Channel Encryption in Wireless Camera Sensor Network

Amr M. Kishk, Nagy W. Messiha, Nawal A. Elfishawy, Abdelrahman A. Elkafs, and Ahmed H. Madian

***Abstract*—Data security is one of the greatest problems in Wireless Camera Sensor Network. Many encryption algorithms are used for encryption purposes. A new encryption algorithm is proposed in this paper. It depends on three secret parameters and four key-updating processes. It is compared with other encryption algorithm depending on key-updating beside Chaos encryption algorithm. Correlation Coefficient (CC), Spatial Frequency (SF), processing time, and histogram are the metrics used for comparison purpose.**

***Index Terms*—Chaos encryption algorithm, chaos block cipher for wireless sensor network, key-updating, s-boxes.**

I. Introduction

The network security is an important objective in the design and implementation of Wireless Camera Sensor Network (WCSN), since components designed without security can become a point of attack [1]. Hacking is one of the greatest problems in WCSN. Many encryption algorithms have been used to prevent the outside attacks to eavesdrop or prevent the data to be transferred to the end-user safely and correctly .Image encryption is defined as mathematical processes that map the plain image to an unintelligible cipher image [2]. In WCSN, the power consumption restricts the design of the encryption algorithms. The year of 2000, chaos started to recognize this security problem widely and obtained an application for secure communication. It is the greatest achievement in chaotic cryptography [3]. Chaotic maps have attracted the attention of cryptographers as a result of the following fundamental properties: deterministic, unpredictable, random, and disorderly [4]. Unfortunately, many of them have been found to have security problems from the cryptographically point of view [5].

Key-updating is one of the tools used to enhance the security level. In Wireless Local Area Network (WLAN), an algorithm proposed to encrypt the entities during the authentication process [6] and another one to encrypt the data during data exchange processing [7] based on key-updating . In WSN, Chaos Block Cipher for Wireless Sensor Network (CBCW) proposed to satisfy some requirements of WSN depending on the key-updating [8]. This algorithm is cryptanalyzed and some comments upon this algorithm are presented.

Manuscript received November 20, 2013; revised January 6, 2014. This work was supported in part by Nuclear Research Centre members of Egyptian Atomic Energy Authority (EAEA) and Faculty members of Faculty Electronics Engineering (FEE), Egypt.

Amr M. Kishk, Abdelrahman A. Elkafs, and Ahmed H. Madian are with Egyptian Atomic Energy Authority, Cairo 13759, Egypt. (e-mail: amr.kishk@yahoo.com, alkafas@yahoo.com, ah_madian@hotmail.com).

Nagy W .Messiha and Nawal A .Elfishawy are with the Faculty of Electronics Engineering, Elmounfya University, Menouf 32951, Egypt (e-mail: dr.nagy_wadie@hotmail.com, nelfishawy@hotmail.com).

In this paper a new encryption algorithm is proposed and based on key-updating process .Because of a great number of multimedia encryption schemes based on chaos, Section II will describe chaos-based algorithm and CBCW. Section III will explain the new encryption algorithm .The results and conclusions in this paper a new encryption algorithm is proposed and based on key-updating process. Because of a great number of multimedia encryption schemes based on chaos, Section II will describe chaos-based algorithm and CBCW. Section III will explain the new encryption algorithm .The results and conclusions will be written down at the end of this paper in Section IV and Section V respectively.

II. Related Work

A. Chaos-Based Algorithm

Chaos is a definite pseudo-random process produced in nonlinear dynamical systems .Logistic map is a kind of chaotic system that was researched early and used widely in many occasions for its high-level efficiency and simplicity . The use of chaos for image encoding yields to three types of keys; these keys may be used together or separately, in order to enhance the privacy. They are the external parameter μ, the initial state x_0, and the number of iterations [9]. In general, the chaotic system model is given as in (1), where: x_n is a real number in the range [0, 1], μ is in the range [3.56 , 4], and if we repeatedly apply it to an initial condition x_0, then we will get a chaotic sequence $\{x_n : n=0, 1, 2\ldots\}$.

$$x_{n+1} = \mu x_n(1-x_n) \tag{1}$$

B. Chaos Block Cipher for Wireless Sensor Network

In Chaos Block Cipher for Wireless Sensor Network (CBCW), the key-updating is based on updating the encryption key K_j with each pixel which is decomposed as four 8-bits sub-keys K_{j1}, K_{j2}, K_{j3}, and K_{j4}, that are used in 4-round iterations of feistel structure, respectively [10].

The scheme could be cryptanalyzed by utilizing differential cryptanalysis theory [10]. The author depends on an assumption that the same key is used to encrypt all plain images although the key is updated with each pixel. So the cryptanalysis assumption needed to be reanalyzed again by assumption of key-updating with each pixel. CBCW is compared with the new algorithm in Section VI. Both algorithms depend on the same idea by different ways (key-updating).

III. Proposed Encryption Algorithm

The proposed encryption algorithm depends on three secret parameters: Initial key K_o, S_1-Box, and S_2-Box. Their contents

DOI: 10.7763/JACN.2014.V2.95

are secrets and random integer values between 0 and 255. K_o size depends on the size of plain image. If the size of plain image is ($M \times N$) in 2-D, then K_o size is Max (M, N). S_1-box and S_2-box size is (16×16). These S-Boxes are used for key-updating processes. For example, if the input value applied to S_1-Box is 8D in a hexadecimal format, then the input value will be mapped to the value of row 8 and column D in S_1-Box.

The encryption of a plain image depends on four keys generated from K_o. These four keys are N_1, N_2, K_1, and K_2. N_1 and N_2 are used for horizontal and vertical circular shift processes respectively. N_1 and N_2 sizes are M and N respectively. They are generated from K_o. The first M-contents of K_o, denoted by N_m, are applied to S_1-Box to generate N_1 while The first N-contents of K_o, denoted by N_n, are applied to S_2-Box to generate N_2. Their contents are updated for each next new image but, the previous contents of N_1 and N_2 will be XORed with N_m and N_n before applying to S_1-Box and S_2-Box respectively .

K_1 and K_2 are used for encryption processes. K_1 is generated from N_2 while K_2 is generated from N_1, and both N_1 and N_2 are updated with each new image .By the same way, N_2 is mapped to K_1 through S_1-Box and N_1 is mapped to K_2 through S_2-Box. K_1 and K_2 contents are updated with each row and column of the processed image but, the previous contents of K_1 and K_2 will be XORed with N_2 and N_1 contents before applying to S_1-Box and S_2-Box respectively. The encryption procedure is shown in Fig. 1. The decryption procedure is the inverse of the encryption procedure and is shown in Fig. 2. The encryption procedure is as follows:

1) The pixels positions in each row of the selected plain image, I_o, from n-plain images P_o will be horizontal right-circular shift (H.R.circular shift) according to the value of element of N_1 having the same index .For example, if the forth index of N_1 is 38 then the contents of row number 4 will be circular shifted by 38.
   Note: in the decryption process, the horizontal left-circular shift (H.L circular shift) is used instead of horizontal Right-circular shift (H.R circular shift).
2) Each row of the resulted image, I_a^r where r refers to row, will be XORed with K_1, and K_1 is updated with each row as shown later.
3) Third, the pixels positions in each column of the resulted image, I_b^c where c refers to column, will be vertical down-circular shift (V.D. circular shift) according to the value of element of N_2 having the same index .
   Note: in the decryption process, the vertical up-circular shift (V.U. circular shift) is used instead of vertical down- circular shift (V.D. circular shift).
4) Each column of the resulted image I_d^c will be XORed with K_2, and K_2 is updated with each column as shown later. The encrypted image, I_f, will be gotten at the end of these operations.
5) The next plain image will be encrypted by updated N_1 and updated N_2 in continuity with the previous image, and updated K_1 and updated K_2 with the last row and column of the previous image. The updating of K_1 and K_2 depends on updated N_1, updated N_2, last updated K_1, and last updated K_2. K_1 and K_2 are updated with each row and column respectively, while N_1 and N_2 are updated with each new image.

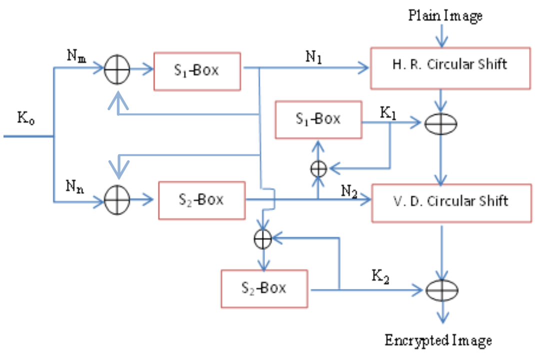

Fig. 1. Proposed encryption algorithm.

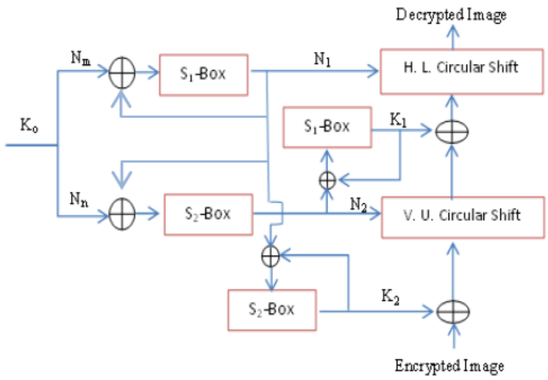

Fig. 2. Proposed decryption algorithm.

IV. Results

The new encryption algorithm depends on three secret parameters: K_o, S_1-Box, and S_2-Box. These parameters are generated randomly. Mandrill and Lena images of size 512×512 are used as plain images. The metrics used to test the encryption algorithm are the Correlation Coefficient (CC) [11], Spatial Frequency (SF) [12], and the histogram.

The CC of the encrypted image is measured as shown in Fig. 3. SF of the new algorithm is shown in Fig. 4. The various values of CC and SF ensure the success of the key-updating to hide the contents of the plain image in each time. The histogram of the encrypted images is measured as in Fig. 5. The same plain image is encrypted 30-times to ensure the success of the key-updating. The time elapsed for the encryption processing is 18.2019 sec.

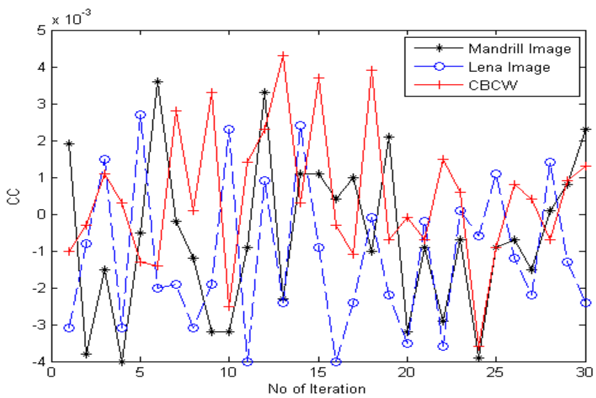

Fig. 3. CC comparison.

Chaos encryption algorithm does not depend on key-updating process. It used a constant encryption key for all plain images. Its CC and SF are measured for the encrypted Mandrill image. Their values are CC =0.1151 and SF = 114.2156. Chaos processing time for the encryption procedures is 7.5 sec.

CBCW is one of the algorithms which depend on key-updating. The CC of the encrypted Mandrill image is measured as shown in Fig. 3 in comparison with the new encryption algorithm for both Mandrill and Lena images. SF is compared with the new algorithm as shown in Fig. 4. Various values of CC and SF of the encrypted images for the same plain-image are due to the key-updating. The processing time of the CBCW during encryption process is 190.538 sec. The reason of longer processing time of CBCW is the key-updating with each pixel in the image. The new algorithm is compared with Chaos and CBCW encryption algorithms as in Table I.

TABLE I: ALGORITHMS COMPARISON

	New Algorithm	CBCW	CHAOS
Nº of Secrets Parameters	**Three** :Initial Key, S1-Box, S2-Box	Initial Key	μ, X_o ,n
Nº of Key-updating Process	**Four**	One	Nothing
Nº of Multiplications Process	**Nothing**	**Huge nº of multiplications** because It depends on key-updating with each pixel.	It depends on the length of Index generation.
CC	**Various and better than CBCW and Chaos.**	Various.	Constant
SF	Various.	Various and better than New algorithm and Chaos.	Constant
Encryption Processing time	18.2019 sec	190.538 sec	7.5 sec

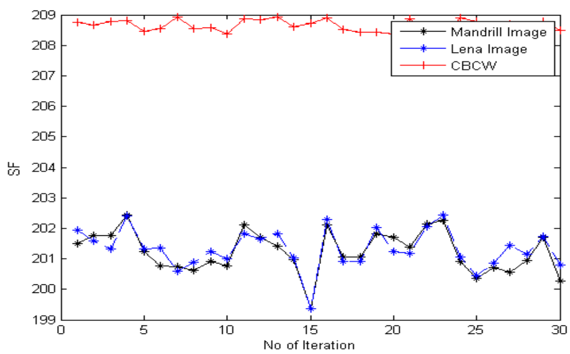

Fig. 4. SF comparison.

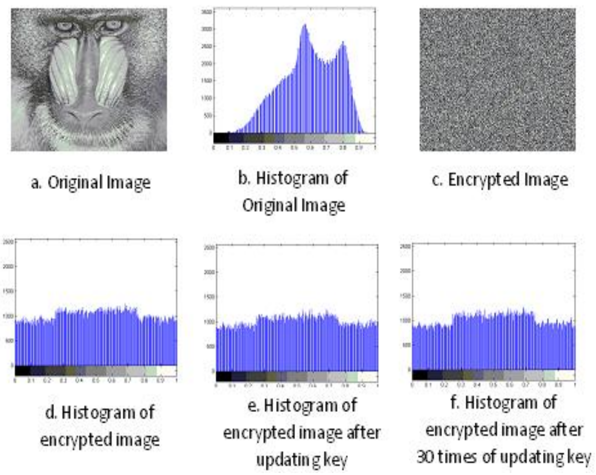

Fig. 5. Encryption processes for the same plain image to ensure key updating process.

V. CONCLUSIONS

The huge numbers of sensors in WCSN gives a great chance for the hackers to crack the transmitted data. The key-updating is one of the tools used to add more difficulties to crack the encrypted data during the transmission. Both new algorithm and CBCW depend on key-updating processes. Various values of metrics for the encrypted images for the same plain image ensure the effectiveness of the key-updating. The new algorithm depends on three secret parameters :initial key, S1-box, and S2-box. It has four key-updating processes rather than CBCW that depends on one key-updating process. It scores less processing time than CBCW.

REFERENCES

[1] J. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Communications of the ACM*, vol. 47, no. 6, pp. 53-57, 2004.

[2] A. Nashwan, S. Abdulfatah, and A. Ibrahim, "New chaos-based image encryption scheme for RGB components of color image," *Computer Science and Engineering*, vol. 2, no. 5, pp. 77-85, 2012.

[3] A. Babu and K. Singh, "Performance evaluation of chaotic encryption technique," *American Journal of Applied Sciences*, vol. 10, no 1, pp. 35-41, 2013.

[4] S. Al-Maadeed, A. Al-Ali, and T. Abdalla, "A new chaos-based image-encryption and compression algorithm," *Journal of Electrical and Computer Engineering*, vol. 2012, 2012.

[5] L. Chengqig, L. Shujun, and L. Kwok-Tung, "Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps," *Communication Nonlinear Science Numerical Simulation*, vol. 16, no. 2, pp. 837-843, 2011.

[6] A. Kishk, N. Messiha, N. Ayad , N. Elfeshawy, and F. Abdel-Samie, "Enhancement in the identities-exchange process during the authentication process," *International Journal of Computer and Network Security*, vol. 1, no. 3, pp. 34-37, 2009.

[7] A. Kishk, N. Messiha, N. Ayad, N. Elfeshawy, and F. Abdel-Samie, "Fast and flexible symmetrical encryption algorithm based on key-updating," presented at the National Radio Science Conference, 2010.

[8] S. Chen, X. Zhong, and Z. Wu, "Block chaos cipher for wireless sensor network," *Science in China Series F: Information Sciences*, vol. 51, no. 8, pp. 1055-1063, August 2008.

[9] R. Liu and X. Tian, "New algorithm for color image encryption using chaotic map and spatial bit-level permutation," *Journal of Theoretical and Applied Information Technology*, vol. 43, no. 1, September 2012.

[10] J. Yang, D. Xiao, and T. Xiang, "Cryptanalysis of a chaos block cipher for wireless sensor network," *Communication Nonlinear Science Numerical Simulation*, vol. 16, no. 2, pp. 844-850, 2011.

[11] N. El-Fishawy and O. Zaid, "Quality of encryption measurement of bitmap images with RC6, MRC6, and Rijndael block cipher

algorithms," *International Journal of Network Security*, vol. 5, no. 3, pp. 241–251, November 2007.

[12] Y. Zheng, E. Essock, B. Hansen, and A. Haun, "A new metric based on extended spatial frequency and its application to DWT based fusion algorithms," *Information Fusion*, vol. 8, no. 2, pp. 177–192, 2007.

Nagy Wadie Messiha received the B.S. in Electrical Engineering Telecommunication Department, Ein Shams University, Cairo, Egypt, June 1965, and M.S. in telecommunication engineering, Helwan University, Cairo, Egypt, 1973, and the german (Dipl. Ing.) and (Dr. Ing.) from University of Stuttgart, in 1978 and 1981 respectively. From 1981 to 1987. Currently, he is a professor at the Department of Communication Engineering, Menoufia University, Menouf, Egypt. His research interested is traffic modeling and performance enhancement in communication and computer networks, cognetive networks, and network security.

Nawal El-Fishawy received the PhD degree in mobile communications in the faculty of Electronic Eng., Menoufia University, Menouf, Egypt, in collaboration with Southampton University in 1991. Now she is a professor at Computer Science and Engineering Dept., Faculty of Electronic Eng. Her research interest includes computer communication networks with emphasis on protocol design, traffic modeling and performance evaluation of broadband networks and multiple access control protocols for wireless communications systems and networks. Now she directed her research interests to the developments of security over wireless communications networks (mobile communications, WLAN, Bluetooth), VOIP, and encryption algorithms.

AbdelRahman A. Elkafas received the B.S. in Nuclear engineering, Alexandria University, alexandria, Egypt, June 1980, and M.S. in analysis of residual heat removal systems in PWR-NPPs, Alexandria University, Alexandria, Egypt, June 1990, and Ph.D in safety analysis of an expert reactor protection system in PWR-NPPs, Alexandria University, Alexandria, Egypt, June 1996. He was an associate professor in 2002, Nuclear Research Centre, Egypt. Currently, he is a professor in the Nuclear Research Centre, Egypt. He is interested in safe operation of nuclear reactors, automatic control of research reactors, and physical protection systems (design and evaluation).

Ahmed H. Madian was born in 1975. He received the B.Sc. degree with honors, the M.Sc., and the Ph.D. degrees in electronics and communications from Cairo University, Cairo, Egypt, in 1997, 2001, and 2007, respectively. He is currently an associate professor in the Electronics Engineering Department, Micro-Electronics Design Center, Egyptian Atomic Energy Authority, and Cairo, Egypt. Dr. Madian served as assistant professor in the Electronics Engineering Department, Faculty of Information Engineering and Technology, German University in Cairo (GUC) from 2008 till now. Dr. Madian is the co-author of 20 research papers in different scientific journals and has served as program and publication chair for many conferences. He is a senior member of IEEE and co-founder for the IEEE Robotics Chapter-Egypt section (best chapter on Region 8 for 2013). His research interests are in circuit theory; low-voltage analog CMOS circuit design, current-mode analog signal processing, digital VLSI, system security and mixed/digital applications on field programmable gate arrays.

Amr M. Kishk was born in Ashmun city, Egypt, on July 11, 1981. He received the B.S. in electronics and electrical communication engineering, Menoufia University, Menouf, Egypt, 2003, and M.S. in data security in wireless local area network, Menoufia University, Menouf, Egypt, 2010. Now, he works as a lecturer assistant in Egyptian Atomic Energy Authority (EAEA), Cairo, Egypt. His research interests include wireless sensor network (WSN), data security in wireless network.