Generalized Majority Logic Criterion to Analyze the Statistical Strength of S-Boxes

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,** 282 – 288 (2012) / DOI: 10.5560/ZNA.2012-0022
Received September 8, 2011 / revised January 4, 2012

The majority logic criterion is applicable in the evaluation process of substitution boxes used in the advanced encryption standard (AES). The performance of modified or advanced substitution boxes is predicted by processing the results of statistical analysis by the majority logic criteria. In this paper, we use the majority logic criteria to analyze some popular and prevailing substitution boxes used in encryption processes. In particular, the majority logic criterion is applied to AES, affine power affine (APA), Gray, Lui J, residue prime, S_8 AES, Skipjack, and Xyi substitution boxes. The majority logic criterion is further extended into a generalized majority logic criterion which has a broader spectrum of analyzing the effectiveness of substitution boxes in image encryption applications. The integral components of the statistical analyses used for the generalized majority logic criterion are derived from results of entropy analysis, contrast analysis, correlation analysis, homogeneity analysis, energy analysis, and mean of absolute deviation (MAD) analysis.

Key words: S-Box; Advanced Encryption Standard; Skipjack; Lui J; Residue of Prime; Mean of Absolute Deviation Analysis; Majority Logic Criterion.

1. Introduction

The block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length plaintext data into cipher text data of the same dimension. This transformation takes place under the action of a user-provided secret key. The decryption is performed by applying the reverse transformation to the cipher text block using the same secret key. Advanced encryption standard (AES) is a widely used and well-known block cipher. The AES consists of four steps which are: byte sub, shift row, mixed column, and add round key. The byte sub step plays a pivotal role in the encryption process because it creates confusion that is reflected in the encrypted data. In this step, the substitution-box (S-box) transformation takes place. The idea of S-box and permutation box (P-box) or (S-P network), was first given by Shannon and Weaver in 1949 [1], which now forms the basis of modern block ciphers. An S-P network is the recent form of a substitution-permutation product cipher. S-P networks are based on the two primitive cryptographic operations, one is substitution and the other is permutation. In the substitution process, the original data is manipulated or altered to form encrypted data. Whereas, in the permutation process, the order of the data contents are modified, resulting in a different arrangement of bits. The substitution function depends on the encryption key and its space depends on the number of bits n which makes the number of keys equal to $2^n!$. The process of permutation is similar to n address lines with 2^n possible addresses as permutations of the input bits to an S-box. The permutation box has the properties of substitution of data as well as its permutation. The permutations used for encryption are considered less secure as compared to substitution implementation. In many circumstances, the combination of substitution and permutation of data bits at the input level makes the encryption more robust.

In this paper, we use statistical analysis to extract and contrast the parameters related to the strength of encryption in images. One of the fundamental approaches to determine the amount of confusion and randomness created in the encrypted data is the use of correlation analysis and entropy analysis [2]. The results obtained from correlation analysis indicate the

amount of difference between the original image and its encrypted version. The entropy analysis quantizes the extent of randomness in the processed data, which in our case is an image. The amount of vividness in the images leads to clear identification of artifacts or objects with human perception or image recognition algorithms. We present contrast analysis [3] to study the amount of diffusion induced in the boundaries of the texture by the encryption process. This process of contrast analysis is carried out for the entire image with respect to the neighbours of the pixels. In order to further strengthen the analysis process, the measure of closeness in the distribution of grey level co-occurrence matrix (GLCM) elements to the GLCM diagonal is determined. The homogeneity analysis [4] is performed to achieve the task of determining the characteristics of underlying distributions of pixels in the images. In the case of under par substitution and scrambling, the patterns are repeated in the image, and the analysis of GLCM elements assists in quantifying these weaknesses [5]. The energy analysis method is cross linked with elements of GLCM in order to determine the behaviour of the energy distribution and its characteristics in plain and encrypted images [6]. It is important to measure the difference between the plain image and the encrypted image with various methods in order to determine the encryption strength. Therefore, the mean of absolute deviation analysis is used to determine the difference in images [7].

The commonly used S-boxes include AES [8], APA [9], Gray [10], Lui J [11], residue prime [12], S_8 AES [13], SKIPJACK [14], and Xyi [15]. In this paper, we process the images encrypted with these S-boxes and present their performance characteristics. Once ample statistical data is accumulated, the proposed generalized majority logic criterion is applied to the results of the above mentioned analyses. The results of the generalized majority logic criterion assist in determining the best encryption method for a particular class of images or in general, all types of images.

The rest of the paper starts with the introduction to the analysis performed on S-boxes in Section 2. In this section, we present issues related to the presented problem of selecting optimal S-box for image encryption applications. The main focus of this section is to highlight the importance of results obtained by statistical analysis that are used in the evaluation of generalized majority logic criterion. In Section 3, the insight of majority logic criterion (MLC) and generalized majority logic criterion (GMLC) are presented and analyzed. The application of this criterion in the selection process of S-boxes is also discussed. A comparison between GMLC and MLC is discussed in the context of image encryption. This paper relies on statistical techniques to extract valuable information to be used by the GMLC; a complete section, that is Section 4, is dedicated to the details of these methods. The proposed methods are tested by simulation on image data sampled from a general class of images. The results of these simulations are presented in Section 5. The formal conclusion and future directions are presented in Section 6.

2. Analysis of S-Box

The size of the S-box can vary depending on the scope of its application to an encryption process. In this work, the size of the S-box is selected to be 8×8. The analysis presented in this paper can be extended to S-boxes of other sizes without any substantial modification in the proposed algorithm. In the proposed algorithm, various parameters derived from statistical analysis on the plain and encrypted images are used by the generalized majority logic criterion. In order to get full insight of the generalized majority logic criterion, it is critical to discuss and analyze the results from these statistical analyses [10]. The initial activity in analyzing images is to quantify the amount of similarity. The correlation algorithm is widely used in communications engineering to process digital signals and extract relevant characteristics. After the encryption process, the correlation analysis is applied to determine the amount of similarity between the pixels or a group of pixels located in different images. The results of this analysis only reflect estimates of similarity between data. In order to make these estimates more accurate and reliable, further analysis methods such as, entropy analysis, contrast analysis, correlation analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis are used. The interpretation of the results of these analyses and their processing with generalized majority logic criterion yields more accurate results and helps in determining the strength of the encryption in an image. In literature, the above listed statistical analyses are used in various applications; however, their usefulness in determining image encryption strength has not yet been tested rigorously.

3. Majority Logic Criterion and Generalized Majority Logic Criterion to Analyze the Effectiveness of S-Boxes

In the majority logic criterion, the algorithm is applied to a particular class of image data [16]. As the characteristics of a family of images are different, the statistical properties of the analysis are also unique. In addition, the human eye perception also plays an important role in identifying artifacts in an image which varies with the properties of images. The majority logic criterion specializes on a class of images and optimizes the evaluation process of encryption in the same scope. While the effectiveness of majority logic criterion has proven its usefulness for a particular family of images, there is a need for a criterion to analyze the encryption strength for any type of image.

In the proposed generalized majority logic criterion, n number of images from different families are processed. The diversity in image contents makes this algorithm more appealing to a wider range of data samples. Although the generalized majority logic criterion seems to be an appealing choice due to its application and suitability to multiple types of images, there are many challenges in determining the optimal S-box for encryption because of the diverse nature of image categories. The results obtained from statistical analysis are processed in a similar fashion to the majority logic criterion, but the interpretation of the results of these parameters is different and has new meanings.

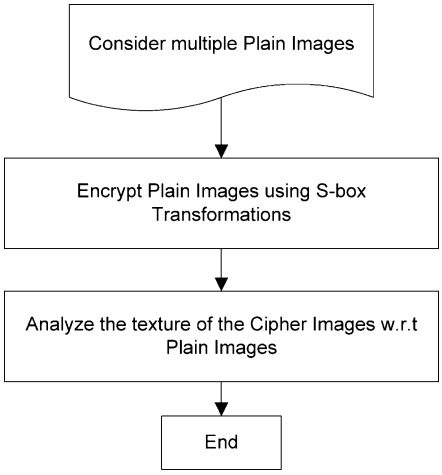

Fig. 1. Generalized majority logic criterion.

Table 1. Algorithm for the proposed criterion to select a suitable S-box for image data encryption.

Proposed Criterion
Input: 'm' plain bitmap Images, $P_1, P_2, \ldots, P_m$ and 'n' S-boxes, $S_1, S_2, \ldots, S_n$.
Objective: create cipher images for all S-boxes
For images $i = 1$ to m,
For S-box $j = 1$ to n
encrypt image P_i by S_j
store cipher images I_{ij}
End for S-box
End for images
For all plain image and cipher image pair,
Create a matrix A of order $m \times n$;
Calculate Entropy, Correlation, Contrast,
Homogeneity, Energy and Mean of absolute deviation for I_{mm} of matrix A.
End for image pairs
The average value of Entropy, Correlation, Contrast, Homogeneity, Energy and Mean of absolute deviation of column 1 of A gives the reading of S-box S_1;
similarly second column determine the reading of S-box S_2 and so on.
We say S-box S_i is better than S_j for $j \in \{1,2\ldots,n\}\backslash\{i\}$ if S_i satisfied majority of the following condition for all considered plain image and corresponding cipher images.
C_1 :If Correlation of pixels of image with its neighbor's pixels of I_i is smaller than I_j for $j \in \{1,2\ldots,n\}\backslash\{i\}$.
C_2: If mean Entropy I_i of is greater I_j than for $j \in \{1,2\ldots,n\}\backslash\{i\}$.
C_3: If Contrast of I_i is greater than I_j for $j \in \{1,2\ldots,n\}\backslash\{i\}$.
C_4: If Homogeneity of I_i is smaller than I_j for $j \in \{1,2\ldots,n\}\backslash\{i\}$.
C_5: If Energy of I_i is smaller than I_j for $j \in \{1,2\ldots,n\}\backslash\{i\}$.
C_6: If MAD of I_i is greater than I_j for $j \in \{1,2\ldots,n\}\backslash\{i\}$.

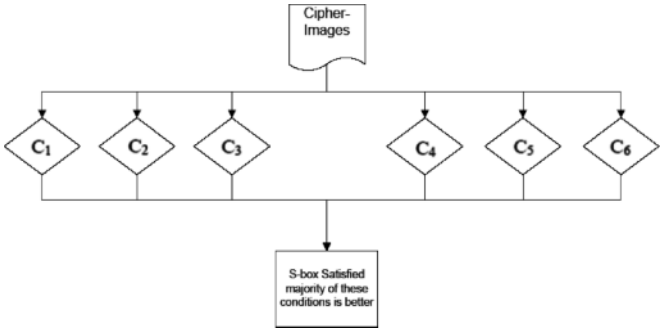

Fig. 2. Details of the generalized majority logic criterion module.

The details of the algorithm for generalized majority logic criterion are presented in Table 1. In this method, several statistical techniques are applied to the results obtained from the encryption of images. In the first step, different types of S-boxes are used to encrypt images. Once the image encryption is completed, the next step is to process and extract statistical parameters from the plain images and encrypted images for the entire set of different S-boxes. The objective is to use this information in the generalized majority logic criterion, in order to determine the best possible S-box for encryption. The generalized majority logic criterion sequentially analyzes the parameters for an image I_i and checks if it satisfies the majority of the conditions of the proposed criteria as compared to I_j. In the case when majority logic is achieved, the corresponding S-box S_i is preferred over S_j.

The generalized majority logic criterion is further emphasized in the flowchart of Figure 1. The process starts with the availability of images at the input level. The process continues with the implementation of image encryption by the use of various S-boxes. In the third step, the parameters resulted from processing cipher images and plain images are processed. The flowchart in Figure 2 further elaborates the arrangement and flow of statistical image processing algorithms. For example, symbols C_1 through C_6 represent various processes of analyzing images. Once these six parameters are calculated, the process of generalized majority logic criterion starts. At the end, the best suitable S-box is predicted which satisfies the majority of the conditions listed in the criterion.

4. Statistical Analysis of S-Boxes for Images

There are several statistical methods employed in this work. The characteristics of the parameters generated by these analyses must be carefully analyzed in order to optimally use the results in an efficient manner. The details of the analyses used in this paper are listed below.

4.1. Entropy Analysis

The entropy is the measure of the amount of randomness in a system. In images, the extent of entropy is related to the arrangement of artifacts which assists the humans to perceive the image. The process of substitution, or application of nonlinear S-box transformation, introduces randomness in the image. The extent of randomness introduced by the encryption process is extremely relevant to the fact that the human eye can perceive the texture in the image. The lack of randomness may result in partial/full recognition of the encrypted image. Therefore, the measurement of entropy may provide important information about the encryption strength, and is measured as

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

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

In Figure 3, the results of the entropy analysis are shown graphically. It is evident from the bar graph that the Skipjack S-box introduces highest amount of entropy among all encryption methods. The prime S-box also introduces a considerable amount or randomness which is comparable to Skipjack and Xyi.

4.2. Contrast Analysis

The amount of contrast in the picture enables the viewer to vividly identify the objects in an image. A reasonable amount of contrast levels in the image

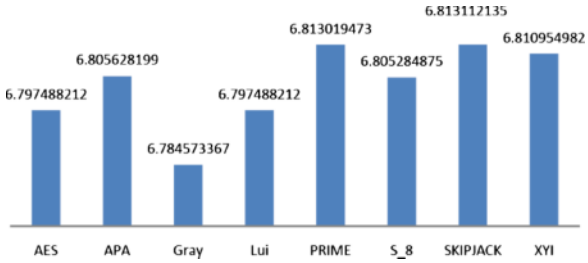

Fig. 3 (colour online). Results of entbropy analysis on encrypted images.

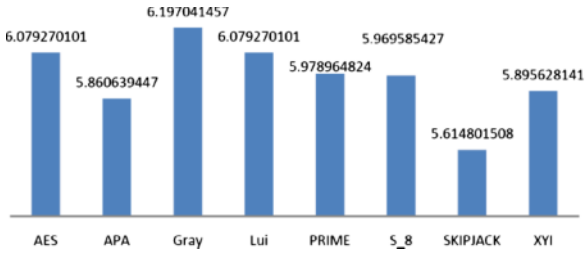

Fig. 4 (colour online). Results of contrast analysis on encrypted images.

also saturates the artifacts which enable the identification of the image more precisely. As the image is encrypted, the amount of randomness increases, as a result, elevates the contrast levels to a very high value. The objects in the image completely smudge because of the nonlinear mapping from the substitution of the image data. We can conclude that a higher level of contrast in the encrypted image depicts strong encryption because it is related to the amount of confusion created by the S-box in the original image. The mathematical representation of this analysis is given as

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

where i and j are the pixels in the image, and the number of grey-level co-occurrences matrices is represented by $p(i,j)$. The whole image is compared with the intensity contrast among pixels and its neighbours.

The results of contrast analysis are shown in Figure 4. In this analysis, the Gray S-box exhibits elevated contrast levels. The original AES S-box and Lui S-box performance is also at a considerable level.

4.3. Correlation

The correlation analysis is divided into three different types. It is performed on vertical, horizontal, and diagonal formats. In addition to analysis on partial regions, the entire image is also included in the processing. This analysis measures the correlation of a pixel to its neighbour by keeping into consideration the texture of the entire image. The mathematical representation of the correlation analysis is given as

$$K = \sum_{i,j} \frac{(i-\mu i)(j-\mu j)p(i,j)}{\sigma_i \sigma_j}\,. \tag{3}$$

In Figure 5, the results of the correlation analysis are shown. The performance of prime S-box is comparatively better than other S-boxes used in this analysis.

4.4. Homogeneity

The image data has a natural distribution which is related to the contents of that image. We perform the homogeneity analysis which measures the closeness of the distributed elements in the GLCM to GLCM diagonal. This is also known as grey tone spatial dependency matrix. The GLCM depicts the statistics of combinations of pixel grey levels in tabular form. The analysis is further extended by processing entries from the GLCM table. The mathematical representation of this analysis is given as

$$\sum_{i,j} \frac{p(i,j)}{1+|i-j|}\,, \tag{4}$$

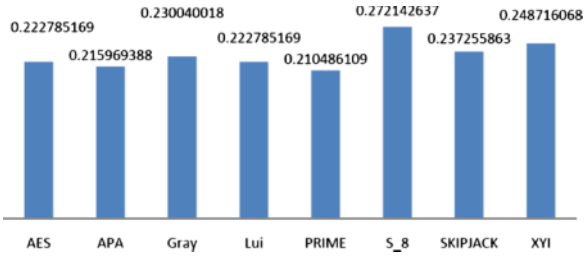

Fig. 5 (colour online). Results of correlation analysis.

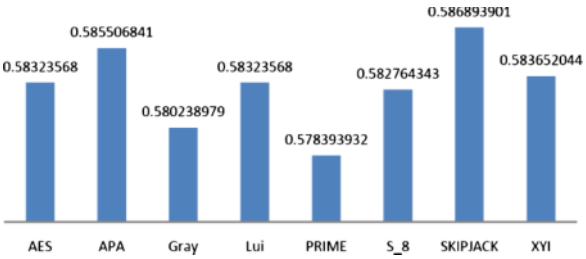

Fig. 6 (colour online). Homogeneity analysis.

where the grey-level co-occurrence matrices in GLCM are represented by $p(i, j)$.

The results of the homogeneity analysis are presented in Figure 6. The comparison between the results of different S-boxes yields that the prime S-Box has the best performance.

4.5. Energy of the Image

The energy analysis is used to measure the energy of the encrypted image. The grey-level co-occurrence matrix is used to perform the energy analysis. The mathematical representation of this analysis is given as

$$\sum_{i,j} p(i, j)^2 . \tag{5}$$

In Figure 7, the results of the energy analysis are depicted. It can be seen from the graph that the performance of the prime S-box is better than the rest of the S-boxes used in the analysis.

4.6. MAD Analysis

In order to distinguish the difference between the original image and the encrypted image, the mean of absolute deviation (MAD) analysis is performed. This analysis is mathematically intensive and requires more computing power as compared to other analysis. The mathematical expression of this analysis is represented as

$$\mathrm{MAD} = \frac{1}{L \times L} \sum_{j=1}^{L} \sum_{i=1}^{L} \left| a_{ij} - b_{ij} \right| , \tag{6}$$

where $a_{i,j}$ are the pixels of the image before encryption, $b_{i,j}$ are the corresponding pixels in the encrypted image, and L represents the dimensions of either one of the images.

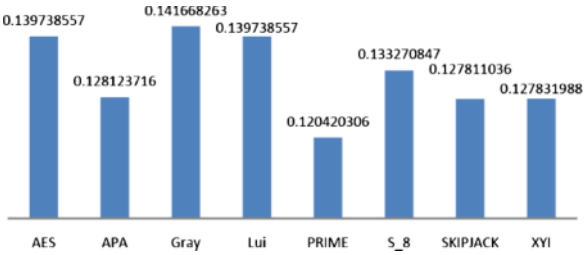

Fig. 7 (colour online). Energy analysis of cipher image.

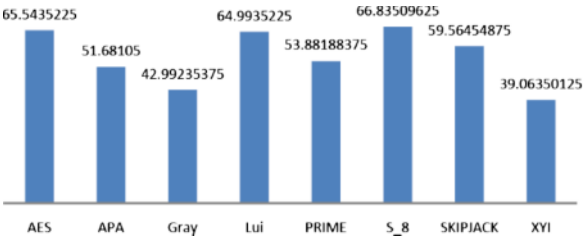

Fig. 8 (colour online). MAD analysis of cipher image.

It is evident from Figure 8 that the S_8 AES S-box performs better in comparison with other S-boxes processed in this work.

The generalized majority logic criterion incorporates the results of the following statistical analyses: entropy analysis, contrast analysis, correlation analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis. Table 2 lists the parameters obtained from the above listed analysis in tabular form. It is important to systematically interpret the visual effects or the texture of the encrypted image by processing the results of the different statistical analysis. The generalized majority logic criterion examines the underlying properties of the results of these analyses and identifies an appropriate S-box for the image encryption application. This majority logic criterion can be tailored to a particular class of images which ev-

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

S-boxes	Average entropy	Average contrast	Average correlation	Average energy	Average homogeneity	Average MAD
AES	6.797488	6.07927	0.22278517	0.139739	0.58323568	65.5435225
APA	6.805628	5.860639	0.21596939	0.128124	0.585506841	51.68105
Gray	6.784573	6.197041	0.23004002	0.141668	0.580238979	42.99235375
Lui	6.797488	6.07927	0.22278517	0.139739	0.58323568	64.9935225
Prime	6.813019	5.978965	0.21048611	0.12042	0.578393932	53.88188375
S_8	6.805285	5.969585	0.27214264	0.133271	0.582764343	66.83509625
SKIPJACK	6.813112	5.614802	0.23725586	0.127811	0.586893901	59.56454875
XYI	6.810955	5.895628	0.24871607	0.127832	0.583652044	39.06350125

idently yields more specific results. On the other hand, the generalized majority logic criterion is applied to any type of image in order to form a first benchmark in determining the strength of S-box encryption.

The results of a generalized majority logic criterion, when applied to a general class of images, shows that the S_8 AES S-box is most suitable for image encryption applications. The proposed generalized criterion systematically processes and analyzes the results of statistical analysis and proposes a suitable S-box. It can also be seen from Table 2 that the APA S-box and the 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.

5. Simulation Results

In the encryption experiments performed in this paper, we use eight well-known S-boxes, which include, AES, APA, Gray, Lui J, residue prime, S_8 AES, Skipjack, and Xyi. The results of the statistical analysis performed on these S-boxes were used in the assessment of a suitable S-box in the image processing applications. The generalized majority logic criterion method is proposed to find out an S-box which has the best properties among all the tested S-boxes. The images used for the purpose of encryption are sampled from diverse collection of images with different properties. This ensemble of plain images covers all types of images in order to ensure maximum coverage.

The S_8 AES S-box, as determined by the generalized majority logic criterion, is suitable for the image processing application.

The generalized majority logic criterion can further be extended by adding more versatile statistical analyses. The incorporation of mean absolute error, number of pixels change, and unified average changing intensity analysis can provide more detailed analysis pertaining to the strength of S-boxes for image encryption applications. Additionally, the proposed criterion can be tested on the encryption for other types of data.

6. Conclusion

In this paper, we present a criterion to determine the suitability of an S-box to image encryption applications. There are several variants of S-boxes which are used in the AES encryption algorithms. As the performance in terms of creating confusion ability of these S-boxes is not similar, therefore, it is useful to present a method to analyze their encryption ability. A generalized majority logic criterion is proposed which determines the best candidate S-box with the assistance of statistical analysis on the original and encrypted image transformed by APA, Gray, Lui J, residue prime, S_8 AES, Skipjack, and Xyi S-boxes. The underlying statistical analyses used in this work are entropy analysis, contrast analysis, correlation analysis, homogeneity analysis, energy analysis, and mean of absolute deviation analysis.

[1] C. E. Shannon and W. Weaver, The University of Illinois Press, Urbana, Illinois 1949.
[2] L. Zhang, X. Liao, and X. Wang, Chaos Solution Fract. **24**, 759 (2005).
[3] S. Y. Chen, W. C. Lin, and C. T. Chen, Graph. Model. Im. Proc. **53**, 457 (1991).
[4] F. Jing, M. Li, H. Zhang, and B. Zhang, Proc. ISCAS **4**, 145 (2002).
[5] E. S. Gadelmawla, NDT & E. Int. **37**, 577 (2004).
[6] S. Zhan and H. Zhang, Signal Process.-Image 600 (2007).
[7] I. Avcibas, N. Memon, and B. Sankur, IEEE T. Improc. **12**, 221 (2003).
[8] J. Daemen and V. Rijmen, Available: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf, (1999).
[9] L. Cui and Y. Cao, Int. J. Innov. Comput. I. **3**, 45 (2007).
[10] M. Tran, T. Bui, and D. K. Doung, Int. Conf. Comp. Intel. Secur. 253 (2008).
[11] J. Lui, B. Wai, X. Cheng, and X. Wang, Int. Conf. Inf. Network. Appl. **1**, 724 (2005).
[12] S. E. Abuelyman and A. A. Alsehibani, Int. J. Comput. Sci. Network. Secur. **8**, 304 (2008).
[13] I. Hussain, T. Shah, and H. Mahmood, Int. J. Cont. Math. Sci. **5**, 1263 (2010).
[14] SKIPJACK, KEA Algorithm Specifications version, 2 (1998).
[15] X. Y. Shi, Xiao, X. C. Hu. You, and K. Y. Lam, Int. Conf. Info. Network. Appl. **2**, 14 (2002).
[16] T. Shah, I. Hussain, M. A. Gondal, and H. Mahmood, Int. J. Phys. Sci. **6**, 4110 (2011).