Channel Encryption in Wireless Camera Sensor Network

Amr M. Kishk, Nagy W. Messiha, Nawal A. Elfishawy, Abdelrahman A. Elkaf, 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.

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 x₀, and the number of iterations [9]. In general, the chaotic system model is given as in (1), where: x₀ 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 x₀, then we will get a chaotic sequence \( \{x_n : n=0, 1, 2,\ldots\} \).

\[ x_{n+1} = \mu x_n (1 - x_n) \]  
(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 \( K_0 \), \( S_1 \)-Box, and \( S_2 \)-Box. Their contents
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 \(\text{Max}(M, N)\). \(S_1\)-box and \(S_2\)-box size is \((16 \times 16)\). 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 \(N_1\) 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 \(N_1\) and \(N_2\) 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.

\[\text{Note: in the decryption process, the horizontal left-circular shift (H.L circular shift) is used instead of horizontal Right-circular shift (H.R circular shift).}\]

2) Each row of the resulted image, \(I'_r\), 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, \(I'_c\), 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.

\[\text{Note: in the decryption process, the vertical up-circular shift (V.U. circular shift) is used instead of vertical down-circular shift (V.D. circular shift).}\]

4) Each column of the resulted image \(I'_d\) will be XORed with \(K_2\), and \(K_2\) is updated with each column as shown later. The encrypted image, \(I_e\), 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.

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.
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 process. It used a constant encryption key for all plain images. Its CC and SF are measured as shown in Fig. 3 in comparison with the new encryption algorithm for both Mandrill and Lena images. SF is compared with Chaos and CBCW encryption algorithms as shown in Fig. 4.

V. CONCLUSIONS

The huge numbers of sensors in WSNs give a great advantage 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


![Fig. 4. SF comparison.](image1)

![Fig. 5. Encryption processes for the same plain image to ensure key updating process.](image2)

### TABLE I: ALGORITHMS COMPARISON

<table>
<thead>
<tr>
<th>Parameters</th>
<th>New Algorithm</th>
<th>CBCW</th>
<th>CHAOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>N° of Secrets Process</td>
<td>Three: Initial Key, S1-Box, S2-Box</td>
<td>Initial Key</td>
<td>μ, Xₜ, n</td>
</tr>
<tr>
<td>N° of Key-updating Process</td>
<td>Four</td>
<td>One</td>
<td>Nothing</td>
</tr>
<tr>
<td>N° of Multiplications Process</td>
<td>Nothing</td>
<td>Huge n² of multiplications because it depends on key-updating with each pixel</td>
<td>It depends on the length of Index generation.</td>
</tr>
<tr>
<td>CC</td>
<td>Various and better than CBCW and Chaos.</td>
<td>Various.</td>
<td>Constant</td>
</tr>
<tr>
<td>SF</td>
<td>Various. and better than New algorithm and Chaos.</td>
<td></td>
<td>Constant</td>
</tr>
<tr>
<td>Encryption Processing time</td>
<td>18.209 sec</td>
<td>190.538 sec</td>
<td>7.5 sec</td>
</tr>
</tbody>
</table>


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 interest is traffic modeling and performance enhancement in communication and computer networks, cognitive 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 interest 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.