International Journal of the Physical Sciences Vol. 6(16), pp. 4110-4127, 18 August, 2011
Available online at http://www.academicjournals.org/IJPS
DOI: 10.5897/IJPS11.531
ISSN 1992-1950 ©2011 Academic Journals

Full Length Research Paper

Statistical analysis of S-box in image encryption applications based on majority logic criterion

Tariq Shah[1], Iqtadar Hussain[1]*, Muhammad Asif Gondal[2] and Hasan Mahmood[3]

[1]Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan.
[2]Department of Sciences and Humanities, National University of Computer and Emerging Sciences, Islamabad, Pakistan.
[3]Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan.

Accepted 2 June, 2011

The S-box is used in various block ciphers and the complexity of encryption essentially depends on the strength of S-box. The strength of an S-box can be measured by analyzing its statistical and algebraic properties. The S-box is the only non-linear component in various block ciphers capable of creating confusion. Many S-boxes have been proposed with similar algebraic and statistical properties. Therefore, it is sometimes difficult to choose an S-box for a particular application. The performances of these S-boxes vary and depend on the nature of data and their application. In this paper, we propose a criterion to analyze the prevailing S-boxes and study their strengths and weaknesses in order to determine their suitability in image encryption applications. The proposed criterion uses the results from correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. These analyses are applied to advanced encryption standard (AES), affine-power-affine (APA), gray, Lui J, residue prime, S_8 AES, SKIPJACK, and Xyi S-boxes. The results of these analyses are further examined and a majority logic criterion is used to determine the appropriateness of an S-box to image encryption applications.

Key words: S-box, advanced encryption standard (AES), affine-power-affine (APA), SKIPJACK, Lui. J, residue of prime, mean of absolute deviation analysis (MAD), differential/linear approximation probability, bit independence criterion, strict avalanche criterion.

INTRODUCTION

The block ciphers play a pivotal role in the area of cryptography. The performance of a cipher depends on the strength of the algorithm which is responsible for creating confusion in the encryption process. This functionality is achieved by the use of an S-box, which is the only nonlinear component included in many block ciphers (Tran et al., 2008). The improvement in the algebraic and statistical properties of S-boxes has been a center of attraction in the field of encryption.

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 analyze the S-box's statistical properties (Zhang et al., 2005). The entropy analysis (Zhan et al., 2007) 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 (Chen et al., 1991), the intensity difference between a pixel and its neighbor 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 (Jing et al., 2003). The GLCM is the tabulation of how often different combinations of pixel brightness values (grey levels) occur in an image (Gadelmawla, 2004). In another method, energy analysis (Zhan et al., 2007), the sum of squared elements in the GLCM is measured. This analysis provides merits and demerits of various S-boxes

*Corresponding author. E-mail: iqtadarqau@gmail.com.

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 (Avcibas et al., 2003). 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 (Prasadh et al., 2009), advanced encryption standard (AES) cryptosystem using the features of mosaic image for extremely secure high data rate (Alam et al., 2010), and image encryption via logistic map function and heap tree (Enayatifar, 2011).

The most common methods used to analyze the statistical strength of S-boxes are the correlation analysis, linear approximation probability, differential approximation probability, and strict avalanche criterion etc. We have included 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 (Daemen and Rijmen, 1999), APA (Cui and Cao, 2007), gray (Tran et al., 2008), Lui J (Lui et al., 2005), residue prime (Abuelyman and Alsehibani, 2008), S_8 AES (Hussain et al., 2010), SKIPJACK (SKIPJACK, 1998), and Xyi (Shi et al., 2002) S-boxes. The results of these analyses are analyzed by the proposed criterion and a majority logic decision is reached by taking in to account the values of all the analysis on different S-boxes.

This paper we emphasized on “problem statement,” which formally introduces the issues and advantages of the analyses presented. Majority logic criterion analyzes 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 experiments performed in order to verify the statistical analysis results are shown in simulation results and discussion.” Finally, the study present “conclusions” and “future direction” related to this work.

PROBLEM STATEMENT

In this manuscript, we analyze 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 (Tran et al., 2008). The strength of an encryption based on 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 majority logic 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 data. 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 analyzed and studied for the evaluation of S-boxes to image encryption application.

Majority logic criterion to analyze the effectiveness of S-boxes

The encryption process produces distortions in the image, and the type of these distortions determine the strength of the algorithm. Therefore, it is pragmatic to study the statistical characteristics and properties of S-box transformations. The process of encryption is similar to byte sub step of AES (Daemen and Rijmen, 1999). A majority logic criterion is used to determine the best S-box which satisfies the decision criteria.

In Figure 1, the proposed criterion is presented in detail. The input to the decision criteria is the statistical data of images obtained from analyzing multiple S-boxes of different types and their data from respective S-box transformed images. The objective is to examine the results of correlation analysis, entropy analysis, contrast analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis and decide by using majority logic, the best S-box candidate. If an image I_i satisfies majority of the conditions of the proposed criteria as compared to I_j, we say that corresponding S-box S_i is superior to S_j.

The flowchart of the proposed criterion is presented in Figure 2. Here also, the method starts with the input of plane image, and the process of encryption is achieved in the second step. The application of the proposed criterion is implemented in order to determine the S-box with best performance. This process is further explained with the help of a flowchart in Figure 3. Various statistical methods are denoted by symbols C_1 through C_6. For example C_1 represents the process of finding the correlation parameters from the encrypted images, and similarly all the remaining methods are represented in this stage. The output from C_1 to C_6 is analyzed by the majority logic criterion which determines the best S-box based on statistical properties.

Statistical image analysis of S-boxes

In this study, we present the details of the statistical analyses used in this work for the purpose of making decisions in the proposed criterion. We start by describing the application of correlation analysis for the cases of vertical, horizontal, and diagonal analyses. The general correlation, which covers the entire plain image and encrypted image, is also performed.

Proposed criterion

Suppose we have n S-boxes, say $S_1, S_2, \dots, S_N$. Let the image encrypted by $S_1, S_2, \dots, S_N$ are $I_1, I_2, \dots, I_n$ respectively

We said S-box S_i is better than S_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$ if

C_1: If Correlation of pixels of image with its neighbor's pixels of I_i is smaller than I_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$.

C_2: If Entropy of I_i is greater than I_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$.

C_3: If Contrast of I_i is greater than I_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$.

C_4: If Homogeneity of I_i is smaller than I_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$.

C_5: If Energy of I_i is smaller than I_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$.

C_6: If MAD of I_i is greater than I_j for $j \in \{1,2,\dots,n\}\backslash\{i\}$.

Figure 1. The proposed criterion to determine the best type of S-box for image encryption.

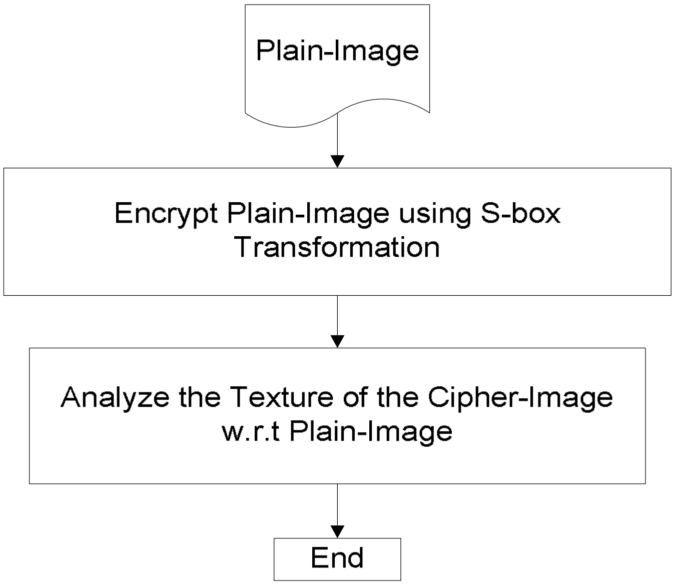
Plain-Image
Encrypt Plain-Image using S-box Transformation
Analyze the Texture of the Cipher-Image w.r.t Plain-Image
End

Figure 2. Flow chart of proposed algorithm.

Correlation analysis

The correlation analysis is the most fundamental method used in determining the similarity between two images, especially in encryption applications. The analysis consists of three parts. In the first step, the correlation among local pixels in both vertical and horizontal neighborhoods is determined. The result of this analysis shows the overall correlation factor of the two images. In addition, we also calculate the correlation between diagonal pixels in order to further evaluate the amount of randomness introduced by the S-box. In order to evaluate the overall similarity between plain image and the encrypted image, the correlation for the entire images is analyzed in a single step. This helps us in evaluating the similarity or randomness in a global perspective. These three cases are presented as:

Case 1: Select all pair of two adjacent pixels in vertical and horizontal direction from the plain image and encrypted image, and calculate the correlation coefficient respectively. The results of this case are depicted in Table 1. It can be seen that the correlation among the images is reduced considerably.

Case 2: In this case, we take into account the pixels located in the diagonal directions. The calculation of correlation parameters begins with the random selection of 1000 pair of diagonally located pixels. The selection criteria and its parameters are identical in plain image and encrypted image. The resulting correlation coefficients are saved for further analysis to be used in the proposed majority logic criterion.

Case 3: Here we consider two variables X and Y which constitute the entire pixel data for the plain image and encrypted image, respectively. The correlation is represented as:

$$r = \frac{\sum_m \sum_n (A_{mn} - \overline{A})(B_{mn} - \overline{B})}{\sqrt{\left(\sum_m \sum_n (A_{mn} - \overline{A})^2\right)\left(\sum_m \sum_n (B_{mn} - \overline{B})^2\right)}}$$

where $\overline{A}$ and $\overline{B}$ are average or mean of matrix elements.

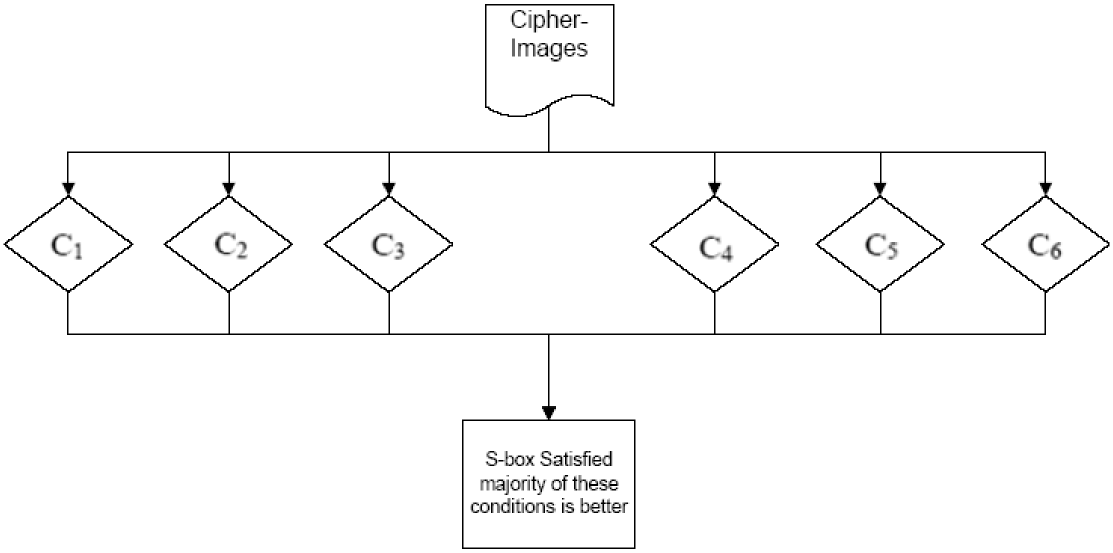

Figure 3. Analysis of texture of cipher image.

Table 1. Correlation coefficient of two adjutant pixels of plain image and ciphered image for different S-boxes.

Images	Vertical correlation	Horizontal correlation	Diagonal correlation	Average (V, H, D)	General correlation
Plain-Image	0.7155	0.9809	0.9351	0.8771	N/A
AES	0.1082	0.1272	0.0092	0.0815	0.1005
APA	0.0991	0.2059	0.0726	0.1258	-0.1048
Gray	0.0967	0.1748	0.0328	0.1014	-0.0719
Lui J	0.1135	0.1395	0.1405	0.1311	0.1005
Prime	0.3129	0.3338	0.1840	0.2769	-0.1084
S_8	0.0092	0.1666	0.0445	0.0734	-0.0827
SKIPJACK	0.4342	0.2615	0.2413	0.3123	-0.1767
X yi	0.1809	0.1852	0.0579	0.1413	-0.0462

The results of correlation analysis are presented in Table 1. The encrypted images corresponding to various S-boxes, include AES, APA, Gray, Lui J, residue prime, S_8 AES, SKIPJACK, and Xyi. Their correlation coefficients are shown in Table 1. In Column 2, 3, and 4, the results of vertical correlation, horizontal correlation, and diagonal correlation are shown for comparison, respectively. The average of the results of these three analyses is calculated and shown in Column 5. In the last column, general correlation is performed on the images and the results are listed for different S-boxes. It can be seen from the Table 1 that the amount of average correlation (V, H, D), that is, locally and for the entire image, is minimum for the case of S_8 AES S-box. In terms of correlation, the performance of different S-boxes can be seen in Figure 4.

It is observed that the S_8 AES S-box has the best confusion capability if evaluated in terms of correlation analysis parameters.

Entropy analysis

Entropy is a statistical measure of randomness that can be used to characterize the texture of the image. Entropy is defined as:

$$H = -\sum_{i=1}^{n} p(x_i)\log_b p(x_i)$$

where $p(x_i)$ contains the histogram counts.

Figure 5 shows the results of entropy analysis of the encrypted images. The entropy of the cipher image corresponding to S_8 AES S-box is 7.9447, which is the highest among all the analyzed S-boxes. This analysis follows a similar trend to the correlation analysis, in which the performance of AES is comparable to that of S_8 S-box.

Contrast analysis

In general, the contrast analysis of the image enables the viewer to vividly identify the objects in texture of an image. The encrypted image has higher contrast levels because of the high level of randomness introduced by application of an S-box in the encryption

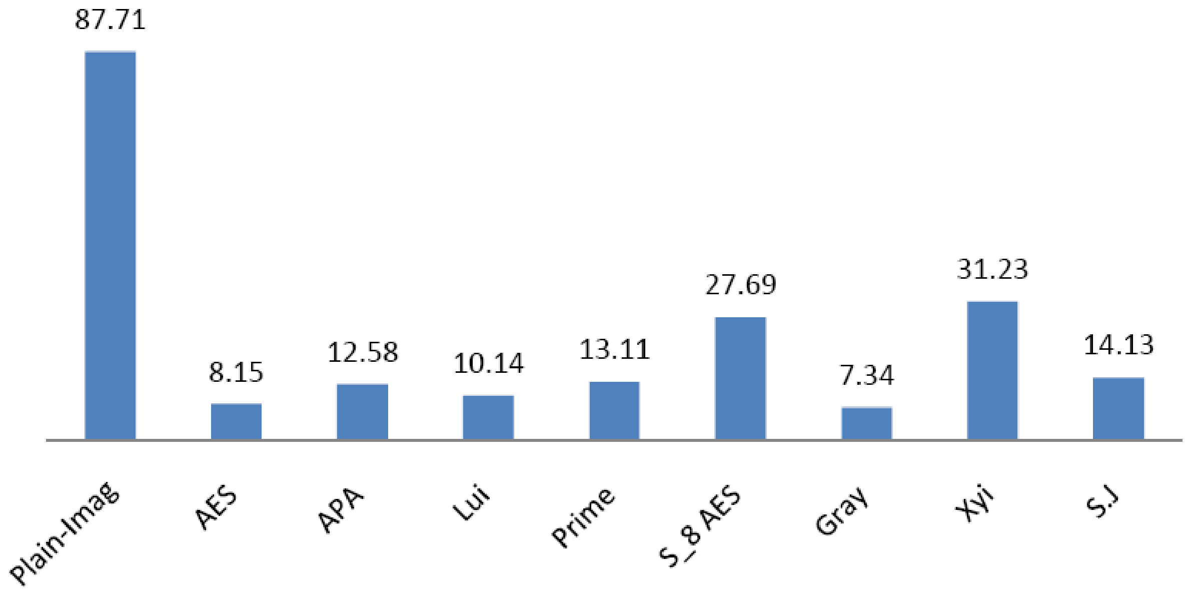

Figure 4. Average correlation coefficient times one hundred.

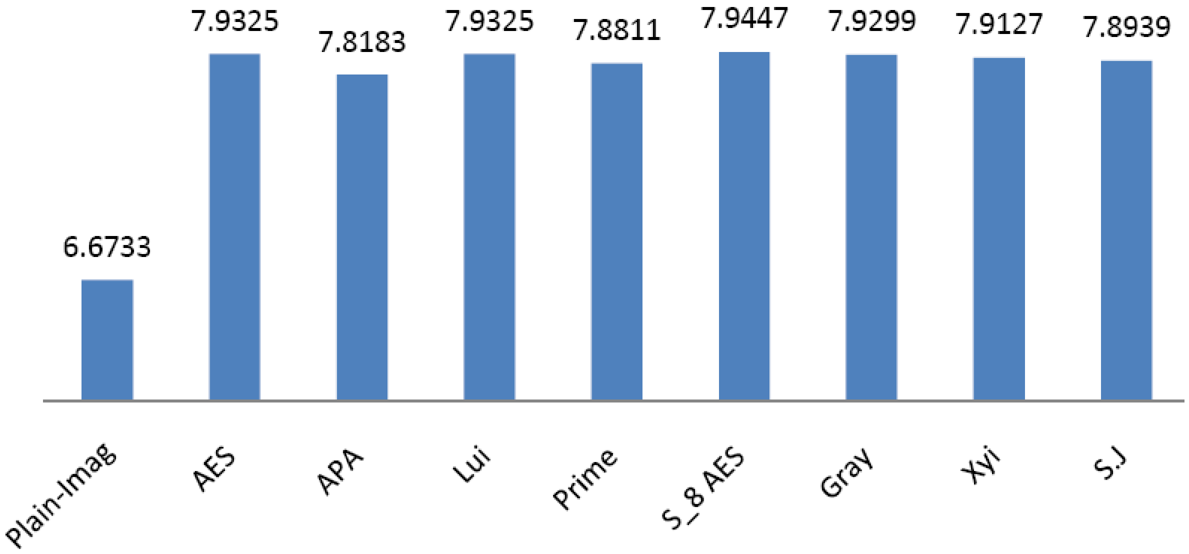

Figure 5. Entropy analysis of encrypted images.

process. We measure the contrast parameters of the encrypted image and evaluate the effectiveness of S-boxes in image encryption applications.

This analysis returns a measure of the intensity contrast between a pixel and its neighbor over the whole image and is mathematically represented as:

$$C = \sum_{i,j} |i - j|^2 p(i, j)$$

where the number of gray-level co-occurrence matrices is represented by p(i, j).

Figure 6 shows the results of contrast analysis when applied to encrypted images corresponding to various S-boxes. It is evident from the results that the APA S-box is capable of elevating contrast level to the highest point. The S_8 AES S-box also performs better as compared to other S-boxes listed in Figure 6.

Homogeneity

The homogeneity analysis measures the closeness of the distribution of elements in the grey level co-occurrence matrix (GLCM), also called grey tone spatial dependency matrix (GTSDM), to GLCM diagonal. The GLCM shows the statistics of combinations

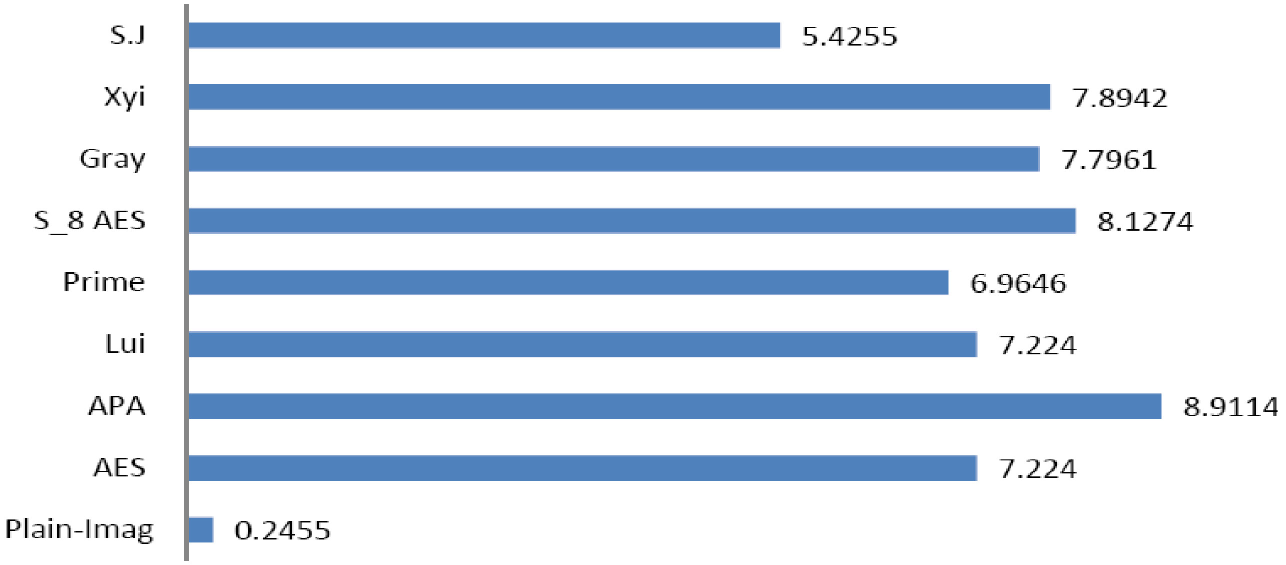

Figure 6. Contrast analysis of cipher-image.

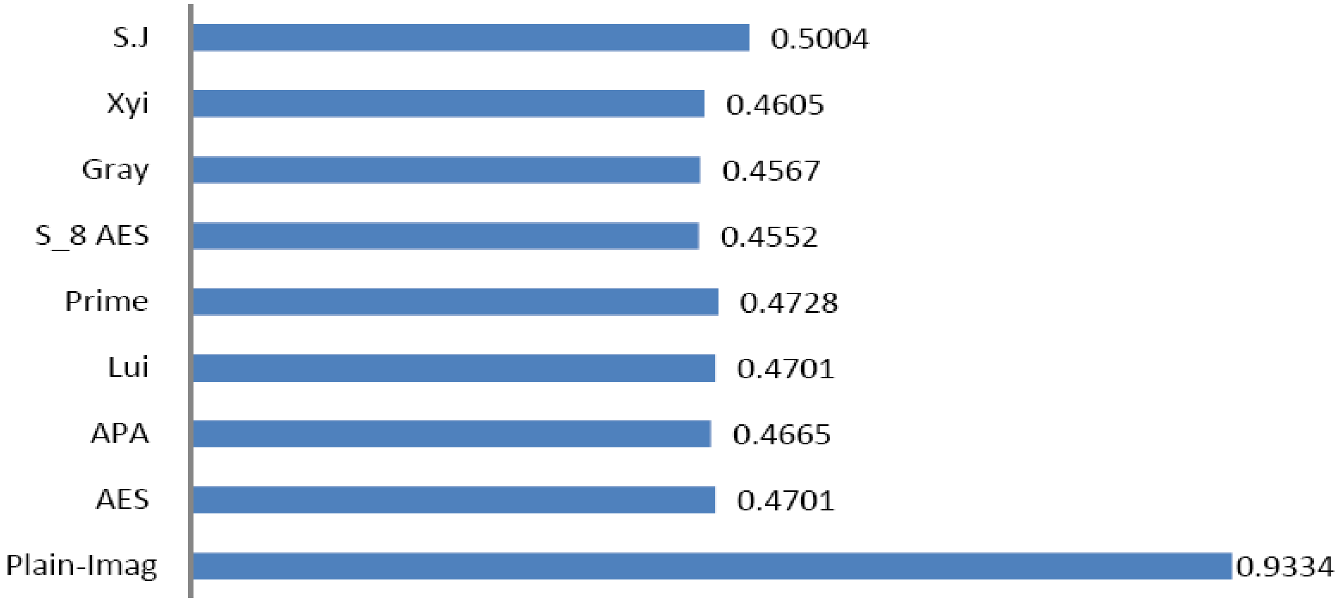

Figure 7. Homogeneity analysis of cipher-image.

of pixel brightness values or grey levels in tabular form. The frequency of the patterns of grey levels can be interpreted from the GLCM table. The homogeneity can be determined as:

$$\sum_{i,j}\frac{p(i,j)}{1+|i-j|}$$

where the gray-level co-occurrence matrices in GLCM is represented by p(i, j).

Figure 7 shows the results of homogeneity analysis for cipher images. In this analysis, we again observe that the performance of S_8 AES S-box is the best. In this category, the images encrypted with Gray and Xyi S-boxes are comparable to the performance of S_8 AES S-box.

Energy of the image

In this analysis, we measure the energy of the encrypted images as processed by various S-boxes. This measure gives the sum of

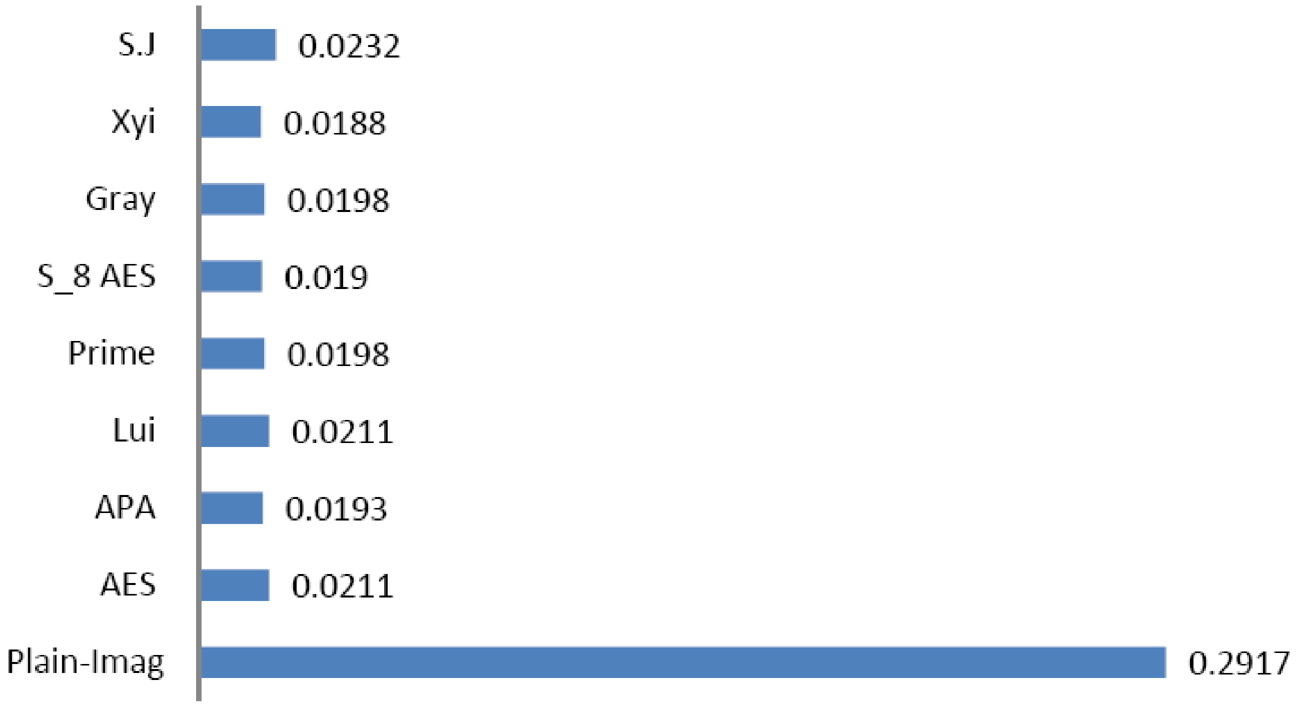

Figure 8. Energy analysis of cipher-image.

squared elements in the gray level co-occurrence matrix:

$$\sum_{i,j} p(i,j)^2$$

where $p(i,j)$ is the number of gray-level co-occurrence matrices.

Figure 8 shows the energy analysis of cipher images. In this analysis Xyi S-box acquires first ranking with 0.0188 and S_8 AES S-box is next in terms of performance parameters.

MAD analysis

This analysis quantifies the difference between original image and the encrypted image. The mean of absolute deviation is determined to evaluate the difference between two images. This analysis can be mathematically represented as:

$$MAD = \frac{1}{L \times L} \sum_{j=1}^{L} \sum_{i=1}^{L} \left| a_{ij} - b_{ij} \right|$$

where ai,j represents the pixels of plain image, bi,j represents the pixels of the corresponding encrypted image, and L represents the dimensions of the image.

Figure 9 shows the MAD analysis of cipher images with respect to plain image for different types of S-boxes. In this analysis, APA S-box is comparatively better with 62.066 and S_8 AES S-box is next with the score of 58.389.

Table 2 shows the results of entropy analysis, contrast analysis, energy analysis, homogeneity analysis, and mean of absolute deviation analysis. In order to apply majority logic criterion as presented in Figure 1, we use the parameters listed in Table 2. The novelty of the proposed criterion lies in the advanced evaluation of the statistical analysis on various S-boxes. According to the criterion presented in Figure 1, the performance of S_8 AES S-box is best, which satisfies majority of the proposed methodologies used in the analysis. It can be seen from Table 2 that APA S-box and Xyi S-box performs better in MAD analysis and energy analysis respectively. While several S-boxes perform better in individual analysis, the majority logic criterion identifies the best candidate S-box with highest level of encryption strength.

SIMULATION RESULTS AND DISCUSSION

In this study, the simulation results for eight popular S-boxes, that is, AES, APA, Gray, Lui J, residue prime, S_8 AES, SKIPJACK, and Xyi S-boxes are presented. A plain image, shown in Figure 10, is used to test the encryption strength of an S-box. Figures 11 to 27 show the experimental results of various images and their histograms for different S-box transformations (Appendix 1). The S-box transformation is only performed once on the sample image in order to statistically and visually analyzes the resulting encrypted image properties and its perception, respectively. The S-box transformation can be performed multiple times if required. In this work, we only analyze the results of single S-box transformation.

In the sample plain image, the histogram shows the intensity distribution which ranges from 1000 to 1. These intensity levels are not uniformly distributed in the images, and as a result, gives a clear perception of the

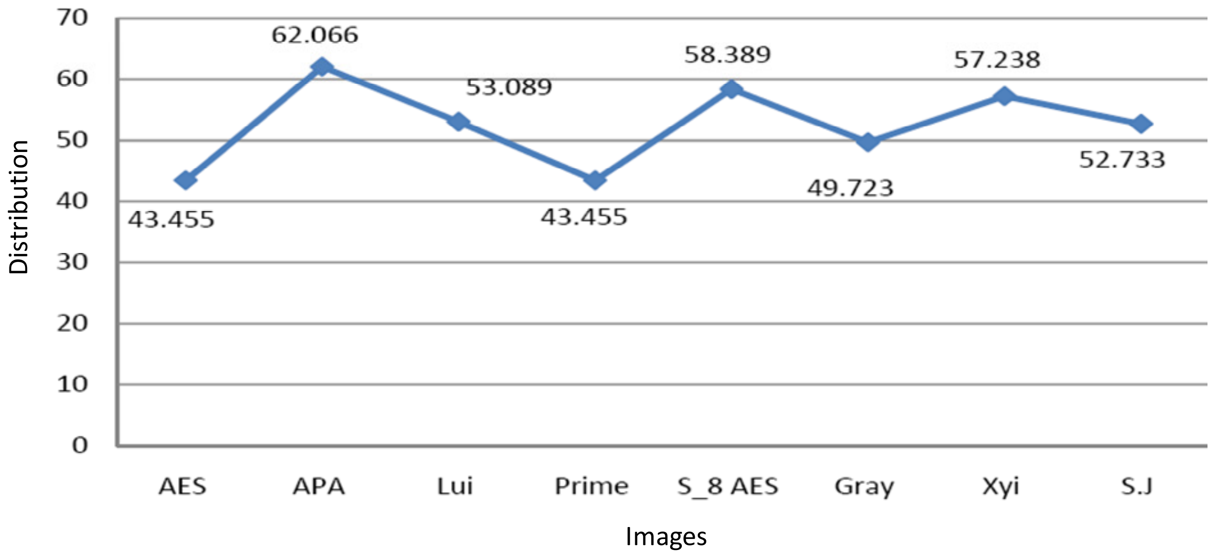

Figure 9. MAD analysis of cipher-image.

Table 2. Entropy, contrast, correlation, energy and homogeneity of plain image and cipher image.

Images	Entropy	Contrast	Average correlation	Energy	Homogeneity	Mean of absolute development
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	43.455
APA	7.8183	8.9114	0.1258	0.0193	0.4665	62.066
Lui	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

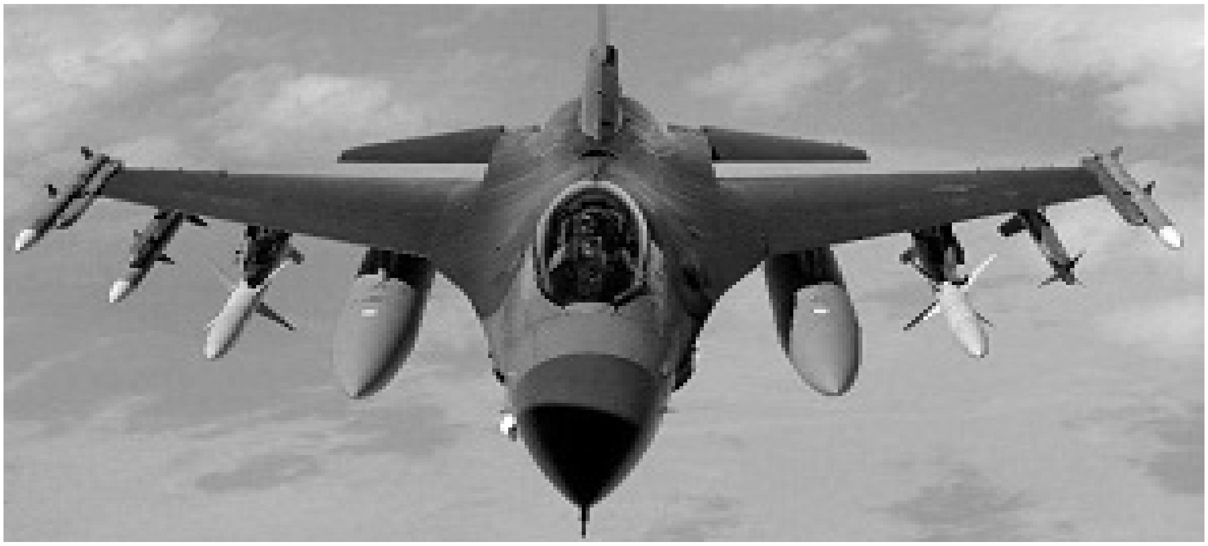

Figure10. Plain image.

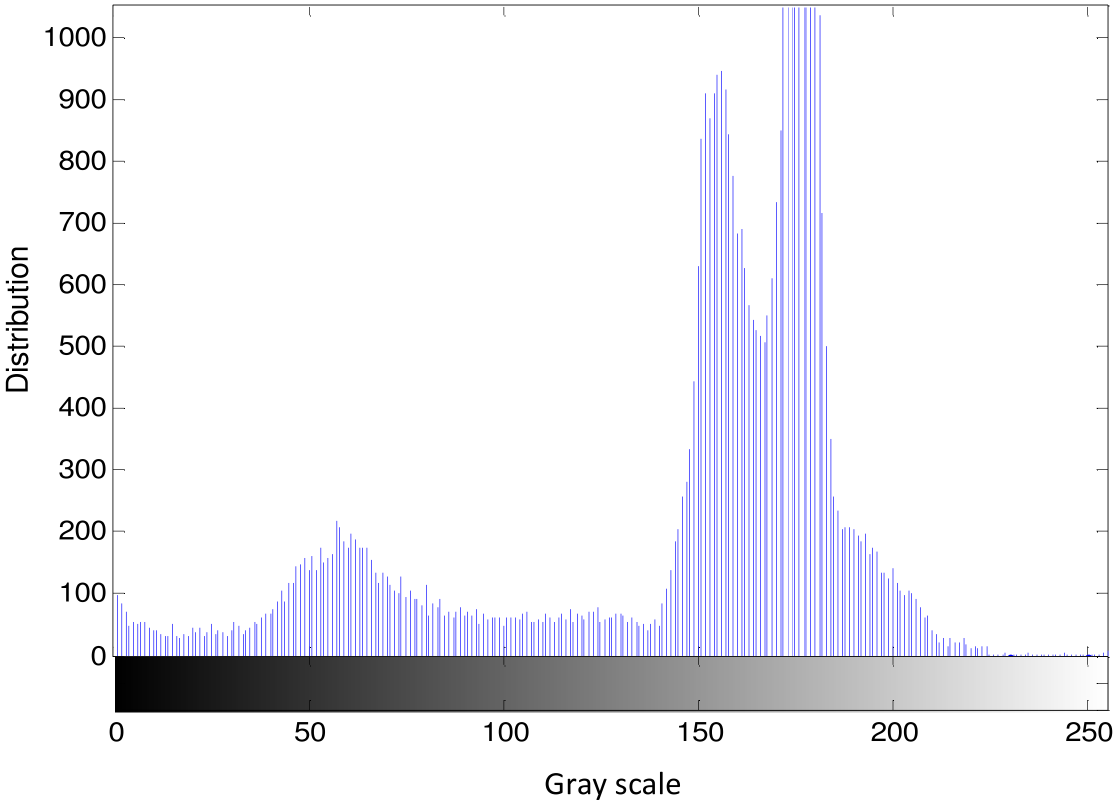

Figure 11. Histogram of plain image.

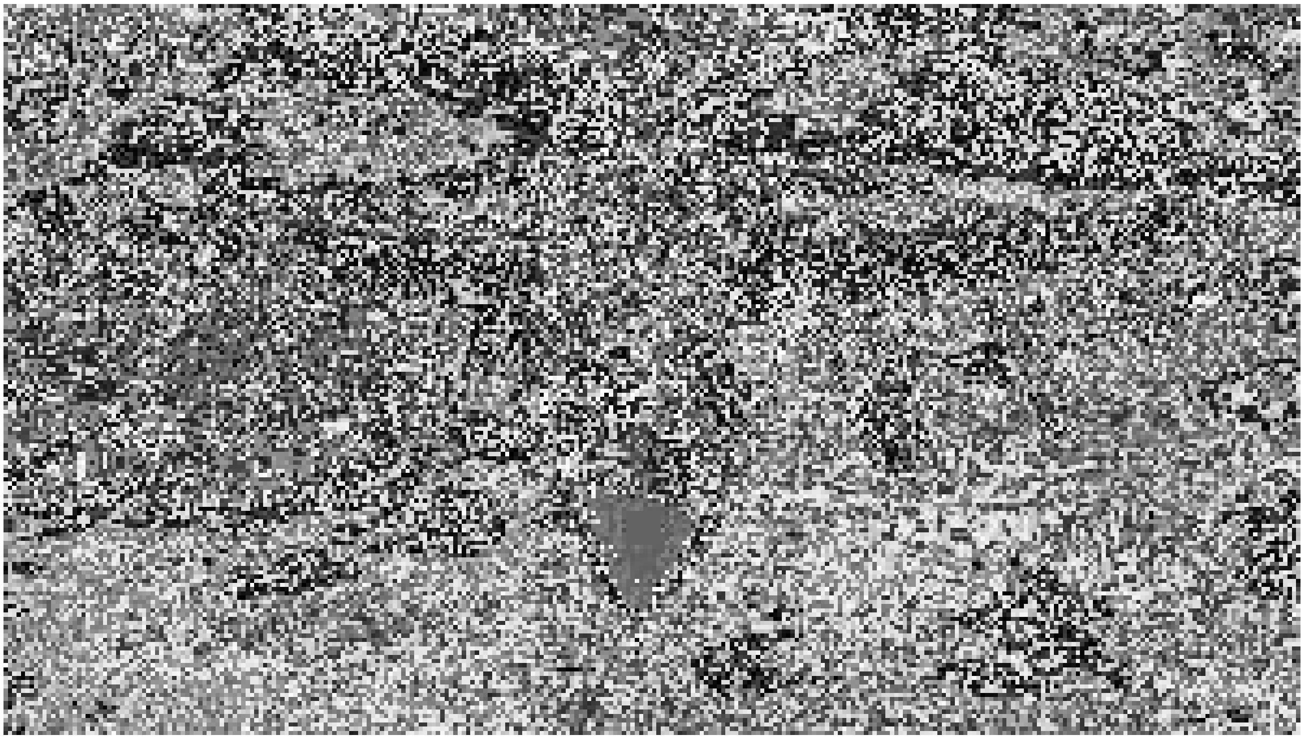

Figure 12. Cipher-image corresponding to AES S-box.

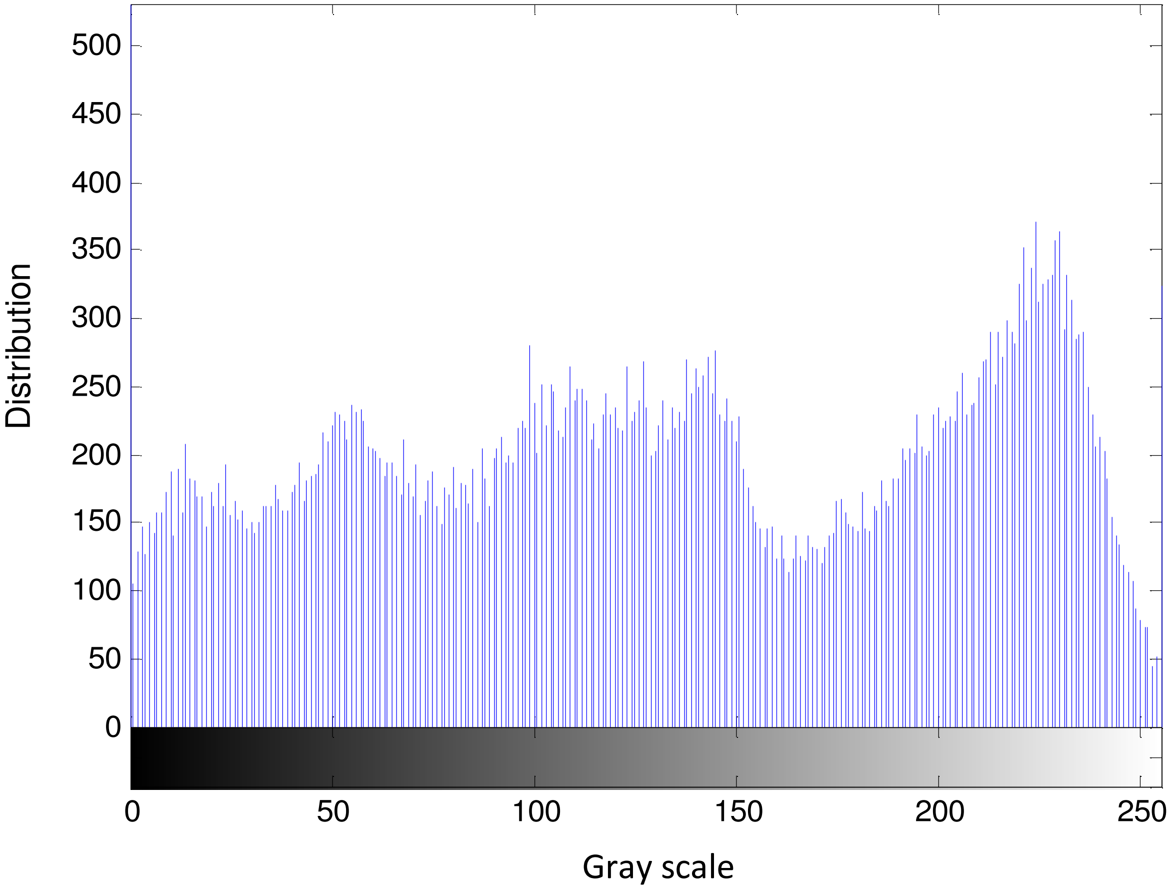

Figure 13. Histogram of cipher-image corresponding to AES S-box.

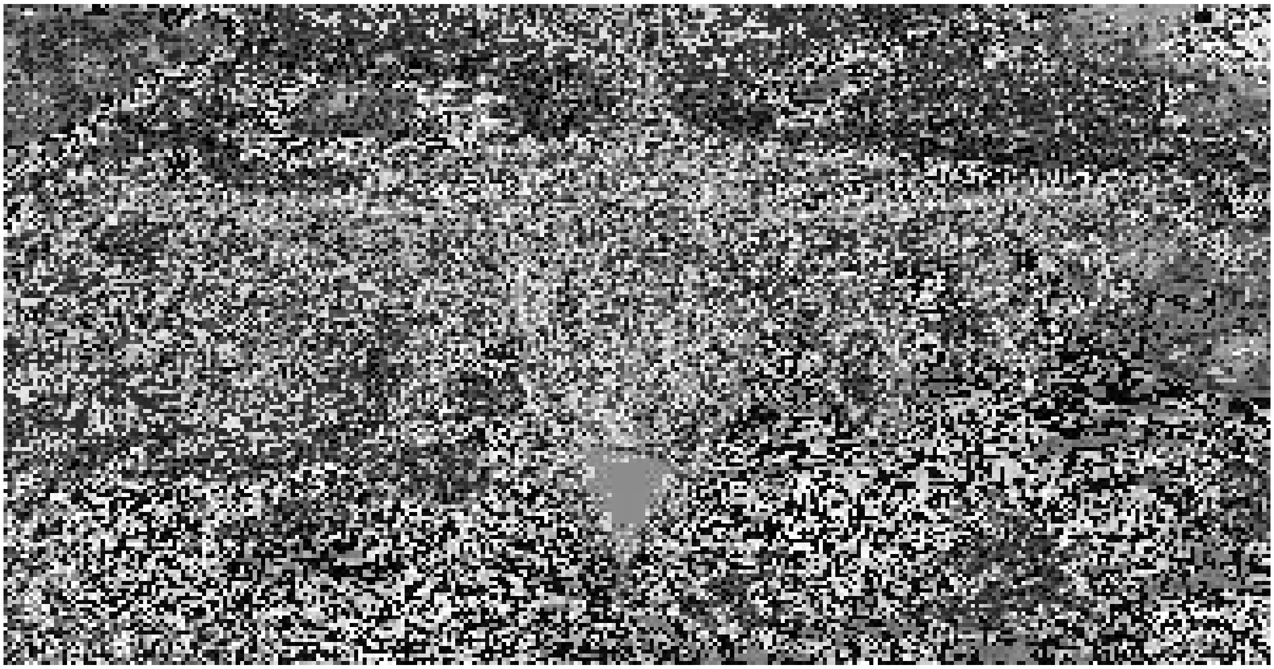

Figure 14. Cipher-image corresponding to APA S-box.

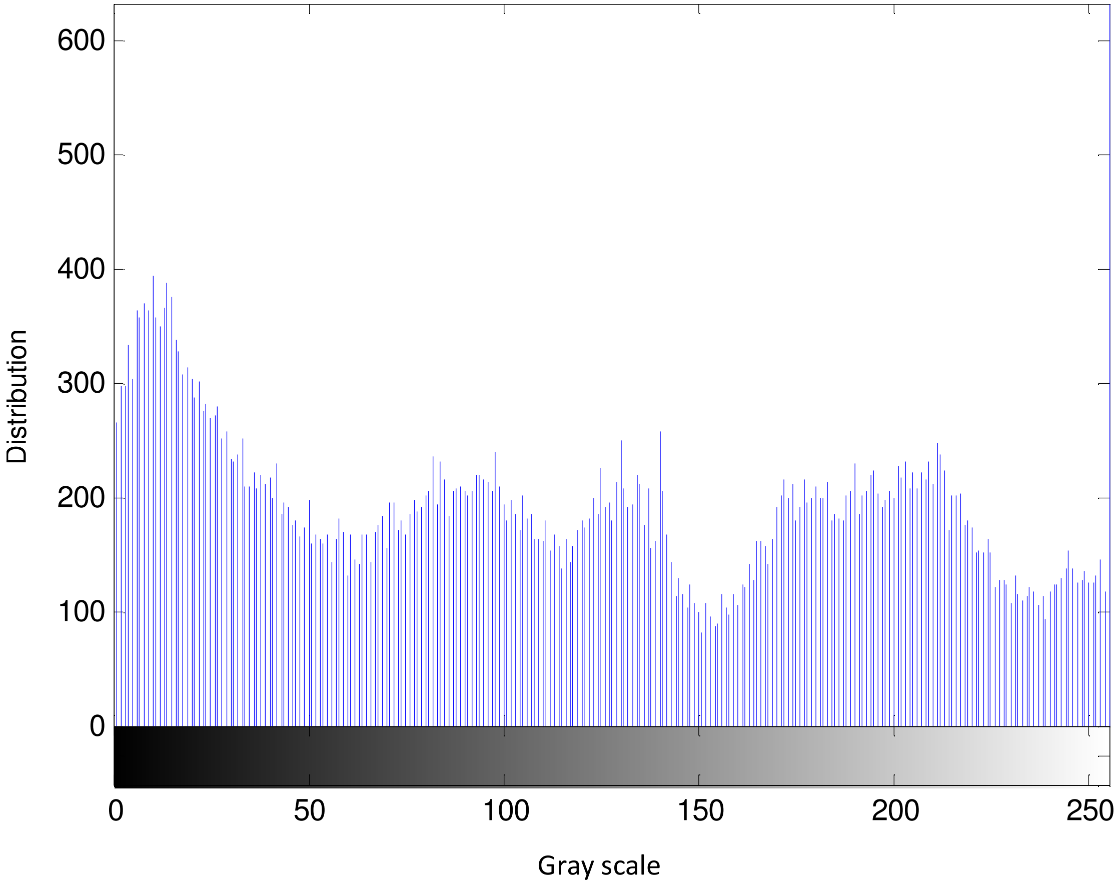

Figure 15. Histogram of cipher-image corresponding to APA S-box.

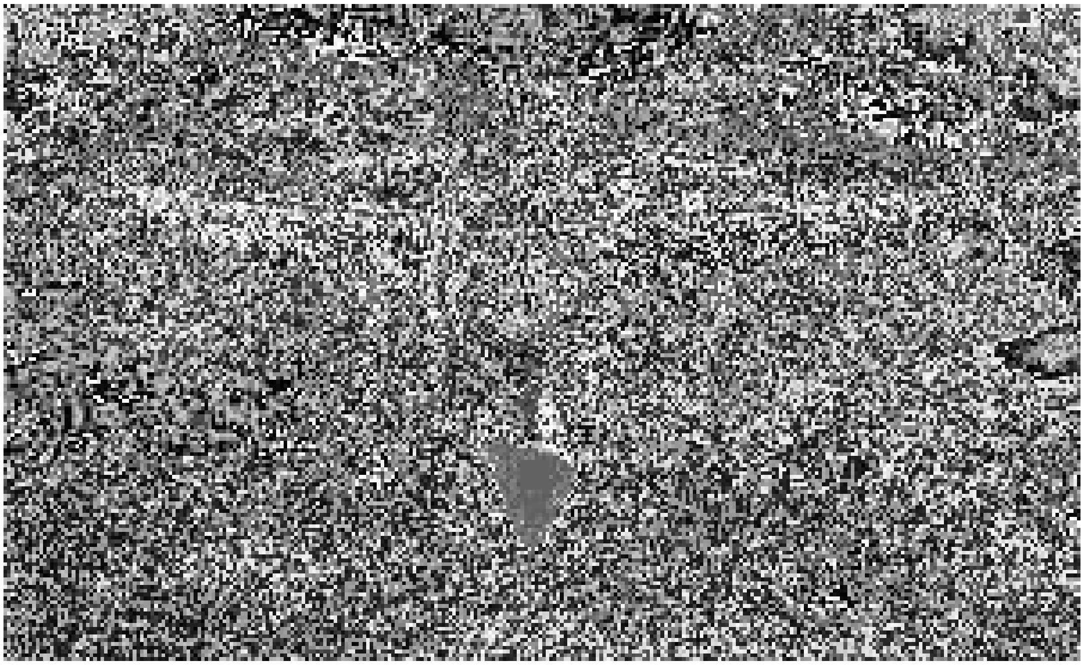

Figure 16. Cipher-image corresponding to Gray S-box.

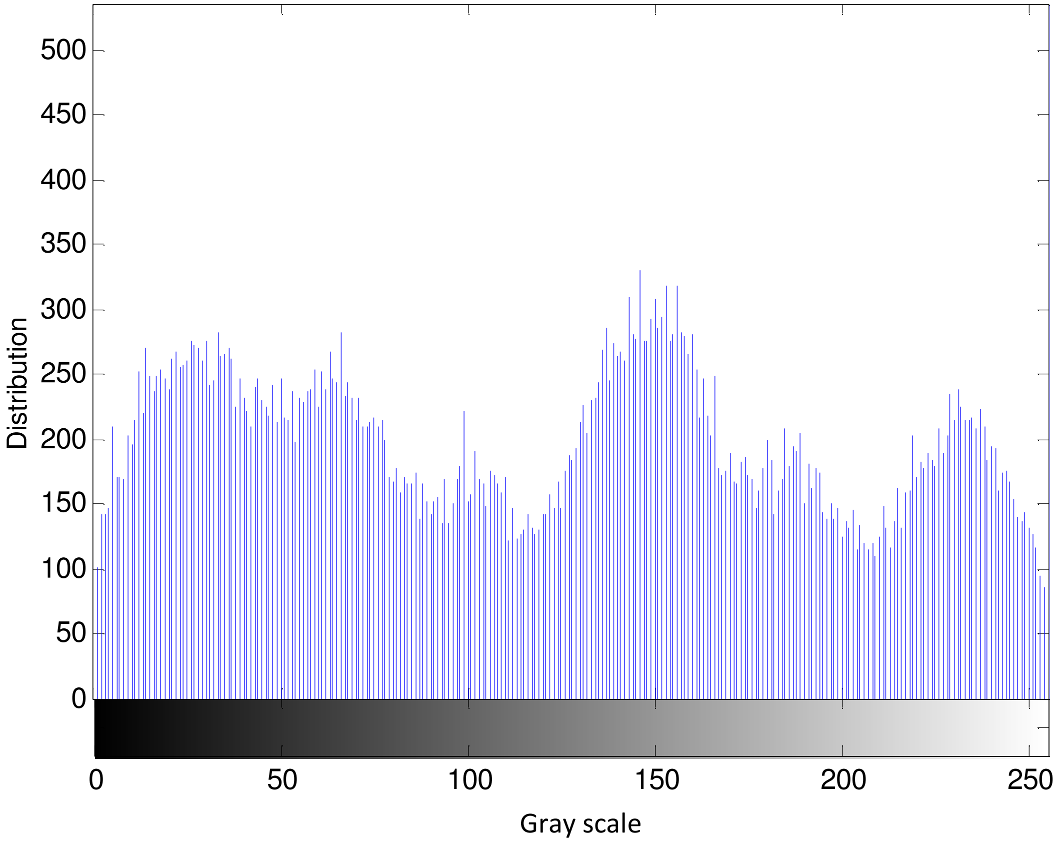

Figure 17. Histogram of cipher-image corresponding to Gray S-box.

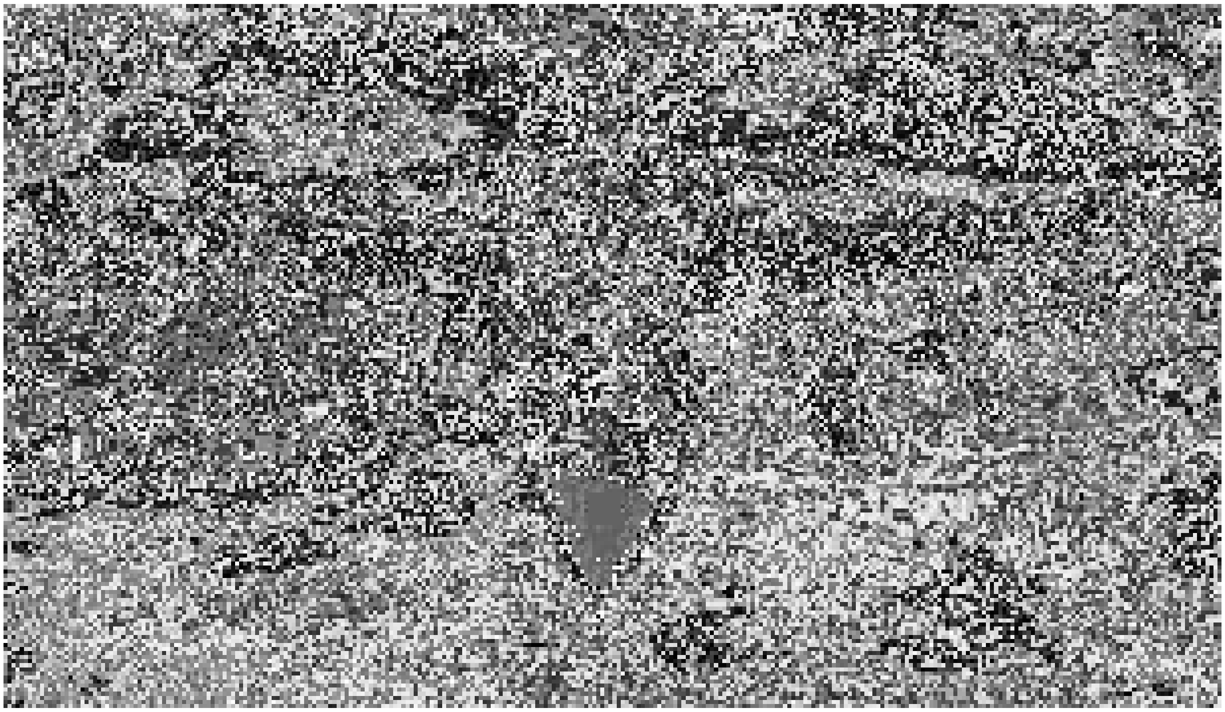

Figure 18. Cipher-image corresponding to Lui J S-box.

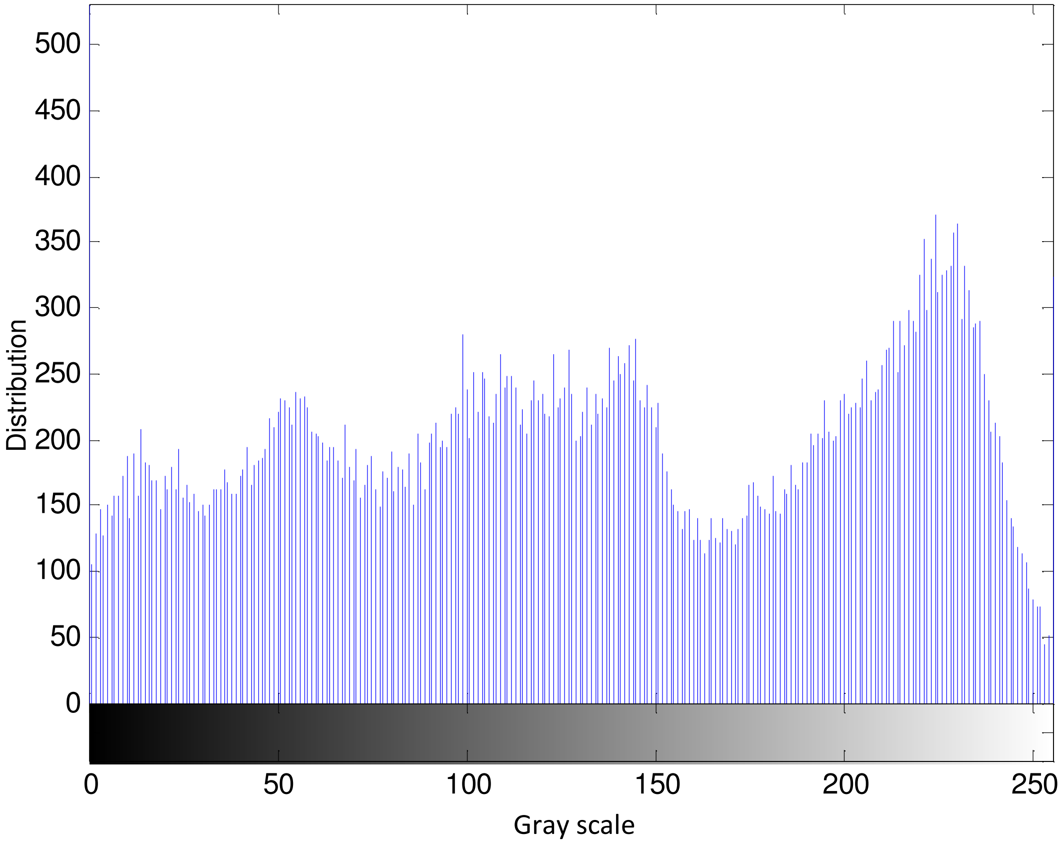

Figure 19. Histogram of cipher-image corresponding to Lui-J S-box.

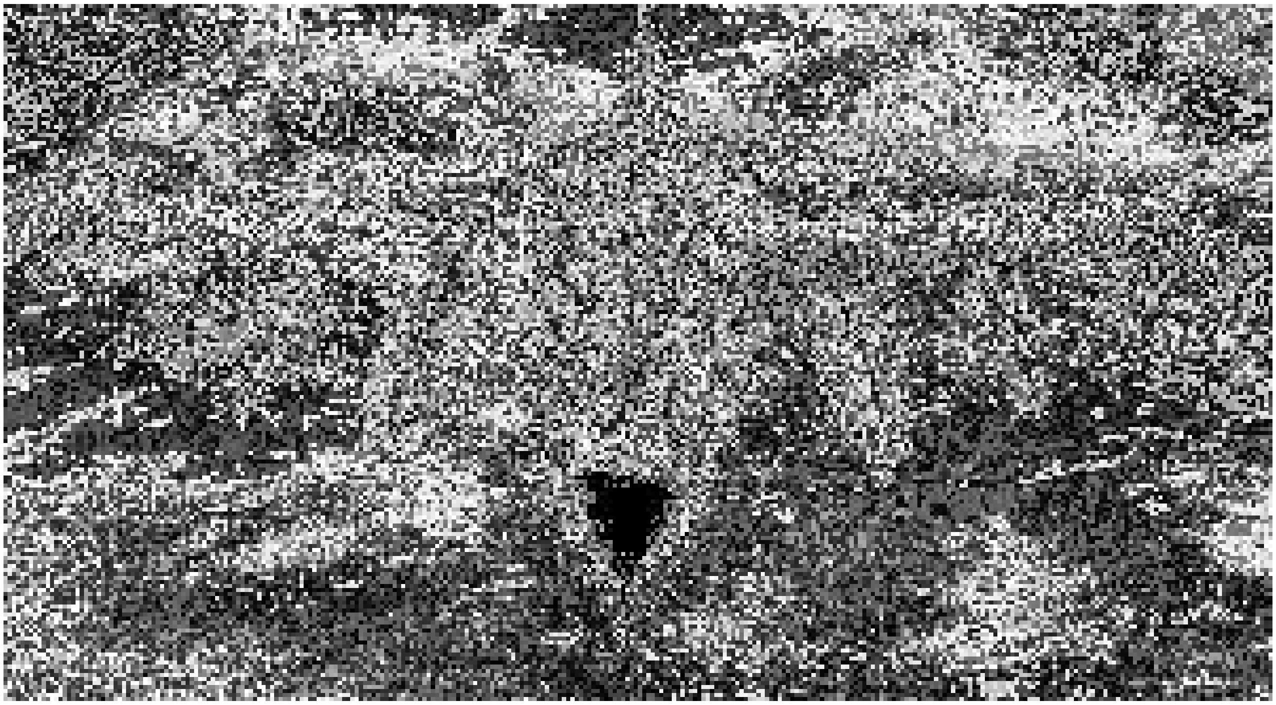

Figure 20. Cipher image corresponding to prime S-box.

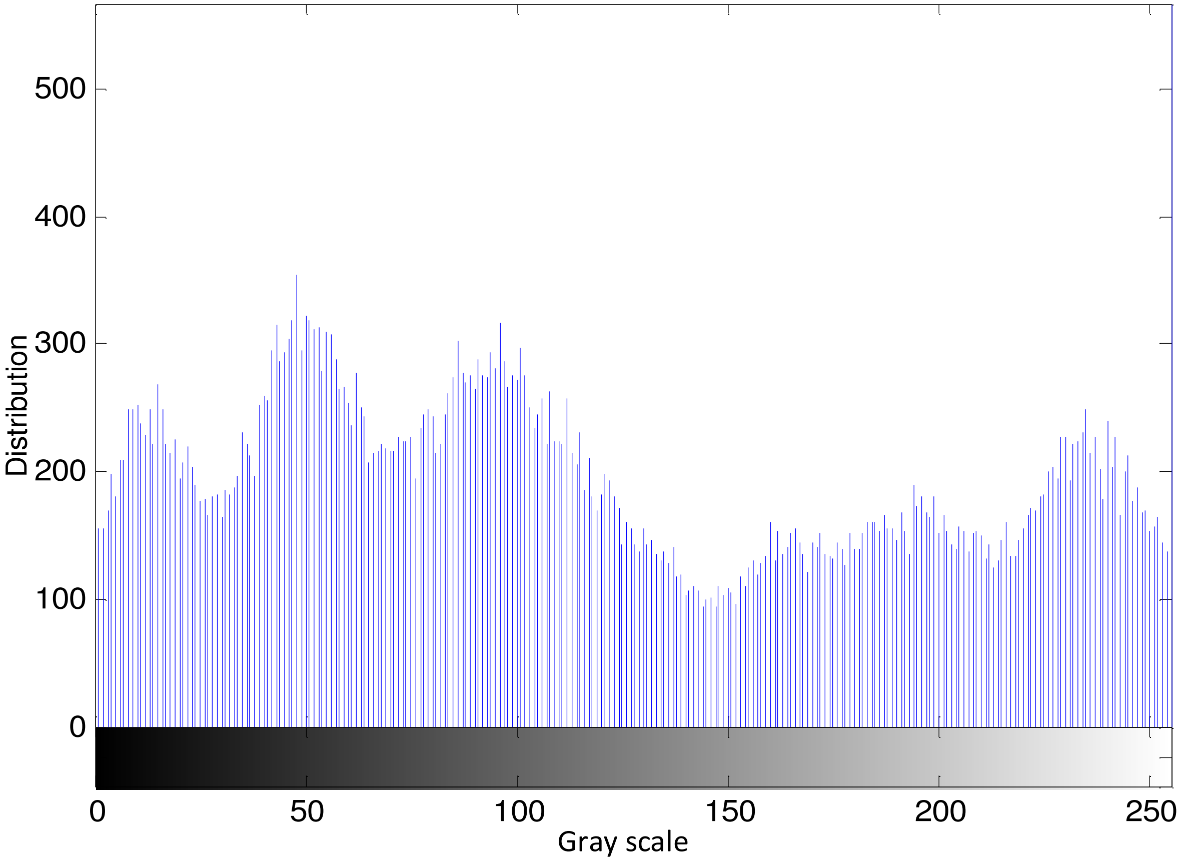

Figure 21. Histogram of cipher-image corresponding to prime S-box.

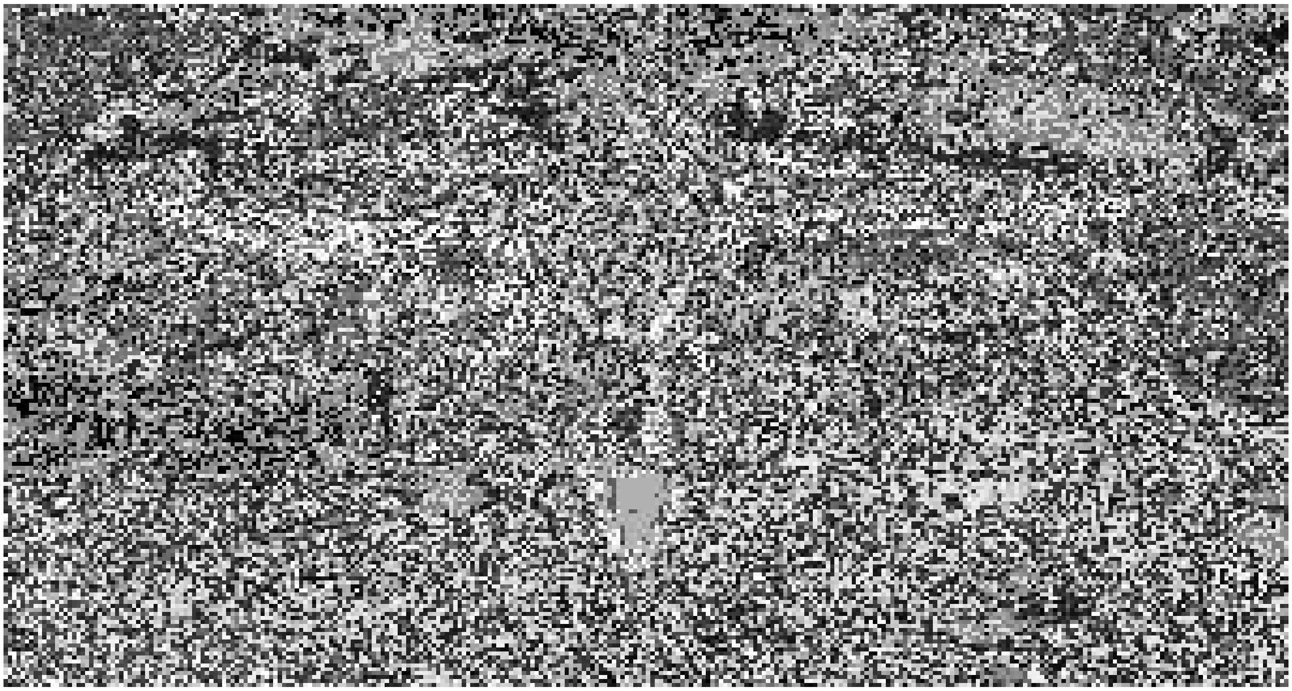

Figure 22. Cipher-image corresponding to S_8 AES S-box.

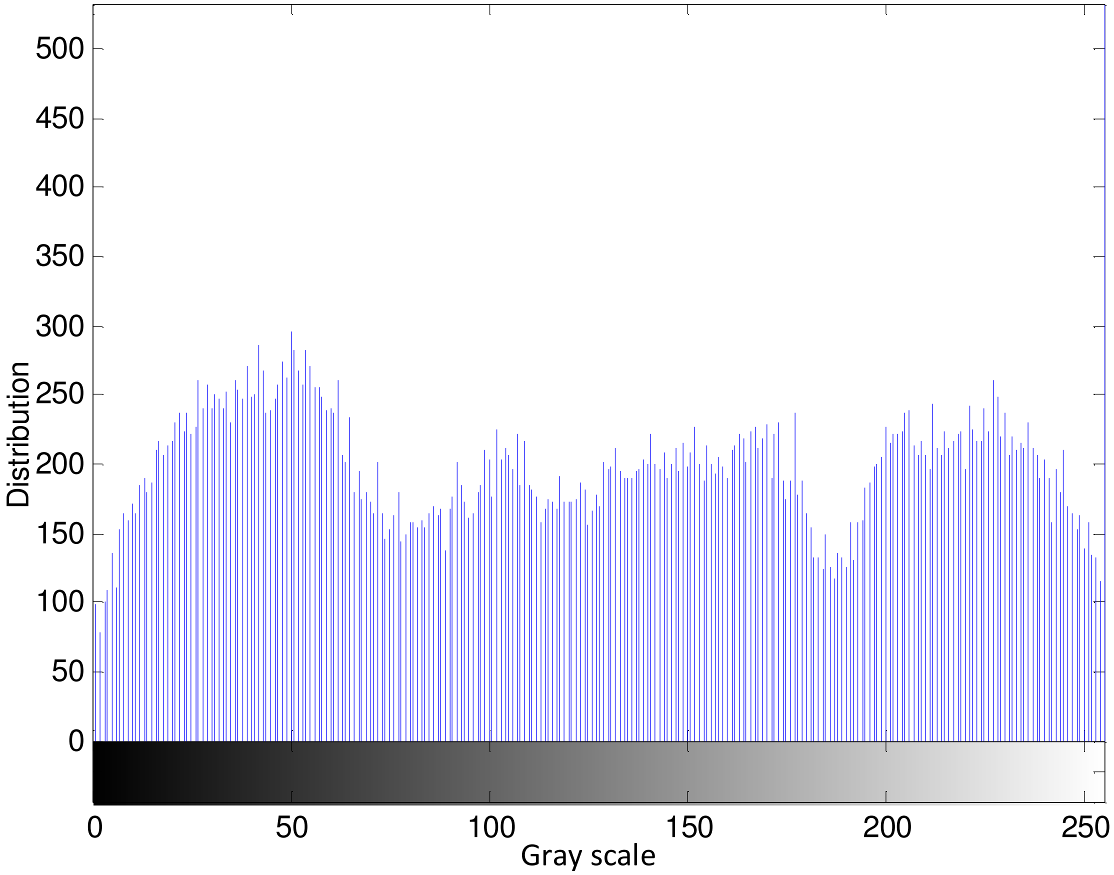

Figure 23. Histogram of cipher-image corresponding to S_8 AES S-box.

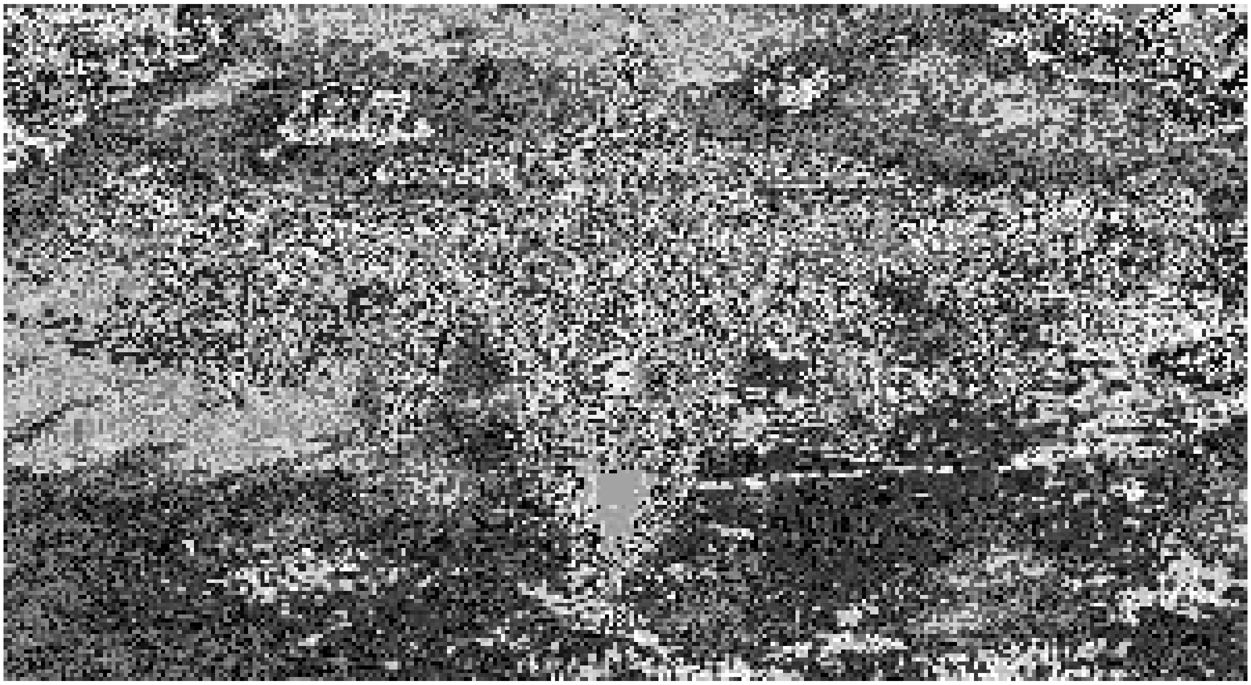

Figure 24. Cipher-image corresponding to SKIPJACK S-box.

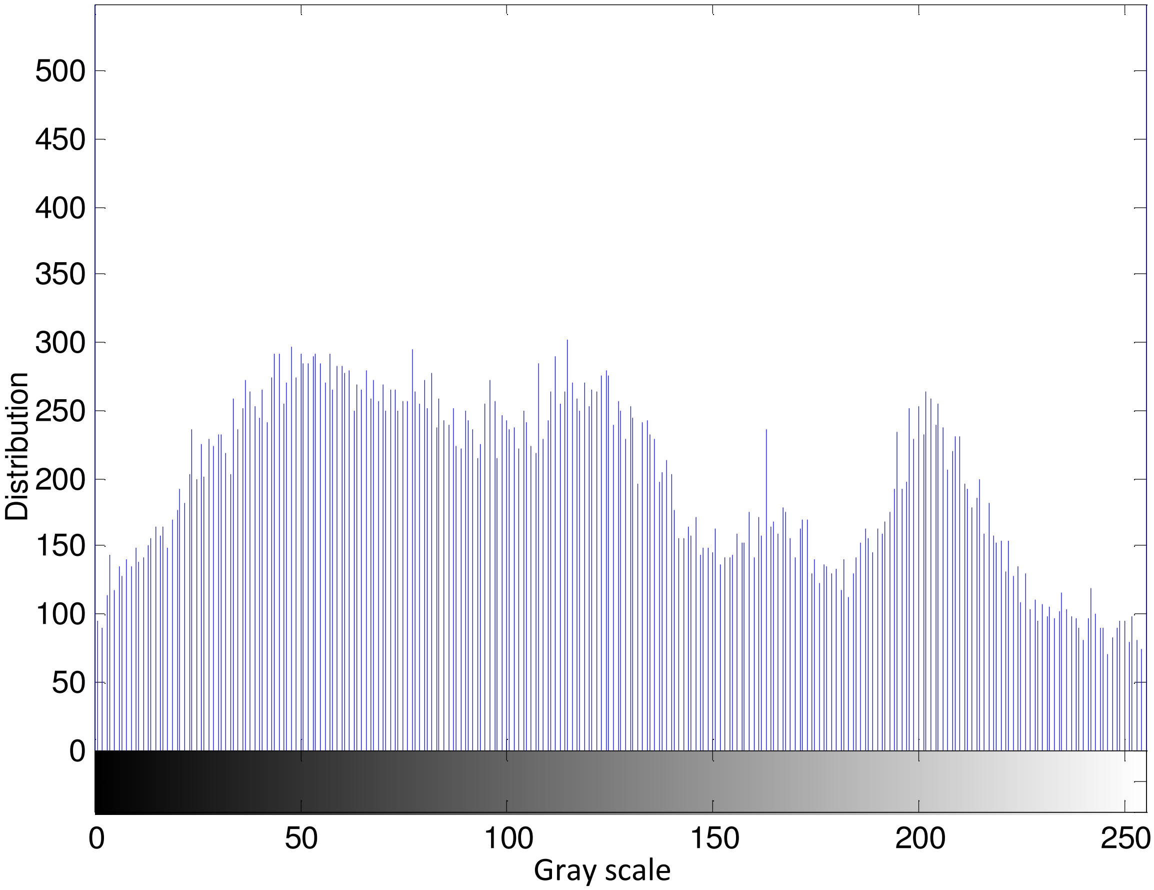

Figure 25. Histogram of cipher-image corresponding to SKIPJACK S-box.

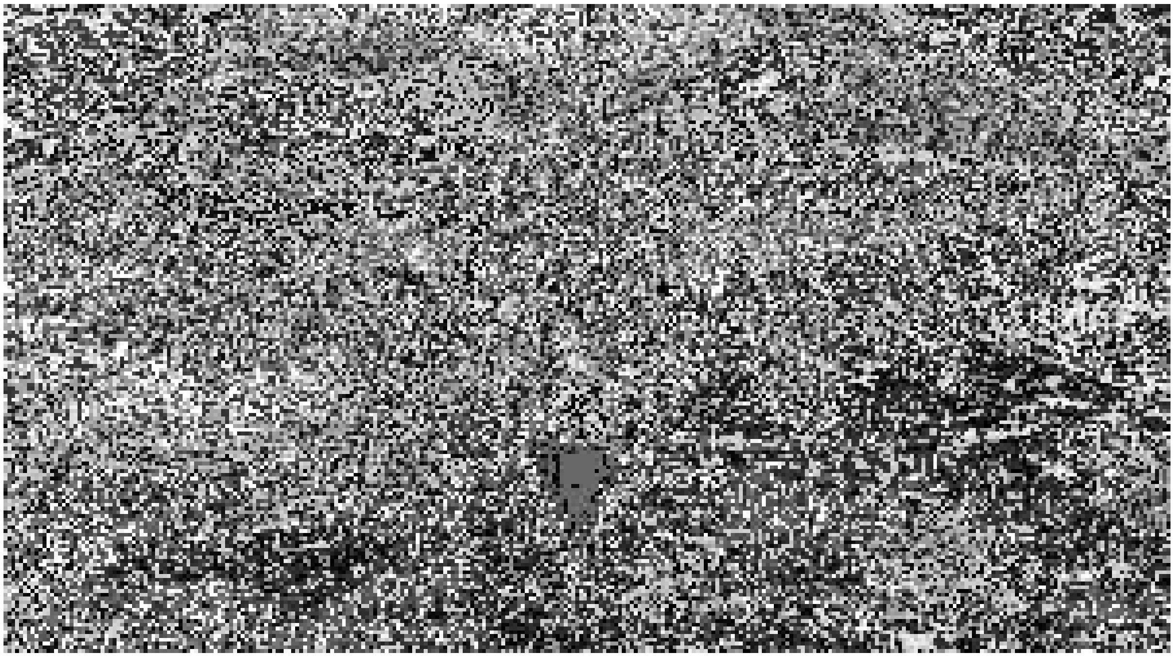

Figure 26. Cipher-image corresponding to Xyi S-box.

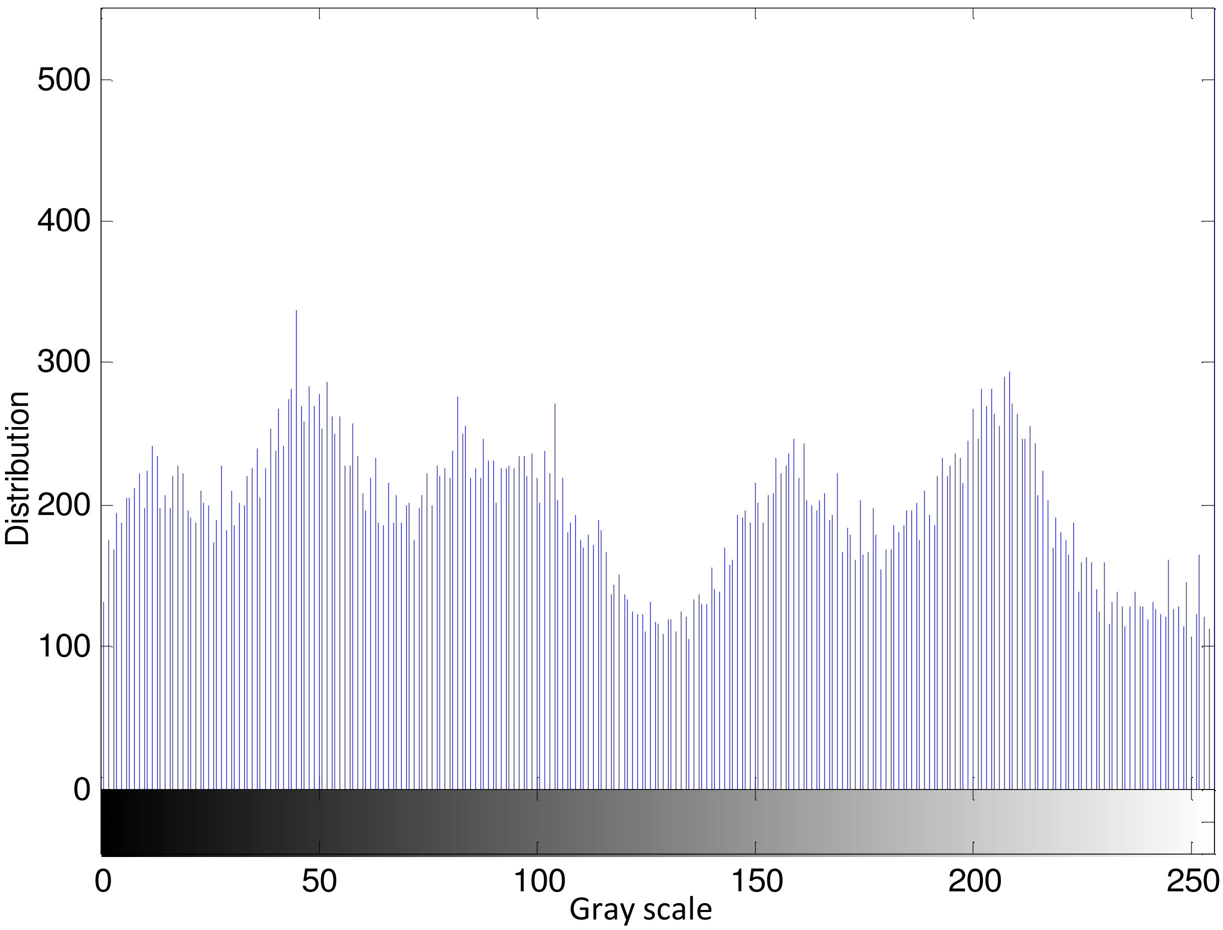

Figure 27. Histogram of cipher-image corresponding to Xyi S-box.

image and its details. The pixels of the plain image are not uniformly distributed. As soon as the image is encrypted, the randomness in the image increases and as a result it becomes difficult to visually identify the encrypted image. If we observe the histogram of the cipher images, it is evident that the trend in these encrypted pictures is very different from the plain image and is evenly distributed. A flat histogram has the maximum entropy; therefore, the strength of encryption can be seen by the trend of this graph. The performance of S_8 AES S-box is superior as compared to other S-boxes as it is evident from their respective histograms.

Various S-boxes are analyzed in this work. The performance of S_8 AES S-box is best when applied to image encryption. The mathematical analysis of the construction of S_8 S-box reveals its superior performance over other classes of S-boxes. The insight of the analytical construction is described by the algebraic structure of S_8 S-box. The construction technique of S_8 AES S-box employs the permutation of symmetric group S_8 on the algebraic structure of AES S-box. The algebraic expression of AES S-box is given as:

$$\text{S - box}_{\text{AES}} = H \circ L \circ F$$

The original S-box of AES is the combination of the power function F(x), the linear transformation L(x), and the affine transformation H(x). The algebraic expression of S_8 AES S-box is of the form:

$$S - box_{S_8\ \text{AES}} = \pi(H \circ L \circ F)$$

where F(x), L(x), and H(x) are the same as in AES S-box, but $\pi \in S_8$ (symmetric group of permutations) represents the permutation. The order of S_8 (symmetric group) is 40320, therefore one can construct 40320 boxes from the AES S-box. Consequently, the application of this permutation operation to the AES S-box increases its strength for image encryption applications.

Conclusion

Table 3 presents the algebraic and statistical properties

Table 3. Non-linearity, SAC, BIC, BIC/SAC, DP, bijective test and LP analysis.

S-box	Non-linearity	SAC	BIC	BIC/SAC	DP	Bijective	LP
AES	112	0.504	112	0.504	0.0156	Yes	0.0625
APA	112	0.500	112	0.499	0.0156	Yes	0.0625
Lui	104.8	0.499	104.17	0.500	0.0390	Yes	0.1289
Prime	99.50	0.516	101.71	0.502	0.2812	Yes	0.1328
S_8	112	0.504	112	0.504	0.0156	Yes	0.0625
Gray	112	0.499	112	0.504	0.0156	Yes	0.0625
Xyi	105	0.502	103.78	0.503	0.0468	Yes	0.1562
S.J	105.5	0.503	104.14	0.499	0.0468	Yes	0.1093

of eight well known S-boxes. These properties are non linearity, strict avalanche criterion (SAC), bit independence criterion (BIC), differential approximation probability (DP), linear approximation probability (LP), etc. (Tran et al., 2008). It is observed that several properties of these boxes are similar. These properties enable the user to determine the strength of an S-box. Although the results of the analyses in Table 3 provide a method to choose an optimal S-box, which is robust against algebraic and statistical attacks, it lacks the ability for the user to clearly identify the best S-box for image encryption application. For example, AES S-box and S_8 AES S-box have identical properties and parameters, as seen in Table 3. The analyses discussed in this paper for image encryption applications in conjunction with the proposed novel criteria to choose the best S-box, further facilitates the user in determining the optimal S-box.

FUTURE DIRECTIONS

In order to further strengthen the proposed criterion, additional analyses can be incorporated in the existing list of methodologies. For example, mean absolute error (MAE), the number of pixel change rate (NPCR), and unified average changing intensity (UACI) analyses can be used in combination with MAD analysis. While the proposed criterion in this work pertains to image encryption applications, this criterion and analyses can be adapted for other important encryption applications such as, voice, video, data, and watermarking. The exploration of the proposed criterion for different encryption applications is the topic of interest for future work.

REFERENCES

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

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

Alam GM, Mat Kiah ML, Zaidan BB, Zaidan AA, Alanazi HO (2010). 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): 3254-3260.

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

Chen SY, Lin WC, Chen CT (1991). Split and merge image segmentation based on localized feature analysis and statistical tests. Graph Model. IM proc., 53(5): 457-475.

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

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

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

Hussain I, Shah T, Mehmood H (2010). A New Algorithm to Construct Secure Keys for AES. Int. J. Cont. Math. Sci., 5(26): 1263-1270.

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

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

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

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

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

Tran MT, Bui DK, Doung AD (2008). Gray S-box for Advanced Encryption Standard. Int. Conf. Comp. Intel. Secur., 253-256.

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