

Analysis of S-box in Image Encryption Using Root Mean Square Error Method

Iqtadar Hussain^a, Tariq Shah^a, Muhammad Asif Gondal^b, and Hasan Mahmood^c

^a Department of Mathematics, Quaid-i-Azam University, Islamabad, Pakistan

^b Department of Sciences and Humanities, National University of Computer and Emerging Sciences, Islamabad, Pakistan

^c Department of Electronics, Quaid-i-Azam University, Islamabad, Pakistan

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

Z. Naturforsch. **67a**, 327–332 (2012) / DOI: 10.5560/ZNA.2012-0023

Received September 22, 2011 / revised November 16, 2011

The use of substitution boxes (S-boxes) in encryption applications has proven to be an effective nonlinear component in creating confusion and randomness. The S-box is evolving and many variants appear in literature, which include advanced encryption standard (AES) S-box, affine power affine (APA) S-box, Skipjack S-box, Gray S-box, Lui J S-box, residue prime number S-box, Xyi S-box, and S₈ S-box. These S-boxes have algebraic and statistical properties which distinguish them from each other in terms of encryption strength. In some circumstances, the parameters from algebraic and statistical analysis yield results which do not provide clear evidence in distinguishing an S-box for an application to a particular set of data. In image encryption applications, the use of S-boxes needs special care because the visual analysis and perception of a viewer can sometimes identify artifacts embedded in the image. In addition to existing algebraic and statistical analysis already used for image encryption applications, we propose an application of root mean square error technique, which further elaborates the results and enables the analyst to vividly distinguish between the performances of various S-boxes. While the use of the root mean square error analysis in statistics has proven to be effective in determining the difference in original data and the processed data, its use in image encryption has shown promising results in estimating the strength of the encryption method. In this paper, we show the application of the root mean square error analysis to S-box image encryption. The parameters from this analysis are used in determining the strength of S-boxes.

Key words: Root Mean Square Error; S-Box Encryption; Image Encryption.

1. Introduction

Block ciphers are an important branch of cryptography, and the substitution box (S-box) is the key component capable of creating confusion in the data [1]. That is why many researcher focus on improving the quality of the S-box. Several methods are presented in literature to analyze the statistical and algebraic strength and weakness of S-boxes; such as nonlinearity, strict avalanche criterion (SAC), bit independence criterion (BIC), linear approximation probability (LP), differential approximation probability (DP) [2], etc. In this paper, we analyze S-boxes in the area of image encryption with the help of a metrology known as root mean square error (RMSE).

The application of root mean square is widely seen in all areas of applied sciences. This method is used in a number of applications such as meteorology, bioin-

formatics, chem-informatics, economics, experimental psychology, geographic information systems (GIS), hydrogeology, imaging science, computational neuroscience, etc. In the area of meteorology, the root mean square error is typically used to predict the behaviour of the atmosphere. The use of this technique is also seen in bioinformatics applications. For example, the average distance between atoms of superimposed proteins is studied. The area of chem-informatics has applications of root mean square analysis. The distance between a crystal structure conformation and docking parameters are evaluated with the help of this technique. The application of this method is also useful in social sciences. In the field of economics, the root mean square is used to determine whether an economic model fits the economic indicators. The study and analysis of the models of perception which explains the abilities of the human senses uses the root mean analysis. In GIS and

hydrogeology, the root mean square analysis is used to assess the accuracy of spatial analysis and remote sensing applications and is also used to evaluate the calibration of groundwater models. In the area of computational neuroscience, the root mean square method is used to assess how well a system learns a given model. The application of the root mean square method is also seen in image processing applications. In this area, this analysis is used to determine the peak signal-to-noise ratio, which is a measure used to assess how well a method to reconstruct an image performs relative to the original image. The root mean square analysis is an important method which reveals useful information in applications where we compare two sets of data and need to evaluate the error characteristics. The application of the root mean square algorithm is seldom seen in image encryption applications where we analyze the strength of encryption and study the confusion capability of these systems. In this work, we use the root mean square method to determine the strength of the S-box used in image encryption applications. In the proposed image encryption application, the S-box is used as a nonlinear component, which has the confusion capability.

2. Problem Statement

The process of encryption creates confusion and randomness in the original data. In the case of image encryption, the objective is similar but additional param-

eters are taken into account. The encrypted image needs to be robust against various attacks in addition to the visual inspection by the observer. The effectiveness of the S-box, which also reflects the randomness in the data, needs to be tested in order to determine the suitability to

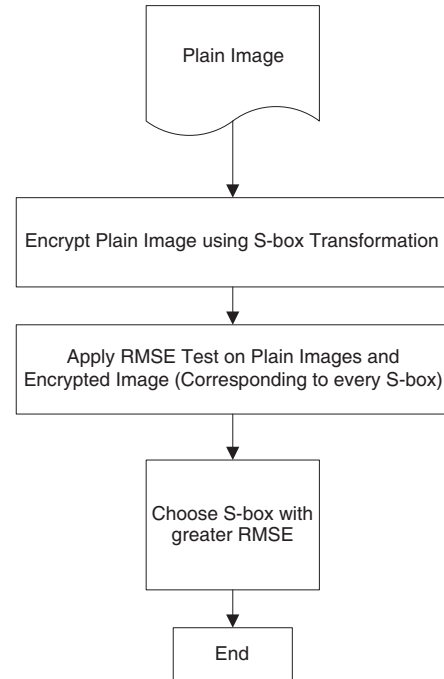


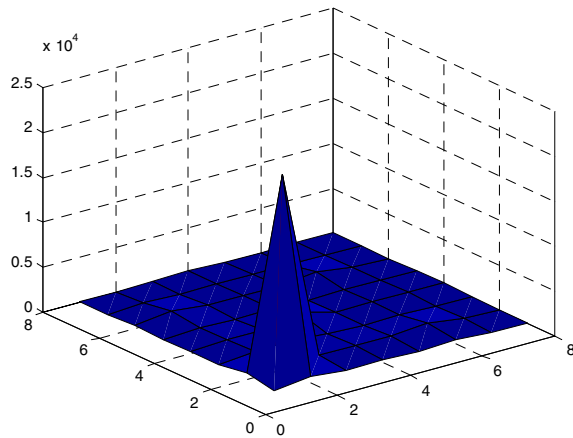
Fig. 1. Flow chart of the root mean square analysis for various S-boxes.

S-boxes	RMS-1 (Image 1)	RMS-2 (Image 2)	RMS-3 (Image 3)	RMS-4 (Image 4)	Average	Standard deviation
Gray	12.36	11.14	11.96	14.6	12.515	1.479854
AES	11.81	11.42	12.15	14.64	12.505	1.454247
Lui J	10.81	11.42	12.15	14.64	12.505	1.681715
APA	12.25	11.03	11.93	14.51	12.43	1.47973
Skipjack	12.51	10.62	11.88	14.61	12.405	1.666823
Prime	12.3	10.6	11.78	14.64	12.33	1.69631
Xyi	11.54	10.46	11.91	14.53	12.11	1.726634
S ₈ AES	11.56	10.69	11.35	14.48	12.02	1.681368

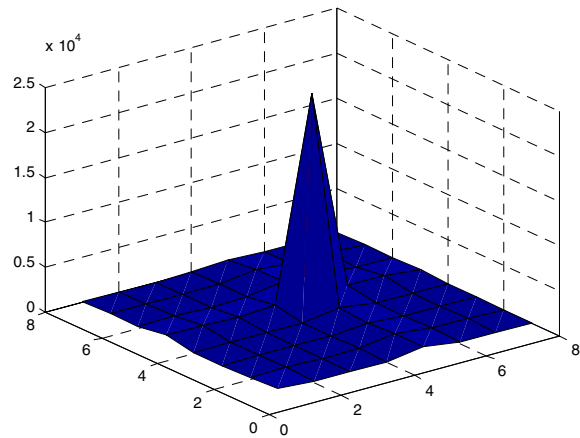
Table 1. Application of the root mean square error method to various S-boxes.

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 J	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 AES	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
Skipjack	105.5	0.503	104.14	0.499	0.0468	Yes	0.1093

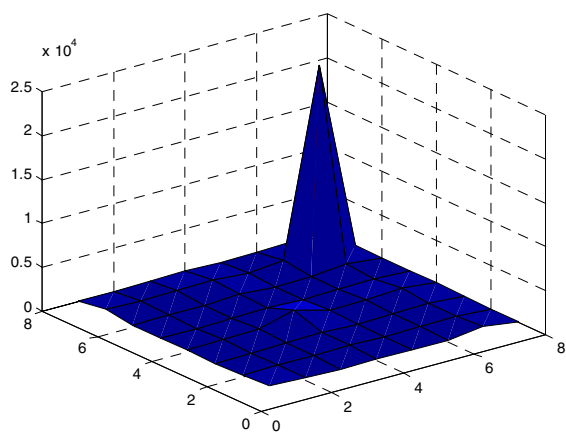
Table 2. Application of various statistical analyses to S-boxes.



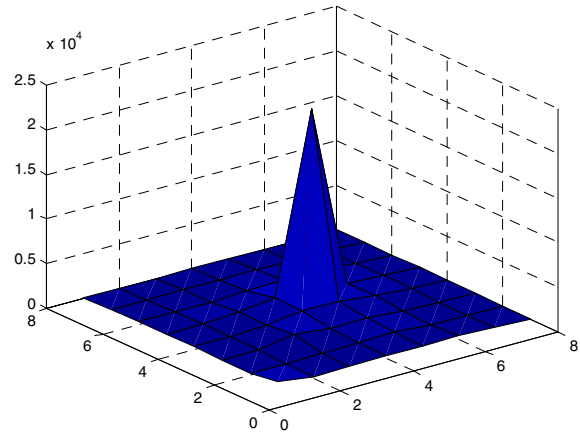
Plot of GLCM of Image-1



Plot of GLCM of Image-2



Plot of GLCM of Image-3



Plot of GLCM of Image-4

Fig. 2 (colour online). Plot of the grey scale co-occurrence matrix for the sample plain images.

a particular application. Various testing methodologies have been proposed [3], which show the effectiveness of S-boxes (Table 2). In Table 1, we present the root mean square properties of those boxes used in this work. Here we propose the application of the root mean square error method to image encryption application and determine the difference in original and encrypted images introduced by S-box transformation.

The process of S-box image encryption is shown with the help of the flow chart in Figure 1. Various S-boxes used in this analysis are AES [4], APA [5], Gray, Lui J [6], residue prime [7], S₈ AES [8], Skipjack [9], and Xyi [10] S-boxes. The image is encrypted step by step with the application of these S-boxes, and the re-

sultant encrypted data is compared with the original image and a root mean square error is calculated. At this stage, the resulting root mean square error for all the S-boxes used in the encryption is analyzed and the S-box with the maximum error is chosen for the image encryption application.

2.1. Root Mean Square Error

The root mean square error (RMSE) is commonly used to evaluate the differences between values predicted by a model or an estimator and the values actually observed from the data being modelled or estimated. The RMSE is a good measure of precision,

whereas in this paper this analysis is used to measure the difference between an image and its encrypted version. In common applications of RMSE, the algorithms generally use the results and try to minimize the error. In the case of image encryption, greater error depicts better encryption. We call the individual differences between two images as residuals, and the RMSE serves to aggregate them into a single measure. Mathematically we can represent RMSE as

$$\text{RMSE} = \left[n^{-1} \sum_{i=1}^n |e_i|^2 \right]^{\frac{1}{2}},$$

where e_i is the difference between the intensity of the pixel of the plain image and the corresponding pixel of the encrypted image. n is the number of pixels in the image being encrypted. The stated rationale for squaring each e_i is usually ‘to remove the sign’ so that the magnitudes of the errors influence the average error measure.

2.2. S-Box Transformation and Image Encryption

In this section, 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. The graph of the grey scale co-occurrence matrix (the grey-level co-occurrence matrix (GLCM)) shows the statistics of combinations of pixel brightness values or grey levels in tabular form) of four plain images is shown in Figure 2 and is used to test the encryption strength of an S-box. The S-box transformation is only performed once on the sample images in order to statistically and visually analyze 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 a single S-box transformation.

The encryption process produces distortions in the image, and the type of these distortions determine the strength of the algorithm. Therefore, it is important to study the statistical characteristics and properties of S-box transformations. The process of encryption (S-box transformation) is similar to byte sub step of AES.

2.3. Effect of Different S-Box Transformation on Plain Image

In this section, we perform an experiment to study the effect of S-box transformation on the image. We have

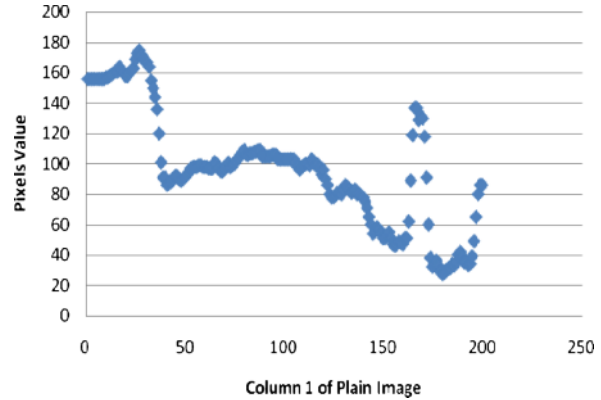


Fig. 3 (colour online). Row-wise pixel intensity of a randomly chosen column from the plain image.

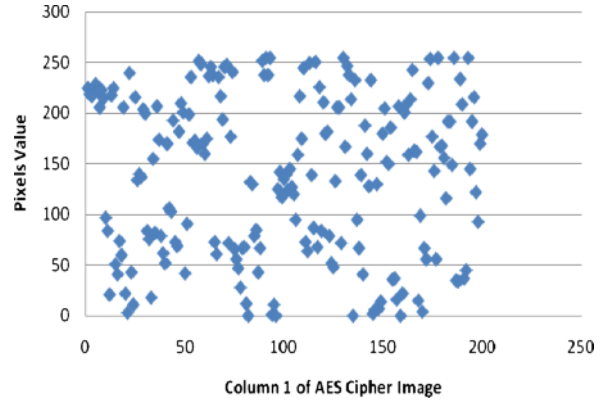


Fig. 4 (colour online). Row-wise pixel intensity of a randomly chosen column of the AES encrypted image.

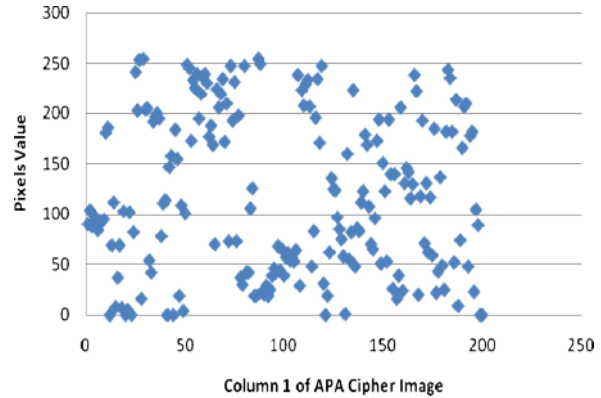


Fig. 5 (colour online). Row-wise pixel intensity of a randomly chosen column of the APA S-box encrypted image.

chosen the standard image of ‘Lena’ as plain image and the pixel values corresponding to the Lena image are shown in Figure 3. One can observe clearly that the

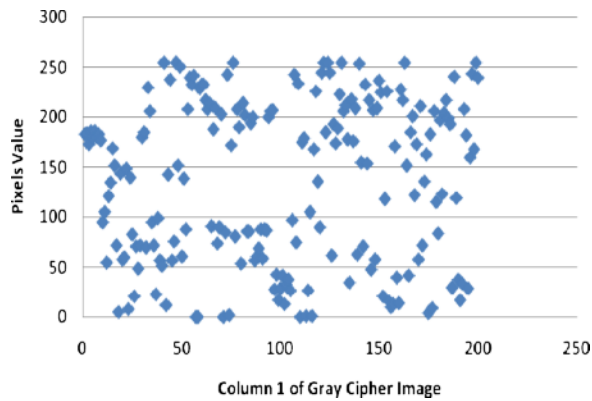


Fig. 6 (colour online). Row-wise pixel intensity of a randomly chosen column of the Gray S-box encrypted image.

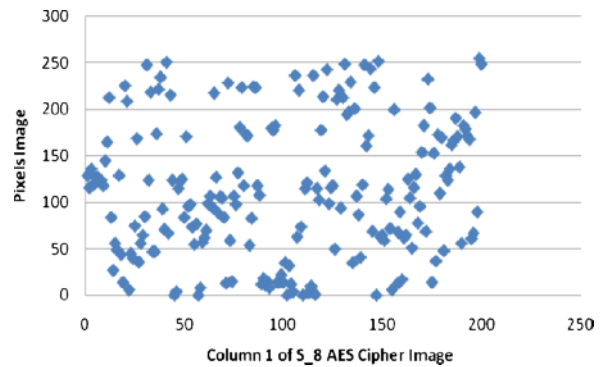


Fig. 9 (colour online). Row-wise pixel intensity of a randomly chosen column of the S₈ AES S-box encrypted image.

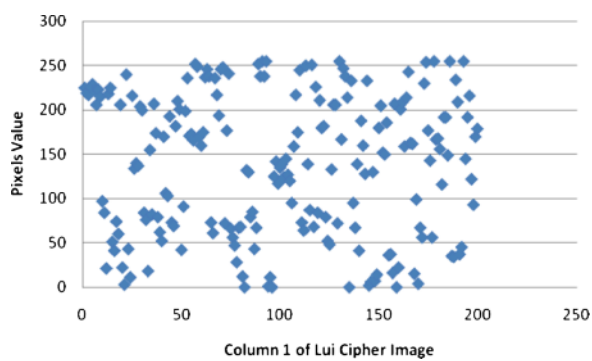


Fig. 7 (colour online). Row-wise pixel intensity of a randomly chosen column of the Lui J S-box encrypted image.

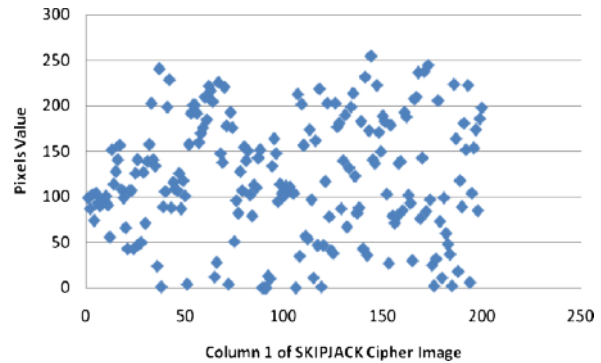


Fig. 10 (colour online). Row-wise pixel intensity of a randomly chosen column of the Skipjack S-box encrypted image.

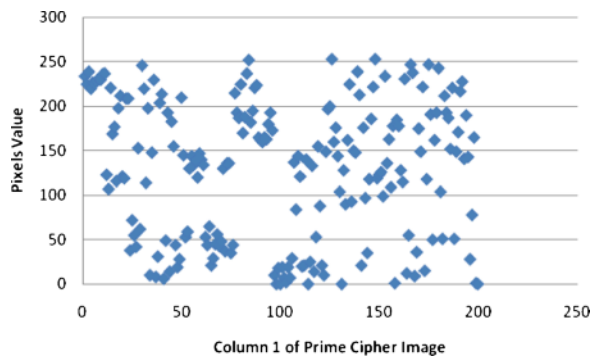


Fig. 8 (colour online). Row-wise pixel intensity of a randomly chosen column of the residue prime S-box encrypted image.

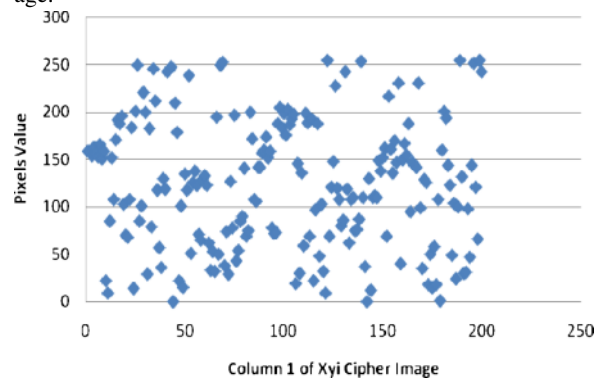


Fig. 11 (colour online). Row-wise pixel intensity of a randomly chosen column of the Xyi S-box encrypted image.

pixel values of the plain image follow some kind of sequence, but in cipher images pixels are scattered in the entire xy -plane corresponding to every S-box transformation. Figures 4 to 11 present the disorder produced by the S-box transformations on pixels of the plain image.

From this experiment, we only understand the effect of S-box transformation as we are not aware of which S-box is more appropriate to use in image encryption application. So, we use the statistical tool of RMSE to distinguish which S-box is comparatively better.

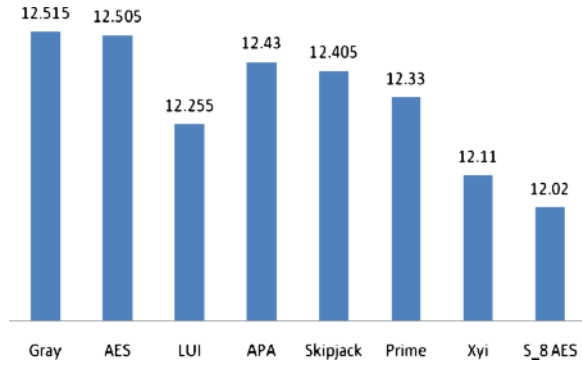


Fig. 12 (colour online). Graphical representation of RMSE for various S-boxes corresponding to different images.

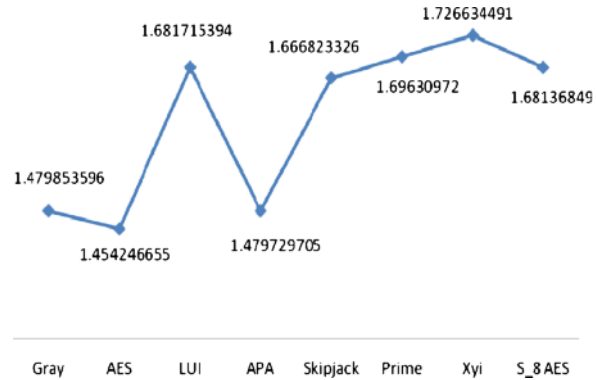


Fig. 13 (colour online). Standard deviation of RMSE for various S-boxes corresponding to different images.

3. Results and Discussion

3.1. Simulation Model

In this paper, we study the encryption strength of various S-boxes. The presented analysis can be used for any type of S-box; in this study we use the following S-boxes: AES, APA, Gray, Lui J, residue prime, S₈ AES, Skipjack, and Xyi. Four different images with distinctive properties are used in the analysis. The plot of the grey scale co-occurrence matrix for the sample plain images is shown in Figure 2. It is evident from these graphs that the peak grey levels are seen at different locations with respect to each other. In the experimental setup, multiple images are encrypted by using various S-boxes. The application of the root mean square analysis is shown in Figure 12. It is observed that the Gray S-box shows a maximum error in between the original image and encrypted image. The AES S-box has very close performance results as compared with the Gray S-box. The analysis of the root mean square method is graphically depicted in Figure 13.

3.2. Conclusions and Future Directions

In this paper, we discuss the application of the root mean square error method in evaluating the strength of an S-box in image encryption application. The results of the analysis are used to select the appropriate S-box to encrypt the image. We conclude that the Gray S-box is comparatively better for the encryption of images. In order to further strengthen the proposed criterion, an additional analyses can be incorporated in the existing list of methodologies. For example, the mean absolute error (MAE), the number of pixel change rate (NPCR), and the unified average changing intensity (UACI) analyses can be used in combination with a mean of absolute deviation (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.

- [1] M. Tran, T. Bui, and D. K. Doung, *Int. Conf. Comp. Intel. Secur.* 253 (2008).
- [2] S. Murphy, J. B. Rabshaw, *LNCS* **2442**, 1 (2002).
- [3] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, *Int. J. Phys. Sci.* **6**, 4110 (2011).
- [4] J. Daemen and V. Rijmen, Available: <http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf>, (1999).
- [5] L. Cui and Y. Cao, *Int. J. Innov. Comput. I.* **3**, 45 (2007).
- [6] J. Liu, B. Wai, X. Cheng, and X. Wang, *Int. Conf. Inf. Network. Appl.* **1**, 724 (2005).
- [7] S. E. Abuelyman and A. A. Alsehibani, *Int. J. Comput. Sci. Network. Secur.* **8**, 304 (2008).
- [8] I. Hussain, T. Shah, and H. Mahmood, *Int. J. Cont. Math. Sci.* **5**, 1263 (2010).
- [9] SKIPJACK, KEA Algorithm Specifications version 2 (1998).
- [10] X. Y. Shi, Xiao, X. C. Hu. You, and K. Y. Lam, *Int. Conf. Info. Network. Appl.* **2**, 14 (2002).