Application of Mean of Absolute Deviation Method for the Selection of Best Nonlinear Component Based on Video Encryption

Amir Anees[a], Waqar Ahmad Khan[b], Muhammad Asif Gondal[b], and Iqtadar Hussain[b]

[a] Department of Electrical Engineering, Hitec University, Taxila, Pakistan
[b] National University of Computer and Emerging Sciences, Fast, Islamabad, Pakistan

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

Z. Naturforsch. **68a,** 479 – 482 (2013) / DOI: 10.5560/ZNA.2013-0022
Received October 29, 2012 / revised February 21, 2013 / published online May 22, 2013

The aim of this work is to make use of the mean of absolute deviation (MAD) method for the evaluation process of substitution boxes used in the advanced encryption standard. In this paper, we use the MAD technique to analyze some popular and prevailing substitution boxes used in encryption processes. In particular, MAD is applied to advanced encryption standard (AES), affine power affine (APA), Gray, Lui J., Residue Prime, S_8 AES, SKIPJACK, and Xyi substitution boxes.

Key words: S-Box; Mean of Absolute Deviation Analysis (MAD).

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 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 a statistical analysis to extract and contrast the parameters related to the strength of encryption in videos. It is important to measure the difference between plain video and the encrypted video with various methods in order to determine the encryption strength. Therefore, the MAD analysis is used to determine difference in videos [2].

The commonly used S-boxes include AES [3], APA [4], Gray [5], Lui J. [6], Residue Prime [7], S_8 AES [8], SKIPJACK [9], and Xyi [10]. In this paper, we process the videos encrypted with these S-boxes and present their performance characteristics. Once ample statistical data is accumulated, the proposed MAD is applied to the results. The results of the MAD assist in determining the best encryption method for a particular class of videos or in general, all types of videos.

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 relating to the presented problem of selecting optimal S-box for video 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 best S-box. A complete section that is, Section 3, is dedicated to the details of the proposed method. The proposed methods are tested by simulation on video data sampled from a general class of videos. The results of these simulations are presented in Section 4. The formal conclusion and future directions are presented in Section 5.

2. Mean of Absolute Deviation Analysis for the Effectiveness of S-Boxes

The method of mean of absolute deviation (MAD) is applied to a particular class of video data [11]. As the characteristics of a family of videos 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 video which varies with the properties of the videos. ADM specializes on a class of videos and optimizes the evaluation process of encryption in the same scope. While the effectiveness of MAD has proven its usefulness for a particular family of videos, there is a need for an algorithm to analyze the encryption strength for any type of video.

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

The details of the algorithm for generalized MAD are presented in Proposition 1:

Proposition 1 (Proposed Criterion)**.**

Input: m plain bitmap videos, $P_1, P_2, \ldots, P_m$ and n S-boxes, $S_1, S_2, \ldots, S_N$.

Objective: create cipher videos for all S-boxes

For videos $i = 1$ to m,
  For S-box $j = 1$ to n
    encrypt video P_i by S_j
    store cipher videos I_{ij}
  End for S-box
End for videos

For all plain video and cipher video pair,
  create a matrix A of order $m \times n$;
    calculate mean of absolute deviation for I_{mm} of matrix A.
End for video pairs

The average value of MAD of column 1 of A gives the reading of S-box S_1; similarly, the second column determines 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 is satisfied.
If MAD of I_i is greater than I_j for $j \in \{1,2,\ldots,n\}\backslash\{i\}$.

In this method, several statistical techniques are applied to the results obtained from the encryption of videos. In the first step, different types of S-boxes are used to encrypt videos. Once the video encryption is completed, the next step is to process and extract statistical parameters from the plain videos and encrypted videos for the entire set of different S-boxes. The objective is to use this information in the generalized MAD, in order to determine the best possible S-box for encryption. The generalized MAD sequentially analyzes the parameters for an video I_i and checks if its value of MAD is greater than I_j. In the case when results are achieved, the corresponding S-box S_i is preferred over S_j.

3. Statistical Analysis of S-Boxes for Videos

The MAD methods are employed in this work. The characteristics of the parameters generated by this analysis must be carefully analyzed in order to optimally use the results in an efficient manner. The details of the analysis used in this paper are below.

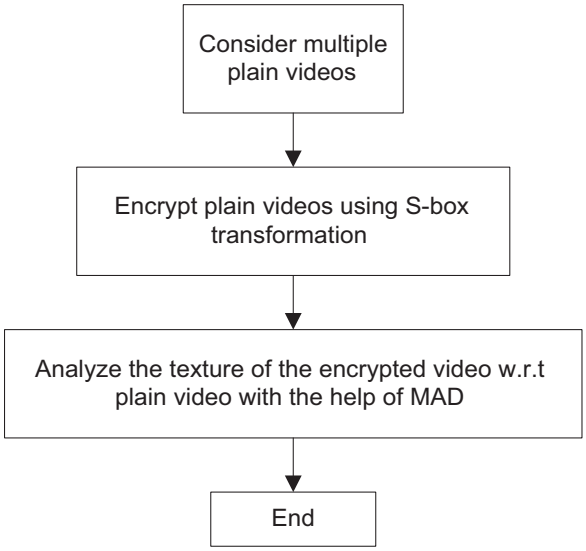

Fig. 1. Proposed criterion.

3.1. MAD Analysis

In order to display the difference between the original video and the encrypted video, the MAD analysis is performed. This analysis is mathematically intensive and requires more computing power as compared to other methods. The mathematical expression of this analysis is represented as

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

where a_{ij} are the pixels of the video before encryption, b_{ij} are the corresponding pixels in the encrypted video, and L represents the dimensions of either one of the videos.

It is evident from Figure 2 that S_8 AES S-box performs better in comparison with other S-boxes processed in this work.

It is important to systematically interpret the visual effects or the texture of the encrypted video by processing the results of MAD analysis. The MAD identifies an appropriate S-box for video encryption application which can be tailored to a particular class of videos, evidently yielding more specific results.

The results of a MAD criterion, when applied to a general class of videos, shows that S_8 AES S-box is most suitable for video encryption applications. The proposed generalized criterion systematically processes and analyzes the results of statistical analysis

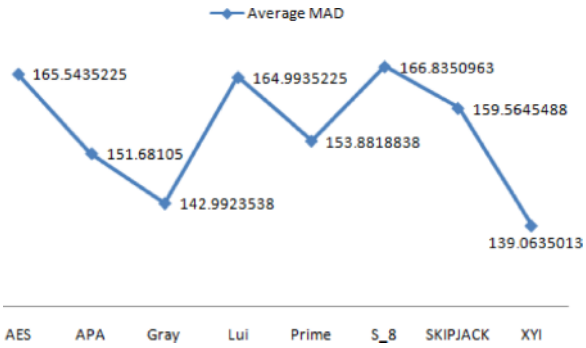

Fig. 2 (colour online). MAD analysis of cipher video.

Table 1. MAD of plain video and cipher video.

S-boxes	Average MAD
AES	165.5435225
APA	151.68105
Gray	142.99235375
Lui	164.9935225
Prime	153.88188375
S_8	166.83509625
SKIPJACK	159.56454875
XYI	139.06350125

and proposes a suitable S-box. It can also be seen from Table 1 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 MAD analysis identifies the best candidate S-box with highest level of encryption strength.

4. 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 video processing applications. The MAD method is used to find out an S-box which has the best properties among all the tested S-boxes. The videos used for the purpose of encryption are sampled from diverse collection of videos with different properties. This ensemble of plain videos covers all types of videos in order to ensure maximum coverage.

The S_8 AES S-box, as determined by MAD, is suitable for the video processing application.

5. Conclusion

In this paper, we use the MAD method to determine the suitability of an S-box to video encryption applications. There are several variants of S-boxes which are used in 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. MAD is used to determine the best candidate S-box with the assistance of statistical analysis on the original and encrypted video transformed by APA, Gray, Lui J., Residue Prime, S_8 AES, SKIPJACK, and Xyi S-boxes. The MAD form video encryption suitability when applied to the S-boxes listed above shows that the S_8 S-box is the most suitable for video encryption applications.

[1] C. E. Shannon, Bell Syst. Tech. J. **28**, 715 (1949).
[2] G. Alvarez, F. Montoya, M. Romera, and G. Pastor, Phys. Lett. A **319**, 334 (2000).
[3] J. Daemen and V. Rijmen, Available: http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf, (1999).
[4] L. Cui and Y. Cao, Int. J. Innov. Comp. Info. Contr. **3**, 45 (2007).
[5] M. T. Tran, D. K. Bui, and A. D. Doung, Int. Conf. Comput. Intell. Sec., **12**, 253 (2008).
[6] J. Liu, B. Wai, X. Cheng, and X. Wang, Proc. Int. Conf. Adv. Info. Net. Appl. **05**, 724 (2005).
[7] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Proc. Pak. Acad. Sci. **48**, 111 (2011).
[8] I. Hussain, T. Shah and H. Mahmood, Int. J. Contemp. Math. Sci. **5**, 1263 (2010).
[9] I. Hussain, T. Shah, H. Mahmood, and M. A. Gondal, Neural Comput. Appl. doi:10.1007/s00521-012-0914-5.
[10] X. Y. Shi, L. Xiao, X. C. Hu. You, and K. Y. Lam, Int. Conf. Info. Network. Appl., **21**, 14 (2002).
[11] I. Hussain, T. Shah, M. A. Gondal, and H. Mahmood, Z. Naturforsch. **67a**, 282 (2012).