An Image Encryption Algorithm with XOR and S-box

Abdelfatah A. Tamimi and Ayman M. Abdalla
Department of Computer Science, Al-Zaytoonah University of Jordan,
P.O. Box 130, Amman 11733, Jordan
E-mail: drtamimi99@gmail.com

Abstract - *This new algorithm performs lossless image encryption by combining variable-length key-dependent XOR encryption with S-box substitution. This algorithm was implemented and tested by performing different permutations of XOR encryption and S-box substitution. Empirical analysis using different types of test images of different sizes showed that this new algorithm is effective and resistant to statistical attacks. The idea presented by this algorithm may be generalized to apply to input data other than images, and may be combined with other encryption methods.*

Keywords: cryptography, block cipher, S-box, XOR.

1 Introduction

The bitwise XOR operation is normally used as a part of a more complex encryption algorithm. Numerous variations of the use of XOR in image encryption can be found in the literature. In the Advanced Encryption Standard (AES), XOR is used as a step in every iteration of the encryption procedure to effectively combine data being encrypted with the encryption key[1]. An algorithm that combines XOR encryption with a rotation operation was designed for effective image encryption[2]. Another algorithm[3] used an affine transform combined with XOR encryption to perform image encryption. Images may also be effectively encrypted using the recursive attributes of the XOR filter[4].

Examples on applying the four steps of AES including, the use of S-box substitution, are available[1]. Many encryption algorithms based on AES were also developed[5,6,7,8,9,10,11]. However, AES has limitations on some multimedia specific requirements[12,13], so other encryption algorithms need to be developed. Some algorithms[14,15] were developed for image encryption using only the S-box substitution from AES as a part of a more complex algorithm that does not use the XOR operation.

In this paper, a new algorithm is presented, which performs lossless encryption via two operations. The first operation performs XOR encryption on the image using variable length blocks. The second operation performs byte substitution using a fixed-size lookup table (S-box). The algorithm was implemented and tested with different combinations of these two operations. Analysis showed effectiveness of the cipher.

2 The New Algorithm

This algorithm takes an image and a key as input. It performs variable-length key-dependent XOR encryption and applies byte substitution using a lookup table called S-box. Different combinations of these two encryptions may be performed, where the decryption performs the inverse of the applied steps in reverse order.

In the XOR encryption operation of the algorithm, the image is regarded as a stream of bytes, and then it is divided into groups (one-dimensional blocks). Let the input image have n bytes and the key have b bytes referred to as $key[0]$ through $key[b-1]$. The image is divided into approximately $n/\sum_{i=0}^{b-1} key[i]$ groups of bytes. Group number j will consist of $key[i]$ bytes where $j = (b \times c + i)$ for some non-negative integer c. For example, for a key of 16 bytes where the value of its $key[5] = 70$, there will be groups in the image consisting of 70 bytes each, namely: the groups numbered 5, 21, 37, 53, 69, etc.

Each of the above groups is encrypted with XOR as follows. Suppose the bytes of group number j are $G[0]$ through $G[key[i] - 1]$. Then, the encrypted values will be:

$$G'[0] = (G[0] \text{ XOR } key[i]), \text{ and}$$

$$G'[p] = (G[p] \text{ XOR } G'[p-1]) \text{ for } 0 < p \le key[i] - 1. \quad (1)$$

Each group is encrypted similarly but independently of the other groups.

The two-dimensional substitution table, known as S-box, is constructed to perform two transformations: multiplicative inverse and affine transformation. This nonlinear key-dependent substitution was presented as a step in each iteration of the AES algorithm[1]. However, in the new algorithm presented here, this substitution is performed at most two times. It is either applied before, after, or both before and after the XOR encryption operation. It is applied to the entire image; block by block. The S-box substitution in this algorithm may also be skipped if needed. If S-box substitution is skipped, another substitution or shuffling operation should be applied in addition to the XOR encryption, so that no encrypted group will remain intact or in

the same location inside the image as produced by the XOR encryption operation.

The decryption algorithm is similar to the encryption algorithm, where each of the above steps can be easily inverted. The inverted steps are performed in reverse order, and the decryption restores the original image without any loss.

3 Implementation and Analysis

The security of the new algorithm comes from combining the two encryption operations; using XOR encryption and S-box byte substitution. If XOR encryption is used alone, the encryption may become vulnerable to brute-force and plaintext attacks. Using S-box substitution alone could make the encryption vulnerable to statistical attacks. A combination of these two encryption operations will provide significant resistance to all of these types of attacks.

If one or more bits in the key are changed, it causes a different grouping in the XOR step and the XOR values are changed. In addition, let an S-box of size 16×16 bytes be used in the S-box substitution step. This S-box has 2,048 different entries where each of these entries consists of 8 bits. This makes the total number of permutations for this step is 2^{11}. Consequently, for an image of ten or more kilobytes input to any combination of these two encryption operations, a brute-force attack is impossible.

The algorithm was applied to 50 images of various types and sizes. When different keys were used with the same image, they produced different encrypted images. In addition, analysis using histograms, correlation, and peak signal to noise ratio (PSNR) showed properties of the algorithm that strongly resist statistical attacks.

The histograms of the images encrypted with any combination of the operations of the new algorithm were uniform and different from the histograms of the original images. They gave no indication that may help statistical attacks.

The mean squared error for two images, stored in matrices *A* and *B*, is computed as follows:

$$MSE = \frac{1}{mn}\sum_{i=1}^{m}\sum_{j=1}^{n}(A[i,j]-B[i,j])^2 \qquad (2)$$

PSNR is computed as:

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \qquad (3)$$

where *MAX* is the maximum pixel value of the image, and the PSNR measurement unit is the decibel (dB). A lower PSNR value is desired for encrypted images since it indicates more noise and, therefore, more resistance to attacks.

Figure 1 shows PSNR computed for encrypted images resulting from encrypting the original image using different combinations of XOR and S-box encryptions: without S-box, S-box first followed by XOR, S-box last (after XOR), and S-box twice (once before and once after XOR). As it appears in the figure, the PSNR values of these methods were similar. The average PSNR values for the results are shown in the first column of Table 1. The average PSNR value was the highest (i.e., best) when applying S-box exactly once, where applying S-box before XOR produced an average close to that when S-box was applied after XOR. The average was slightly lower when S-box was used twice and the lowest (worst) when it was not used at all.

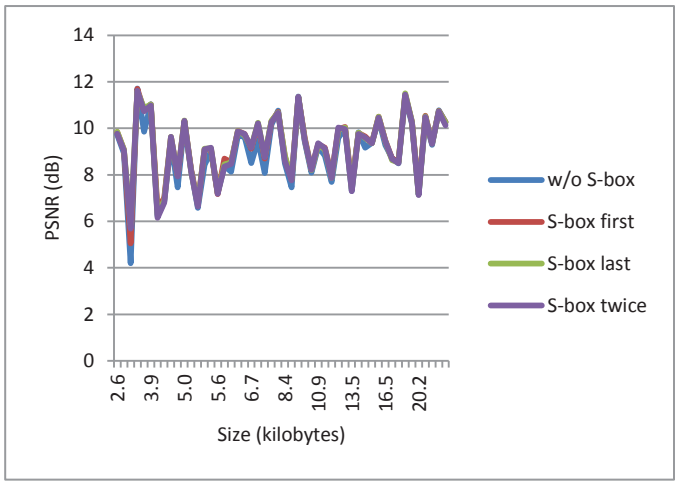

Figure 1. PSNR resulting from different combined operations

Table 1. Average values with different combinations of encryption operations

Operation Combination	PSNR	Correlation
XOR without S-box	8.999649	0.028833
S-box before XOR	9.216589	0.006321
S-box after XOR	9.208713	0.006116
S-box before & after XOR	9.174472	0.008030

The correlation, *r*, between two images, stored in matrices *A* and *B*, is computed as follows, where $\bar{A}$ and $\bar{B}$ are mean values for matrices *A* and *B*, respectively:

$$r = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(A[i,j]-\bar{A})(B[i,j]-\bar{B})}{\sqrt{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(A[i,j]-\bar{A})^2\right)\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(B[i,j]-\bar{B})^2\right)}} \qquad (4)$$

A lower correlation value between an image and its encryption indicates less resemblance between them, which provides more resistance to attacks.

The correlation value computed for encrypted images resulting from encrypting the original image using different combinations of XOR and S-box encryptions is shown in Figure 2. As seen in the figure, using XOR without S-box generally gave the highest (worst) value of all four encryption combinations, while other encryption combinations gave values similar to each other. This observation is supported by the average correlation value computed for each operation combination, shown in the second column of Table 1, where the average was taken for the absolute values of correlation for the sample images. The average correlation computed when applying S-box once was lower than the average computed when S-box was used twice, and did not make much difference whether S-box was applied before or after XOR.

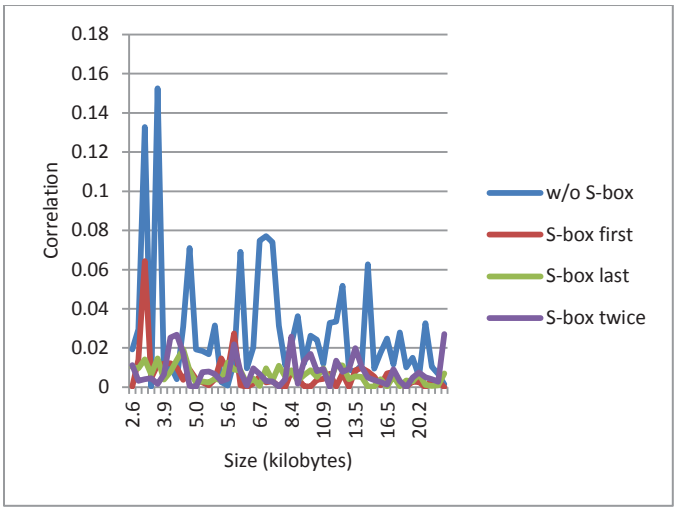

Figure 2. Correlation resulting from different combined operations

Overall, all PSNR values were high and all correlation values were low. This indicates resistance to statistical attacks. The correlation results agreed with the PSNR results in showing the best and worst combinations of XOR and S-box encryptions.

4 Conclusions

A new encryption algorithm was presented. The new algorithm performs encryption using an XOR encryption and S-box substitution. Analysis of different combinations of these two encryptions showed that applying S-box substitution once with XOR encryption produced the best results compared to using it twice or not using it at all.

Statistical analysis using histograms, PSNR, and correlation showed the algorithm is not vulnerable to statistical attacks. In addition, the huge number of possible keys combined with a huge number of possible substitutions makes a brute-force attack on the algorithm impossible.

For future work, the XOR encryption method presented in this paper may be combined with other encryption methods. It is recommended that it should be combined with methods that change the order of bytes through substitution or shuffling. In that case, S-box may not be necessarily used.

5 References

[1] Federal Information Processing Standards (FIPS 197). The Advanced Encryption Standard, 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[2] M.A.F. Al-Husainy, "A novel encryption method for image security," Int. J. Security & Its Applications, vol. 6(1), pp. 1-8, 2012.

[3] A. Nag, J.P. Singh, S. Khan, S. Biswas, D. Sarkar and P.P. Sarkar, "Image encryption using affine transform and XOR operation," Proc. 2011 Int. Conf. Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), Thuckafay, India. 21-22 July 2011. DOI: 10.1109/ICSCCN.2011.6024565

[4] S.A. Chatzichristofis, L. Bampis, O. Marques, M. Lux and Y. Boutalis, "Image encryption using the recursive attributes of the exclusive-or filter," J. Celluar Automata, vol. 9, pp. 125-137, 2014.

[5] M. Benabdellah, M.M. Himmi, N. Zahid, F. Regragui and E.H. Bouyakhf. "Encryption-compression of images based on FMT and AES algorithm"; Appl. Math. Sci. (Hikari Ltd.), vol. 1 (45), pp. 2203–2219, 2007.

[6] D.A. Duc, T.M. Triet and L.H. Co. "The extended Rijndael-like block ciphers"; Proc. Int. Conf. Info. Tech.: Coding and Computing, pp. 183-188, 2002. DOI: 10.1109/ITCC.2002.1000384

[7] N. El-Fishawy and O.M. Abu Zaid. "Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher algorithms"; Int. J. Net. Sec. (Femto Technique Co.), vol. 5 (3), pp. 241-251, 2007.

[8] A. Yahya and A. Abdalla. "An AES-based encryption algorithm with shuffling"; Proc. 2009 Int. Conf. Security & Management (SAM '09), pp. 113-116, 2009.

[9] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki. "A modified AES based algorithm for image encryption"; Int. J. Comp. Sci. & Eng. (World Academy of Science, Engineering and Technology), vol. 1 (1), pp. 70-75, 2007.

[10] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki. "A modified AES based algorithm for image encryption"; Enformatika (World Enformatika Society), vol. 21, pp. 206-211, 2007.

[11] J.-M. Do and Y.-J. Song, "Secure streaming media data management protocol," Int. J. Security & Its Applications, vol. 8(2), pp. 193-202, 2014. DOI: 10.14257/ijsia.2014.8.2.20

[12] D. Socek, S. Magliveras, D. C'ulibrk, O. Marques, H. Kalva and B. Furht. "Digital video encryption algorithms based on correlation-preserving permutations"; EURASIP J. Inform. Security, 2007.

[13] J.W. Yoon and H. Kim. "An image encryption scheme with a pseudorandom permutation based on chaotic maps"; Commun. Nonlinear Sci. Numer. Simulat., 2010. DOI: 10.1016/j.cnsns.2010.01.041

[14] A. Abdalla and A. Tamimi, "Algorithm for image mixing and encryption," Int. J. Multimedia & Its Applications, vol. 5(2), pp. 15-21, 2013.

[15] A. Tamimi and A. Abdalla, "A Double-Shuffle Image-Encryption Algorithm," Proc. 2012 Int. Conf. Image Processing, Computer Vision, and Pattern Recognition (IPCV '12), pp. 496-499, 2012.