Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 27 (2024), No. 3, pp. 1087–1103
DOI : 10.47974/JDMSC-1853

Selection of best cipher system using fuzzy soft decision methodology

Ram Ratan *
Scientific Analysis Group
Defence Research and Development Organization
Delhi 110054
India

Arvind Yadav †
Department of Mathematics
Hansraj College
University of Delhi
Delhi 110007
India

Chaman Prakash Arya §
Scientific Analysis Group
Defence Research and Development Organization
Delhi 110054
India

Abstract

Selection of a most suitable cipher system among several such systems is an important problem of the customers which help to acquire a right cipher system for meeting the requirements of information security to safeguard the vital data. Any mistake in the selection of a right cipher system is very harmful as it may lead to compromise the security of vital information. In the paper, we propose a multi-criterion fuzzy soft decision making methodology to select one of the most suitable cipher system. Proposed methodology uses fuzzy soft set, fuzzy soft matrix, dominancy matrix and Σ-fuzzy set to compute score values and take a right decision. It exhibits out performance over existing methods as shown by explaining some examples. We apply proposed methodology in selecting a most suitable

* *E-mail:* `ramratan_sag@hotmail.com` (Corresponding Author)
† *E-mail:* `drarvind@hrc.du.ac.in`
§ *E-mail:* `carya28@gmail.com`

cipher system from a set of systems with respect to the choice of desired security attributes required by the customers.

Subject Classification: *62H86.*

Keywords: *Cipher system, Cryptography, Information security, Fuzzy soft set, Multi-criterion decision.*

1. Introduction

A cipher system provides security to sensitive data during its transition or at rest to safeguard it from adversaries. It is developed by incorporating appropriate approaches of cryptography for transforming plain data into cipher data[42][43]. Security of a system depends on the difficulties of cracking its encryption algorithm apart from other parameters, primitives and provisions of access controls mechanism, integrity mechanism, key management, emergency erasure, tamper detection and response mechanism etc. In modern era of advanced technology, communication and computer systems where adversaries may access sensitive data over the open networks and misuse it if a customer is not equipped with appropriate cipher systems, and adequate security measures. The use of cipher systems is increasing day-by-day because of their major role in vast security applications in defence services, government organizations, diplomatic agencies, banking, telemedicine, and even in entertainment industries. Nowadays, there are many vendors providing cipher systems to the customers and claiming that their products provides high security to sensitive data. Some of the encryption algorithms claimed secure are found insecure and one may obtain meaningful information about key, algorithm and data from ciphered data [4][11][12] [14][23][24][25][34][35][37][38][39][40][42][43]. So, it has become an important task for the customers to collect critical details of all security parameters and identify a most suitable system among a number of available systems to meet desired security requirements prior to its acquisition. Problem of selecting a most suitable system becomes challenging and difficult when there are many such systems available with desired attributes. In this scenario, a fuzzy soft decision based methodology may be an appropriate approach to decide and select a best one cipher system.

There are many multi-criteria decision making techniques [2] [18] reported viz. Delphi method [18] by Dalkey in 1967, decision matrix approach [18] by Frie and Ruloff in 1989, forced decision matrix approach

[18] by Gokarn in 1970 and analytic hierarchy process [18] by Saaty in 1980. These methods are applicable when the quantitative information about the systems is available but these methods become inapplicable without such quantitative information and these depend on the judgement of experts. There have been some fuzzy computing theories, viz. fuzzy set [47] [46], rough set [31], soft set [29], fuzzy soft set [7][27] [41] useful in multi-criteria based decision solutions. Soft set was described in 1999 by Molodtsov and applied in many areas [29]. Maji et al. studied soft set theory and found its applications in decision making problems [27]. Zakri et al. [48] applied it to make decisions in educational obstacles. Since soft set deals with binary situations therefore for dealing with non-binary situations there need to fuzzyfy soft sets. Fuzzy soft sets are studied by many researchers and found their applications in decision making problems[9][13][16][17][21][30][32][33][44][45]. Maji at el.[27] defined fuzzy soft set and studied their various operations, Roy et al. have also shown its application [41]. Cagman et al. [7] redefined the fuzzy soft sets and applied it in decision making. Cagman et al [6] defined fuzzy soft matrices and applied in decision making tasks. Pan and Zhan [30] gave decision making approaches based on intuitionistic fuzzy soft sets. Kirişci [20] applied fuzzy soft sets in making decision in medical applications.

Paper proposes the use of multi-criteria based fuzzy soft decision methodology to find best one option to choose a most suitable system for required applications. This method uses both dominancy as well as score values, and gives decision accurately on more extended data whereas other methods based on score or dominancy values are not able to give right decision. Data of attributes and sub-attributes are taken from testing of systems. Once data of systems has been taken, a best one system can be chosen through proposed methodology.

In the paper, Section 2 presents preliminary definitions. Section 3 presents an introduction of cipher system and its security attributes/sub-attributes. Section 4 presents the multi-criteria decision methodology. Section 5 presents the performance results. Paper concludes in Section 6 followed by references.

2. Preliminary Definitions

Let U, $\mathcal{P}(U)$ & E be the universal, power and attributes sets respectively. Following are the definitions of fuzzy soft set, fuzzy soft matrix, Σ -fuzzy set and dominancy matrix:

Definition 2.1: [29] A pair (F,A) is a soft set if F maps A into power set $\mathcal{P}(U)$. The $F(e)$, $e \in A$ is an e-approximate element of (F,A), $(F,A) = \{(e,F(e)) \mid e \in E,\ F(e) \in \mathcal{P}(U)\}$

Example: Let $U=\{u_1,u_2,u_3,u_4,u_5\}$, & $E=\{e_1,e_2,e_3,e_4\}$. If $a=\{e_1,e_2\}$, $F(e_1) = \{u_2,u_4\}$, $F(e_2) = \{u_1,u_3,u_4\}$ then $(F,A) = \{(e_1, \{u_2,u_4\}), (e_2, \{u_1,u_3,u_4\})\}$.

Definition 2.2: [47][50] A fuzzy set A over U is defined as $\mu_A : U \to [0,1]$, μ_A is a membership function of A & $\mu_A(u)$ is membership value of $u \in U$. It is also known as belongingness of u to A. Fuzzy set A is expressed as $A=\{\mu_A(u) \mid u \in U,\ \mu_A(u) \in [0,1]\}$.

Definition 2.3: [27] A fuzzy soft set Γ_A over U is defined by a function $\gamma_A : E \to F(U)$, γ_A is fuzzy approximate function of Γ_A & $F(U)$ is set of fuzzy sets over U. Since $\gamma_A(e) \in F(U)$, $\mu_{\gamma_A(e)} : U \to [0,1]$ is a membership function of $\gamma_A(e)$ for every $e \in E$. A fuzzy soft set is expressed as $\Gamma_A = \{(e, u \,/\, \mu_{\gamma_A(e)}(u)) \mid e \in E,\ u \in U,\ \gamma_A(e) \in F(U)\}$.

Definition 2.4: [3][6] A subset of $U \times E$ is defined uniquely as a relation of Γ_A by $R_A = \{u \times e \mid e \in A,\ \mu_{\gamma_A(e)}(u) > 0\}$ where Γ_A is a fuzzy soft set over U. Characteristic function of R_A is given by $\chi_A : U \times E \to [0,1]$, where

$$\chi_A(u,e) = \begin{cases} \mu_{\gamma_A(e)}(u), & \text{if } (u,e) \in R_A \\ 0, & \text{Otherwise} \end{cases}$$

Let $U=\{u_1,u_2,\ldots u_m\}$, $E=\{e_1,e_2,\ldots,e_n\}$, $A \subseteq E$ & $A_{ij} = \chi_{R_A}(u_i,e_j)$, $i=1,2,\ldots,m$ & $j=1,2,\ldots,n$. Fuzzy soft matrix of Γ_A over U is expressed by

$$[A_{ij}]_{m\times n} = \begin{bmatrix} A_{11} & A_{12} & \ldots A_{1m} \\ A_{21} & A_{22} & \ldots A_{2m} \\ . & . & . \\ . & . & . \\ . & . & . \\ A_{m1} & A_{m2} & \ldots A_{mn} \end{bmatrix}$$

Example: Let $U=\{u_1,u_2,u_3,u_4,u_5\}$ & $E=\{e_1,e_2,e_3,e_4\}$. If $A=\{e_1,e_2\}$, $\gamma_A(e_1)=\{u_1/.2, u_4/.4\}$, $\gamma_A(e_2)=\{u_1/.3, u_3/.6\}$, the γ_A is written as

$$\Gamma_A = \{(e_1,\{u_1/.2,u_4/.4\}),(e_2,\{u_1/.3,u_3/.6\})\}.$$

For Γ_A, the $[A_{ij}]_{5\times 4}$ is obtained as

$$[A_{ij}]_{5\times 4} = \begin{bmatrix} 0.2 & 0.3 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.6 & 0.0 & 0.0 \\ 0.4 & 0.0 & 0.0 & 0.0 \\ 0.0 & 0.0 & 0.0 & 0.0 \end{bmatrix}$$

Definition 2.5: [4] Dominancy Matrix is obtained by comparing parametric values of objects and its entries are defined by $d_{ik} = \#\{j : A_{ij} \geq A_{kj}\}$, where $i, k \in \{1,2,\ldots,m\}$ & $j \in \{1,2,\ldots,n\}$.

Definition 2.6: The Σ-fuzzy set corresponding to $\Gamma_A \in FS(U)$ is defined by $\Upsilon_{\Gamma_A} = \{u / \mu_{\Upsilon_{\Gamma_A}} \mid u \in U\}$ where $\mu_{\Upsilon_{\Gamma_A}} : U \to [0,1]$, $\mu_{\Upsilon_{\Gamma_A}}(u) = \frac{1}{|A|}\sum_{e\in A} f_e(u)$, $u \in U$, $|A|=$ number of attributes in A, function $f : U \to [0,1]$, $f_e(u) = min_{u\in U}\,(AV(e), \mu_{\gamma_A(e)}(u))$ for each $e \in A$, $AV : E \to [0,1]$ and $AV(e) = max_{u\in U}\,(\mu_{\gamma_A(e)}(u))$.

3. Cipher System

Cipher system [5][36][37] is a cryptography system which provides security to vital data for its exchange and storage. There are various parts of a cipher system some of these are the input-output modules for giving input data for encryption and sending out encrypted data to receiver, random source module for generating required random sequences, key scheduling module for finding appropriate input bits for assigning encryption and decryption algorithms to get encrypted/decrypted data. At the time of initiating a call by sender, random source module produces key bits for key scheduling to get initialization bits for initializing encryption/decryption algorithm accordingly. Encryption algorithm generates pseudo random sequence to encrypt input data. The encrypted data is sent to receiver through secure protocols and communication networks to it decrypted and find the original data as send by sender.

A cipher system which is to be used for information security applications should be analysed and evaluated carefully to ensure its cryptographic strength and safeguard it against attacks. Primitives of such system should meet expected characteristics so that an attacker is not able to find any system/key/message details [1]. As per Shannon criteria, it should be any leakage of information even though an attacker has unlimited computing resources as well as availability of encrypted data[42]. As per Kerckhoffs criteria, the security lies on the key but not on the obscurity of algorithm[19]. Apart from encryption/decryption block, the security also depends on various attributes and sub-attributes of system. Some are listed in Table 1. One can extend the list of attributes and sub-attributes depending on various cryptographic parameters for high security applications.

Table 1

Some attributes and respective sub-attributes of a cipher system

Attributes	Sub-attributes
Availability	Electronic failure, Power failure, Channel failure, Network failure
Confidentiality	Crypto strength, Key diversity, Attack resistibility
Integrity	Algo integrity, Platform integrity, System data integrity
Key management	Key generation, Key distribution, Key loading, Key change period, Key auditing
System access control	Physical control, Role based password, Biometric signature
System data protection	Tamper mechanism, Data eraser type, Eraser of data type, Physical distraction
Trust	Make, Verifiability

4. Multi-Criteria Decision Methodology

The proposed methodology is presented to select the best one alternative. Following are the steps:

Step 1. Find fuzzy soft set with respect to choice attributes.

Step 2. Find fuzzy soft matrix.

Step 3. Construct dominancy matrix D

Step 4. Construct Σ -fuzzy set and find corresponding matrix M.

Step 5. Calculate final score matrix $S = D * M$ and generate final decision table corresponding to final score matrix.

Step 6. Find maximum final score from score table.

Object corresponding to maximum of decision table would be the decision. Let $S=(U,E)$ be the knowledge representation system where U and E are finite non-empty sets. Attribute $e \in E$, and $e: U \rightarrow V_e$ is a total function, V_e is the domain of e.

Let $U=\{C_1,C_2,C_3,\ldots,C_m\}$ & $E=\{E_1,E_2,\ldots,E_n\}$ be the sets of systems and attributes. The $S=(U,E)$ is the knowledge representation system and each E_k is the set of sub-attributes, $k=1,2,\ldots,n$. Let $\gamma_{E_k}: E_k \rightarrow F(U)$ be the mapping from E_k into $F(U)$ over U. The Γ_{E_k} is a fuzzy soft sets over U and $[A_{ij}]_{m\times n_k}$ is the fuzzy soft matrix corresponding to Γ_{E_k}, n_k is the number of sub-attributes in E_k. A value of each sub-attribute here indicates the superiority of a system and domain of attributes $V_{E_k}=[0,1]$. Let E_k = $\{e_j^k \mid j=1,2,\ldots,n_k\}$ where $e_j^k: U \rightarrow V_{E_k}$. The $\gamma_{E_k}(e_j^k)$ for each k is given by $\mu_{\gamma_{E_k}(e_j^k)}(C_i)=e_j^k(C_i)$, $i=1,2,\ldots,m$, $j=1,2,\ldots,n_k$, $k=1,2,\ldots,n$.

Now, new attribute set $E_{n_k n_l}$ is constructed from E_k and E_l as $E_{n_k n_l}=E_k \wedge E_l$. There are $n_k \times n_l$ number of attributes in $E_{n_k n_l}$ and $\Gamma_{E_{n_k n_l}}$ is a fuzzy soft set over U, the corresponding fuzzy soft matrix is given as $[E_{ij}]_{m\times(n_k\times n_l)}$ = $min\{[A_{ij}]_{m\times n_k}, [B_{ir}]_{m\times n_l}\}$, $i=1,2,\ldots,m$, $j=1,2,\ldots,n_k$, $r=1,2,\ldots,n_l$, $k=1,2,\ldots,n-1$, $l=2,3,\ldots,n$. The $[A_{ij}]_{m\times n_k}$ and $[B_{ir}]_{m\times n_l}$ are the fuzzy soft matrices corresponding to Γ_{E_k} and Γ_{E_l}.

Similarly, the attribute set can be constructed by taking together all the sub-attribute sets $E_1,E_2,\ldots,E_n$. Then the combined attribute set is given by $E_{n_1 n_2 \ldots n_n}$ = $\wedge_{k=1}^{n} E_k$. It has $n_1 \times n_2 \times \ldots \times n_n$ number of attribute parameters. The $\Gamma_{E_{n_1 n_2 \ldots n_n}}$ is a fuzzy soft set and $[E_{ij}]_{m\times(n_1\times n_2\times\ldots\times n_n)}$ is its fuzzy soft matrix.

Following are the steps:

Step 1. Fuzzy soft set $\Gamma_{E_{n_1 n_2 \ldots n_n}}$.

Step 2. Fuzzy soft matix $[E_{ij}]_{m\times(n_1\times n_2\times\ldots\times n_n)}$.

Step 3. Dominancy Matrix D of order $m\times m$.

Step 4. Σ -fuzzy set corresponding to $\Gamma_{E_{n_1 n_2 \ldots n_n}}$, and matrix corresponding to it is M of order $m\times 1$.

Step 5. Final score matrix is $S=D\times M$ of order $m\times 1$. The scores for different systems are given in Table 2.

Table 2

Score values for different systems

System	C_1	C_2	C_3	.	.	.	C_m
Final Score	rd_1	rd_2	rd_3	.	.	.	rd_m

5. Performance Results

Let $U = \{C_1, C_2, C_3, C_4, C_5, C_6, C_7\}$ be a set of seven systems & E = {Availability (E_1), Confidentiality (E_2), Integrity (E_3), Key management (E_4), System access control (E_5), System data protection (E_6), Trust (E_7)} be the attribute sets.

Sub-attributes of attributes are taken as

(i) E_1 = {Electronic failure (e_1^1), Power failure (e_2^1), Channel failure (e_3^1), Network failure (e_4^1)},

(ii) E_2 = {Crypto strength (e_1^2), Key diversity (e_2^2), Attack resistibility (e_3^2)},

(iii) E_3 = {Algo integrity (e_1^3), Platform integrity (e_2^3), System data integrity (e_3^3)},

(iv) E_4 = {Key generation (e_1^4), Key distribution (e_2^4), Key loading (e_3^4), Key change period (e_4^4), Key auditing (e_5^4)},

(v) E_5 = {Physical control (e_1^5), Role based password (e_2^5), Biometric signature (e_3^5)},

(vi) E_6 = {Tamper mechanism (e_1^6), Data eraser type (e_2^6), Eraser of data type (e_3^6), Physical distraction (e_4^6)},

(vii) E_7 = {Make (e_1^7), Verifiability (e_2^7)}.

Now we have decision making problem of selecting the best cipher system out of seven systems according to set of choice parameters.

Fuzzy soft sets corresponding to each attribute set are taken as

$$\Gamma_{E_1} = \{e_1^1, \{C_1/0.99, C_2/0.92, C_3/0.8, C_4/0.99, C_5/0.9, C_6/0.9, C_7/0.95\},$$
$$e_2^1, \{C_1/0.99, C_2/0.82, C_3/0.8, C_4/0.99, C_5/0.9, C_6/0.9, C_7/0.98\},$$
$$e_3^1\{C_1/0.98, C_2/0.9, C_3/0.9, C_4/0.99, C_5/0.9, C_6/0.8, C_7/0.92\},$$
$$e_4^1, \{C_1/0.97, C_2/0.97, C_3/0.8, C_4/0.99, C_5/0.9, C_6/0.85, C_7/0.91\}\}$$

$$\Gamma_{E_2} = \{e_1^2, \{C_1 / 1.0, C_2 / 1.0, C_3 / 0.3, C_4 / 1.0, C_5 / 1.0, C_6 / 0.7, C_7 / 0.3\},$$
$$e_2^2, \{C_1 / 0.7, C_2 / 1.0, C_3 / 0.7, C_4 / 1.0, C_5 / 0.82, C_6 / 0.7, C_7 / 0.7\},$$
$$e_3^2, \{C_1 / 1.0, C_2 / 1.0, C_3 / 0.3, C_4 / 0.3, C_5 / 1.0, C_6 / 0.7, C_7 / 1.0\}\}$$

$$\Gamma_{E_3} = \{e_1^3, \{C_1 / 1.0, C_2 / 0.3, C_3 / 0.7, C_4 / 0.7, C_5 / 0.3, C_6 / 1.0, C_7 / 0.7\},$$
$$e_2^3, \{C_1 / 0.7, C_2 / 0.7, C_3 / 0.3, C_4 / 0.7, C_5 / 0.1, C_6 / 1.0, C_7 / 0.7\},$$
$$e_3^3, \{C_1 / 1.0, C_2 / 1.0, C_3 / 0.3, C_4 / 0.3, C_5 / 1.0, C_6 / 0.7, C_7 / 1.0\}\}$$

$$\Gamma_{E_4} = \{e_1^4, \{C_1 / 1.0, C_2 / 0.7, C_3 / 1.0, C_4 / 1.0, C_5 / 0.7, C_6 / 0.3, C_7 / 1.0\},$$
$$e_2^4, \{C_1 / 1.0, C_2 / 1.0, C_3 / 0.7, C_4 / 1.0, C_5 / 0.3, C_6 / 0.7, C_7 / 0.7\},$$
$$e_3^4, \{C_1 / 1.0, C_2 / 0.7, C_3 / 0.3, C_4 / 1.0, C_5 / 1.0, C_6 / 0.7, C_7 / 1.0\},$$
$$e_4^4, \{C_1 / 0.1, C_2 / 0.3, C_3 / 0.05, C_4 / 0.3, C_5 / 0.5, C_6 / 0.6, C_7 / 1.0\},$$
$$e_3^5, \{C_1 / 1.0, C_2 / 0, C_3 / 1.0, C_4 / 1.0, C_5 / 1.0, C_6 / 1.0, C_7 / 0\}\}$$

$$\Gamma_{E_5} = \{e_1^5, \{C_1 / 1.0, C_2 / 0.7, C_3 / 1.0, C_4 / 0.3, C_5 / 0.7, C_6 / 0.7, C_7 / 1.0\},$$
$$e_2^5, \{C_1 / 1.0, C_2 / 0.7, C_3 / 0.7, C_4 / 0.3, C_5 / 0.3, C_6 / 1.0, C_7 / 0.7\},$$
$$e_3^5, \{C_1 / 1.0, C_2 / 0.3, C_3 / 0.7, C_4 / 1.0, C_5 / 1.0, C_6 / 0.7, C_7 / 0.3\}\}$$

$$\Gamma_{E_6} = \{e_1^6, \{C_1 / 1.0, C_2 / 0, C_3 / 1.0, C_4 / 0, C_5 / 0, C_6 / 0, C_7 / 1.0\},$$
$$e_2^6, \{C_1 / 1.0, C_2 / 1.0, C_3 / 1.0, C_4 / 0.7, C_5 / 1.0, C_6 / 0.7, C_7 / 0.7\},$$
$$e_3^6, \{C_1 / 1.0, C_2 / 0.7, C_3 / 1.0, C_4 / 0.7, C_5 / 1.0, C_6 / 0.7, C_7 / 0.3\},$$
$$e_4^6, \{C_1 / 1.0, C_2 / 0, C_3 / 0, C_4 / 1.0, C_5 / 1.0, C_6 / 1.0, C_7 / 0\}\}$$

$$\Gamma_{E_7} = \{e_1^7, \{C_1 / 1.0, C_2 / 0.5, C_3 / 1.0, C_4 / 0.3, C_5 / 1.0, C_6 / 0.5, C_7 / 1.0\},$$
$$e_2^7, \{C_1 / 0.8, C_2 / 0.6, C_3 / 0.7, C_4 / 0.4, C_5 / 0.6, C_6 / 0.7, C_7 / 0.8\}\}$$

Values of the attributes and sub-attributes can be obtained from their actual values depending on the opinion of field experts. Now as an example, we find the decision by considering the two attributes and then all the attributes of the system.

5.1 *Decision based on two attributes*

Let us take the choice attributes sets E_2 and E_3. A combined attributes set is given by $E_{23} = E_2 \wedge E_3$. It has 9 attribute parameters. The fuzzy soft set $\Gamma_{E_{23}}$ of the combined attribute set is given by

$$\{(e_1^2 \wedge e_1^3, \{C_1/1.0, C_2/0.3, C_3/0.3, C_4/0.7, C_5/0.3, C_6/0.7, C_7/0.3\}),$$
$$(e_1^2 \wedge e_2^3, \{C_1/0.7, C_2/0.7, C_3/0.3, C_4/0.7, C_5/1.0, C_6/0.7, C_7/0.3\}),$$
$$(e_1^2 \wedge e_3^3, \{C_1/1.0, C_2/1.0, C_3/0.3, C_4/0.7, C_5/0.7, C_6/0.7, C_7/0.3\}),$$
$$(e_2^2 \wedge e_1^3, \{C_1/0.7, C_2/0.3, C_3/0.7, C_4/0.7, C_5/0.3, C_6/0.7, C_7/0.7\}),$$
$$(e_2^2 \wedge e_2^3, \{C_1/0.7, C_2/0.7, C_3/0.3, C_4/0.7, C_5/0.7, C_6/0.7, C_7/0.7\}),$$
$$(e_2^2 \wedge e_3^3, \{C_1/0.7, C_2/1.0, C_3/0.7, C_4/0.7, C_5/0.7, C_6/0.7, C_7/1.0\}),$$
$$(e_3^2 \wedge e_1^3, \{C_1/1.0, C_2/0.3, C_3/0.3, C_4/0.3, C_5/0.3, C_6/0.7, C_7/0.7\}),$$
$$(e_3^2 \wedge e_2^3, \{C_1/0.7, C_2/0.7, C_3/0.3, C_4/0.3, C_5/1.0, C_6/0.7, C_7/0.7\}),$$
$$(e_3^2 \wedge e_3^3, \{C_1/1.0, C_2/1.0, C_3/0.3, C_4/0.3, C_5/0.7, C_6/0.7, C_7/1.0\})\}$$

Fuzzy soft matrix $[A_{ij}]_{7\times 9}$ for fuzzy soft set $\Gamma_{E_{23}}$ is given by

$$[A_{ij}]_{7\times 9} = \begin{bmatrix} 1.0 & 0.7 & 1.0 & 0.7 & 0.7 & 0.7 & 1.0 & 0.7 & 1.0 \\ 0.3 & 0.7 & 1.0 & 0.3 & 0.7 & 1.0 & 0.3 & 0.7 & 1.0 \\ 0.3 & 0.3 & 0.3 & 0.7 & 0.3 & 0.7 & 0.3 & 0.3 & 0.3 \\ 0.7 & 0.7 & 0.7 & 0.7 & 0.7 & 0.7 & 0.3 & 0.3 & 0.3 \\ 0.3 & 1.0 & 0.7 & 0.3 & 0.7 & 0.7 & 0.3 & 1.0 & 0.7 \\ 0.7 & 0.7 & 0.7 & 0.7 & 0.7 & 0.7 & 0.7 & 0.7 & 0.7 \\ 0.3 & 0.3 & 0.3 & 0.7 & 0.7 & 1.0 & 0.7 & 0.7 & 1.0 \end{bmatrix}$$

Dominancy matrix is given by

$$D = \begin{bmatrix} 9 & 8 & 9 & 9 & 7 & 9 & 8 \\ 6 & 9 & 8 & 7 & 7 & 6 & 7 \\ 2 & 3 & 9 & 5 & 4 & 2 & 4 \\ 4 & 5 & 9 & 9 & 6 & 6 & 5 \\ 4 & 6 & 8 & 7 & 9 & 6 & 5 \\ 5 & 6 & 9 & 9 & 7 & 9 & 7 \\ 5 & 7 & 9 & 6 & 6 & 6 & 9 \end{bmatrix}$$

Σ -fuzzy set is given by $\Upsilon_{\Gamma_{E_{23}}} = \{C_i / \mu_{\Upsilon_{\Gamma_{E_{23}}}}(C_i) \mid C_i \in U\}$,

where $\mu_{\Upsilon_{\Gamma_A}}(C_i) = \frac{1}{9}\sum_{1\le j\le 9} f_{e_j}(C_i), u \in U$.

$$\Upsilon_{\Gamma_{E_{23}}} = \{C_1/0.8333, C_2/0.6667, C_3/0.3889, C_4/0.5667, C_5/0.6333,$$
$$C_6/0.7000, C_7/0.6333\}.$$

Matrix corresponding to Σ -fuzzy set is given by

$$M = \begin{bmatrix} 0.8333 & 0.6667 & 0.3889 & 0.5667 & 0.6333 & 0.7000 & 0.6333 \end{bmatrix}$$

Final score matrix is $S = D \times M'$

$$S = \begin{bmatrix} 9 & 8 & 9 & 9 & 7 & 9 & 8 \\ 6 & 9 & 8 & 7 & 7 & 6 & 7 \\ 2 & 3 & 9 & 5 & 4 & 2 & 4 \\ 4 & 5 & 9 & 9 & 6 & 6 & 5 \\ 4 & 6 & 8 & 7 & 9 & 6 & 5 \\ 5 & 6 & 9 & 9 & 7 & 9 & 7 \\ 5 & 7 & 9 & 6 & 6 & 6 & 9 \end{bmatrix} \begin{bmatrix} 0.8333 \\ 0.6667 \\ 0.3889 \\ 0.5667 \\ 0.6333 \\ 0.7000 \\ 0.6333 \end{bmatrix} = \begin{bmatrix} 37.2333 \\ 31.1444 \\ 16.4667 \\ 26.4333 \\ 27.4778 \\ 31.9333 \\ 29.4333 \end{bmatrix}$$

Table 3

Score values for different systems

Systems	C_1	C_2	C_3	C_4	C_5	C_6	C_7
Final Score	37.2333	31.1444	16.4667	26.4333	27.4778	31.9333	29.4333

Score values for different systems are written in Table 3 in which maximum final score is 37.2333 for C_1 system. Therefore, a best system selected is C_1.

5.2 *Decision based on all the attributes*

Let us take choice attributes E. Combined attributes set is given by $E_{123..7} = \wedge_{k=1}^{7} E_k$. It has 4320 attribute parameters. $\Gamma_{E_{123...7}}$ is fuzzy soft set.

The fuzzy soft matrix is given by $[E_{ij}]_{7\times 4320}$

Dominancy matrix is given by

$$D = \begin{bmatrix} 4320 & 3888 & 4320 & 3672 & 3624 & 3672 & 3656 \\ 432 & 4320 & 2616 & 2664 & 2328 & 1896 & 3072 \\ 432 & 3376 & 4320 & 2664 & 2296 & 1704 & 3216 \\ 648 & 3744 & 2952 & 4320 & 3168 & 1728 & 3072 \\ 936 & 3936 & 2984 & 4176 & 4320 & 2592 & 3104 \\ 648 & 3936 & 2952 & 4248 & 3456 & 4320 & 3072 \\ 1040 & 3936 & 3512 & 2664 & 2328 & 1800 & 4320 \end{bmatrix}$$

Σ -fuzzy set is given by $\Upsilon_{\Gamma_{E_{123...7}}} = \{C_i / \mu_{\Upsilon_{\Gamma_{E_{123...7}}}}(C_i) \mid C_i \in U\}$,

where $\mu_{\Upsilon_{\Gamma_A}}(C_i) = \frac{1}{4320} \sum_{1 \le j \le 4320} f_{e_j}(C_i), u \in U$.

$$\Upsilon_{\Gamma_{E_{123...7}}} = \{C_1 / 0.6480, C_2 / 0.1533, C_3 / 0.2275, C_4 / 0.2317, C_5 / 0.3106, C_6 / 0.3450, C_7 / 0.2530\}.$$

Matrix corresponding to Σ -fuzzy set is given by

$$M = \begin{bmatrix} 0.6480 & 0.1533 & 0.2275 & 0.2317 & 0.3106 & 0.3450 & 0.2530 \end{bmatrix}$$

Final score matrix is $S = D \times M'$

$$S = \begin{bmatrix} 4320 & 3888 & 4320 & 3672 & 3624 & 3672 & 3656 \\ 432 & 4320 & 2616 & 2664 & 2328 & 1896 & 3072 \\ 432 & 3376 & 4320 & 2664 & 2296 & 1704 & 3216 \\ 648 & 3744 & 2952 & 4320 & 3168 & 1728 & 3072 \\ 936 & 3936 & 2984 & 4176 & 4320 & 2592 & 3104 \\ 648 & 3936 & 2952 & 4248 & 3456 & 4320 & 3072 \\ 1040 & 3936 & 3512 & 2664 & 2328 & 1800 & 4320 \end{bmatrix} \begin{bmatrix} 0.6480 \\ 0.1533 \\ 0.2275 \\ 0.2317 \\ 0.3106 \\ 0.3450 \\ 0.2530 \end{bmatrix} = \begin{bmatrix} 8546.4 \\ 4309.0 \\ 4512.2 \\ 5023.7 \\ 5877.6 \\ 6020.1 \\ 5130.6 \end{bmatrix}$$

Table 4

Score values for different systems

DT	C_1	C_2	C_3	C_4	C_5	C_6	C_7
Final Score	8546.4	4309.0	4512.2	5023.7	5877.6	6020.1	5130.6

Score values for different systems are written in Table 4 in which maximum final score is 8546.4 for a system C_1. Therefore, a best system selected is C_1.

5.3 *Performance*

The methodology is applied on following data sets to study its performance.

5.3.1 Data Set 1

Let the set of systems and set of attributes are given by

$U = \{C_1, C_2\}$ & $E = \{e_1, e_2, e_3, e_4\}$ and

$$\Gamma_E = \{(e_1\{C_1/0.8, C_2/0.9\}),\ (e_2,\{C_1/0.8, C_2/0.8\}),\ (e_3,\{C_1/0.85, C_2/0.8\}),)$$
$$(e_4,\{C_1/0.8, C_2/0.8\})\}$$

Decisions obtained by proposed and other methods are shown in Table 5.

Table 5

System selected by different methods

Systems	Proposed Method		Maji Method [27]		Kong Method [22]	
	Final Score	Decision	Final Score	Decision	Final Score	Decision
C_1	5.73	C_2	0	C_1, C_2	-0.05	C_2
C_2	5.74		0		0.05	

Here, Maji et al.[27] methods stuck and not able to make decision. However, the proposed methodology is able to make the right decision as shown in Table 5.

5.3.2 Data Set 2

Let the set of systems and set of attributes are given by

$$U=\{C_1,C_2,C_3,C_4,C_5,C_6,C_7\} \ \& \ E=\{e_1,e_2,e_3\}$$

Fuzzy soft set is

$$\Gamma_E=\{(e_1\{C_1/0,C_2/0.3,C_3/0.5,C_4/0.1,C_5/0.8,C_6/0.7,C_7/0\}),$$
$$(e_2,\{C_1/0.4,C_2/0.4,C_3/0.9,C_4/0.3,C_5/0,C_6/0,C_7/0\}),$$
$$(e_3,\{C_1/0.2,C_2/0.5,C_3/0,C_4/0,C_5/0.1,C_6/0.7,C_7/1.0\})\}$$

Table 6

Decisions obtained for different systems

Systems	Proposed Method		Maji Method		Kong Method	
	Final Score	Decision	Final Score	Decision	Final Score	Decision
C_1	4.84		-2		-2.70	
C_2	5.40		5		1.50	
C_3	5.42		3		2.90	
C_4	4.26	C_6	-7	C_2	-4.10	C_3
C_5	5.34		0		-0.60	
C_6	5.80		4		2.90	
C_7	5.12		-3		0.10	

Here, decision is different for each method as shown in Table 6. However, decision of proposed method is the best decision. It is clear that C_6 is the best amongst all systems because C_6 is dominated in two attributes with respect to C_2 and C_3. However, C_3 is also dominated in two attributes with respect to C_2 and in one attribute with respect to C_6. Therefore, C_3 is best than C_2 but both decisions are incorrect and not the best options.

Maji method uses dominancy values and Kong method [22] uses general scoring to decide best option. For data set 1, dominancy based method fail to make right decision. For data set 2, general scoring based methods given in [7] [22] and dominancy based method given in [27] fail to select best option. Proposed method uses combination of both dominancy values and general scoring values. Hence, proposed method works on more extended data correctly whereas other methods based on dominancy values or general scoring values do not provide the best decision correctly.

6. Conclusion

A fuzzy soft set based multi criterion decision methodology has been proposed for selecting a most suitable system among a number of different available cipher systems according to desired multi-attributes considered for meeting the required information security of vital data. Proposed methodology has used fuzzy set, fuzzy soft set, dominancy matrix and score matrix to find best one option. It has been shown that the proposed methodology outperformed comparative to the existing methodologies due to combined use of dominancy matrix and score matrix. The supremacy of the proposed methodology for selecting the most suitable system has been demonstrated by considering different attributes and data sets. Proposed methodology can be applied comfortably and successfully in many such similar applications to select a most suitable product among a number of different available products according to customer requirements and satisfaction.

References

[1] Arvind and R. Ratan, Identifying traffic of same keys in cryptographic communications using fuzzy decision criteria and bit-plane measures, *Int J Syst Assur Eng Manag*, 11(2), 466-80, (2020).

[2] Emel Kizilkaya Aydogan, Cevriye Gencer and Saim Ayturk, Evaluation of a light machine gun using analytic network process, *Defence Sci J,* 59(3), 2731-283, (2009).

[3] Emin Aygun, Soft matrix product and soft cryptosystem, Filomat 32(19), 6519-6530, (2018).

[4] A. Bahramali, A. Houmansadr, R. Soltani, D. Goeckel and D. Towsley, Practical traffic analysis attacks on secure messaging. In the Proceedings of the Network and Distributed Systems Security (NDSS) Symposium 2020, https://dx.doi.org/10.14722/ndss.2020.24347.

[5] H. Beker and F. Piper, Cipher Systems: The Protection of Communications. Northwood Books, London, (1983).

[6] N, Cagman and S. Engnoglu, Fuzzy Soft Matrix Theory and its application in decision making, *Iran J Fuzzy Syst*, 9(1), 109-119, (2012).

[7] N. Cagman, S. Engnoglu and F. Citak, Fuzzy Soft Set Theory and Its Applications, *Iran J Fuzzy Syst*, 8(3), 137-147, (2011).

[8] N. Cagman and S. Engnoglu, Soft Set Matrix Theory and Its decision making, *Comput Math Appl*, 598 (10), 3308-3314, (2010).

[9] N. Cagman, S. Engnoglu and F. Citak, Soft Set theory and uni-int making, *Eur J Oper Res*, 207, 8484-855, (2010).

[10] D. Chen, E.C.C. Tsang, D.S. Yeung and X. Wang, The parametrization reduction of soft sets and its applications, *Comput Math Appl* 49, 757-763, (2005).

[11] M. Din, A.K. Bhateja and R. Ratan, Cryptanalysis of Geffe generator using genetic algorithm. In Proceedings of the SocProS 2013, AISC, Springer, 259, 509-515, (2014).

[12] A. Dainotti, A. Pescape and K.C. Claffy, Issues and future directions in traffic classification, *IEEE Network*, 26(1), 35-40, (2012).

[13] Feng Feng, Young BeaJun, Xiaoyan Liu and Lifeng Li, Adjustable approach to fuzzy soft set based decision making, *J Comput Appl Math*, 234, 10-20, (2010).

[14] X. Ge, B. Lu, F. Liu and X. Luo, Cryptanalyzing an image encryption algorithm with compound chaotic stream cipher based on perturbation, Nonlinear Dynam, 90(2), 1141-1150, (2017).

[15] M.K. Hasan and Mod. Yasin Ali, A Sultana and N.K. Mitra, Decision Making withe help of the repeated average method of fuzzy soft matrix, *Int J Adv Math*, 2019(1), 83-91, (2019).

[16] Seyyed Hossein, Jafari Petroudi, Zahra Nabati and Alireza Yaghobit, Some new results on fuzzy soft matrices, *Turk J Fuzzy Syst*, 8(1), 52-62, (2017).

[17] Junhua Hu, Li Pan, Yan Yang and Haiwei Chen, A group medical diagnosis model based on intuitionistic fuzzy soft sets, *Appl Soft Comput*, 77, 453-466, (2019).

[18] N.K. Jaiswal, Military Operations Research: Quantitative Decision Making, Kluwer Boston/Dordrecht/London (1997).

[19] A. Kerckhoffs, La cryptographhie militaire, *Journal des Sciences Militaires.* IX, 161-91, (1883).

[20] Murat Kirişci, Medical decision making with respect to the fuzzy soft sets, *J Interdiscipl Math*, 23(4), 767-776, (2020).

[21] Zhi Kong, Liqun Gao, Lifu Wang and Steven Li,The normal parameter reduction of soft sets and its algorithm, *Computer and Mathematics with Application,* 56(12), 3029-3037, (2008).

[22] Zhi Kong, Liqun Gao and Lifu Wang, Comment on a fuzzy soft set theoretic approach to decision making problems, *J Comput Appl Math*, 223, 540-542, (2009).

[23] C. Li, D. Lin and J. Lü, Cryptanalyzing an image-scrambling encryption algorithm of pixel bits, *IEEE Multimedia*, 3(3), 64-71, (2017).

[24] C. Li, Y. Zhang and E.Y. Xie, When an attacker meets a cipher-image in 2018: A year in review. *J Inf Secur Appl*, 48, (2019).

[25] C. Li, D. Lin, J. LÃ¼ and F. Hao, Cryptanalyzing an image encryption algorithm based on autoblocking and electrocardiography, *IEEE MultiMedia*, 25(4), 46-56, (2018).

[26] P.K. Maji, R. Biswas and A.R. Roy, An Application of soft sets in decision making problem, *Comput Math Appl,* 44(8-9), 1077-1083, (2002).

[27] P.K. Maji, R. Biswas and A.R. Roy, Fuzzy soft sets, *J Fuzzy Appl Math,* 9, 589-602, (2001).

[28] A. Menezes, S. Vanstone and P. Van Oorschot, Handbook of Applied Cryptography. CRC Press, Boca Raton, (1996).

[29] D. Molodtsov, Soft set theory-first result, *Comput Math Appl,* 37, 19-31, (1999).

[30] Wenjun Pan and Jianming Zhan, Two novel products of IFP-intuitionistic fuzzy soft sets and corresponding decision making methods, *Journal of Discrete Mathematical Sciences and Cryptography*, 21(3), 631-646, (2018).

[31] Z. Pawlak, Rough sets: Theoretic aspects of reasoning about data. Kluwer Academic Publishers, Boston, (1991).

[32] Xindong Peng and Harish Garg, Algorithm for interval-valued fuzzy soft sets in emergency decision making based on WDBA and CODAS with new information measure, *Computers and Industrial Engineering,* 119, 439-452, (2018).

[33] Xingdong Peng and Yong Yang, Algorithm for interval-valued fuzzy soft sets in stochastic multi-criteria decision making based on regret theory and prospect theory with combined weight, *Appl Soft Comput*, 54, 415-430, (2017).

[34] R. Ratan, Key independent decryption of graphically encrypted images. In Proceedings of the PAISI 2010, LNCS, Springer, 6122, 88-97, (2010).

[35] R. Ratan, Key independent retrieval of chaotic encrypted images. In Proceedings of the PReMI 2009, LNCS, Springer, 5909, 483-488, (2009).

[36] R. Ratan, Applications of Genetic Algorithms in Cryptology. In Proceedings of the SocProS 2013, AISC, Springer, 258, 821-831, (2014).

[37] R. Ratan and Arvind, Cryptanalysis of an image cipher using multi-entropy measures and the countermeasures, *Defence Sci J*, 74(4), 425-439 (2020).

[38] R. Ratan and Arvind, Security analysis of bitplane level image encryption schemes, *Defence Sci J*, 71(2), 209-221 (2021).

[39] R. Ratan and Arvind, Key independent image deciphering using neighbourhood similarity characteristics and divide-and-conquer attack, *Recent Patents on Engineering*, 15(4), 34-44 (2021).

[40] R. Ratan and Arvind, Bitplane specific measures and its applications in analysis of image ciphers, Advances in Signal Processing and Intelligent Recognition Systems, CCIS, Springer, 968, 282-297 (2019).

[41] A.R. Roy and P.K. Maji, A fuzzy soft set theoretic approach to decision making problems, *J Comput Appl Math*, 203(2), 212-218, (2007).

[42] C.E. Shannon, Communication theory of secrecy systems, *Bell System Technical Journal*, 28(4) 656-715, (1949).

[43] W. Stallings, Cryptography and Network Security. Prentice Hall, Englewood Cliffs, (2003).

[44] Zhifu Tao, Xi Liu, Huayou Chen, Jinpei Liu and Fei Guan, Linguistic Z-number fuzzy soft sets and its application on multiple attribute group decision making problems, *Int J Intell Syst*, 35, 105-124, (2020).

[45] Yong Yang, Chencheng Liang, Shiwei Ji and Tingting Liu, Adjustable soft disernibility matrix based on picture fuzzy soft sets and applications in decision making, *J Intell Fuzzy Syst*, 29(4), 1711-1722, (2015).

[46] D. Yong and S. Cheng, Evaluating the main battle tank using fuzzy number arithmetic operation, *Defence Sci J*, 56(2), 251-257, (2006).

[47] L.A. Zadeh, Fuzzy sets, *Information and Control*, 8(3), 338-353, (1965).

[48] A.H. Zarkri, H.M. Hussen, L.Y. Erwi and E. Al-Sharif, Application of soft sets to diagnose the educational obstacles for students, *Journal of Innovative Technology and Education*, 3(1), 61-70, (2016).

[49] Jianming Zhan and Jose Carlos R Alcantud, A survey of parameter reduction of soft sets and corresponding algorithms, *Artificial Intelligence Review*, 52(3), 1839-1872, (2019).

[50] H.J. Zimmermann, Fuzzy Sets, Decision Making and Expert Systems. Kluwer, Boston, (1987).

Received August, 2022