Analyses of S-boxes based on interval valued intuitionistic fuzzy sets and image encryption

Saleem Abdullah[1], Sanam Ayub[2], Iqtadar Hussain[3], Benjamin Bedregal[4] and Muhammad Yaqub Khan[5]

[1] Department of Mathematics, Abdul Wali Khan University,
*Mardan, KPK, Pakistan**
E-mail: saleemabdullah81@yahoo.com, saleemabdullah@awkum.edu.pk

[2,5] Department of Mathematics & Statistic, Riphah International University
Islamabad, Pakistan
sanumayub@gmail.com[2] muhammad.yaqub@riphah.edu.pk[5]

[3]Department of Mathematics, King Khalid University Abha, Saudi Arabia
iqtadarqau@gmail.com

[4]Department of Informatics and Applied Mathematics, Federal University of Rio Grande do Norte,
Natal - Rio Grande do Norte- Brazil
bedregal@dimap.ufrn.br

Abstract

Decision making implies selection of the best decision from a set of possible options. In some cases, this selection is based on past experience. Past experience is used to analyse the situations and the choice made in these situations. The aim of this work is to analyse the strength of the nonlinear component (S-box) of block cipher for image encryption applications based on Interval Valued Intuitionistic Fuzzy Sets (IVIFS). S-box is the only component in every block cipher which creates confusion in the data. First, we transform the three dimensional matrix corresponding to colour image with the help of nonlinear component and then use the algebraic structure of IVIFS to choose the best substitution box for image encryption based on entropy, contrast, homogeneity, correlation, energy and mean of absolute devotion. The analyses show that the readings of S8 S-box is very good for image data.

Keywords: S-box, Image encryption, IVIFS, TOPSIS Method, Decision Making

1. Introduction

The notion of fuzzy set was originally proposed by Zadeh (1965) [1] as a mathematical model to grip real world problems, uncertainty and vagueness in data analysis. This theory provided some new mathematical modeling to handle uncertainty and vagueness problems in the fields of computer science, management,

Corresponding author Saleem Abdullah

economic, electronic, computer science and engineering. In 1986, Atanassov introduced the notion of an intuitionistic fuzzy set (IFS) [2] as a generalization of a fuzzy set. After the introduction of an IFS, researchers engaged in the developing of IFSs. An interval valued intuitionistic fuzzy set (IVIFS) was introduced by Atanassov and Gargov (1989) [3] as another tool to handle real life problems. It is natural to believe that IVIFSs show a momentous character in inspiring decision modelling. However, the generalization from particular numbers to interval values of the membership and non-membership functions of intuitionistic fuzzy sets [4,5,6] poses considerable tasks in working with IVIFSs. There is still at an inceptive stage to use IVIFSs to decision modelling and the limited literature exists in this specialized area. The most important model of interval valued intuitionistic fuzzy set is decision making problems. Decision making problems have been studied by many researchers in different papers [7-16]. There are several methods for decision making, like multi-criteria decision making [7,8], group decision making [9,10], TOPSIS method [11-16]. The most fruitful method in these models is TOPSIS method. There is a lot of qualitative information in complex decision making, where decision maker easily evaluated the results by using TOPSIS method. The decision maker's limited attention and information processing capabilities. There are several extensions of the TOPSIS for interval-valued intuitionistic fuzzy environment. Here is being used the approach of [33]. But I suggest that we propose a variant of this proposal. In this paper, we use the interval valued intuitionistic fuzzy TOPSIS method as criterion for the S-boxes in image encryption. We try to find suitable and best S-box for image encryption on base of interval valued intuitionistic fuzzy TOPSIS method as new criterion.

The block ciphers (symmetric key cryptosystem) play a vital character in the field of secure communications. The security of an encryption algorithm is connected with the depiction of the structure block which is responsible for generating fuzziness in the cipher. We use the S - box to achieve this functionality, so this element is identical to a nucleus in an atom [17]. The excellence in the assets of S-boxes has been a supreme imperative difficulty of research in the subject of cryptology. In this paper, we show the entropy analysis, contrast analysis, correlation analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis for prevailing S-boxes. The correlation analysis is mostly applied to calculate the S-box's statistical chattels [18]. The entropy analysis is a statistical technique, applied to evaluate the uncertainty in the image data. The amount of vagueness in an encrypted image portrays the consistency of an image. The intensity difference between a pixel and its neighbours over the whole image is evaluated by contrast analysis [19]. The imperative reading of contrast analysis imitates the quantity of randomness in encrypted images and possessions in enhanced security. In homogeneity [20], Jing et. al., calculated the closeness in the distribution of grey level co-occurrence matrix (GLCM) elements to the GLCM diagonal. The GLCM is the formulation of how frequently different amalgamations of pixel brightness values (grey levels) occur in an image [21]. In energy analysis, Gadelmawla measured the sum of squared elements in the GLCM.. This analysis is responsible for the merits and demerits of different S-boxes in terms of energy of the ensuing encrypted image. The final method that Avcibas et. al., appliance on the encrypted image is the mean of absolute deviation (MAD) analysis [22]. This analysis decides the alteration in the original and an encrypted image. Many methods are proposed for emerging encryption in literature. Although these algorithms perform to be favourable, their stoutness is not yet recognized and they are sprouting to become standards. Some of these algorithms, wealth, revealing, are the public key cryptosystems constructed on chaotic Chebyshev polynomials [23], advanced encryption standard (AES) cryptosystem are exhausting the features of montage image for immensely secure, high data rate [24] and image encryption via logistic map function and heap tree [25]. The most fruitful technique applied to analyse the statistical strength of S-boxes are the differential approximation, linear approximation, correlation analysis, probability, fuzzy set theory and strict avalanche criterion etc. We have incorporated correlation method as a benchmark for the remaining analysis used in this work. With the exception of correlation analysis, the solicitation and application of the results of statistical analysis, presented in this paper, have not been used to estimate the strength of S-boxes. The correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis are performed on AES [26], APA [27], gray [17], Lui J [28], residue prime [29], S8 [30], SKIPJACK [31], and Xyi [32] S-boxes. The results of these S-boxes based on these criteria are not clearly identified the most suitable and best S-box for image encryption. The results of these analyses are analysed by the proposed criterion and an interval valued intuitionistic fuzzy TOPSIS method. In this paper, we highlighted on "problem statement", which properly describes the problems and compensations of the analyses given. Interval valued intuitionistic fuzzy TOPSIS criterion analyses the effectiveness of S-boxes of the anticipated criterion to identify the strength of an S-box. Statistical image analysis of S-boxes" describes the statistical analysis applied in this work. The details of experiments performed in order to verify the statistical analysis results are shown in simulation results and discussion." Finally, the study presents "conclusions" and "future direction "related to this work.

2. Basic Concept

Learn more in this section we will start with the basic definitions of intuitionistic fuzzy set (IFS), interval valued intuitionistic fuzzy set (IVIFS) and score functions. Further study of this article we need the following terms

2.1. Interval Valued Intuitionistic Fuzzy Sets (IVIFS)

There are still some difficulties to solve real world problems by classical models. In crisp and set case, we have many problems to construct a better model due to actuality of information and clarifications of the characteristics of the real world. Regrettably, these models are excessively complex and we didn't catch the precise solutions. There are permanently many hesitations mixed up in the data. The classical model applied to deal with these hesitations is appropriate only under assured environment. For example, vagueness or hesitation in the boundary between states or between urban and rural areas or the exact growth rate of population in a country's rural area. Therefore, recently many theories have been established as mathematical models to deal these uncertainties, for example, fuzzy set theory, interval valued fuzzy set theory, intuitionistic fuzzy set theory, vague set theory and interval valued intuitionistic fuzzy set theory. The most generalize and fruitful theory is interval valued intuitionistic fuzzy set. We use an interval valued intuitionistic fuzzy set as mathematical models. We apply interval valued intuitionistic fuzzy TOPSIS model based on new accuracy function. We further define the basic notions for this model.

Definition 1. [2] Let X be fixed set. An intuitionistic fuzzy set in X is defined as

$$A = \{< x,\ \mu_A(x),\ \nu_A(x) > |x \epsilon X\},$$

where $\mu_A: X \to [0,1]$ and $\nu_A: X \to [0,1]$ are degree of membership and degree of non-membership of each x in X with subject to $0 \leq \mu_A(x) + \nu_A(x) \leq 1$.

Definition 2. [3] The subintervals of $[0,1]$ denoted by $D\ [0,1]$ and let X be non-empty fixed set. An interval valued intuitionistic fuzzy set A in X is defined as follows;

$$\tilde{A} = \{< x,\ \widetilde{\mu_A}(x),\ \widetilde{\nu_A}(x) > |x \epsilon X\},$$

where $\widetilde{\mu_A}: X \to D\ [0,1]$ and $\widetilde{\nu_A}: X \to D\ [0,1]$ are degree of membership and degree of non-membership of each x in X with subject to $0 \leq \sup(\widetilde{\mu_A}(x)) + sup(\widetilde{\nu_A}(x)) \leq 1$ for all $x \epsilon X$. For each $x \epsilon X$, $\widetilde{\mu_A}(x)$ and $\widetilde{\nu_A}(x)$ are closed sub-interval of $[0,1]$ whose lower and upper end points are $\mu_{AL}(x),\ \mu_{AU}(x)$ and $\nu_{AL}(x),\ \nu_{AU}(x)$, respectively. An IVIFS value is represented by $\tilde{A} = ([a,b],[c,d])$

Definition 3 [3] Let $\tilde{A}$ and $\tilde{B}$ be two IVIFS. Then A is an interval valued intuitionistic fuzzy subset of $\tilde{B}$ and denoted by $A \subseteq B$ if and only if $\mu_{AL}(x) \leq \mu_{BL}(x),\ \mu_{AU}(x) \leq \mu_{BU}(x)$ and $\nu_{AL}(x) \geq \nu_{BL}(x),\ \nu_{AU}(x) \geq \nu_{BU}(x)$. The complement of IVIFS

$A = \{< x,\ \widetilde{\mu_A}(x),\ \widetilde{\nu_A}(x) > |x \epsilon X\}$ is defined by $\tilde{A}^c = \{< x,\ \widetilde{\nu_A}(x),\ \widetilde{\mu_A}(x) > |x \epsilon X\}$.

2.2. Score Functions

In this subsection we define different types of score functions related to interval valued intuitionistic fuzzy sets.

Definition 4 [36] The accuracy function for IVIF number $\tilde{A} = ([a,b],[c,d])$ is denoted by $H\ (A)$ and defined by $H(A) = \frac{a+b+c+d}{2}$ and score function is defined by $S(A) = \frac{a+b-c-d}{2}$

Definition 5 [33] Let $\tilde{A} = ([a,b],[c,d])$ be an IVIFS value, it improved score function is denoted by $I(A)$ and defined by the following formula

$$I(A) = \frac{a + a(1-a-c) + b + b(1-b-d)}{2}$$

3. Problem Statement

An $m \times n$ S-box takes some number of input bits, m, and transforms them into some number of output bits, n, where n is not necessarily equal to m.[39] An m×n S-box can be implemented as a lookup table with 2^m words of n bits each, when $\mathrm{n} = \mathrm{m} = 8$, then $m \times n$ S-box is 8×8 S-box. In this manuscript, we analyze 8×8 S-boxes (AES, APA, Gray, Lui J, Residue Prime and S_8) used in popular block ciphers. Without loss of generality, the analysis can be extended to S-boxes of other sizes. The statistical analysis is used to determine the application and suitability of an S-box to image encryption application (Tran et al., 2008). The strength of an encryption based on the S-box can be calculated by examining various parameters generated by numerous statistical analyses. It is imperative to be familiar with the significance and relationship between the outcomes of different types of analyses. Therefore, we develop a criterion which carefully inspects and scrutinizes the available parameters and makes a decision based on interval valued intuitionistic fuzzy decision making assessment using score function.

We use the correlation information to examine the similarity of pixel patterns in the given image and its encrypted version. Although this scrutiny has been broadly used to estimate different image encryption algorithms, it is incorporated here with other methods due to its significance and acceptability in matching images and determining similarities. The correlation analysis under some circumstances does not provide sufficient information in determining the strength of encryption; therefore, in order to increase the reliability of the decision, we employ further techniques such as entropy analysis, contrast analysis, homogeneity analysis, energy analysis and mean of absolute deviation analysis on image. These analyses, when applied in combination, provide more brilliant results and accordingly assist in assessing the enactment of S-boxes. To the best of our knowledge, entropy analysis, contrast analysis, homogeneity analysis, energy analysis and mean of absolute deviation analysis, have not been extensively analyzed and studied for the evaluation of S-boxes to image encryption application. (See Table 1).

In Figure 1 clearly explains the results of entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of plain image. Since it clears from Figure 1 that the date of the original image is quite utilized, our main objective is to depatternized the data of the plain image with the help of standard S-box transformations.

In Figure 2 clearly describes the reading of Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation after the application of Affine-Power-Affine S-box transformation of the plain image of Lena Image. Now we check the effects of APA S-box transformation on plain image is as follows, the entropy is altered from 6.773 to 7.8183, the contrast of the plain image is altered from 0.2455 to 8.9114. This means that the APA S-box transformation create a huge disorder in the contrast of the plain image. The correlation of plain image is misleading from 0.8771 to 0.1258, the energy is transformed from 0.2917 to 0.0193, the homogeneity is altered from 0.9334 to 0.4665, at the end the difference between the original image and cipher image corresponding to APA S-box is dignified with the help of mean of absolute deviation analysis and we conclude that the cipher image is dissimilar from plain image with the reading of 43.544. It is pretty vibrant from Figure 1 and 2 that the APA S-box transformation create a huge disorder in plain image. Therefore, there exist some uncertainty and not clearly describes through these parameters.

Next we compare Figure 1 with Figure 3. We discuss the result of entropy in Figure 3, after applying the Advanced Encryption Standard S-box transformation on plane image, is altered from 6.733 to 7.9325 which is different from APA cipher image entropy. The effect of contrast of the AEA cipher image is transformed from 0.2455 to 7.2240, which is also changed from the contrast of the APA cipher image. From the above analysis, we conclude that in both transformation in Figure 2 and Figure 3 for entropy it is pretty clear that APA S-box transformation is better than AES S-box transformation. Next we discuss the evaluation of correlation of AEA cipher image is changing from 0.8771 to 0.0815. This concludes that the AES S-box transformation is better than APA S-box transformation in the sense to produce un-correlation in the pixels of the plain image. The energy of plain image is changed from 0.2917 to 0.0193. Also in this case, the energy of the APA cipher image is better than the energy of the AES cipher image. The homogeneity is transformed from 0.9334 to 0.4665. From this we come to know that the APA cipher image is better than the AES cipher image. By comparison of Figure 2 and Figure 3 for absolute deviation, we conclude that the APA S-box transformation brings a huge disorder in the pixels of the plain image with value 62.066 as matched to AES S-box transformation. Finally, we conclude with a comparison of Figure 2 and Figure 3 that there arises some uncertainty due to in some cases the AES S-box transformation is superior but in some situation APA S-box transformation shows good results.

Now we show the analysis among Figure 2, 3 and 4. In Figure 2, 3, 4, it’s clear that the entropy of AES S-box transformation and Liu J S-box transformation is identical and well than APA S-box transformation. The contrast analysis of the Liu J S-box is slighter than APA S-box transformation as show in Figure 2 and 4. The effect of the correlation analysis in Figure 4, the reading of Liu J S-box transformation is 0.1311. Its mean that the value of Liu J S-box transformation for correlation analysis is weak as we compare to the value of APA S-box transformation. From Figure 2 and Figure 4, if we compare the energy analysis of APA S-box transformation and Liu J S-box transformation, its clear depict that the energy analysis of APA S-box transformation is better than Liu J S-box transformation. Also, if we see the figure 2 and figure 4, the readings of the homogeneity and MAD analysis of APA S-box transformation are also reasonably better than Liu J S-box transformation. Finally we know that from the above discussion, the APA S-box transformation is moderately worthy as we compare with Liu J S-box and AES S-box transformation for image encryption applications. By comparison of Figure 5 with other S-box transformation, we conclude that APA S-box transformation is also enhanced than residue prime S-box transformation.

The values of the S_8 S-box transformation in figure 6 for these parameters is much better than every other S-box transformation that is discussed in this manuscript. But in some case it does not clear whether which one S-box is better. Finally, the construction of S_8 S-box depends on the symmetric group of permutation and Galois field. The basic condition for an S-box is to deliver confusion in the data, but this box delivers an added step of security which is diffusion. Diffusion complicates the relationship between the plaintext and cipher text. The diffusion in S_8 S-box transformation is due to the permutations of S_8 group.

If we compare Figure 7 with other Figures, we observe that the strength of Gray S-box transformation is better in some cases but in some analysis this transformation is below average.

The Xyi S-box transformation exhibits very good results for different analysis, but in case of correlation analysis this transformation is not as good, which is required for a good image encryption. The results of energy analysis of Figure 4 transformation are much better than many other transformations. Hence, overall this is a secure S-box transformation.

The Skipjack box is constructed for sequential circuits use, but its transformation shows some good results for image encryption applications. But in many analyses this transformation is not on the first position so we can make use of it for secure communication.

The encrypted image of the plain image through each S-box transformation shown in figure 8, 9, 10, 11, 12, 13, 14 respectively. Finally, we didn’t say for these S-box through these parameters to which one is better and suitable for image encryption everyone has own quality and dis-quality at different stages. Therefore, there arise some uncertainty and vagueness in these analyses. Now, we use the TOPSIS method through interval valued intuitionistic fuzzy set to determine the suitability and best S-box for image encryption applications.

4. TOPSIS Method with Interval Valued Intuitionistic Fuzzy Information

Decision Support Systems are a precise class of computer-based information systems that support your decision-making activities. A decision support system analyzes data and provide interactive information support to professionals during the decision-making process. Decision making implies selection of the best decision from a set of possible options. In some cases, this selection is based on past experience. Past experience is used to analyze the situations and the choice made in these situations. In 1981 the TOPSIS technique was established by Hwang and Yoon [11], is a humble classification technique in information and applications. The standard TOPSIS technique endeavours to select alternatives that instantaneously have the direct distance from the positive ideal solution and the farthest distance from the negative-ideal solution. The positive ideal solution minimizes the cost criteria and maximizes the benefit criteria, whereas the negative ideal solution minimizes the benefit criteria and maximizes the cost criteria. TOPSIS sort's full procedure of attribute information, affords a prime ranking of alternatives, and does not require attribute preferences to be independent (Chen and Hwang, 1992; Yoon & Hwang, 1995). To apply this technique, attribute values must be numeric, monotonically increasing or decreasing, and have commensurable units. In this section we are using the concept of interval valued intuitionistic fuzzy TOPSIS Method to cryptography and through an interval valued intuitionistic fuzzy TOPSIS algorithm based on improved score function. We intend to choose only the very best possible S-box. The procedure of method description in flow chart: see in Fig

Let $X = \{A_1, A_2, A_3, A_4, A_5, A_6, A_7,\}$ be a set of seven alternatives. The alternatives are: 1) A_1 is $plain\ image;$ 2) A_2 is $AES;$ $A_3\ is\ APA;$ $A_4\ is\ Lui;$ $A_5\ is\ S_8;$ $A_6\ is\ Prime;$ $A_7\ is\ Gray$. The decision maker takes a decision according to the following five criteria: 1) C_1 is entropy; 2) C_2 is a contrast; 3) C_3 is an average correlation; 4) C_4 is energy; 5) C_5 is homogeneity. In this analysis, the decision maker carefully inspects and scrutinizes the available criteria and makes a decision based on interval valued intuitionistic fuzzy TOPSIS method. The procedure starts with correlation analysis and we use the correlation information to analysis the similarity of pixel patterns in the given image and encrypt version. The seven possible alternatives are to be evaluated using the interval valued intuitionistic fuzzy information from the decision maker under the above five criteria. The description of seven alternatives on basis of five criteria as give in Table 2:

Table 2: Decision matrix $D_{7\times5}(x_{ij})$,

$$\begin{bmatrix}
([0.6,0.7],[0.2,0.3]) & ([0.5,0.6],[0.3,0.4]) & ([0.3,0.4],[0.4,0.5]) & ([0.4,0.5],[0.3,0.5]) & ([0.7,0.8],[0.1,0.2]) \\
([0.3,0.4],[0.5,0.6]) & ([0.1,0.2],[0.5,0.7]) & ([0.4,0.6],[0.2,0.4]) & ([0.6,0.8],[0.1,0.2]) & ([0.3,0.6],[0.1,0.3]) \\
([0.5,0.7],[0.1,0.2]) & ([0.3,0.7],[0.1,0.3]) & ([0.5,0.7],[0.2,0.3]) & ([0.3,0.5],[0.4,0.5]) & ([0.4,0.6],[0.3,0.4]) \\
([0.6,0.8],[0.1,0.2]) & ([0.5,0.7],[0.2,0.3]) & ([0.2,0.5],[0.4,0.5]) & ([0.3,0.6],[0.3,0.4]) & ([0.3,0.5],[0.3,0.5]) \\
([0.3,0.4],[0.5,0.6]) & ([0.4,0.6],[0.1,0.3]) & ([0.5,0.6],[0.2,0.3]) & ([0.3,0.7],[0.2,0.3]) & ([0.2,0.4],[0.4,0.6]) \\
([0.4,0.5],[0.2,0.3]) & ([0.4,0.6],[0.1,0.4]) & ([0.1,0.2],[0.7,0.8]) & ([0.1,0.3],[0.6,0.7]) & ([0.4,0.7],[0.2,0.3]) \\
([0.3,0.5],[0.4,0.5]) & ([0.6,0.7],[0.1,0.3]) & ([0.3,0.4],[0.5,0.6]) & ([0.5,0.6],[0.1,0.3]) & ([0.7,0.8],[0.1,0.2])
\end{bmatrix}$$

Let suppose that the weights of alternatives; entropy, contrast, average correlation, energy, homogeneity are 0.1, 0.25, 0.2, 0.15 and 0.3, respectively. Then, decision maker utilizes the approach of developers to get most suitable and best S-box for image encryption by using an interval valued intuitionistic fuzzy TOPSIS method based on improved score function. We can first find a square matrix $R_{7\times5}\left(I_{ij}(x_{ij})\right)$, by converting interval valued intuitionistic fuzzy decision matrix $D_{7\times5}(x_{ij})$. Table 3 is the score matrix after applies the improved score function to decision matrix.

Table 3: Score matrix $R_{7\times5}\left(I_{7\times5}\left(x_{7\times5}\right)\right)$.

$$R_{7\times5}\left(I_{7\times5}(x_{7\times5})\right)=\begin{bmatrix}0.55 & 0.45 & 0.15 & 0.30 & 0.15\\ 0.25 & -0.1 & 0.30 & 0.55 & 0.10\\ 0.15 & 0.20 & 0.45 & 0.25 & 0.35\\ 0.55 & 0.45 & 0.15 & 0.25 & 0.20\\ 0.25 & 0.20 & 0.35 & 0.25 & 0.10\\ 0.15 & 0.25 & 0.05 & 0.05 & 0.35\\ 0.25 & 0.50 & 0.25 & 0.30 & 0.65\end{bmatrix}$$

Now we can write equations for positive ideal solution for S-boxes (alternatives) are denoted by [33]

$$A^{+}=\{\langle C_j,[1,1],[0,0]\rangle \mid C_j\in C\},\ j=1,2,3,4,5,6,7,$$

and negative ideal solution for S-boxes (alternatives) are denoted [33] by

$$A^{-}=\{\langle C_j,[0,0],[1,1]\rangle \mid C_j\in C\},\ j=1,2,3,4,5,6,7$$

Now we find the separation measure based on score function $d^{+}(A^{+},A_i)\ and\ d^{-}(A^{-},A_i)$ of each S-box from positive ideal and negative solutions, respectively [33]. The separation measure Equations are given as follows [33]:

$$d^{+}(A^{+},A_i)=\sqrt{\sum_{j=0}^{n}\left[w_j\left(1-I_{ij}(x_{ij})\right)\right]^2}\ and$$

$$d^{-}(A^{-},A_i)=\sqrt{\sum_{j=0}^{n}\left[w_j\left(I_{ij}(x_{ij})\right)\right]^2}$$

Compute the numerical values of separation measure of each S-box. In table 4, the separation measure of each S-box.

In Fig 1a, we describe the separation measure w.r.t positive ideal solution and w.r.t negative ideals solution of the each S-box. Now we compute the relative closeness of each S-box with respect to the positive ideal solution A^{+} are defined as the following equation.

$$C_i(A_i)=\frac{d^{-}(A^{-},A_i)}{d^{+}(A^{+},A_i)+d^{-}(A^{-},A_i)}$$

where $C_i(A_i)$ $(i=1,2,\dots,n)$ is the relative closeness coefficient of each S-box (Alternatives) w. r. t the positive ideal solution A^{+} and the value of $C_i(A_i)\epsilon[0,1]$ for each S-box. Therefore, we will choose the best S-box through the descending order of $C_i(A_i)$. i.e., The best S-box will be those whose have high values of $C_i(A_i)$. We write the relative closeness coefficient of each S-box in table 5. We describe the maximum value of the relative closeness coefficient of each S-box in Fig 2a. In table 5 the maximum value of each S-box is S8 as shown in fig 2a the graph of S8 is high among all other S-box.

Table: 5 Relative Closeness Coefficient Table

S-box	$C_i(A_i)$
Plain Image	0.2881
AES	0.2098
APA	0.3150
Lui	0.2977
Gray	0.2089
Prime	0.2506
S8	0.4860

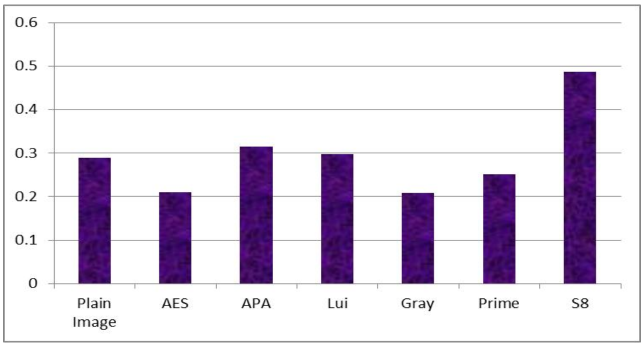


Figure 2a

Table 4: Seperation Measure from Negative Ideal Solution and Positive Ideal Solution

$d^+(A^+,A_i)$	Values	$d^-(A^-,A_i)$	Values
$d^+(A^+,A_1)$	0.3548	$d^-(A^-,A_1)$	0.1436
$d^+(A^+,A_2)$	0.4223	$d^-(A^-,A_2)$	0.1121
$d^+(A^+,A_3)$	0.3317	$d^-(A^-,A_3)$	0.1525
$d^+(A^+,A_4)$	0.3465	$d^-(A^-,A_4)$	0.1469
$d^+(A^+,A_5)$	0.3848	$d^-(A^-,A_5)$	0.1016
$d^+(A^+,A_6)$	0.3699	$d^-(A^-,A_6)$	0.1237
$d^+(A^+,A_7)$	0.2565	$d^-(A^-,A_7)$	0.2425

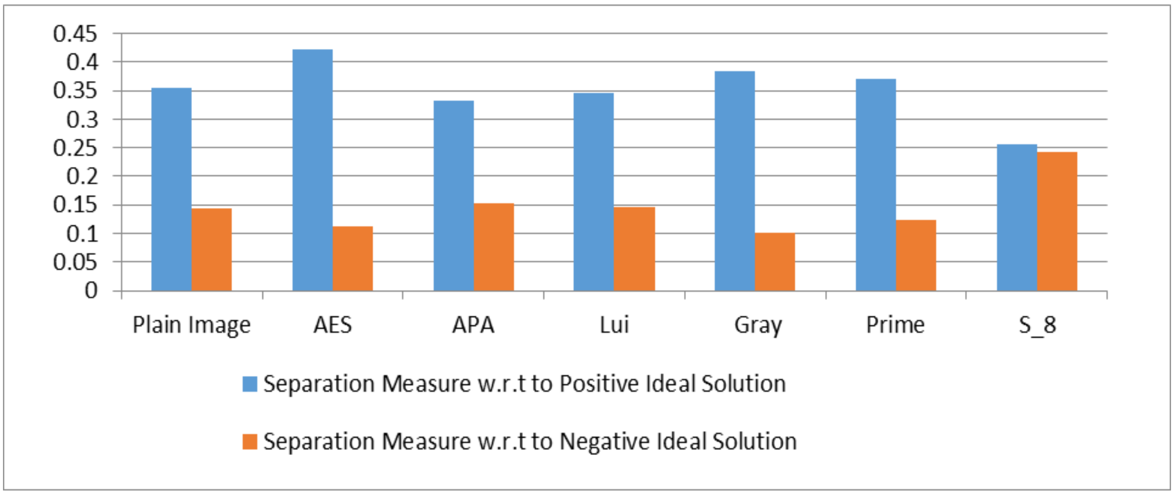


Figure 1a

5. New TOPSIS Method for IVIF Numbers

A set $A = \{a_1, a_2, a_3, \dots, a_m,\}$ of alternatives, a set $A = \{c_1, c_2, c_3, \dots, c_m,\}$ criteria, a weighted vector $W = (w_1, w_2, w_3, \dots, w_m,)$ such that $\sum_{j=1}^{n} w_j$, an parameter $\alpha \in [0,1]$ and a matrix M of dimension $n \times m$ such that M_{ij} (the content of the position (i,j) in the matrix M) is the IVIF number which reflect when the alternative a_i satisfy the criterion c_j.

Step 1. Generate from M two score matrices as follows:

a) The first matrix, M^l, is obtained by applying to each position of the decision matrix the following operator

$$K_\alpha^l(([a,b],[c,d]) \ = \alpha a + (1-\alpha)(1-d)$$

that is $M_{ij}^l = K_\alpha^l(M_{ij})$; and

b) The second matrix M^r is obtained by applying to each position of the decision matrix the following operator

$$K_\alpha^r(([a,b],[c,d]) \;= \alpha c + (1-\alpha)(1-b)$$

that is, $M_{ij}^r = K_\alpha^r(M_{ij})$;.

Step 2. Calculate the weighted normalised decision matrices MW^l and MW^r which is defined by the following equations;

$MW_{ij}^l = w_j M_{ij}^l$ and $MW_{ij}^r = w_j M_{ij}^r$.

Step 4. Define the worst and the best alternatives based, respectively, on MW^l and MW^r as follows:

$$A^{lw} = \{\max\{MW_{ij}^l : j \in J_-\} : i \in N_m\} \cup \{\min\{MW_{ij}^l : j \in J_+\} : i \in N_m\} \equiv (A_j^{lw})_{j\in N_n}$$

$$A^{lb} = \{\max\{MW_{ij}^l : j \in J_+\} : i \in N_m\} \cup \{\min\{MW_{ij}^l : j \in J_-\} : i \in N_m\} \equiv (A_j^{lb})_{j\in N_n},$$

$$A^{rw} = \{\max\{MW_{ij}^r : j \in J_-\} : i \in N_m\} \cup \{\min\{MW_{ij}^r : j \in J_+\} : i \in N_m\} \equiv (A_j^{rw})_{j\in N_n}, \text{ and}$$

$$A^{rb} = \{\max\{MW_{ij}^r : j \in J_+\} : i \in N_m\} \cup \{\min\{MW_{ij}^r : j \in J_-\} : i \in N_m\} \equiv (A_j^{rw})_{j\in N_n}$$

where, $J_- = \{j \in N_n : c_j\}$, and $J_+ = \{j \in N_n : c_j\}$

Step 5. Calculate the distance between the alternative a_i to the worst alternatives A^{lw}, A^{rw}, A^{lb} and A^{rb} as follow:

$$d_i^{lw} = \sqrt{\sum_{j=1}^{n}(MW_{ij}^l - A_j^{lw})^2}$$

$$d_i^{lb} = \sqrt{\sum_{j=1}^{n}(MW_{ij}^l - A_j^{lb})^2}$$

$$d_i^{rw} = \sqrt{\sum_{j=1}^{n}(MW_{ij}^r - A_j^{rw})^2}$$

$$d_i^{rb} = \sqrt{\sum_{j=1}^{n}(MW_{ij}^r - A_j^{rb})^2}$$

where, $J_- = \{j \in N_n : c_j\}$, and $J_+ = \{j \in N_n : c_j\}$

Step 6. Calculate

$$s_{iw}^l = \frac{d_i^{lb}}{d_i^{lw} + d_i^{lb}} \text{ and } s_{iw}^r = \frac{d_i^{rb}}{d_i^{rw} + d_i^{rb}}$$

$$s_{iw} = \frac{s_{iw}^l + s_{iw}^r}{2}$$

Step 7. Rank the alternatives according to s_{iw} with $i \in N_m$.

6. Implementation of New TOPSIS Method for IVIFS.

Step 1. Find the two score matrices from table 2 of decision matrix by using the following two equations. The values of score matrixes are shown in Table 6a & 6b.

Table 6a: Score Matrix

$$M_{7\times5}^l = \begin{bmatrix} 0.67 & 0.57 & 0.44 & 0.47 & 0.77 \\ 0.37 & 0.24 & 0.54 & 0.53 & 0.58 \\ 0.71 & 0.58 & 0.57 & 0.44 & 0.54 \\ 0.74 & 0.64 & 0.85 & 0.51 & 0.44 \\ 0.37 & 0.61 & 0.64 & 0.58 & 0.34 \\ 0.61 & 0.54 & 0.17 & 0.24 & 0.61 \\ 0.44 & 0.67 & 0.37 & 0.64 & 0.77 \end{bmatrix}$$

Table 6b: Score Matrix

$$M_{7\times5}^r = \begin{bmatrix} 0.42 & 0.6 & 0.47 & 0.5 & 0.8 \\ 0.4 & 0.27 & 0.6 & 0.8 & 0.67 \\ 0.77 & 0.7 & 0.7 & 0.5 & 0.6 \\ 0.8 & 0.7 & 0.5 & 0.6 & 0.5 \\ 0.4 & 0.67 & 0.67 & 0.7 & 0.4 \\ 0.64 & 0.6 & 0.2 & 0.7 & 0.7 \\ 0.5 & 0.7 & 0.4 & 0.67 & 0.8 \end{bmatrix}$$

Step 2. Find the weighted normalized decision matrices by using the following. The detail of weighted normalized decision matrixes are given in Table 7a & 7b.

Table 7a: Weighted Normalized Decision Matrix

$$MW_{7\times5}^l = \begin{bmatrix} 0.067 & 0.1425 & 0.088 & 0.0705 & 0.231 \\ 0.037 & 0.06 & 0.108 & 0.795 & 0.174 \\ 0.71 & 0.145 & 0.114 & 0.066 & 0.162 \\ 0.074 & 0.16 & 0.17 & 0.765 & 0.132 \\ 0.37 & 0.1525 & 0.128 & 0.087 & 0.102 \\ 0.061 & 0.135 & 0.034 & 0.036 & 0.183 \\ 0.044 & 0.1675 & 0.074 & 0.094 & 0.231 \end{bmatrix}$$

Table 7b: Weighted Normalized Decision Matrix

$$MW^r_{7\times 5} = \begin{bmatrix} 0.042 & 0.15 & 0.094 & 0.075 & 0.24 \\ 0.04 & 0.0675 & 0.120 & 0.120 & 0.201 \\ 0.077 & 0.175 & 0.140 & 0.075 & 0.180 \\ 0.08 & 0.175 & 0.100 & 0.090 & 0.150 \\ 0.04 & 0.168 & 0.040 & 0.105 & 0.120 \\ 0.064 & 0.150 & 0.040 & 0.105 & 0.210 \\ 0.05 & 0.175 & 0.080 & 0.101 & 0.180 \end{bmatrix}$$

Step 3. Define the worst and the best alternatives based, respectively, on MW^l and MW^r as follows. The detail of worst and the best alternatives ae given in Table 8.

Table 8. Worst and the best alternatives

A^{lw}	0.0740	0.1675	0.0740	0.0960	0.2310
A^{lb}	0.0370	0.0600	0.0340	0.0360	0.1020
A^{rw}	0.0800	0.1750	0.1400	0.1200	0.2400
A^{rb}	0.0400	0.0675	0.0400	0.0750	0.1200

Step 3. Calculate the distance between the alternative A_i to the worst alternatives A^{lw} and A^{rw} as follow. The detail of distance between the alternative A_i to the worst alternatives are given in Table 9.

Table 9. Distance Measure

	d_i^{lw}	d_i^{lw}	d_i^{rw}	d_i^{rw}
A_1	0.6530	0.1687	0.0790	0.1553
A_2	0.6449	0.1120	0.1230	0.0918
A_3	0.6309	0.1389	0.0751	0.1629
A_4	0.5789	0.1114	0.1030	0.1542
A_5	0.6268	0.1414	0.1280	0.1049
A_6	0.7110	0.1130	0.1096	0.1403
A_7	0.0300	0.7553	0.0920	0.1131

Step 5. Calculate the relative closeness separation measure by using the equations in step 5. Detail values see in table 10.

Table 10. Relative closeness

	S_i^l	S_i^r	$\frac{S_i^l+S_i^r}{2}$
A_1	0.2053	0.6628	0.4341
A_2	0.1480	0.4274	0.2877
A_3	0.1804	0.6845	0.4325
A_4	0.1614	0.5995	0.3810
A_5	0.1841	0.4541	0.3191
A_6	0.1371	0.5614	0.3493
A_7	0.9618	0.5514	0.7566

The result of relative closeness worst and best alternative shown in fig 3a. The final relative closeness of each alternative shown in Fig 3b. The S8 S-box has the maximum value of averaging relative closeness. The final selection of S-box is S8 S-box.

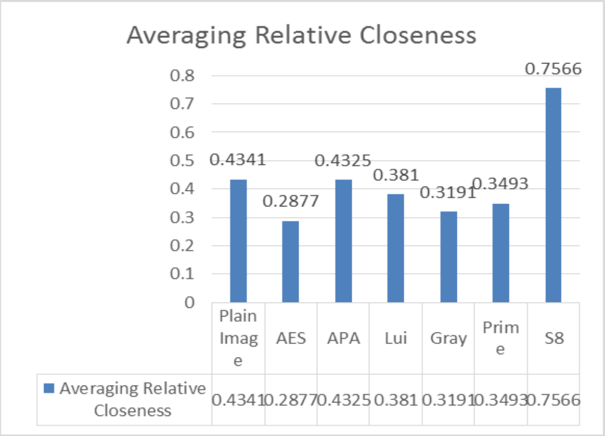
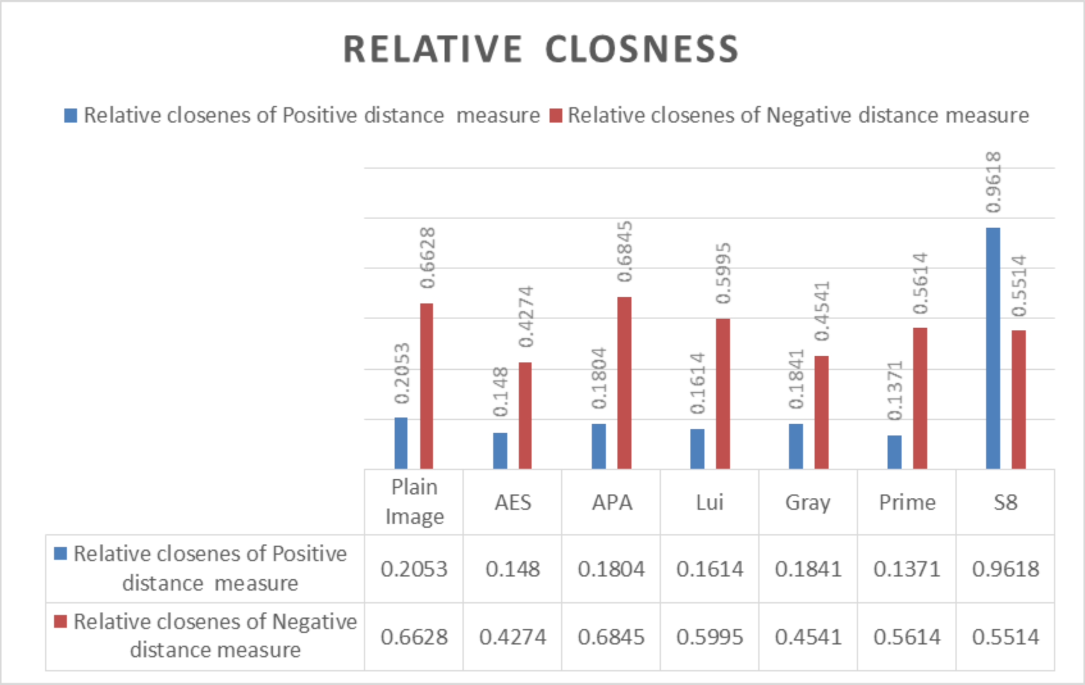


Figure 3a



	Plain Image	AES	APA	Lui	Gray	Prime	S8
🟦 Relative closenes of Positive distance measure	0.2053	0.148	0.1804	0.1614	0.1841	0.1371	0.9618
🟥 Relative closenes of Negative distance measure	0.6628	0.4274	0.6845	0.5995	0.4541	0.5614	0.5514

Figure 3b

Conclusion: Application of intuitionistic fuzzy set has been studied in different applied branches of information science and computer science. Decision support system is a precise class of computer-based information systems that support your decision-making activities. A decision support system analyzes data and provide interactive information support to professionals during the decision-making processes. The result of Decision making systems based on intuitionistic fuzzy set and interval valued intuitionistic fuzzy systems is almost excellent with compared to other analysis. The aim of this manuscript to combine the decision support system based on interval valued intuitionistic fuzzy set and image encryption to analyze the different S-box transformation. In this work we have joined the concept of interval valued intuitionistic fuzzy sets (IVIFS) with secure communication. Basically an S-box is very important component in a block cipher cryptosystem which have the responsibility to induce confusion in the data. So there is a need to find the confusion capability of different 8×8 S-boxes for image encryption application and also which box is best among others. In this paper we have analyzed prevailing S-box and come to know that S_8 S-box have very good readings. Our study will start a new direction in the field of decision support systems and cryptosystems. In future we will focus some other types of S-box transformation based on other criterion.

Acknowledgement

The authors would like to express their gratitude to King Khalid University Saudi Arabia for providing administrative and technical support.

References

1. LA .Zadeh, Fuzzy sets. *Inform. and Control*. 8: (1965), 338-353.

2. K. Atanassov, Intuitionistic fuzzy sets. *Fuzzy Sets and Systems*. 20: (1986), 87-96.

3. K. Atanassov and G. Gargov Interval-valued intuitionistic fuzzy sets, *Fuzzy Sets Syst*., 31, (1989), 343–349.

4. K. Atanassov, Operators over interval-valued intuitionistic fuzzy sets, *Fuzzy Sets Syst*., 64, (1994), 159–174.

5. H. Bustince and P. Burillo, Correlation of interval-valued intuitionistic fuzzy sets, *Fuzzy Sets Syst*., 74, (1995), 237–244.

6. D.H. Hong, A note on correlation of interval-valued intuitionistic fuzzy sets, *Fuzzy Sets Syst*., 95, (1998), 113–117.

7. Y.B. Luo, J. Ye and X.W. Ma, Multi criteria fuzzy decision-making method based on weighted correlation coefficients under interval-valued intuitionistic fuzzy environment, in: *IEEE 10th International Conference on Computer-Aided Industrial Design & Conceptual Design*, Wenzhou, China, 3, 2057–2060, (2009).

8. J. Ye, Multi criteria fuzzy decision-making method based on a novel accuracy function under interval-valued intuitionistic fuzzy environment, *Expert Syst. Appl.*, 36 (2009) 6899–6902.

9. Z.J. Wang, K.W. Li and W.Z. Wang, An approach to multi-attribute decision-making with interval valued intuitionistic fuzzy assessments and incomplete weights, *Inform. Sci.*, 179, (2009), 3026–3040.

10. D.G. Park, Y.C. Kwun, J.H. Park and I.Y. Park, Correlation coefficient of interval-valued intuitionistic fuzzy sets and its application to multiple attribute group decision-making problems, *Math. Comput. Model.*, 50, (2009), 1279–1293,

11. C L . Hwang and K. P.Yoon, *Multiple attribute decision making: Methods and applications*. New York: Springer-Verlag (1981)

12. D.F. Li, TOPSIS-based nonlinear-programming methodology for multi attributes decision making with interval-valued intuitionistic fuzzy sets, *IEEE Transactions on Fuzzy Systems*, 18(2), (2010).299-311,

13. G.R. Jahanshahloo, F.H. Lotfi and A. R. Davoodi, Extension of TOPSIS for decision-making problems with interval data: Interval efficiency, *Mathematical and Computer Modeling*, 49, (2009), 1137-1142,

14. G.R. Jahanshahloo, F.H. Lotfi and M. Izadikhah, An algorithmic method to extend TOPSIS for decision-making problems with interval data, *Applied Mathematics and Computation*, 175, (2006), 1375-1384,

15. VLG. Nayagam, S. Muralikrishnan, G. Sivaraman, Multi-criteria decision-making method based on interval-valued intuitionistic fuzzy sets, *Expert Syst. Appl.*, 38, (2011), 1464–1467,

16. J. Ye, Multicriteria fuzzy decision-making method using entropy weights-based correlation coefficients of interval-valued intuitionistic fuzzy sets, *Applied Mathematical Modelling*, 34, (2010), 3864–3870,

17. M. T. Tran, D. K. Bui and A. D. Doung, Gray S-box for Advanced Encryption Standard. *Int. Conf. Comp. Intel. Secure*., (2008), 253-256,

18. L. Zhang, X. Liao and X. Wang, An Image encryption approach based on chaotic maps. *Chaos Solution Fract.*, 24: (2005), 759-765,.

19. S. Y. Chen, W.C. Lin and C. T. Chen, Split and merge image segmentation based on localized feature analysis and statistical tests. *Graph Model. IM pros.*, 53 (5): (1991), 457-475,

20. F. Jing M. Li, H. Zhang and B. Zhang, Unsupervised image segmentation using local homogeneity analysis. *Proc. ISCAS,* 2: (2003), 456-459,.

21. F. S. Gadelmawla, A vision system for surface roughness characterization using the gray level co-occurrence matrix. *NDT & E. Int.*, 37(7): (2004). 577-588.

22. I. Avcibas N. Memon and B. Sankur, Steganalysis using image quality metrics. IEEE T. IM proc., 12(2): 221-229, (2003). .

23. K. Prasadh K. Ramar and R. Gnanajeyaraman, Public key cryptosystems based on chaotic Chebyshev polynomials. *Int. J. Phys. Sci.*, 1(7): (2009), 122-128.

24. G. M. Alam GM, ML . Mat Kiah, B. B. Zaidan, A. A. Zaidan, and H. O. Alanazi, Using the features of mosaic image and AES cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study. *Int. J. Phys. Sci.*, 5(21) (2010), 3254-3260.

25. R. Enayatifar, Image encryption via logistic map function and heap tree. *Int. J. Phys. Sci.*, 6(2): (2011), 221:228,.

26. J. Daemen and V. Rijmen, AES Proposal: Rijndael. AES Algorithm Submission, Available: http://csrc.nist.gov/archive/aes/rijndael/ Rijndael-ammended.pdf. (1999).

27. L. Cui, Y. Cao, A new S-box structure named Affine-Power-Affine. *Int. J. Innov. Comput.* 3(3): (2007), 45-53,

28. J. Lui, B. Wai, X. Cheng and X. Wang, An AES S-box to increase complexity and cryptographic analysis. *Int. Conf. Infor. Network. Appl.*, 1: (2005), 724-728

29. E. S. Abuelyman A. A. S. Alsehibani, An optimized implementation of the S-Box using residue of prime numbers. *Int. J. Comput. Sci. Ntwk. Secur.*, 8(4): (2008), 304-309.

30. I. Hussain, T. Shah and H. Mehmood, A new algorithm to construct secure keys for AES. *Int. J. Cont. Math. Sci.*, 5(26): (2010), 1263-1270,

31.SKIPJACK, KEA Algorithm. Specifications version, 2(29): 1-23, (1998).

32. X. Y. Shi, Xiao Hu You XC, Lam KY A Method for Obtaining Cryptographically Strong 8x8 S-boxes. Int. Conf. Info. Network. Appl., 2(3): 14-20, (2002).

33. Z. Bai, An interval-valued intuitionistic fuzzy TOPSIS method based on an improved score function, *The Scientific World Journal*, 12: (2013)1-6.

34. S. J. Chen and C. L. Hwang, *Fuzzy multiple attribute decision making: Methods and applications*. Berlin: Springer-Verlag, (1992).

35. K. P. Yoon and C. L. Hwang, *Multiple attribute decision making. Thousand Oaks*, CA: Sage Publication, (1995).

36. Z. Xu, Methods for aggregating interval-valued intuitionistic fuzzy information and their application to decision making, *Control and Decision*, 22, (2007), 179–1187,

37. D. F. Li, TOPSIS-based nonlinear-programming methodology for multi-attribute decision making with interval-valued intuitionistic fuzzy sets. *IEEE Transactions on Fuzzy Systems*, 18(2): (2010), 299–311.

38. R. R. Yager, Pythagorean membership grades in multi-criteria decision making. *IEEE Trans. Fuzzy Syst.*, 22, (2014), 958-965.

39. X. Zang and Z. S. Xu, Extension of TOPSIS to multiple criteria decision making with Pythagorean fuzzy sets, *International Journal of Intelligent Systems*, 29 (2014) 1061-1078.

40. J. Chandrasekaran, A Chaos Based Approach for Improving Non Linearity in the S-Box Design of Symmetric Key Cryptosystems. *First International Conference on Computer Science and Information Technology, CCSIT 2011*, Bangalore, India, January 2-4, 2011. Proceedings, Part 2. Springer. p. 516 (2011).

Appendix 1 Figures

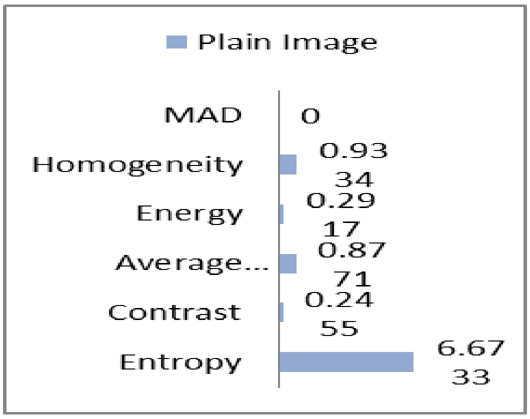


Figure 1. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of plain image.

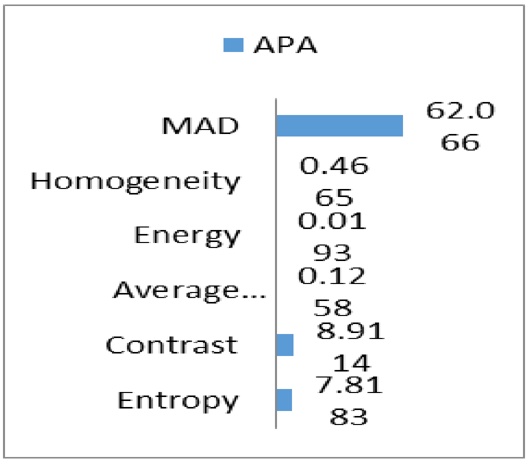


Figure 2. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to affine-power-affine S-box transformation.

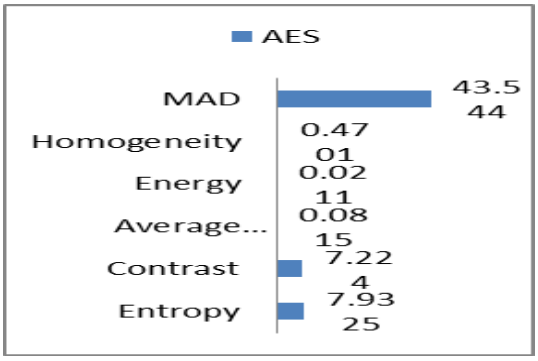


Figure 3. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to advance encryption standard S-box transformation.

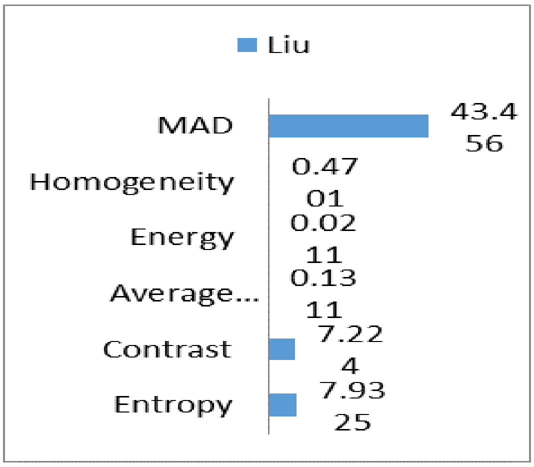


Figure 4. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to Prime S-box transformation.

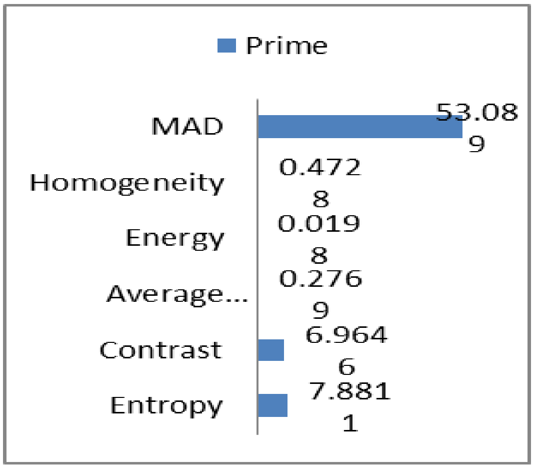


Figure 5. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to Liu J S-box transformation.

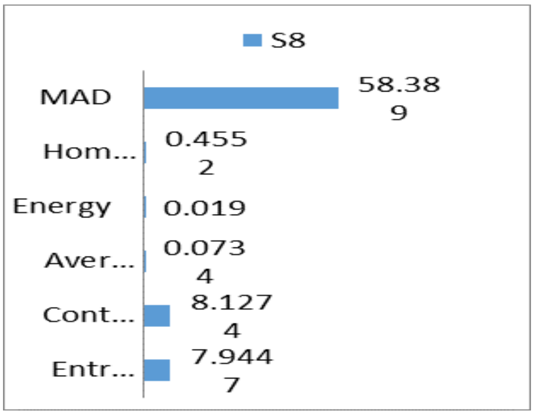


Figure 6. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to S_8 S-box transformation.

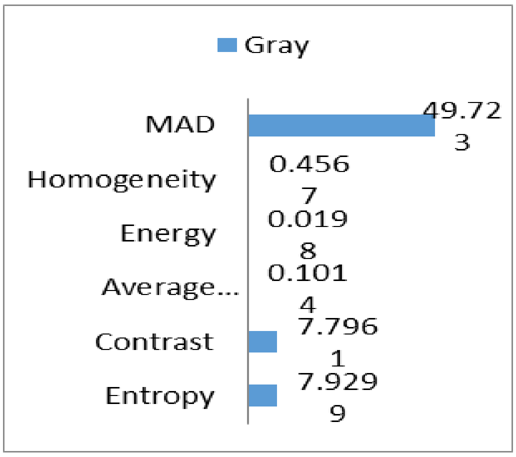


Figure 7. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to Gray S-box transformation.

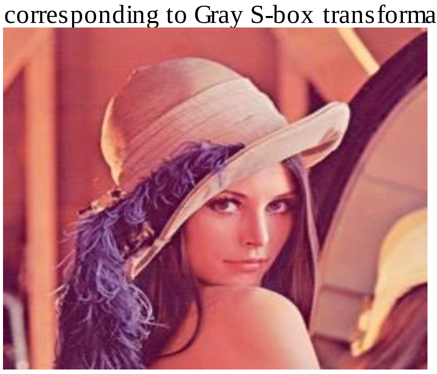


Figure 8. Plaintext Lena Image.

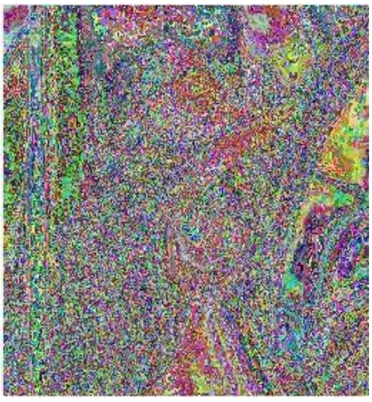


Figure 9. Cipher text Image corresponding to one round of Affine Power Affine (APA) S-box transformation.

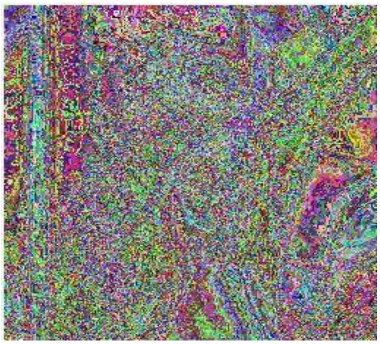


Figure 10. Cipher text Image corresponding to one round of Advanced Encryption Standard (AES) S-box transformation.

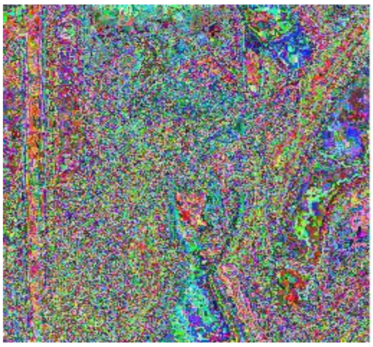


Figure 11. Cipher text Image corresponding to one round of Residue Prime S-box transformation.

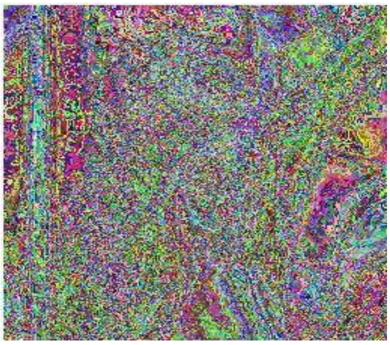


Figure 12. Cipher text Image corresponding to one round of Liu J S-box transformation.

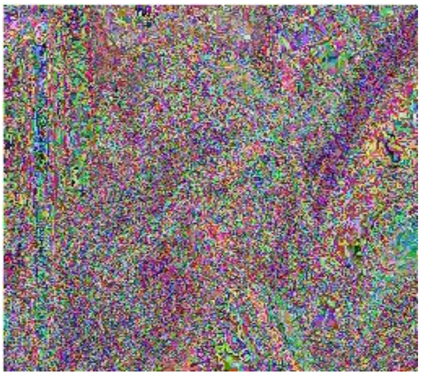


Figure 13. Cipher text Image corresponding to one round of S_8 S-box transformation.

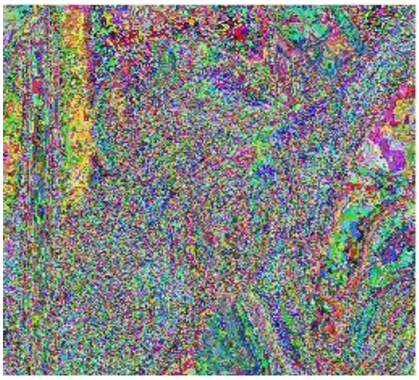


Figure 14. Cipher text Image corresponding to one round of Gray S-box transformation.

□