_4/0.49, CHS_5/0.73, CHS_6/1,$

Γ_{E_2} =

$\{e_1^2, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/0.04, CHS_5/0.09, CHS_6/0.63, CHS_7/0.0008, CHS_8/0, CHS_9/1, CHS_{10}/0\};$
$e_2^2, \{CHS_1/0, CHS_2/0, CHS_3/1, CHS_4/0, CHS_5/0, CHS_6/1, CHS_7/0, CHS_8/0, CHS_9/0, CHS_{10}/0\};$
$e_3^2, \{CHS_1/0, CHS_2/0, CHS_3/0, CHS_4/1, CHS_5/0, CHS_6/1, CHS_7/0, CHS_8/0, CHS_9/0, CHS_{10}/0\};$
$e_4^2, \{CHS_1/0, CHS_2/0, CHS_3/0, CHS_4/0, CHS_5/0, CHS_6/1, CHS_7/1, CHS_8/0, CHS_9/0, CHS_{10}/0\};$
$e_5^2, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/1, CHS_5/1, CHS_6/1, CHS_7/1, CHS_8/1, CHS_9/1, CHS_{10}/1\};$
$e_6^2, \{CHS_1/0, CHS_2/1, CHS_3/0, CHS_4/0, CHS_5/1, CHS_6/1, CHS_7/1, CHS_8/1, CHS_9/1, CHS_{10}/0\};$
$e_7^2, \{CHS_1/0, CHS_2/0, CHS_3/0, CHS_4/0, CHS_5/1, CHS_6/1, CHS_7/0, CHS_8/0, CHS_9/0, CHS_{10}/0\};$
$e_8^2, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/1, CHS_5/1, CHS_6/1, CHS_7/1, CHS_8/1, CHS_9/1, CHS_{10}/1\};$
$e_9^2, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/1, CHS_5/1, CHS_6/1, CHS_7/1, CHS_8/1, CHS_9/1, CHS_{10}/1\};$
$e_{10}^2, \{CHS_1/1, CHS_2/0, CHS_3/1, CHS_4/0, CHS_5/0, CHS_6/1, CHS_7/0, CHS_8/0, CHS_9/0, CHS_{10}/0\};$
$e_{11}^2, \{CHS_1/0, CHS_2/0, CHS_3/1, CHS_4/0, CHS_5/0, CHS_6/1, CHS_7/0, CHS_8/0, CHS_9/0, CHS_{10}/0\};$
$e_{12}^2, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/1, CHS_5/1, CHS_6/1, CHS_7/0, CHS_8/1, CHS_9/0, CHS_{10}/1\};$
$e_{13}^2, \{CHS_1/1, CHS_2/1, CHS_3/1, CHS_4/0, CHS_5/1, CHS_6/1, CHS_7/1, CHS_8/1, CHS_9/1, CHS_{10}/1\};$
$e_{14}^2, \{CHS_1/1, CHS_2/1, CHS_3/0, CHS_4/0, CHS_5/0, CHS_6/1, CHS_7/1, CHS_8/1, CHS_9/1, CHS_{10}/1\}\}$

Here, the values of the first and second attribute sets are computed for the above-said chaotic systems[6,44,46-53] using computing methods discussed in Section 4. We consider the following examples to demonstrate the identification of the best chaotic map by considering two attributes.

Example 1: Decision based on attributes with few sub-attributes

To illustrate the computing of methodology, we restrict U={CHS_1,CHS_2,CHS_3}, and $E_1 = \{e_1^1, e_2^1, e_3^1\}, E_2 = \{e_1^2, e_2^2\}$ so that E_1 has three sub-attributes and E_2 has two sub-attributes to identify the best system. Here, the sub-attribute values corresponding to each chaotic system are taken from the major set Γ_{E_1} and Γ_{E_2}. The fuzzy soft sets are

$\Gamma_{E_1} = \{e_1^1, \{CHS_1/0.06, CHS_2/0.04, CHS_3/0.63\}; e_2^1, \{CHS_1/0.73, CHS_2/0.61, CHS_3/0.67\};$
$e_3^1, \{CHS_1/0.8, CHS_2/0.57, CHS_3/0.65\}\}$ and $\Gamma_{E_2} = \{e_1^2, \{CHS_1/1, CHS_2/1, CHS_3/1\};$
$e_2^2, \{CHS_1/0, CHS_2/0, CHS_3/1\}\}$.

Let $[A_{i,j}]_{3\times3}$ and $[B_{i,k}]_{3\times2}$ are the fuzzy soft matrices corresponding to Γ_{E_1} and Γ_{E_2} fuzzy soft sets respectively.

Then

$$[A_{i,j}]_{3\times3} = \begin{pmatrix} 0.06 & 0.73 & 0.80 \\ 0.04 & 0.61 & 0.57 \\ 0.63 & 0.67 & 0.65 \end{pmatrix} \text{and } [B_{i,k}]_{3\times2} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \end{pmatrix}$$

Corresponding to the choice attributes sets E_1 and E_2, the combined attributes set is given by $E_{12} = E_1 \Lambda E_2$. It has $|E_1| \times |E_2| = 3 \times 2 = 6$ attribute parameters. $\Gamma_{E_{12}}$ is a fuzzy soft set over U and

$$\Gamma_{E_{12}} = \{(e_1^1 \Lambda e_1^2, \{CHS_1/0.06, CHS_2/0.04, CHS_3/1\}),$$
$$(e_1^1 \Lambda e_2^2, \{CHS_1/0, CHS_2/0, CHS_3/0\}),$$
$$(e_2^1 \Lambda e_1^2, \{CHS_1/0, CHS_2/0, CHS_3/0\}), (e_2^1 \Lambda e_2^2, \{CHS_1/1, CHS_2/1, CHS_3/1\}),$$
$$(e_3^1 \Lambda e_1^2, \{CHS_1/0, CHS_2/1, CHS_3/0\}), (e_3^1 \Lambda e_2^2, \{CHS_1/0, CHS_2/0, CHS_3/0\})\}$$

The corresponding fuzzy soft matrix is given by $[E_{ij}]_{3\times(3\times2)} = \min\{[A_{ij}]_{3\times3}, [B_{ik}]_{3\times2}\}$ and equals to

E=

0.06	0.00	0.73	0.00	0.80	0.00
0.04	0.00	0.61	0	0.57	0.00
0.03	0.67	0.67	0.67	0.656	0.65

The dominancy matrix is given by

$$D = [d_{ik}]_{3\times3} = \#\{j : E_{ij} \geq \mathrm{E}_{kj}\},\quad i,k \in \{1,2,3\},$$

$$j = \{1,2,\ldots,6\} = \begin{pmatrix} 6 & 6 & 2 \\ 3 & 6 & 0 \\ 4 & 6 & 6 \end{pmatrix}.$$

The Σ-fuzzy set is obtained using Eqn. (5) and given as $\gamma_{\Gamma_{E12}} = \{CHS_i / \mu_{\gamma_{\Gamma_{E12}}}(CHS_i) \mid CHS_i \in U\}$,

where

$$\mu_{\gamma_{\Gamma \mathrm{E}_A}}(CHS_i) = \frac{1}{6}\sum_{j=1}^{6} f_{e_j}(CHS_i), CHS_i \in U.$$

So,

$$\mu_{\gamma_{\Gamma \mathrm{E}_A}}(CHS_1) = \frac{1}{6}(0.06 + 0 + 0.73 + 0 + 0.8 + 0) = 0.265\ .$$

Similarly,

$\mu_{\gamma_{\Gamma \mathrm{E}_A}}(CHS_2)$=0.2033 and $\mu_{\gamma_{\Gamma \mathrm{E}_A}}(CHS_3) = 0.65$

which gives $\gamma_{\Gamma_{E12}} = \{CHS_1 / 0.265, CHS_2 / 0.2033, CHS_3 / 0.65\}$.

The matrix corresponding to the Σ-fuzzy set is given by M=[0.265 0.2033 0.65]

The final Score matrix S is obtained by the formula:

$$S = D \times M' = \begin{pmatrix} 6 & 6 & 2 \\ 3 & 6 & 0 \\ 4 & 6 & 6 \end{pmatrix}\begin{pmatrix} 0.265 \\ 0.2033 \\ 0.65 \end{pmatrix} = \begin{pmatrix} 4.1098 \\ 2.0148 \\ 6.1798 \end{pmatrix}$$

Score values for different chaotic systems are shown by S in which the maximum final score is 6.1798 for CHS_3 chaotic system. Therefore, the best chaotic system is CHS_3.

Example 2: Decision based on attributes with all sub-attributes

This considers chaotic characteristics E_1 and E_2 two attributes where, E_1 have seven sub-attributes and E_2 has fourteen sub-attributes to identify the best system. Corresponding to the original choice attributes sets E_1 and E_2, the combined attributes set is given by $E_{12} = E_1 \Lambda E_2$. It has 98 attribute parameters. The $\Gamma_{E_{12}}$ is fuzzy soft set, obtained using Eqn. (1) given as:

$$\Gamma_{E_{12}} = \{(e_1^1 \Lambda e_1^2, \{CHS_1 / 0.06, CHS_2 / 0.04, ..., CHS_{10} / 0\}),$$
$$(e_1^1 \Lambda e_2^2, \{CHS_1 / 0, CHS_2 / 0, ..., CHS_3 / 0\}), ..., \cdot$$
$$(e_7^1 \Lambda e_{14}^2, \{CHS_1 / 0.06, CHS_2 / 0.05, CHS_3 / 0.09\}))\ .$$

Using Eqn. (2-3), we have the fuzzy soft matrix $[E_{ij}]_{10\times98}$ as:

0.0000	0.0000	…	…	0.0600
0.0400	0.0000			0.0500
0.6300	0.6300			0.0000
0.0000	0.0000			0.0000
0.0900	0.0000			0.0000
0.6300	0.6300			1.0000
0.0008	0.0000			0.0400
0.0000	0.0000			0.0400
0.0008	0.0000			1.0000
0.0000	0.0000	…	…	0.0900
0.0000	0.0000	…	…	0.0600
0.0400	0.0000			0.0500
0.6300	0.6300			0.0000
0.0000	0.0000			0.0000
0.0900	0.0000			0.0000
0.6300	0.6300			1.0000
0.0008	0.0000			0.0400
0.0000	0.0000			0.0400
0.0008	0.0000			1.0000
0.0000	0.0000	…	…	0.0900

The dominancy matrix D is obtained using Eqn. (4) as

98	91	70	87	60	8	78	85	73	86
49	98	47	83	56	8	77	91	77	86
63	78	98	87	66	9	67	74	69	81
46	54	39	98	46	0	51	65	55	68
66	77	59	87	98	0	66	73	67	81
90	90	89	98	98	98	98	98	91	98
48	56	45	75	60	0	98	79	63	71
48	49	45	75	60	7	66	98	67	80
60	63	50	78	66	21	84	79	98	76
54	54	45	79	52	6	67	79	69	98

The Σ−fuzzy set is obtained using Eqn. (5) as:

$$\gamma_{\Gamma_{E_{12}}} = \{CHS_i / \mu_{\gamma_{\Gamma_{E_{12}}}}(CHS_i) \mid CHS_i \in U\}$$

where,

$$\mu_{\gamma_{\Gamma \mathrm{E}_A}}(CHS_i) = \frac{1}{98}\sum_{1\leq j\leq 98} f_{e_j}(CHS_i), CHS_i \in U$$

Therefore,

$$\mu_{\gamma_{\Gamma \mathrm{E}_A}}(CHS_1) = \frac{1}{6}(0.06 + 0 + ... + 0.06) = 0.3233.$$

Similarly, all the values are obtained as:

$\gamma_{\Gamma_{E12}} = \{CHS_1 / 0.3233, CHS_2 / 0.2522, CHS_3 / 0.4050, CHS_4 / 0.1173, CHS_5 / 0.3478, CHS_6 / 0.9995, CHS_7 / 0.2332, CHS_8 / 0.1923, CHS_9 / 0.3042, CHS_{10} / 0.1992\}$. The matrix corresponding to the Σ−fuzzy set is given by M=[0.3233 0.2522 0.4050 0.1173 0.3478 0.9995 0.2332 0.1923 0.3042 0.1992]

The final Score matrix S is obtained by the formula $S = D \times M' =$

[195.9273 172.8149 188.8666 126.4520 174.8878 320.2757 148.8869 153.3178 188.3631 153.9802]'

Score values for different chaotic systems are shown by S in which the maximum final score is 320.2757 for CHS_6. Therefore, the best chaotic system is CHS_6. In this example, the best solution is obtained based on 98 attribute parameters.

The above illustrations show that the identified chaotic system is the most suitable system for cryptographic applications without any error. Such problems of the larger size of attributes/sub-attributes can be taken as a real-world problem to identify from numerous chaotic systems provided by various vendors each with high-security claim.

6. CONCLUSION

Finding the best suitable chaotic system which is an important task before embedding it in the chaotic cipher system for high security has been discussed. A multi-criteria decision methodology based on the fuzzy soft set criterion has been presented to find the best system among different chaotic systems utilizing desired attributes. The attribute values of chaotic systems that have been obtained for different chaotic characteristics appears graphically by computing and quantifying their proportionate coverage regions in the plots. These attribute values have been used in selection methodology which uses fuzzy set, soft fuzzy set, dominant matrix, sigma fuzzy soft set, and score matrix computed from attributes values to find the best chaotic system. It has also been seen that the presented method works very well to obtain the most suitable chaotic system among several such systems for different attributes. A system has been considered the best one for which the score value is highest and considered worst for which the score value is lowest. The chaotic systems having lower score values can be improvised by modifying their attributes suitably. The methodology can be extended further for additional desired cryptographic attributes/sub-attributes to find the best system. The same can be done for hardware attributes/sub-attributes to find the best chaotic cipher system among such systems meeting the requirements of high-security requirements. It can also be easily and successfully used in several comparable applications to choose the best product using different options to meet user satisfaction and requirements.

REFERENCES

1. Shannon, C.E. Communication theory of secrecy systems. *The Bell Syst. Technic. J.*,1949, **28**(4), 656-715. doi:10.1002/j.1538-7305.1949.tb00928.x
2. Stallings, W. Cryptography and network security. Prentice Hall, Englewood Cliffs, 2003.
3. Lu, Q.; Yu, L. & Zhu, C. Symmetric image encryption algorithm based on a new product trigonometric chaotic map. *Symmetry*, 2022, **14**(2), 373. doi: 10.3390/sym14020373
4. Zhu, H.; Zhao, Y. & Song, Y. 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access*, 2019, **7**, 14081-14098. doi: 10.1109/ACCESS.2019.2893538
5. Jain, A. & Rajpal, N. A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps. *Multimedia Tools Appl.*, 2016, **75**, 5455–5472. doi: 10.1007/s11042-015-2515-7
6. Huang, X. Image encryption algorithm using chaotic Chebyshev generator. *Nonlinear Dyn.*, 2012, **67**(4), 2411–2417. doi: 10.1007/s11071-011-0155-7
7. Zhou, Y.; Bao, L. & Chen, C.P. A new 1D chaotic system for image encryption. *Signal Process.*, 2014, **97**(11), 172–182. doi: 10.1109/ICSSE.2012.6257151
8. Xian, C.; Du, J.; Shahzad, F.; Xu, L. & Jin, S. Complexity and chaos control of dynamic evolution in energy vehicle production decisions. *Heliyon*, 2023, **9**(2). doi:10.1016/j.heliyon.2023.e12889
9. Chai, X.; Fu, X.; Gan, Z.; Lu, Y. & Chen, Y. A color image cryptosystem based on dynamic DNA encryption and chaos. *Signal Process.*, 2019, **155**, 44–62. doi: 10.1016/j.sigpro.2018.09.029
10. Khan, J.; Khan, M.; Ahmad, J.; Hwang, S. & Ahmed, W. An improved image encryption scheme based on a non-linear chaotic algorithm and substitution boxes. *Informatica*, 2017, **28**(4), 629–649. doi: 10.15388/Informatica.2017.149
11. Lin, L.; Shen, M.; So, H.C. & Chang, C. Convergence analysis for initial condition estimation in coupled map lattice systems. *IEEE Trans. Signal Process.*, 2012, **60**(8), 4426–4432. doi: 10.1109/TSP.2012.2195659
12. Li, C.; Lin, D. & Lu, J. Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Multimedia*, 2017, **3**(3), 64-71. doi: 10.1109/MMUL.2017.3051512
13. Ratan, R. & Arvind. Key independent image deciphering using neighborhood similarity characteristics and divide-and-conquer attack. *Recent Patents on Eng.*, 2021, **15**(40), 34-44. doi: 10.2174/1872212114999200719144548
14. Ratan, R. Key independent retrieval of chaotic encrypted images. *In* Proc. of the PReMI, LNCS, Springer, 2009, **5909**, pp. 483-488. doi: 10.1007/978-3-642-11164-8_78
15. Ratan, R. & Arvind. Cryptanalysis of an image cipher using multi-entropy measures and the countermeasures. *Defence Sci. J.*, 2020, **74**(4), 425-439. doi: 10.14429/dsj.70.15467
16. Bahramali, A.; Houmansadr, A.; Soltani, R.; Goeckel, D. & Towsley, D. Practical traffic analysis attacks on secure messaging. *In* Proc. of the Network and Distributed Systems Security (NDSS) Symposium, 2020. doi: 10.14722/ndss.2020.24347
17. Ratan, R. & Arvind. Bit-plane specific measures and its applications in analysis of image ciphers. *In* Signal Processing and Intelligent Recognition Systems. CCIS, Springer, 2019, **968**, pp. 282-297. doi:10.1007/978-981-13-5758-9_24
18. Jaiswal, N.K. Military operations research: quantitative decision making. Kluwer Boston/Dordrecht/London, 1997.
19. Aydogan, E.K.; Gencer, C. & Ayturk, S. Evaluation of a light machine gun using analytic q process. *Def. Sci. J.*, 2009, **59**(3).
20. Zadeh, L.A. Fuzzy sets. *Inf. and Control*, 1965, **8**(3), 338-353.
21. Arvind & Ratan, R. Identifying traffic of same keys in cryptographic communications using fuzzy decision criteria and bit-plane measures. *Int. J. Syst. Assur. Eng. Manag.*, 2020, **11**(2), 466-480. doi: 10.1007/s13198-019-00878-7
22. Mellaku, M.T. & Sebsibe, A.S. Potential of mathematical model-based decision making to promote sustainable performance of agriculture in developing countries: A review article. *Heliyon*, 2022, **8**(2). doi: 10.1016/j.heliyon.2022.e08968
23. Roy, A.R. & Maji, P.K. A fuzzy soft set theoretic approach to decision making problems. *J. Comput. Appl. Math.*, 2007, **203**(2), 212-218. doi: 10.1016/j.cam.2006.04.008
24. Feng, F.; Jun, Y.B.; Liu, X. & Li, L. An adjustable approach to fuzzy soft set-based decision making. *J. Comput. Appl.*

Math., 2010, **234**(1), 10-20.
doi: 10.1016/j.cam.2009.11.055

25. Yong, D. & Cheng, S. Evaluating the main battle tank using fuzzy number arithmetic operation. *Def. Sci J.,* 2006, **56**(2), 251-257.
doi: 10.14429/dsj.56.1887
26. Pawlak, Z. Rough sets: Theoretical aspects of reasoning about data. *Springer Sci. & Bus. Media*, 1991, **9**.
27. Molodtsov, D. Soft set theory-first result. *Comput. Math. Appl.*, 1999, **37**, 19-31.
doi: 10.1016/S0898-1221(99)00056-5
28. Maji, P.K.; Biswas, R. & Roy, A.R. Fuzzy soft sets. *J. Fuzzy Appl. Math.*, 2001, **9**, 589-602.
doi: 10.4236/ajcm.2023.131008
29. Cagman, N.; Engnoglu, S. & Citak, F. Fuzzy soft set theory and its applications. *Iran J. Fuzzy Syst.*, 2011, **8**(3), 137-147.
doi: 10.22111/IJFS.2011.292
30. Zarkri, A.H.; Hussen, H.M.; Erwi, L.Y. & Al-Sharif, E. Application of soft sets to diagnose the educational obstacles for students. *J. of Innovative Technol. Edu.*, 2016, **3**(1), 61-70.
doi: 10.12988/jite.2016.626
31. Gupta, P.; Mehlawat, M.K.; Grover, N. & Pedrycz, W. Multi-attribute group decision making based on extended TOPSIS method under interval-valued intuitionistic fuzzy environment. *Appl. Soft Comput.*, 2018, **69**, 554-567.
doi: 10.1016/j.asoc.2018.04.032
32. KiriŞci, M. Medical decision making with respect to the fuzzy soft sets. *J. Interdiscipl. Math.*, 2020, **23(4)**, 767-776.
33. Solangi, Y.A.; Longsheng, C., Shah, S.A.A.; Alsanad, A.; Ahmad, M.; Akbar, M.A.; Gumaei, A.; & Ali, S. Analyzing renewable energy sources of a developing country for sustainable development: An integrated fuzzy based-decision methodology. *Processes*, 2020, **8(7)**, 825.
34. Tao, Z.; Liu, X.; Chen, H.; Liu, J.; & Guan, F. Linguistic Z-number fuzzy soft sets and its application on multiple attribute group decision making problems, *Int. J. Intell. Syst.*, 2020, **35**, 105-124.
35. Salih, M.M.; Zaidan, B.B. & Zaidan, A.A. Fuzzy decision by opinion score method. *Appl. Soft Comput.*, 2020, **96**, 106595.
doi: 10.1016/j.asoc.2020.106595
36. Cagman, N.; Engnoglu, S. & Citak, F. Soft Set theory and uni-int making. *Eur. J. Oper. Res.*, 2010, **207**, 8484-855.
doi: 10.1016/j.ejor.2010.05.004
37. Petroudi, S.H.J.; Nabati, Z. & Yaghobit, A. Some new results on fuzzy soft matrices. *Turk. J. Fuzzy Syst.*, 2017, **8**(1), 52-62.
38. Hu, J.; Pan, L.; Yang, Y. & Chen, H. A group medical diagnosis model based on intuitionistic fuzzy soft sets. *Appl. Soft Comput.*, **2019**, 77, 453-466.
doi: 10.1016/j.asoc.2019.01.041
39. Kong, Z.; Gao, L.; Wang, L. & Li, S. The normal parameter reduction of soft sets and its algorithm. *Comput. Math. with Appl.*, 2008, **56**(12), 3029-3037.
doi: 10.1016/j.camwa.2008.07.013
40. Ratan, R. Cryptanalysis of cipher systems using data characteristics, attacks, and fuzzy computation methods. University of Delhi, Delhi, 2020. (PhD Thesis).
41. Wei, G.W.; Wang, H.J. & Lin, R. Application of correlation coefficient to interval-valued intuitionistic fuzzy multiple attribute decision-making with incomplete weight information. *Knowl. and Inf. Syst.*, 2011, **26**, 337-349.
doi: 10.1007/s10115-009-0276-1
42. Xiao, Z.; Chen, W. & Li, L. A method based on interval-valued fuzzy soft set for multi-attribute group decision-making problems under uncertain environment. *Knowl. and Inf. Syst.*, 2013, **34**, 653-669.
doi: 10.1007/s10115-012-0496-7
43. Agarwal, M.; Yadav, A. & Ratan, R. On the characteristics of 1D-HD chaotic maps for cryptographic applications. *NeuroQuantology*, 2022, **20**(9), 6073-6081.
doi: 10.14704/nq.2022.20.9.NQ44708
44. Agarwal, M.; Yadav, A. & Ratan, R. Analysis of Bao-Zhou-Chen-Liu's hybrid chaotic system. *In* Soft Computing: Theories and Applications, LNNS, Springer, 2023, **627**, 303-315.
doi: 10.1007/978-981-19-9858-4_26
45. Agarwal, M.; Arvind & Ratan, R. MARCS: A novel secure hybrid chaotic system. *In* Int. Conference on Innovative Computing and Communication, LNNS, Springer, 2023, **731**, 27-39.
doi: 10.1007/978-981-99-4071-4_3
46. Rukhin, A; Soto, J.; Nechvatal, J.; Smid, M; Barker, E.; Leigh, S.; Levenson, M.; Vangel, M.; Banks, D.; Heckert, A. & Dray, J. A statistical test suite for random and pseudorandom number generators for cryptographic applications. *NIST Special Publication SP*, 2010, pp. 800-822.
47. Ratan, R.; Yadav, A.; & Arya, C. P. Selection of best cipher system using fuzzy soft decision methodology. *J. Discrete Mathematical Sci. Cryptography*, 2024, **27**(3), 1087- 1103.
48. Bao, L.; Zhou, Y.; Chen, C.P. & Liu, H. A new chaotic system for image encryption. *In* 2012 International Conference on System Science and Engineering (ICSSE), 2012.
doi: 10.1109/ICSSE.2012.6257151
49. Farah, M.A.; Farah, A. & Farah, T. An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. *Nonlinear Dynamics*, 2020, **99**(1), 1-24.
doi: 10.1007/s11071-019-05413-8
50. Zhang, T.; Li, S.; Ge, R.; Yuan, M. & Ma, Y. A novel 1D hybrid chaotic map-based image compression and encryption using compressed sensing and Fibonacci-Lucas transform. *Mathematical Problems in Engin.*, 2016, 3, 1-15.
doi: 10.1155/2016/7683687
51. Pourjabbar, K.A.; Habibizad, N.A.; Bidgoli, A.M. & Mirnia, M. A new image encryption scheme based on hybrid chaotic maps. *Multimedia Tools Appl.*, 2021, **80**(6), 1-20.
doi: 10.1007/s11042-020-09648-1

52. Zhou, Y.; Bao, L.; & Chen, C. P. A new 1D chaotic system for image encryption. *Signal Processing*, 2014, **97**, 172-182.
doi: 10.1109/ICSSE.2012.6257151
53. Alnajim, A.M.; Abou-Bakr, E.; Alruwisan, S.S.; Khan, S. & Elmanfaloty, R.A. Hybrid chaotic-based PRNG for secure cryptography applications. *Applied Scie.*, 2023, **13**(13), 7768.
doi: 10.3390/app13137768
54. Daoui, A.; Yamni, M.; Chelloug, S.A.; Wani, M.A.; & El-Latif, A.A.A. Efficient image encryption scheme using novel 1D multiparametric dynamical tent map and parallel computing. *Mathematics*, 2023, **11**(7), 1589.
doi: 10.3390/math11071589
55. Malik, A. W.; Zahid A. H.; Bhatti, D. S.; Kim, H. J.; & Kim, K. I. Designing s-box using tent-sine chaotic system while combining the traits of tent and sine map. *IEEE Access*, 2023.

CONTRIBUTORS

Ms Meenakshi Agarwal is the PhD Scholar in the Department of Mathematics, University of Delhi, Delhi. Her research interests include: Mathematics, chaotic theory, and information security. In the current study, she has studied the literature on fuzzy computing and chaotic systems, developed programs for evaluating chaotic and randomness characteristics

Dr Arvind Yadav is a Professor at Hansraj College, University of Delhi, Delhi. His research interests include: Mathematics, cryptography, and information security.
In the current study, he has considered different chaotic systems to evaluate and analyze the results.

Dr Chaman Prakash Arya is a Scientist at DRDO-SAG, Delhi. His research interests include: Information security, cryptography, and mathematics.
In the current study, he has developed the identification methodology using fuzzy soft computing to find the best system.

Dr Ram Ratan is a former Scientist at DRDO-SAG, Delhi. His research interests include: Information security, cryptography, image processing, pattern recognition, and applied mathematics. In the current study, he has conceptualised and finalised the manuscript by incorporating fuzzy computing and identification methodologies.