I. J. Computer Network and Information Security, **2017, 9, 30-37**
Published Online September 2017 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2017.09.04

Performance Evaluation of Authentication-Encryption and Confidentiality Block Cipher Modes of Operation on Digital Image

Narges Mehran
Department of Computer Architecture,
Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran
E-mail: n.mehran@eng.ui.ac.ir

Mohammad Reza Khayyambashi
Department of Computer Architecture,
Faculty of Computer Engineering, University of Isfahan, Isfahan, Iran
E-mail: m.r.khayyambashi@comp.ui.ac.ir

Received: 11 March 2017; Accepted: 08 May 2017; Published: 08 September 2017

Abstract—Recently, security of digital images has attracted significant attention. This paper evaluates the performance of authentication-encryption and confidentiality block cipher modes of operation, on digital image. Authentication-encryption scheme, such as Offset Code Book (OCB) mode, offers both privacy and authenticity; that is to say, this scheme provides data authenticity without increasing the cost of encryption. The performance of this mode is compared with other confidentiality modes of operation, such as the fast counter (CTR) mode that just encrypts the image without verification. Various statistical methods, such as correlation coefficient, Number of Pixels Change Rate (NPCR), and Unified Average Changing Intensity (UACI) are utilized to analyze the efficiency of different modes. Results show that the model based on OCB scheme, by both AES and Serpent algorithms, exhibits good performance on a digital image compared to the models based on other modes. OCB-AES based scheme, associated with its own authentication, has considerable speed in comparison with other confidentiality modes.

Index Terms—Authentication-Encryption, Block cipher modes of operation, Image encryption, Authenticated-Encryption with Associated-Data modes, Offset Code Book.

I. Introduction

In communication systems, such as the Internet, it is almost impossible to avoid intruders and attackers. However, users need to securely transmit information throughout the network. The information travelling through computer networks may be intercepted, modified, fabricated or even interrupted by an unauthorized third party. While transmitting digital images and videos over modern communication channels, security is an important factor. Due to the increasing applications of this type of multimedia in industrial processes, it is essential to protect confidential image data against unauthorized access by third parties. The first step in preparing security services and having a secure channel is to apply cryptographic algorithms, such as symmetric-key algorithms (e.g., AES), wherein the decryption key is the same as the encryption key. These algorithms provide confidentiality by allowing the receiver to exclusively retrieve the contents of the original message. The second step is to provide authentication and integrity services so that the sender and receiver correctly recognize each other [1], [2].

Block cipher algorithms are in category of symmetric-key algorithms, which operate on blocks of plain text and cipher text. The blocks are occasionally longer than 128 bits; therefore, block cipher algorithms are just applicable to a single 64-bit or 128-bit block; however, a 64×64-pixel image consists of approximately 256 128-bit blocks. Each image is divided up into 4×4 integer matrixes or 128-bit binary blocks. By using the following modes, an image is encrypted. In this paper, we have tried to compare the secure algorithms for image authentication and encryption. Two modern popular block cipher algorithms are exploited: Rijndael-128[3] and Serpent [4], both of which were finalists at the Advanced Encryption Standard (AES) contest. Rijndael algorithm has been extensively employed, even in mobile and desktop messaging applications such as Telegram [5]. As these algorithms just encrypt 128-bit data, it is essential to have a mode of operation to encrypt 128-bit blocks of an image. This article evaluates OCB-v3, an Authentication-Encryption mode of operation, in an image authentication-encryption system. The performance is evaluated and compared with that of five various encryption modes of operation.

The remainder of this paper is organized as follows. Section 2 provides a survey of the relevant work. Section 3 describes the OCB model. The evaluations are presented in Section 4, after which Section 5 concludes the paper.

II. Related Works

In this section, we review the previous works about block cipher modes and the related image encryption schemes. Firstly, the image block-cipher Encryption schemes are studied and then the researches on confidentiality and authenticated-encryption block cipher modes of operation are discussed.

A. Image block-cipher Encryption Schemes

There have been many implementations of AES since its invention. Authors in [6] have proposed a Modified Advanced Encryption Standard (MAES) to reflect high-level security and better image encryption. The algorithm does not impose greater overhead than the original AES and merely changes the strategy behind the shifting-row part. Their statistical results show that the MAES algorithm exhibits better performance in comparison with AES.

In [7], a new modified version of AES, to design a secure symmetric image encryption technique, has been also proposed. The AES is extended to support a key stream generator for image encryption, which can overcome the problem of textured zones existing in other known encryption algorithms. The modification is done by adding a key stream generator, such as (A5/1, W7), to the AES image encryption algorithm in order to increase the image security and the encryption performance.

In [8], authors have used baker’s map and S-AES algorithm to construct their approach. Their scheme is based on combination of pixel shuffling and a new modified version of simplified AES.

In the following, the confidentiality modes of operation, as well as the authentication-encryption mode of operation, are briefly explained.

B. Confidentiality Block Cipher Modes

The Electronic Code Book (ECB) confidentiality mode separately enciphers each block of data with the same key [1]. Authors in [9] use the ECB mode of encryption to parallelize the AES algorithm. Hence, with a powerful block cipher algorithm, similar blocks will be encrypted to the same encrypted blocks; for instance, the background of image remains unchanged and its outline is easily recognizable. This mode is operated on Tux, the penguin mascot of Linux OS, *RGB* image. As shown in Fig. (1), the same parts of the image are clearly recognizable, allowing an attacker to easily substitute with arbitrary data. As the image is in *RGB* format, prior to enciphering, it is broken into its three principal components: Red, Green and Blue. Then, after deciphering, they are combined to form the decrypted *RGB* image.

Other encryption modes include Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB). However, none of these modes is suitable for large-size images. Therefore, another mode of operation is needed to store and retrieve an arbitrary block in a system file in a parallel manner. Counter (CTR) mode is used in high-speed networks. At first, counter values are encrypted. Subsequently, these encrypted values are eXclusive-ORed with each block of image. In order to prevent an attack, the same pair of keys and counter values should not be used for different messages because they are vulnerable to attacks. During transmission, the CTR mode does not propagate the error, thus only the erroneous block is damaged [1], [2].

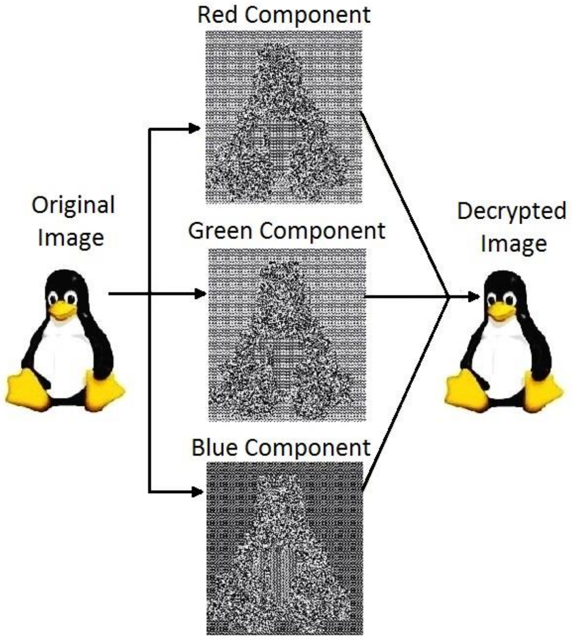


Fig.1. Encryption of the Linux logo, Tux, by AES Algorithm in Cooperation with ECB mode of Operation.

C. Authenticated-Encryption Block Cipher Modes

Authors in [10] present a parallelized block cipher mode of operation that simultaneously provides privacy and authenticity. These modes are called *Authentication-Encryption (AE)* schemes. The authors compare their proposal with the CTR encryption mode (to compute the overhead of the *AE* modes) and other *AE* modes, namely CCM (CTR encryption with CBC MAC). Their experimental findings, for 4 KB messages on an Intel i5 (“Clarkdale”) processor is observed in Table (1).

Table 1. Empirical Performance of Modes on x86-64 Architecture [10].

Mode	**CPU cycles (in CPU cycles per byte)**
CCM (CTR encryption with CBC MAC)	4.17
CTR	1.27
OCB	1.48

Across different hardware architectures, such as Intel, ARM, PowerPC, SPARC, with various message lengths, Offset Code Book (OCB) is found to be faster than CCM and GCM [11]. CCM uses CBC serial mode to compute the authentication code and CTR mode to encrypt the message with the authentication code. GCM is another standard *AE* mode that computes the MAC based on

GF(2^{128}) and then encrypts it with CTR mode. This mode is a block cipher mode of operation that provides both confidentiality and authenticity. The designers of OCB have tested x86 Intel processor by the secure version of the AES algorithm named AES_NI (AES with seven New Instructions added to make it secure against side channel attacks). For other platforms, they have used an OpenSSL library, which supports different cryptographic algorithms such as AES. The OCB-v3 scheme has significantly lower computational cost than others that encipher data and then authenticate it with a MAC algorithm. In all of these five platforms, OCB is faster than other *AE* modes, with message length varying from one to *k* bytes. The OCB scheme has been improved since 2001 and has been patented three times. The last one is named OCB-v3 [12]. In this paper, the updated version of this mode, i.e. OCB-v3, is applied on image. As there is little work on image Authentication-Encryption schemes, this research is specially focused on one of these algorithms and the proved reliability of block cipher algorithms such as AES in GF (2^n). The results are then compared with image encryption of other famous modes.

III. Image Autehntication-Encryption Procedure by OCB Scheme

Several confidentiality modes mentioned in the previous section demonstrate good, but inadequate, performance. None of them, however, provides authenticity and confidentiality for images, at the same time. Some types of attacks, such as an acknowledgement that is not from the true receiver of a message or even replay attacks carried out by sending an old message to start exchanging data by an intruder, can be prevented through message authentication code, named Message Authentication Code (MAC), which is an extraction of the message and approves its integrity. However, *AE* has been adopted into many widely implemented standards such as Secure Shell (SSH)[13], Mobile Shell (Mosh)[14], Secure Sockets Layer/ Transport Layer Security (SSL/TLS), IPsec, IEEE 802.11 (Wi-Fi), ANSI C12.22-2008 (for Smart Grid), and ISO/IEC 19772 [15].

In this work, an *AE* OCB-v3 scheme is adopted, which is faster than other modes across different platforms [11]. Fig. (2) describes the authentication encryption according to OCB using a block diagram. The character ⊕ denotes bitwise eXclusive OR operation.

A grayscale image can be represented as a two-dimensional array, in which the elements are between [0, 256); the x^th^ and y^th^ elements of this array measure the grayscale value at the pixel position (x+1, y+1) of image.

A *RGB* color image is an M×N×3 array of pixels (height×width×3), where each pixel is a triplet corresponding to the red, green and blue components of the image. Each component of a *RGB* image is a single two-dimensional M×N array with the values between [0, 256), in which “0” indicates (total absence, black), and “255” (total presence, white) [16].

As observed in Fig. (3), in order to encrypt an image, it is firstly broken into 4×4 blocks, meaning that each block consist of 4×4 pixels or 128 bits. Then 128-bit value is computed (eXclusive-OR of all the 128-bit blocks). Associated data with the key produce the MAC or *Auth* (Authentication) value, whose length is also 128 bits. The transmitted value has ((128 × *m*) + *r*) bits, where *m* is the number of blocks and *r* is *tag* or *Auth* length for information assurance and image integrity. When image is not a multiple of 128 bits, a “1” and a few “0”s are added to its end and the $Checksum = M_1 \oplus ... \oplus M_m \oplus M_* 10^*$ is computed. By having the *Checksum* and considering an arbitrary associated data, the *Auth* is computed. Then it is added to the encrypted image as a *tag*. The receiver gets $CT = C_1\, C_2\, ...\, C_m\, T$. After computing the message *M*, tag T^* is recomputed. If $T^*=T$, the cipher image is valid; else if T*≠T, the cipher image is invalid and the received image is dropped.

IV. Statistical Evaluation Methods and The Results

This section analyzes the security of encrypted images with five statistical methods in order to measure encryption efficiency. The five statistical quantities are Number of Pixels Change Rate (NPCR), Unified Average Changed Intensity (UACI), Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and the correlation between two horizontal adjacent pixels [17].

The results illustrate that NPCR and UACI quantities of the *AE* mode were satisfactory in comparison with other modes. In our work, the encryption algorithms, the security analysis and the test methods for evaluations, were implemented and designed using the MATLAB 7 environment, on a machine with Intel(R) Core(TM)2 Duo ~1.8GHz CPU and a 2-GB of RAM. The tests are applied on a grayscale standard image, named *Lena*, which has been in use since 1973. As shown in Fig. (4), the pattern of encrypted images is invisible.

A. Differences between Plain and Encrypted Images

NPCR measures the number of different pixels between the original and the encrypted images, Equation (1). UACI, computed according to Equation (2), measures the average intensity of differences between the plain and cipher images. To resist differential cryptanalysis, the values of NPCR and UACI should be large enough. If the two images, i.e. the original and the encrypted ones, are the same, these quantitative criteria will be zero. If the two images are completely different, these will be 100% [17]-[18]:

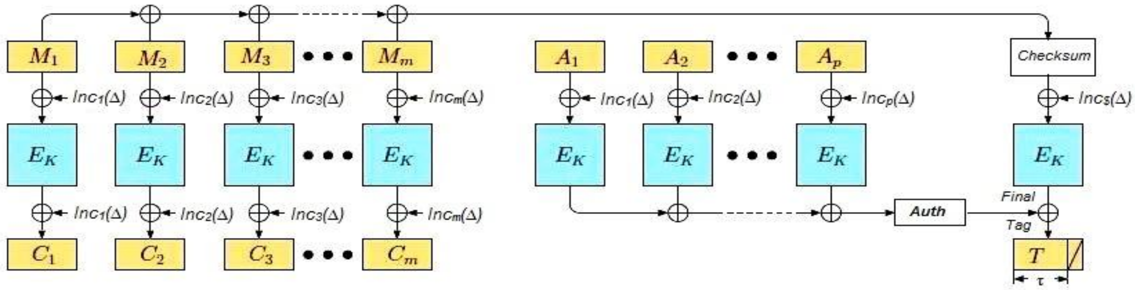


Fig.2. Overview of the Encryption and Authentication Parts of OCB.

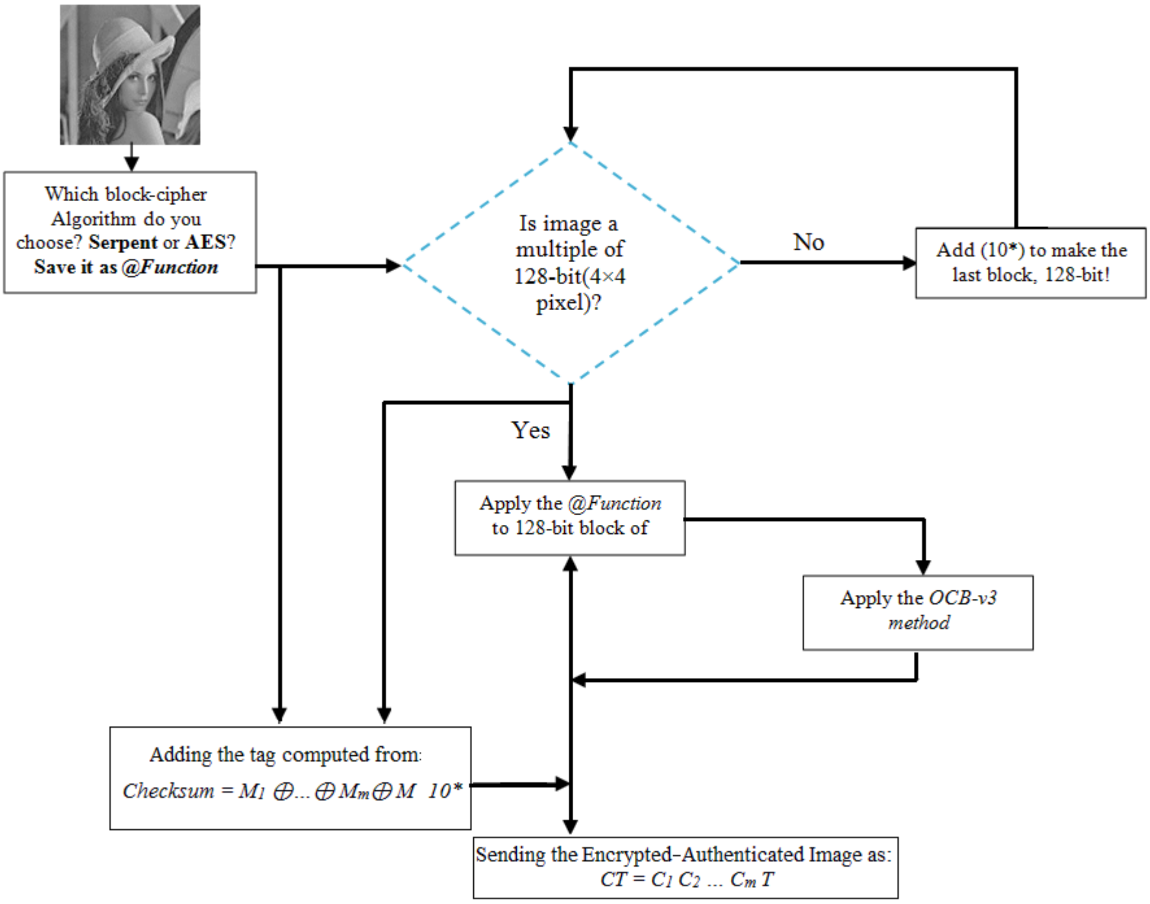
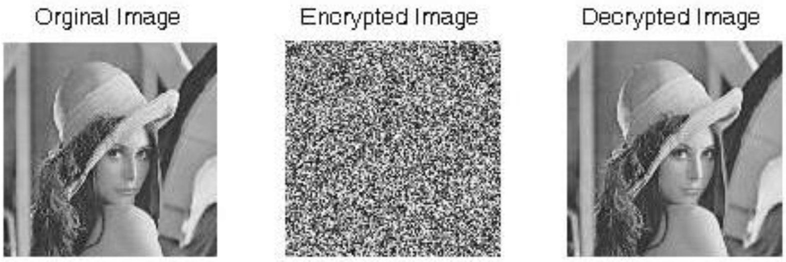
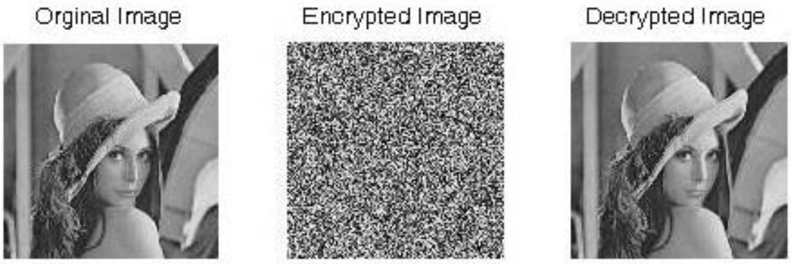

Which block-cipher Algorithm do you choose? Serpent or AES? Save it as @Function
Is image a multiple of 128-bit(4×4 pixel)?
No
Add (10*) to make the last block, 128-bit!
Yes
Apply the @Function to 128-bit block of
Apply the OCB-v3 method
Adding the tag computed from:
Checksum = M1 ⊕... ⊕Mm⊕M 10*
Sending the Encrypted-Authenticated Image as:
CT = C1 C2 ... Cm T

Fig.3. Image Encryption Flowchart with OCB-v3 with any block Cipher Algorithm.



(a) Image Encryption by OCB-v3 and AES Block Cipher



(b) Image Encryption by OCB-v3 and Serpent Block Cipher

Fig.4. The 128 × 128 gray-scale Lena image: Original, Encrypted and Decrypted Images with: a) AES Algorithm, b) Serpent Algorithm.

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} D(i,j)}{m \times n} \times 100\% \qquad (1)$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} \left|A(i,j) - B(i,j)\right|}{255 \times m \times n} \times 100\% \qquad (2)$$

where *A* is the original image and *B* is the encryption of *A*. Both images are of size m×n. The value of 255 denotes the largest supported pixel value that is compatible with the encrypted image format. *D(i, j)* is defined in Equation (3) [18]:

$$D(i,j) = \begin{cases} 0, A(i,j) = B(i,j) \\ 1, A(i,j) \neq B(i,j) \end{cases} \qquad (3)$$

PSNR is the ratio of maximum intensity value of the original image (MAX_I) to maximum intensity value of the encrypted image. By having 8 bits for each pixel, 256 (from 0 to 255) values can be represented; therefore, the MAX_I value is 255. In the case of 6 bits for each pixel, MAX_I value is decreased to 63. The PSNR ratio computes reduction of signal quality. Equation (4) is used to compute this ratio in Decibels [19]:

$$\mathrm{PSNR} = 10.\log_{10} {}^{MAX_I^2}\!/_{MSE} \qquad (4)$$

where Mean Square Error (MSE) [19] is computed as Equation (5). The power of two has a larger influence on the variations and makes them larger; however, the effect of small differences is reduced.

$$\mathrm{MSE} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} \left[A(i,j) - B(i,j)\right]^2}{m \times n} \qquad (5)$$

Tables (2) and (3) show the values in different modes of operation with both AES and Serpent. According to the evaluations, horizontal correlation coefficients of all modes are almost zero; therefore, the encrypted images are uncorrelated. The results show that a slight change in the original image results in a great change in the encrypted image, implying that the OCB algorithm is sufficiently capable of resisting attacks. By observing NPCR and UACI, it is realized that the NPCR is near 100% and the UACI is about 30%. In addition, it is noticed that OCB with AES can disrupt the unified intensity of the image, as in the other modes. MSE is an estimation of the quality of cipher image—it is always non-negative, and values further from zero show a better performance. The MSE values in Tables (2) and (3) indicate that OCB with AES scheme acts better than OFB mode. PSNR is a widely used mathematical metric for digital image and shows the visual quality of an encrypted image in comparison with the plain image. Larger values are indicative of better quality; a small PSNR value reveals the difficulty in retrieving the plain image from the cipher image, without the secret key. PSNR value of OCB is near the maximum PSNR value, which is obtained for OFB mode. Therefore, a more considerable drop in quality is observed compared to the other modes.

The encryption times shown in Table (4) indicate that OCB mode displays good performance. The Serpent algorithm requires a larger amount of time, which is predictable because the 32-round Serpent encryption process takes more time than the 10-round AES encryption process. Among different modes, both OFB and CFB last more than other modes. Although the OCB mode also has an authentication process, it takes slightly longer to execute; nevertheless, its encryption time approaches that of CTR.

B. Histogram

A histogram is a graph that shows the distribution of data values or the repetition of each pixel in an image [20]. The histogram of an encrypted image shows that the correlation between two adjacent pixels, in all directions, is insignificant and there are various pixels in the encrypted image; therefore, the attacker can hardly attain any crucial information. As depicted in Fig. (5), the histogram of the original image does not contain different values; for example, a pixel with a value of 250 is not observed. However, the encrypted image does have an extensive range of pixels, showing diffusion in encryption algorithm. In other words, histogram of the encrypted image is uniform and considerably different from the histogram of original image. Hence, the opponents cannot perform any statistical analysis attack on the encrypted image since no worthwhile information can be inferred. As shown in Fig. (5), it can be concluded that the OCB mode does possess the confusion and diffusion characteristics.

C. Correlation Coefficient

Correlation Coefficient determines the degree of similarity and the dependence between two adjacent variables in a certain direction [21]. It is employed as a remarkable parameter to evaluate the quality of a cryptosystem [22]. In this paper, the correlation between two horizontally adjacent pixels is tested, because the image is horizontally broken into blocks. If the correlation coefficient is near zero, it is incomplete and the images are uncorrelated. If the result is in the (0,1) interval, the correlation is incomplete and direct. However, if the result is in (-1,0) interval, the correlation is incomplete and indirect. The horizontal correlation of the original *Lena* image is 0.86756, which shows a direct correlation between the adjacent pixels of this image. The results in the last columns of Tables (2) and (3) depict that the correlation of the *AE* scheme with Serpent block cipher algorithm, is significantly approaching the OFB scheme, more robust than other modes. By operating AES block cipher with the OCB mode, the correlation of adjacent pixels is close to the other modes. As shown in Fig. (6), the OCB mode with AES block cipher can produce an enciphered image with uncorrelated adjacent pixels in comparison with plain image.

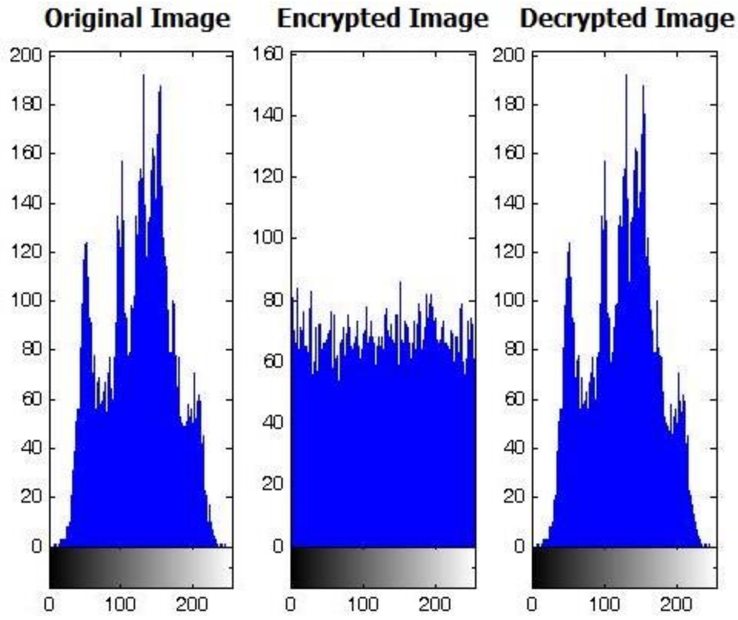


Fig.5. Histogram of Original Image and Encrypted One with Serpent block Cipher and the OCB Mode.

Table 2. AES Tests with Different Modes

Block Cipher Mode of Operation	*AES*				
	NPCR%	*UACI%*	*MSE*	*PSNR*	*Correlation*
ECB	99.68	30.46	8.835×10^3	8.6688	0.01250
CBC	99.68	30.64	8.985×10^3	8.5956	0.00940
CFB	99.51	29.98	8.734×10^3	8.7188	-0.00799
OFB	99.68	29.96	8.673×10^3	8.7492	0.00536
CTR	99.54	30.26	8.816×10^3	8.6776	-0.00389
OCB	99.59	30.06	8.723×10^3	8.7244	0.00984

Table 3. Serpent Tests with Different Modes

Block Cipher Mode of Operation	*Serpent*				
	NPCR%	*UACI%*	*MSE*	*PSNR*	*Correlation*
ECB	99.76	30.12	8.699×10^3	8.7358	0.022068
CBC	99.58	30.10	8.801×10^3	8.6858	0.009201
CFB	99.61	30.12	8.764×10^3	8.7039	0.014448
OFB	99.66	30.56	9.058×10^3	8.5608	-0.00265
CTR	99.68	30.24	8.832×10^3	8.6703	-0.03392
OCB	99.51	30.08	8.726×10^3	8.7226	0.007053

Table 4. Execution Time of AES & Serpent Algorithm with Different Modes

Block Cipher Mode of Operation	*AES*	*Serpent*
ECB	0 min 29.626450 sec	0 min 43.11353 sec
CBC	0 min 29.459779 sec	0 min 45.496993 sec
CFB	4 min 34.098195 sec	11 min 38.630156 sec
OFB	4 min 27.822738 sec	11 min 47.059977 sec
CTR	0 min 21.903469 sec	0 min 42.935126 sec
OCB	0 min 31.39594 sec	1 min 11.038356 sec

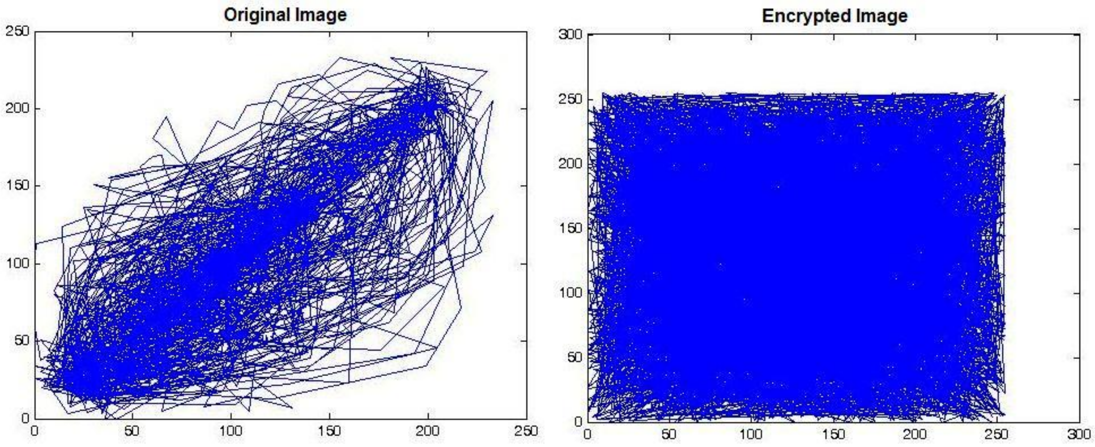


Fig.6. Correlation Coefficients of the Original and Encrypted Images with AES Block Cipher and the OCB Mode

V. Conclusion

In image-based applications, encryption alone does not provide sufficient security. To improve security, dedicated authenticated-encryption (*AE*) modes are designed. In this paper, an *AE* block cipher mode of operation, namely OCB-v3, was successfully evaluated, which provides both confidentiality and integrity security services for image encryption and authentication. This mode has the speed and parallelism characteristics as in CTR confidentiality mode of operation. In this paper, we evaluated OCB authentication-encryption and confidentiality modes of operation, with AES and Serpent block cipher algorithms, to encipher a digital image. Evaluations confirmed the good performance of this mode in comparison with other encryption modes of operation.

In the future, other schemes can also be used to support a non-repudiation service while transmitting multimedia. By exploiting both visual cryptography and standard ciphering methods, a double layer security in transmitting images in the network will be obtained. *AE* methods can also be implemented on FPGA boards for image-based industrial purposes.

Acknowledgments

The authors would like to thank Zahra Fattaholmanan for her suggestions and feedback.

References

[1] W. Stallings, “Cryptography and network security principles and practices,” 5th ed., NY, USA: Prentice Hall, ISBN-13: 0-13-609704-9, pp. 145-214, 2010.

[2] B. Schneier, “Applied cryptography: protocols, algorithms, and source code in C,” Wiley Computing Publishing, John Wiley & Sons, Inc., pp. 210-230, Jan. 2007.

[3] Federal Information Processing Standards Publication 197 (FIPS197), “Announcing the advanced encryption standard (AES),” Nov. 2001, [Online]. Available: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [Accessed July 2017]

[4] R. Anderson, E. Biham and L. Knudsen, “Serpent: a

proposal for the advanced encryption standard," *NIST AES Proposal*, July 2012. [Online]. Available at: http://www.cl.cam.ac.uk/~rja14/serpent.html [Accessed July 2017]

[5] J. Job, V. Naresh, and K. Chandrasekaran, "A modified secure version of the Telegram protocol (MTProto)," *IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT)*, 2015.

[6] S.H. Kamali, R. Shakerian, M. Hedayati and M. Rahmani, "A new modified version of advanced encryption standard based algorithm for image encryption," *Electronics and Information Engineering (ICEIE)*, 2010.

[7] M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki, "A modified AES based algorithm for image encryption," *International Journal of Computer Science and Engineering*, vol. 1, no. 1, pp.70-75, 2007.

[8] A. Jolfaei, and A. Mirghadri, "Image encryption using chaos and block cipher," *Computer and Information Science*, vol. 4, no. 1, p.172, 2010.

[9] W. Bielecki, D. Burak. "Parallelization of the AES Algorithm," in *Proc. of the 4th WSEAS Int. Conf. on Information Security*, Communications and Computers, Tenerife, Spain, pp. 224-228, 2005.

[10] T. Krovetz, and P. Rogaway, "The OCB authenticated-encryption algorithm," May 2014. Online Available at: http://tools.ietf.org/html/rfc7253 [Accessed July 2017]

[11] T. Krovetz and P. Rogaway, "The software performance of authenticated-encryption modes," in *18th international workshop in Fast Software Encryption* (FSE2011), Springer, 2011, pp. 306-327.

[12] P. Rogaway, "Method and apparatus for facilitating efficient authenticated encryption," U.S. Patent 8,321,675, Nov. 2012.

[13] M. Bellare, T. Kohno, and C. Namprempre, "Authenticated encryption in SSH: provably fixing the SSH binary packet protocol," in *Proc. of the 9th ACM conference on Computer and communications security*, pp. 1-11, 2002.

[14] K. Winstein and H. Balakrishnan, "Mosh: an interactive remote shell for mobile clients," in *Proc. of the 2012 USENIX Annual Technical Conference*, pp. 177–182, Boston, MA, 2012.

[15] D. Maimut and R. Reyhanitabar, "Authenticated Encryption: Toward Next-Generation Algorithms," in *IEEE Security & Privacy*, vol. 12, no. 2, pp. 70-72, Mar. 2014.

[16] R.C. Gonzalez, R.E. Woods and S.L. Eddins, "Digital image processing using MATLAB", 2nd ed., New Jersey, Prentice Hall, 2009.

[17] L. Yan and R. YE, "Image encryption using novel mappings over GF (2^n)," *Studies in Mathematical Sciences*, vol. 2, no. 1, pp. 96-106, 2011.

[18] R. Ye, and W. Zhou, "A Chaos-based image encryption scheme using 3D skew tent map and coupled map lattice," *I. J. Computer Network and Information Security,* no. 1, pp. 38-44, 2012.

[19] Z. Liu, et al. "Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains," *Optics Communications*, vol. 284, no. 1, pp.123-128, 2011.

[20] C.K. Huang, C.W. Liao, S. L. Hsu, and Y. C. Jeng. "Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system," *Telecommunication Systems,* vol. 52, no. 2, pp. 563-571, 2013.

[21] S. Etemadi Borujeni, and M. Eshghi, "Chaotic image encryption design using Tompkins-Paige algorithm," *Mathematical Problems in Engineering*, 2009.

[22] N. Ahmed, H.M.S. Asif, and G. Saleem, "A benchmark for performance evaluation and security assessment of image encryption schemes," *I. J. Computer Network and Information Security*, vol.8, no.12, pp.18-29, 2016.

Authors' Profiles

Narges Mehran received her B.S. degree in Computer Hardware Engineering (2012), and her M.S. in Computer Architecture (2016) from University of Isfahan. Her current research interests include Future Internet Architectures with an emphasis on Caching, and Cryptographic Protocols on the Internet.

Mohammad Reza Khayyambashi received the B.S. degree in Computer Hardware Engineering from Tehran University, Tehran, Iran in 1987. He received his M.S. in Computer Architecture from Sharif University of Technology (SUT), Tehran, Iran in 1990. He got his Ph.D. in Computer Engineering, Distributed Systems from University of Newcastle upon Tyne, Newcastle upon Tyne, England in 2006. He is now an associate professor at the Faculty of Computing Engineering, University of Isfahan, Isfahan, Iran. His research interests include Distributed Systems, Computer Networks, Fault Tolerance in Software Defined Network (SDN), Social Networks, and E-Commerce.

How to cite this paper: Narges Mehran, Mohammad Reza Khayyambashi,"Performance Evaluation of Authentication-Encryption and Confidentiality Block Cipher Modes of Operation on Digital Image", International Journal of Computer Network and Information Security(IJCNIS), Vol.9, No.9, pp.30-37, 2017.DOI: 10.5815/ijcnis.2017.09.04