Analyses of S-Box in Image Encryption Applications Based on Fuzzy Decision Making Criterion

Inayatur Rehman[a], Tariq Shah[b], and Iqtadar Hussain[c]

[a] Department of Mathematics, Sokoto State University, Nigeria
[b] Department of Mathematics, Quaid-i-Azam University Islamabad Pakistan
[c] National University of Computer and Emerging Sciences, Islamabad, Pakistan

Reprint requests to I. H.; E-mail: iqtadarqau@gmail.com

Z. Naturforsch. **69a**, 207 – 214 (2014) / DOI: 10.5560/ZNA.2014-0023
Received November 7, 2013 / revised February 4, 2014 / published online May 21, 2014

In this manuscript, we put forward a standard based on fuzzy decision making criterion to examine the current substitution boxes and study their strengths and weaknesses in order to decide their appropriateness in image encryption applications. The proposed standard utilizes the results of correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to well-known substitution boxes. The outcome of these analyses are additional observed and a fuzzy soft set decision making criterion is used to decide the suitability of an S-box to image encryption applications.

Key words: Soft Set; Fuzzy Set; Fuzzy Parametrizeed Set; S-Box; Advanced Encryption Standard (AES); Affine–Power–Affine (APA); SKIPJACK; Lui J.
PACS numbers: 0.3.65.Fd; 0.3.67.Dd; 84.40.Ua

1. Introduction

The block ciphers (symmetric key cryptosystem) present an essential job in the area of secure communications. The security of an encryption algorithm is related to the performance of the building block which is liable for producing uncertainty in the cipher. This functionality is attained by the use of an S-box, so this component is like a nucleus in an atom [1]. The perfection in the properties of an S-boxes have been a major problem of research in the area of cryptology. In this paper, we show the correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis for existing S-boxes. The correlation analysis is widely used to analyse the S-box's statistical properties [2]. The entropy analysis is a statistical method used to measure the uncertainty in an image data. The amount of uncertainty in an encrypted image characterizes the texture of the image. In contrast analysis [3], the intensity difference between a pixel and its neighbour over the whole image is calculated. The elevated values of contrast analysis reflect the amount of randomness in encrypted images and results in enhanced security. The measure of closeness in the distribution of grey level co-occurrence matrix (GLCM) elements to the GLCM diagonal is calculated by the use of homogeneity analysis [4]. The GLCM is the tabulation of how often different combinations of pixel brightness values (greylevels) occur in an image [5]. In another method, energy analysis the sum of squared elements in the GLCM is measured. This analysis provides merits and demerits of various S-boxes in terms of energy of the resulting encrypted image. The final method that we implement on the encrypted image is the mean of absolute deviation (MAD) analysis [6]. This analysis determines the difference in the original and an encrypted image. There are numerous emerging encryption methods recently proposed in literature. Although these algorithms appear to be promising, there robustness is not yet established and they are evolving to become standards. Some of these algorithms worth mentioning are the public key cryptosystems based on chaotic Chebyshev polynomials [7], the advanced encryption standard (AES) cryptosystem using the features of mosaic image for extremely secure high data rate [8], and image encryption via logistic map function and heap tree [9]. The most common methods used to analyse the statistical strength of S-boxes are the correlation analysis, linear approximation probability, differential

approximation probability, and strict avalanche criterion, etc. We have included the correlation method as a benchmark for the remaining analysis used in this work. With the exception of correlation analysis, the application and use of the results of statistical analysis, presented in this paper, have not been applied to evaluate 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 [10], APA [11], Gray [1], Lui J [12], residue prime [13], S_8 AES [14], SKIPJACK [15], and Xyi [16] S-boxes. The results of these analyses are studied by the proposed criterion, and a fuzzy soft set decision is reached by taking into account the values of all the analysis on the different S-boxes. Section 4 formally introduces the issues and advantages of the analyses presented. Fuzzy soft set decision criterion analyses the effectiveness of S-boxes of the proposed 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 the 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. Historical Perspective of Soft Sets

For our urgent and straight understanding, the real world is multifaceted. Many problems in different disciplines such as engineering, social sciences, medical sciences, physics, computer sciences, and artificial intelligence are usually not specific. We construct 'models' of reality that are simplifications of aspects of the real world. Unluckily, these mathematical models are too intricate, and we cannot find the precise solutions. There are always many uncertainties mixed up in the data. The traditional tools used to deal with these uncertainties are applicable only under a certain environment. These may be owing to the uncertainties of natural environmental phenomena, of human awareness about the real world or to the confines of the means used to measure objects. For example, elusiveness or uncertainty in the boundary between states or between urban and rural areas or the exact growth rate of population in a country's rural area or making decisions in a machine based environment using database information. Thus the classical set theory, which is based on crisp and exact case, may not be fully suitable for conduct such problems of uncertainty.

Recently, many theories have been developed to deal with uncertainties, for example, the theory of fuzzy sets [17], theory of intuitionistic fuzzy sets [18], theory of vague sets, theory of interval mathematics [19, 20], and theory of rough sets [21]. Though many techniques have been developed as a result of these theories, yet difficulties seem to be there. The reason for these difficulties is, possibly, the inadequacy of the parameterization tool of the theory as it was mentioned by Molodtsov [22]. He initiated the concept of soft set theory as a new mathematical tool which is free from the problems mentioned above, and he presented the fundamental results of new theory and successfully applied it into several directions such as smoothness of functions, game theory, operations research, Riemann integration, Perron integration, theory of probability, etc. A soft set is a collection of approximate descriptions of an object. He also showed how soft set theory is free of the parameterization inadequacy syndrome of fuzzy set theory, rough set theory, probability theory, and game theory. Soft systems provide a very general framework with the involvement of parameters. Research works on soft set theory and its applications in various fields are progressing rapidly in these years.

Table 1. Entropy, contrast, correlation energy, and mean of absolute deviation analyses of prevailing S-box.

Image	Entropy	Contrast	Average correlation	Energy	Homogeneity	MAD
Plain Image	6.6733	0.2455	0.8771	0.2917	0.9334	N/A
AES	7.9325	7.2240	0.0815	0.0211	0.4701	43.544
APA	7.8183	8.9114	0.1258	0.0193	0.4665	62.066
Liu J	7.9325	7.2240	0.1311	0.0211	0.4701	43.456
Prime	7.8811	6.9646	0.2769	0.0198	0.4728	53.089
S_8	7.9447	8.1274	0.0734	0.0190	0.4552	58.389
Gray	7.9299	7.7961	0.1014	0.0198	0.4567	49.723
Xyi	7.9127	7.8942	0.1413	0.0188	0.4605	57.238
SKIPJACK	7.8939	5.4255	0.3123	0.0232	0.5004	52.733

In [23] and [24], Maji et al. presented an application of soft sets in decision making problems that is based on the reduction of parameters to keep the optimal choice objects. In [25], Chen presented a new definition of soft set parameterization reduction and a comparison of it with an attributes reduction in rough set theory. Pie and Miao [26] showed that soft sets are a class of special information systems. Kong et al. [27] introduced the notion of normal parameter reduction of soft sets and its use to investigate the problem of sub-optimal choice and added parameter set in soft sets. In [28], Zuo and Xiao discussed the soft data analysis approach. Cagman et al. [29] introduced fuzzy parametrized (FP) soft sets and their related properties. They proposed a decision making method based on FP-soft set theory.

In the present paper, we use the concept of soft set theory to cryptography and through an algorithm, we intend to choose the best possible S-box.

3. Soft Sets

In this section, we recall some definitions from [22 – 24] and an algorithm from [29] which are subsequently needed for further discussions.

Definition 1. [22] Let U be an initial universe and E be a set of parameters. Let $P(U)$ denote and be power set of U and A be a non-empty subset of E. A pair (F,A) is called 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 parameterized family of subsets of the universe U. For $\varepsilon \in A$, $F(\varepsilon)$ may be considered as the set of ε-approximate elements of the soft set (F,A). Clearly, a soft set is not a set.

Definition 2. [24] For two soft sets (F,A) and (G,B) over a common universe U, we say that (F,A) is a soft subset of (G,B) if

(a) $A \subseteq B$ and
(b) for all $e \in A$, $F(e)$ and $G(e)$ are identical approximations.

We write $(F,A) \tilde{\subseteq} (G,B)$.

(F,A) is said to be a soft super set of (G,B), if (G,B) is a soft subset of (F,A). We denote it by $(F,A) \tilde{\supseteq} (G,B)$.

Definition 3. [24] Two soft sets (F,A) and (G,B) over a common universe U are said to be soft equal if (F,A) is a soft subset of (G,B) and (G,B) is a soft subset of (F,A).

Definition 4. [24] Let $E = \{e_1, e_2, \ldots, e_n\}$ be a set of parameters. The NOT set of E denoted by $\sim E$ is defined by $\sim E = \{\sim e_1, \sim e_2, \ldots, \sim e_n\}$ where, $\sim e_i = \text{not}\, e_i$ for all i.

The following results are obvious.

Proposition 1. [24]

1. $\sim (\sim A) = A$;
2. $\sim (A \cup B) = \sim A \cup \sim B$;
3. $\sim (A \cap B) = \sim A \cap \sim B$.

Definition 5. [24] The complement of a soft set (F,A) is denoted by $(F,A)^c$ and is defined by $(F,A)^c = (F^c, \sim A)$ where, $F^c : \sim A \to P(U)$ is a mapping given by $F^c(\alpha) = U - F(\sim \alpha)$, for all $\alpha \in \sim A$.

Let us call F^c to be the soft complement function of F. Clearly $(F^c)^c$ is the same as F and $((F,A)^c)^c = (F,A)$.

Definition 6. [24] A soft set (F,A) over U is said to be a NULL soft set denoted by Φ if for all $\varepsilon \in A$, $F(\varepsilon) = \Phi(\text{null set})$.

Definition 7. [24] A soft set (F,A) over U is said to be absolute soft set denoted by $\tilde{A}$ if for all $\varepsilon \in A$, $F(\varepsilon) = U$.

Clearly $\tilde{A}^c = \Phi$ and $\Phi^c = \tilde{A}$.

Definition 8. [24] If (F,A) and (G,B) are two soft sets then, (F,A) AND (G,B) denoted by $(F,A) \wedge (G,B)$ is defined by $(F,A) \wedge (G,B) = (H, A \times B)$, where $H((\alpha,\beta)) = F(\alpha) \cap G(\beta)$, for all $(\alpha,\beta) \in A \times B$.

Definition 9. [24] If (F,A) and (G,B) are two soft sets then (F,A) OR (G,B) denoted by $(F,A) \vee (G,B)$ is defined by $(F,A) \vee (G,B) = (O, A \times B)$ where, $O((\alpha,\beta)) = F(\alpha) \cup G(\beta)$ for all $(\alpha,\beta) \in A \times B$.

Proposition 2.

1. $((F,A) \vee (G,B))^c = (F,A)^c \wedge (G,B)^c$
2. $((F,A) \wedge (G,B))^c = (F,A)^c \vee (G,B)^c$.

Definition 10. [24] Union of two soft sets (F,A) and (G,B) over the common universe U is the soft set

(H,C), where $C = A \cup B$ and for all $e \in C$,

$$H(e) = \begin{cases} F(e) & \text{if } e \in A - B, \\ G(e) & \text{if } e \in B - A, \\ F(e) \cup G(e) & \text{if } e \in A \cap B. \end{cases}$$

We write $(F,A) \cup (G,B) = (H,C)$.

Definition 11. [24] The intersection (H,C) of two soft sets (F,A) and (G,B) over a common universe U, denoted $(F,A) \cap (G,B)$, is defined as $C = A \cap B$, and $H(e) = F(e) \cap G(e)$ for all $e \in C$.

Algorithm [29] Here in the following, we use a decision making method/algorithm as proposed by Cagman [29].

Once a fuzzy decision set of an FP-soft set has been arrived at. It may be necessary to choose the best single alternative from the alternatives. Thus we can make a decision by the following algorithm:

Step 1. Construct a soft set F_X over U.
Step 2. Compute the fuzzy decision set F_X^{d}.
Step 3. Select the largest membership grade $\max \mu_{F_X^{\mathrm{d}}}(u)$.

4. Problem Statement

In this paper, we analyse 8×8 S-boxes (AES, APA, Gray, Lui J, Residue Prime, S_8 AES, SKIPJACK, and Xyi) used in popular block ciphers. Without the loss of generality, the analysis can be extended to S-boxes of other sizes. The statistical analysis is used to determine the application and appropriateness of an S-box to image encryption application [1]. The strength of an encryption based S-box can be evaluated 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 fuzzy soft set decision making assessment. The procedure begins with the correlation analysis. In this method, we use the correlation information to determine the similarity of pixel patterns in the given image and its encrypted version. Although this analysis has been widely used to evaluate various image encryption algorithms, it is included here with other methods due to its importance and acceptability in comparing 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 vivid results and consequently assist in evaluating the performance 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 analysed and studied for the evaluation of S-boxes to image encryption application.

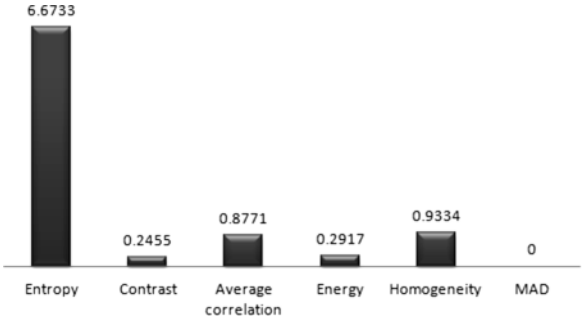

Fig. 1. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of plain image.

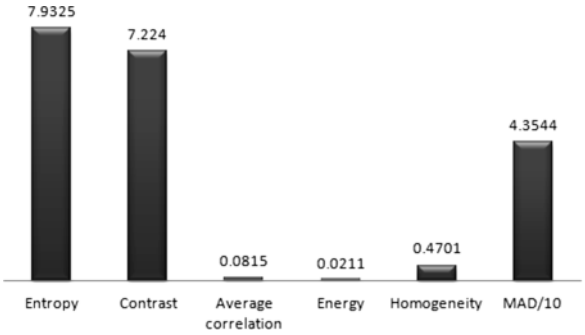

Fig. 2. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to advance encryption standard S-box transformation.

Figure 1 describes the results of entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of plain image. Since it is clear from Figure 1 that the date of original image is quite

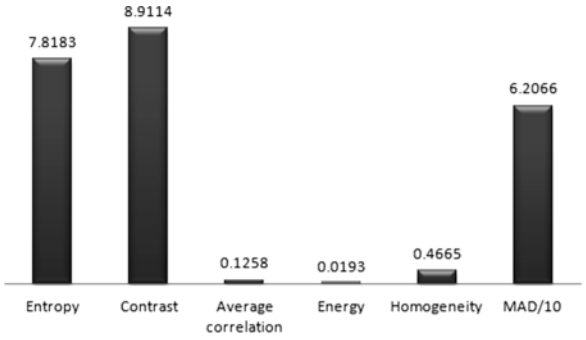

Fig. 3. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to affine–power–affine S-box transformation.

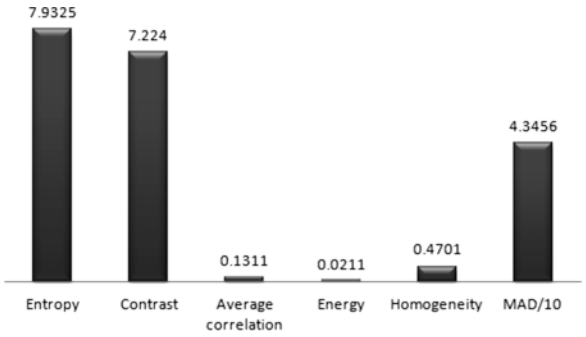

Fig. 4. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to Liu J S-box transformation.

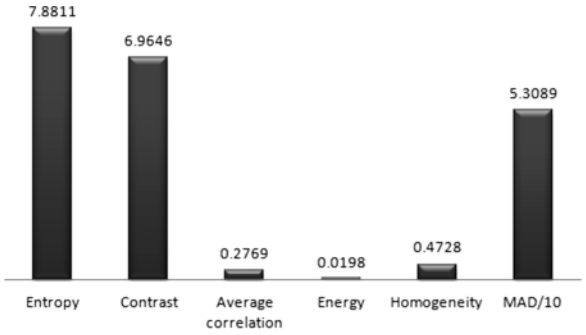

Fig. 5. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to prime S-box transformation.

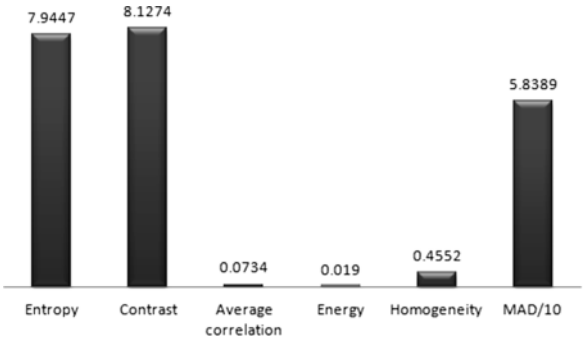

Fig. 6. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to S_8 S-box transformation.

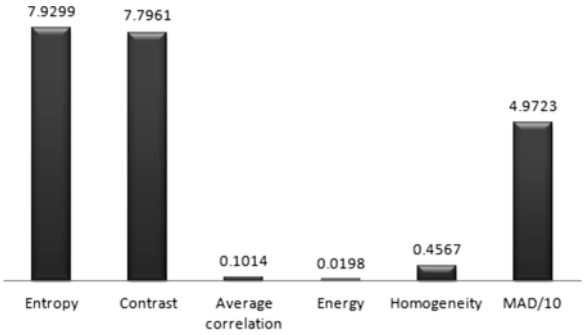

Fig. 7. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to Gray S-box transformation.

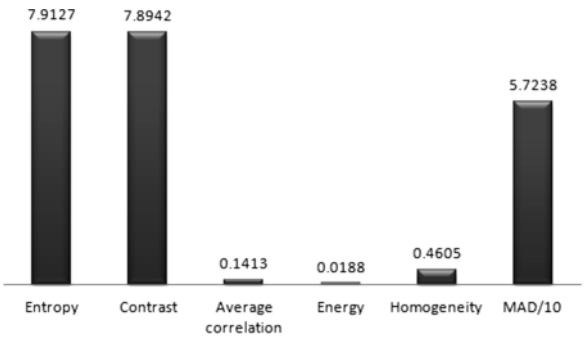

Fig. 8. Entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation of cipher image corresponding to Xyi S-box transformation.

paternized, our goal is to depaternized the data of the plain image with the help of prevailing S-box transformations.

Figure 2 presents the reading of entropy, contrast, average correlation, energy, homogeneity, and mean of absolute deviation after the application of AES S-box transformation on a three dimensional plain image of F-16. The affects of AES S-box transformation on these analysis are as follows: the entropy is changed from 6.733 to 7.9.25, the contrast of the plain image is changed from 0.2455 to 7.224, that means that the AES S-box transformation produce a big disorder in the contrast of the plain image. The correlation of the plain image is distorted from 0.8771

to 0.0815, the energy is changed form 0.2917 to 0.0211, the homogeneity is changed from 0.9334 to 0.4701. At the end the difference between the original image and cipher image corresponding to AES S-box is measured with the help of MAD analysis and come to know that the cipher image is different from the plain image with the reading of 4.3544. It is quite clear from Figures 1 and 2 that the AES S-box transformation induced a huge diorder in the plain image.

Now we present the comparison of Figures 1 and 3. The result of entropy in Figure 3 after the affine–power–affine (APA) S-box transformation is changed from 6.773 to 7.8183 which is different from AES cipher image entropy. The result of contrast of APA cipher image is changed from 0.2455 to 8.9114, which is also different from 7.244, the contrast of AES cipher image. But if we compare the results of both transformations of Figures 2 and 3 for entropy, it is quite clear that APA S-box transformation is better than AES S-box transformation. Furthermore, the reading of correlation of APA cipher image is changed from 0.8771 to 0.1258, but the correlation of AES cipher, which is 0.0815, is much better than for the APA cipher image. That means that the AES S-box transformtion is better than the APA S-box transformation in the sence of producing uncorrelation in the pixels of the plain image. The energy of plain image is changed from 0.2917 to 0.0193 which is better than the energy of the AES cipher image. The homogeneity is changed from 0.9334 to 0.4665 which is also better than AES cipher image. If we compare the MAD of Figures 2 and 3, we come to know that the APA S-box transformtion induces a big disorder in the pixels of the plain image with reading 6.2066 as compared to AES S-box transformation. That means in some case the AES S-box transformation is better and in senario APA S-box transformation shows good results.

It can be seen from the comparison of Figures 2, 3, and 4 that the entropy of AES S-box transformation and Liu J S-box transformation is the same and better than the APA S-box transformation. The contrast, the analysis of Liu J S-box is 7.224 which is lesser than APA S-box transformation. The correlation analysis of Figure 4 is 0.1311 which is also weak reading as compared to APA S-box transformation. The energy analysis of APA transformation is also better than Liu J transformation. The homogeneity and MAD analysis of APA S-box transformation are also comparitively better than Liu J S-box transformation. From the above discussion, it is clear that the APA S-box transformation is quite good as compared with Liu J and AES S-box transformation for image encryption applications.

If we compare Figure 5 with other S-box transformation, we have come to know that APA S-box transformation is also better than residue prime S-box transformation.

The reading of S_8 S-box transformation is much better than every other S-box transformation that is discussed in this manuscript. The reason behind this is the fact that the construction of S_8 S-box depends on symmetric group of permutation and Galois field. The basic requirement of an S-box is to provide confussion in the data but this box provides an addition step of security which is diffusion. Diffusion complicates the relationship between the plain text and cipher text. The diffusion in the S_8 S-box transformation is due to the permuatations of the S_8 group.

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

The Xyi S-box transformation exhibites very good results for different analysis but in case of correlation analysis this transformation is not as good, what is required for a good image encryption. The results of energy analysis of Figure 4 transformations 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

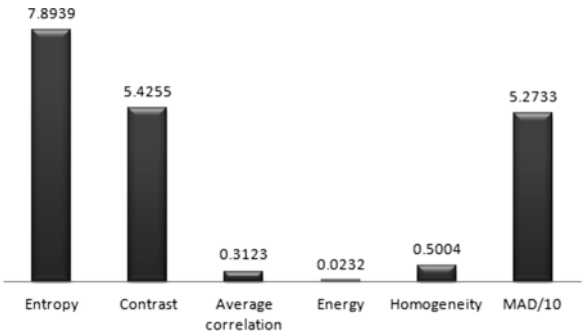

Fig. 9. Entropy, contrast, average correlation, energy, homogeneity and mean of absolute deviation of cipher image corresponding to Skipjack S-box transformation.

analysis this transformation is not on the first position so we can make use of it for secure communication.

Although in literature, we may find different tools/methods to analyse and choose a best S-box.

Here in our discussion keeping in view the above Table 1 and Figures 1–9, we want to use the concept of soft set to choose the best S-box.

Let $U = \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_8, u_9\}$ be the set of alternatives, where u_i $(i = 1,2,3,4,5,6,7,8,9)$ are S-boxes and the alternatives u_i represent plain image, AES, APA, Lui, Prime, Gray, Xyi, S_8, and SKIPJACK, respectively. To evaluate the S-boxes, we take the set of parameters as $E = \{e_1, e_2, e_3, e_4, e_5, e_6\}$. For $i = 1,2,3,4,5,6$, the parameters e_i stand for entropy, contrast, average correlation, energy, homogeneity, and mean of absolute development, respectively. These parameters are important with degree $0.9, 0.8, 0.2, 0.5, 0.6, 0.1$, respectively. Then we have the set of parameters:

$$X = \{0.9/e_1, 0.8/e_2, 0.2/e_3, 0.5/e_4, 0.6/e_5, 0.1/e_6\}.$$

Now we are in the position to select the best S-box by the following steps.

Step 1. Keeping in mind all tools and methods as already described in [5] and after a serious discussion, we evaluate the alternative by choosing a set X to construct an FP-soft set

$$F_X = \left\{ \begin{array}{c} (0.9/e_1, \{u_1, u_4, u_6, u_8\}), \\ (0.8/e_2, \{u_2, u_3, u_5, u_8\}), \\ (0.2/e_3, \{u_1, u_2, u_3, u_4, u_6\}), \\ (0.5/e_4, \{u_2, u_4, u_6, u_7\}), \\ (0.6/e_5, \{u_3, u_5, u_7, u_8\}), \\ (0.1/e_6, \{u_1, u_2, u_3, u_4, u_5, u_6, u_7, u_9\}). \end{array} \right\}$$

Step 2. From Step 1, it is obvious that for all elements of X, $f_X(x) \neq \emptyset$. Thus $\left|\mathrm{Supp}(X)\right| = 6$.

Now

$$\mu_{F_X^{\mathrm{d}}}(u_1) = \frac{1}{6}\Big[(0.9)(1) + (0.8)(0) + (0.2)(1) + (0.5)(0) + (0.6)(0) + (0.1)(1)\Big] = 0.2.$$

Similarly, we have

$$\mu_{F_X^{\mathrm{d}}}(u_2) = 0.26,\ \mu_{F_X^{\mathrm{d}}}(u_3) = 0.28,\ \mu_{F_X^{\mathrm{d}}}(u_4) = 0.28,$$
$$\mu_{F_X^{\mathrm{d}}}(u_5) = 0.25\ \mu_{F_X^{\mathrm{d}}}(u_6) = 0.283,\ \mu_{F_X^{\mathrm{d}}}(u_7) = 0.2,$$
$$\mu_{F_X^{\mathrm{d}}}(u_8) = 0.38 \text{ and } \mu_{F_X^{\mathrm{d}}}(u_9) = 0.01.$$

Thus, the fuzzy decision set of F_X can be found as

$$F_X^{\mathrm{d}} = \Big\{0.2/u_1, 0.26/u_2, 0.28/u_3, 0.28/u_4, 0.25/u_5, 0.28/u_6, 0.2/u_7, 0.38/u_8, 0.01/u_9\Big\}.$$

Step 3. Finally, the largest membership grade can be chosen by $\max \mu_{F_X^{\mathrm{d}}}(u) = 0.38$. So we concluded that the alternative u_8, i. e the S-box S_8, has the largest membership grade, hence it is selected as the best S-box among them all.

5. Conclusion

In this paper, we have provided a connection between the fuzzy decision theory and secure communication theory. The basic goal of this work is to show the security comparison of prevailing S-boxes for image encryption applications. From all the analyses of image processing, we have come to know that the S_8 S-boxes are extraordinary against all the existing S-boxes including the advanced encryption standard S-box. So we can use the proposed criterion for other kinds of 8×8 S-boxes.

[1] M. T. Tran, D. K. Bui, and A. D. Doung, Int. Conf. Comput. Intel Secur. **51**, 253 (2008).
[2] L. Zhang, X. Liao, and X. Wang, Chaos Solut. Fract. **24**, 759 (2005).
[3] S. Y. Chen, W. C. Lin, and C.T. Chen, Graph. Models Imag. Proc. **53**, 457 (1991).
[4] F. Jing, M. Li, H. Zhang, and B. Zhang, Proc. ISCAS **2**, 456 (2003).
[5] E. S. Gadelmawla, Nondestr. Test. Eval. Int. **37**, 577 (2004).
[6] I. Avcibas, N. Memon, and B. Sankur, IEEE Trans. Imag. Proc. **12**, 221 (2003).
[7] K. Prasadh, K. Ramar, and R. Gnanajeyaraman, Int. J. Phys. Sci. **1**, 122 (2009).
[8] G. M. Alam, M. L. Kiah, B. B. Zaidan, A. A. Zaidan, and H. O. Alanazi, Int. J. Phys. Sci. **5**, 3254 (2010).
[9] R. Enayatifar, Int. J. Phys. Sci. **6**, 221 (2011).
[10] J. Daemen and V. Rijmen, AES Proposal: Rijndael. AES Algorithm Submission, Available:

http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf (1999).
[11] L. Cui and Y. Cao, Int. J. Innov. Comput. I. **3**, 45 (2007).
[12] J. Lui, B. Wai, X. Cheng, and X. Wang, Int. Conf. Inform. Network. Appl. **1**, 724 (2005).
[13] E. S. Abuelyman and A. A. S. Alsehibani, Int. J. Comput. Sci. Network Secur. **8**, 304 (2008).
[14] I. Hussain, T. Shah, and H. Mehmood, Int. J. Cont. Math. Sci. **5**, 1263 (2010).
[15] SKIPJACK, Spec. Vers. **2**, 1 (1998).
[16] X. Y. Shi, H. U. Xiao, X. C. You, and K. Y. Lam, Int. Conf. Inform. Network. Appl. **2**, 14 (2002).
[17] L. A. Zadeh, Inform. Contr. **8**, 338 (1965).
[18] K. Atanassov, Fuzzy Sets Syst. **20**, 87 (1986).
[19] K. Atanassov, Fuzzy Sets Syst. **64**, 159 (1994).
[20] M. B. Gorzalzany, Fuzzy Sets Syst. **21**, 1 (1987).
[21] Z. Pawlak, Int. J. Inform. Comput. Sci. **11**, 341 (1982).
[22] D. Molodtsov, Comput. Math. Appl. **37**, 19 (1999).
[23] P. K. Maji, R. Biswas, and R. Roy, Comput. Math. Appl. **44**, 1077 (2002).
[24] P. K. Maji, R. Biswas, and R. Roy, Comput. Math. Appl. **45**, 555 (2003).
[25] D. Chen, Comput. Math. Appl. **49**, 757 (2005).
[26] D. Pie and D. Miao, IEEE Inter. Conf. **2**, 617 (2005).
[27] Z. Kong, L. Gao, L. Wong, and S. Li, J. Comput. Appl. Math. **56**, 3029 (2008).
[28] Y. Zou and Z. Xiao, Knowl.-Based Syst. **21**, 941 (2008).
[29] N. Cagman, F. Citak, and S. Enginoglu, Ann. Fuzzy Math. Inform. **2**, 219 (2011).