Secure Encryption for Wireless Multimedia Sensors Network

Amina Msolli
Laboratory of Micro-Optoelectronics and
Nanostructures (LMON),
Faculty of Sciences,
Monastir University,
Tunisia

Abdelhamid Helali
Laboratory of Micro-Optoelectronics and
Nanostructures (LMON),
Faculty of Sciences,
Monastir University,
Tunisia

Haythem Ameur
Laboratory of Micro-Optoelectronics and
Nanostructures (LMON),
Faculty of Sciences,
Monastir University,
Tunisia

Hassen Maaref
Laboratory of Micro-Optoelectronics and
Nanostructures (LMON),
Faculty of Sciences,
Monastir University,
Tunisia

***Abstract*—The security in wireless multimedia sensor network is a crucial challenge engendered by environmental, material constraint requirements and the energy consumption. Standard encryption algorithms do not agree with the real-time applications on this network. One of the solutions to the challenges mentioned above is to maintain the safety and reduce the energy consumption. In this article, a new approach with a high-energy efficiency, a high level of security and a big robustness against the statistics and differential attacks is presented in this paper. The new approach called Shift-AES admits simple operations such as the substitution, the transposition by or-exclusive and shift. It keeps the principle of Shannon for the diffusion and the confusion. Some criteria to measure the performances of the approach such as the visual inspection, histogram analysis, entropy images, the correlation of two adjacent pixels, the analysis against differential attacks, and the analysis of performance at the level run-time and throughput are successfully realized. The experimental evaluation of the proposed algorithm Shift-AES proves that the algorithm is ideal for wireless multimedia sensor network. With a satisfactory level of security, best term timeliness and throughput of transmission, compared with the AES standard encryption algorithm, this approach allows us to increase the lifetime of the network.**

Keywords*—*Wireless Multimedia Sensor Network (WMSN); image encryption; Shift-AES; security

I. Introduction

The wireless sensor network (WSN) has evolved very quickly in the scientific research field during the last years. This type of network is the result of a fusion of two poles of the modern computing: the embarked systems and the wireless communications. A wireless sensor network is established by a set of sensor nodes. These sensor nodes are deployed in a geographical zone in a random way. The environmental data is obtained, harvested and transmitted with nodes towards the sink in an autonomous way. The communication between the user and the network takes place through a satellite and the internet.

A node sensor is specified by a sensor unit, a processing unit, and a wireless transmission unit. All these units are fed by a battery. Therefore, in a wireless sensor network, every node captures the physical quantities (such as temperature, humidity, heat, power ...), transforms them into a digital greatness to attribute all data processing and storage and then transmitted.

The field of sensor network applications is more and more widened due to the technical developments facing the domains of electronics and telecommunications. These developments include the reduction in the size and cost of the sensors, as well as the expansion of the ranges of available sensors (movement, temperature ...) and the evolution of the wireless communication mediums, besides civil applications (environment, buildings, industries, transport, medical, commercial, etc.). Indeed, the sensor network applications can be military (intrusion detection, localization fighters, enemy position, weapons, etc. on a battlefield, underwater ...) or the development of other low-cost devices such as micro-cameras expanded areas of wireless sensor network application.

Thus a new generation of the network named Wireless Multimedia Sensor Network has appeared (WMSN) [1]-[3]. In this type of network, nodes are equipped with multimedia devices such as cameras, wireless microphones: often deployed in harsh environments and the energy limitation are factors which make the wireless sensor networks very vulnerable again and subject to several types of attacks, hence the safety in the WSN being of crucial importance. Consequently, the symmetric key encryption algorithm with weak power consumption is necessary for this type of network. Contrary to the public key, encryption algorithm is a fundamental technology and is used widely in the world. But it has its material limits such as the memory and the battery power, cannot therefore be applied to sensor networks [4].

One of the solutions to the challenges mentioned above to preserve the safety and reduce energy consumption presented in this paper. Is presented in this paper: a new approach with high-energy efficiency, a high level of security and a big robustness against the statistics and differential attacks. The new approach called Shift-AES admits simple operations as the substitution, the transposition by or-exclusive and shift. It maintains the principle of Shannon for the diffusion and the confusion. Certain criteria to measure the performances of the approach such as the visual inspection, histogram analysis, entropy images, the correlation of two adjacent pixels, the analysis against differential attacks, and the analysis of performance at the level run-time and throughput are successfully carried out. The experimental evaluation of the proposed algorithm Shift-AES proves that the algorithm is ideal for wireless multimedia sensor network. Because it has a satisfactory level of safety, better term in speed of execution and throughput of transmission, compared with the AES standard encryption algorithm. Hence this approach allows us to increase the lifetime of the network.

The rest of the paper is planned in five parts. First, a bibliographical study on related work for cryptographic algorithms is presented. Afterwards a brief description of the symmetric key cryptographic algorithm AES in Section III. Then, the proposed approach (Shift-AES) is described in Section IV. Section V discusses the results of experimental performances and security analysis, and finally the paper is concluded.

II. Related Works

Cryptography is a very vast domain allowing information data protection to ensure the confidentiality, the integrity and the authenticity. This protection is made by means of a secret or a key. Depending on keys, there are two encryption techniques the public key encryption, and the secret key encryption. The public key encryption, called also the asymmetric cryptography, consists of two keys, the public key is of use to the encryption and the private key ensures the decryption. The use of the asymmetric cryptography allows the abolition of the problem of secure transmission of key. But it remains less successful compared with symmetric cryptography because it consumes more processing times and a large key size for the same level of security.

The private key encryption, also called symmetric cryptography, uses a single key for the encryption and the decryption of the data. It admits less mathematical problems. This encryption mode is established of two main types: by stream and by block.

Cryptography by stream: The encryption of the data is made character-by-character or bit by bit. This type has for advantages the insensitivity in the phenomenon of the propagation of the errors, because as if one erroneous bit there is only. But it puts a secure channel for key distribution, a large size of keys similar to the size of data.

Cryptography by block: The data divide into blocks according to the size of the key. As well as the encryption of the data bases itself on a model of repeated conscript round, where from the result of a block depends on the previous result.

This paper is focused on the symmetric cryptography by block because it is more adapted to the wireless sensor network. The most popular algorithms of this approach are DES, the Triple DES, the AES and the Blowfish.

A. *Data Encryption Standard (DES)*

DES (Data Encryption Standard) [5] is an American national standard data encryption adapted from the American National Standards Institute (ANSI) in the 1977.

The operation principle of DES is based on 16 rounds. The encryption algorithm operates on blocks of 64 bits, an initial key size of 64 bits contains only 56 bits effective [6] and other 8-bits of parity allow errors to be detected and do not enter the encryption process. First step, the input undergoes a permutation then a fraction in two blocks of 32 bits. The encryption undergoes in the round process. At each round, both halves of 32-bit input and a sub-key undergo several transformations of permutation, substitution and or-exclusive. There are six various permutation operations used in the key extension and the encryption process. Furthermore, the decryption process is similar to the encryption, except that the inverse order of round sub-key is taken.

Nowadays numerous registered attacks show the weaknesses of DES and its insecurity [7], [8].

B. *Triple DES (3-DES)*

During the development of key safeties, the triple-DES algorithm replaces the DES to correct their weaknesses. It was standardized for the norm EFT of the ANSI X9.17 [5], ISO 8732 and PEM for the key management. The Triple DES algorithm is equivalent to DES when admitting three equal keys ($k_1 = k_2 = k_3$). The length of the key is 168 bits or each key with a length of 56 bits. The principle of the triple DES algorithm is based on the encryption and the decoding by every key according to the following Equation (1):

$$\text{Ciphertext} = DES_{k_3}\{\, DES_{k_2}^{-1}\{\, DES_{k_1}(Plaintext)\}\} \quad (1)$$

where $DES_{k_i}$is the DES encryption with (a) key k_i with i = 1 and 3, and $DES_{k_2}^{-1}$is the decryption by using the key k_2.

C. *Advanced Encryption Standard (AES)*

The AES (Advanced Encryption Standard) [9], [10], is a new standard of symmetric encryption by block developed to replace the former Data Encryption Standard (DES) which was published by the National Institute of Standards and Technology (NIST) of the United States as Federal Information Processing Standard Pub 197 (FIPS 197) on 26 November 2001. After a standardization process of five years, the NIST adopted the Rijndael algorithm as AES. The AES algorithm is composed of three main parts: encryption, decryption and key extension. Extension Key generates a schedule Key derived from the secret key which is used in the encryption and decryption procedures.

The AES algorithm is used to realize four different simple transformations applied in succession to the bits of data blocks, in a number of iterations, called rounds. These transformations are: SubBytes, ShiftRows, MixColumns and AddRoundKey represented more exactly in the following section. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks operating on 128 bits. The number of rounds depends on the corresponding cryptographic keys 10, 12 and 14.

D. Blowfish

The Blowfish encryption algorithm [11] was proposed by Bruce Schneier in the 1993. The Blowfish algorithm uses a key of variable length (32 bits - 448 bits) with a 64-bit block size.

The Blowfish algorithm is constituted by logical or-exclusive operation between halves of the inverted blocks of input, the sub-keys and a function. This function consists of four S-box connected between them by operations of or-exclusive and two modulo 2^{32} additions. This process is repeated 16 times, except in the last round, replaced by a simple reversal block and XOR.

In the same direction of the symmetric cryptography by block, there may be mentioned other algorithms such as: IDEA [12], RC 6 [13], TEA [14], SEA [15], etc.

III. Advanced Encryption Standard (AES)

The AES is an encryption algorithm used to protect electronic data. AES in special peculiarities adapted for WSN applications [16]-[19]. Consequently, the secure AES implementation can greatly influence the nodes of networks resources extremely limited.

AES is based on a matrix N_b x N_k of bytes referred to as ("state"). The number of lines N_b is equal to the size of the data block / 32, which equals 4. Similarly for the key, the number of columns is N_k = key length / 32. The algorithm undergoes various transformations. These transformations (sub Bytes, Shift Rows, Mix Columns and add Round Key) run in a number of iterations proportional to the size of the key.

1) *SubByte:* SubByte is a non-linear substitution function of byte in GF (2^8). Every byte of the State is replaced by another one by means of a substitution table (S-box). S-box which is derived from the multiplicative inverse of a finite field.

2) *ShiftRows:* ShiftRows is a permutation function. Each line of the State is moving towards the left by an offset equal to the line number.

3) *MixColumns*: MixColumns is a mixing function. This processing operates in the State column by column. The four bytes in each column of the State are combined by using an invertible linear transformation. This processing returns the column as a polynomial of four words over GF (2^8). The MixColumns transformation in charge of multiplying a constant matrix with the State as shown in the following equation (2), which is equivalent to GF (2^8) to multiply the fixed polynomials with the polynomial of the column modulo $x^4 + 1$.

$$\begin{pmatrix} b_{0,x} \\ b_{1,x} \\ b_{2,x} \\ b_{3,x} \end{pmatrix} = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} a_{0,x} \\ a_{1,x} \\ a_{2,x} \\ a_{3,x} \end{pmatrix} \qquad (2)$$

4) *AddRoundKey:* AddRoundKey is an XOR function. For each round, a sub-key is diverted from the main key in the help Rijndael key schedule, XORed with the State matrix.

During the decryption, the AES algorithm reverses the encryption by performing the inverse transformation by taking the block of 128 bits of encrypted image and to convert it to an image light by the application of the four opposite operations. AddRoundKey is the same for the encryption and the decryption. However, the other three functions are reversed in the decryption process: inverse SubBytes (InvSubBytes), inverse ShiftRows (InvShiftRows), and inverse MixColumns (InvMixColumns).

IV. Proposed Approach (Shift-AES)

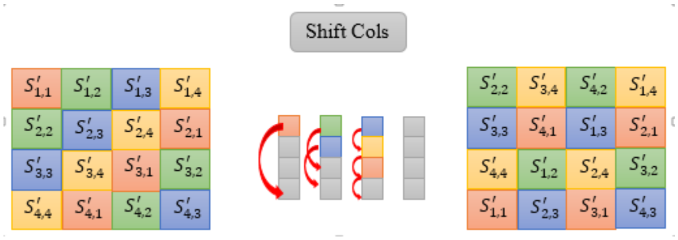
Wireless multimedia sensor network allows defining several constraints. The constraints of the multimedia are the real-time execution, the quantity of enormous information, etc. One of the constraint of the network is the physical constraint of the sensor node or a supply of battery and a small memory size. The proposed approach reconciles between the various constraints.

After the exhaustive research on the AES, it is noted that the MixColumns processing consumes more processing time because it counts on the operations of addition and multiplication. This transformation indicates a weakness in the wireless multimedia sensors network. The aim of the intervention is to minimize as much as possible the run time, whereby decreasing the arithmetic operations.

The idea of the approach is based on the AES algorithm with shifts instead of the arithmetic operations named the Shift-AES. In this approach, the MixColumns process of the AES algorithm is replaced by another shift transformation of columns. The principle of shift makes an order of shift

α: shift for the first column
ɳ: shift for the second
β: shift for the third
ɣ: shift for the fourth column,

To determine the security in the cryptography, it is necessary to keep the capacities of confusion and diffusion by the best choice of the shift parameters (α, ɳ, β, ɣ). The experimental study below allows us to select the exact parameter values, as shown in Fig. 1. Therefore, this approach maintains the principle of Shannon for the diffusion and better reduces the execution time.



$S'_{1,1}$	$S'_{1,2}$	$S'_{1,3}$	$S'_{1,4}$
$S'_{2,2}$	$S'_{2,3}$	$S'_{2,4}$	$S'_{2,1}$
$S'_{3,3}$	$S'_{3,4}$	$S'_{3,1}$	$S'_{3,2}$
$S'_{4,4}$	$S'_{4,1}$	$S'_{4,2}$	$S'_{4,3}$

$S'_{2,2}$	$S'_{3,4}$	$S'_{4,2}$	$S'_{1,4}$
$S'_{3,3}$	$S'_{4,1}$	$S'_{1,3}$	$S'_{2,1}$
$S'_{4,4}$	$S'_{1,2}$	$S'_{2,4}$	$S'_{3,2}$
$S'_{1,1}$	$S'_{2,3}$	$S'_{3,1}$	$S'_{4,3}$

Fig. 1. The Transformation Shift-Cols after the whole processing SubByte and ShiftRows of AES.

After the application of Shift-AES, a better earning in run time is achieved. To improve the entropy of the approach, a modification of the general structure of Shift-AES is realized. ShiftCols transformation enhances the various transformations in the process of iterations of encryption. Tables 1 and 2 represent the algorithm of the general structure of the Shift-AES approach and Shift-Cols.

TABLE. I. STRUCTURE OF THE PROPOSÉD CIPHER ALGORITHM SHIFT-AES

```
Algorithm 1 : Pseudo code cipher Shift-AES
Input : Clair image, key
Output  : cipher image
Procedure :
S_Box ⟵ Initialize Shift-AES
Expansion key ⟵ Initialize Shift-AES
image ⟵ Initialize Shift-AES
l ⟵ Number of image blocks initialize Shift-AES
k ⟵ image size initialize par Shift-AES
For l = 1 to k do
        State ⟵ image(l)
        State ⟵ AddRoundKey(State, key)
        For r=1 to (Nr-1) do
                State ⟵ ShiftCols(State)
                State ⟵ SubBytes(State, S_Box)
                State ⟵ ShiftRows(State)
                State ⟵ AddRoundKey(State, key)
        End for
        State ⟵ SubBytes(State, S_Box)
        State ⟵ ShiftRows(State)
        State ⟵ AddRoundKey(State, key)
        C ⟵ State(l)
End for
Cipher_Image =C
```

TABLE. II. STRUCTURE OF SHIFT-COLS ALGORITHM

```
Algorithm 2 : Process ShiftCols (state)
Input : state, offset_Shift
Output : state
Procedure :

Nb=4
Offset_Shift=1
For col = 0 to 3 do
        Offset_Shift (col) ⟵ Offset-Shift + col
        State(row, col) ⟵ State(((row + offset_Shift(col)) mod Nb),
        row)
End for
```

V. EXPERIMENTAL PERFORMANCE RESULTS AND ANALYSIS OF SAFETY

In this section, a study of experimental performance is defined to verify the results stemming from the statistical analysis of the security and to prove the efficiency of the proposed approach. The experimental result involves the collection of all the test standard images required for the simulation trial. Then, the new Shit-AES approach is feigned and tested on the standard images to estimate their performances. The evaluation parameters [20] are made by the histogram, entropy image, the correlation, its resistance against the differential attack and the run time. These quantitative parameters are the most suitable and the most used for the analysis.

A. *Experimental results*

The simulation of several test standard images of different size and dimension allows us to observe a total invisibility in the coded image, with the parameters α = 3, ɳ = 2, β = 1, ɣ = 0 shifts below (choice of parameters is below). The simulation results of the Shift-AES approach are very satisfactory. The visual inspection of the images in Fig. 2 allows to count the proposed Shift-AES approach, because it is effective in hiding the information contained in them.

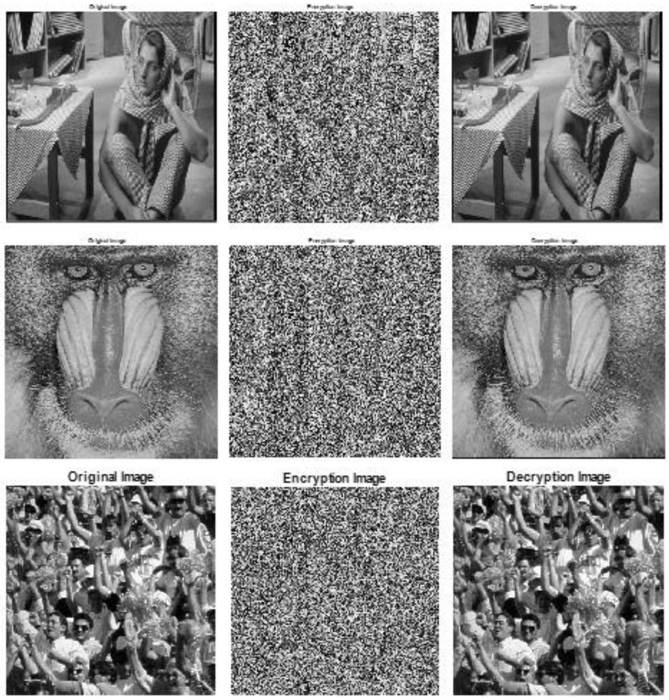


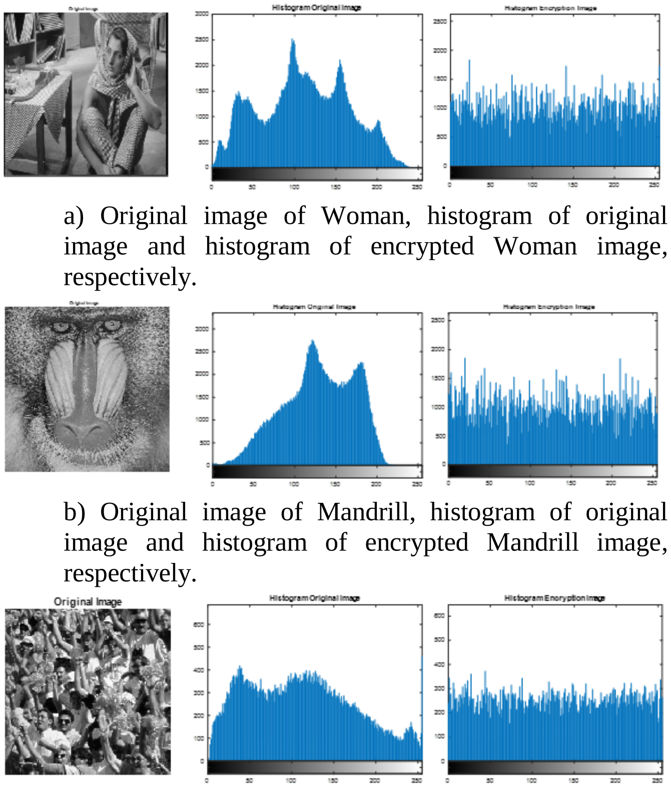
Fig. 2. Encryption and decryption of the standard images (Woman, Mandrill, and Crowd respectively) with the proposed Shift-AES approach.

B. *Statistical analysis of the security*

The statistical analysis of the security provided the analysis of the histogram, the entropy and the correlation of the original and encrypted images to have the efficiency of the proposed approach. So, it analyzes the robustness of approach against any statistical and differential attack by the parameters NPCR (Number of Pixels Exchange Rate) and UACI (Unified Average Changing Intensity).

1) Histogram of the image: The histogram of the image is the most recently used way to prove the effect of the proposed encryption algorithm. If the histogram of encrypted image does not contain a statistical similarity to the original image, then, it avoids the data leakage to the opponent. The histogram illustrates the random distribution of pixels in a digital image by the number of pixels at each level of gray intensity.

The simulation of the selected standard images Woman, Mandrill, and Crowd respectively, of various dimensions 256x256 and 512x512 by Shit-AES algorithm allows to calculate the histograms of the original images and encrypted, as shown in Fig. 3. The comparison of analysis histogram shows a total difference in the content of pixels intensity between the original image as well as the encrypted images. The histograms of the coded images are almost uniform and appreciably different compared with the histograms of the original images. These rather adequate results hide the information during transmission and defend against the statistical attacks.



a) Original image of Woman, histogram of original image and histogram of encrypted Woman image, respectively.

b) Original image of Mandrill, histogram of original image and histogram of encrypted Mandrill image, respectively.

c) Original image of Crowd, histogram of original image and histogram of encrypted Crowd image respectively

Fig. 3. Histogram of the standard images (Woman, Mandrill, and Crowd respectively) of original and encrypted with the proposed AES-Shift approach.

2) Image entropy: The digital images are a combination of discrete values of the pixels, organized together to form a visual perception of the image. The entropy allows to analyze the information contained in random data. The entropy of an image calculated by the Equation (3):

$$E = -\sum_{i=1}^{N} X_i \,(log2(X_i)) \tag{3}$$

Where E is the entropy of the image expressed in bits, X is the probability of the level of intensity in the image and N is the total number of intensity levels.

The ideal value of the entropy of a random source of 2^8 intensity levels is eight according to (3). In fact, the entropy of the encrypted images has to be approximately eight. The measures of entropy are presented in Table 1. The result proves that the entropy of the encrypted images is around eight.

Table 3 indicates the percentage of entropy between the entropy of encrypted image and the original one. The average value of entropy is 12.13% for standard images with different extensions and dimensions.

TABLE. III. IMAGE ENTROPY

Images	Dimensions	Entropy of the images		
		original	***encrypted***	***%***
lena.jpg	256x256	7.5691	7.9247	4.6980
cameraman.tif	256x256	7.0097	7.7758	10.9291
peppers.png	512x384	6.9917	7.8668	12.5162
football.jpg	320x256	6.7134	7.8466	16.8796
pout.tif	240x291	5.7599	7.6106	32.1307
rice.png	256x256	7.0115	7.9402	13.2453
woman.jpg	512x512	7.6631	7.9638	3.9239
mandrill.png	512x512	7.3579	7.9550	8.1150
The average value of the entropy		7.0095	7.8604	12.1392

3) Correlation of adjacent pixels: Another parameter analyzes the safety and studies the performance of the new approach, it is the correlation of adjacent pixels in vertical and horizontal direction.

Equations (4) and (5) allows to calculate the coefficients of vertical and horizontal correlations of the original image and the encrypted image.

$$cov(x,y) = E\big(x - E(x)\big)\big(y - E(y)\big) \tag{4}$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \tag{5}$$

Where x and y are the gray level values of two adjacent pixels in the image. The results are mentioned in Table 4. The correlation values show a difference between the original and encrypted image. For example, in vertical direction, the original image admitted a correlation coefficient of about 0.9894 while in the coded image the value is equal to 0.0577.

TABLE. IV. COMPARISON CORRELATION COEFFICIENT VERTICAL AND HORIZONTAL

Direction	original Image	encrypted Image
Vertical	0.9894	0.0577
Horizontal	0.9995	0.5740

There is another procedure to calculate the correlation of two adjacent pixels. This method selects 1024 pairs of two adjacent pixels in vertical direction of a standard image Lena 256x256 size. The numerical calculation is made by the discrete Equations (6), (7) and (8);

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (6)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2 \qquad (7)$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))\,(y_i - E(y)) \qquad (8)$$

Fig. 4 illustrates a distribution of the correlation coefficient of two adjacent pixels in the original and encrypted image. The simulation results show that the coefficients are strongly correlated with the original image, while in the encrypted image the coefficients are scattered, that is to say, a negligible correlation in the encrypted image.

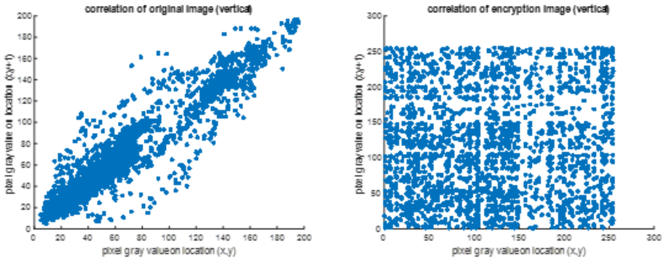


Fig. 4. Correlation coefficient of two adjacent pixels to the original and encrypted image respectively.

4) Differential attack: Among the principle of security in the wireless communication is the confidentiality of the information during transmission against attacks.

To guarantee the safety in the proposed Shift-AES approach, it is necessary to verify the resistance against differential attacks through the common parameters: NPCR and UACI [21]. These parameters test the influence of the change of a single pixel in the original image on the encrypted image.

NPCR (Number of Pixels Exchange Rate) and UACI (Unified Average Changing Intensity) are defined as follows by (9) and (10):

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\% \qquad (9)$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{C_1(i,j) - C_2(i,j)}{225}\right] \times 100\% \qquad (10)$$

Where W and H are the C_1 and C_2 dimensions. C_1 and C_2 are two corresponding encrypted images to the original image and that modified by a single pixel. Thus, D is a bipolar matrix determined from C_1 and C_2.

In the simulation, the Lena original image on a dimension 256x256 is used as an image test to estimate the proposed Shift-AES algorithm according to the influence of change of a pixel to 256 gray levels. The obtained quantitative results are NPCR = 99.63% and UACI=30.71%. These quantitative and qualitative results imply that a small change in the original image will be translated by a significant modification in the encrypted image, whereby the effectiveness of Shift-AES has the resistance against differential attacks.

a) Choice of shift parameters

The choice of the offsets is realized to obtain the good performance. A study on the shift is summarized in Table 5. The study is done on a cameraman image of 256x256 size. The six combinations of the shift values represent all the existing possibilities.

The evaluation of the proposed AES-Shift algorithm is successfully realized by some statistical criteria well known as the statistical analysis and differential attack parameters. Shift-AES is designated as an ideal and robust algorithm in the wireless multimedia sensor network. Because it demonstrates a robust against the statistical, differential attack and an efficiency in the histogram, entropy and the correlation of adjacent pixel analysis.

5) Performance of approach Shift-AES:

Execution time: The search for security in the wireless multimedia sensor network imposes crucial another issue as the energy consumption which must be considered during the multimedia real-time application and under the constraints of hardware sensor node. In this sense it is necessary to try always to decrease the run time most rather possible.

In this section, the evaluation of the Shift-AES algorithm is performed by comparing the execution time of the standard AES algorithm with the proposed Shift-AES algorithm, through several image tests of different sizes on disk and by comparing the encryption time in relation to different key sizes.

Fig. 5 shows that the execution time of the Shift-AES approach is more successful and shorter compared with the time of the AES algorithm, in the different sizes of images. This result supports the efficiency of Shift-AES in the wireless multimedia sensor network.

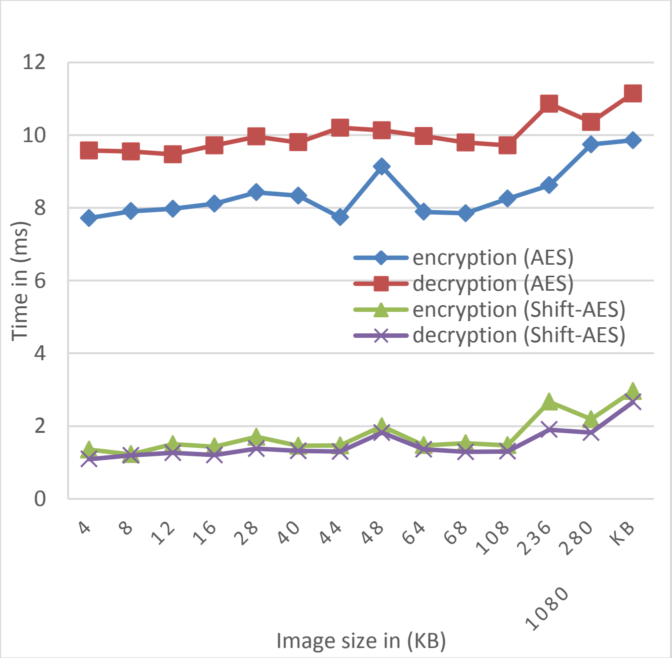


Fig. 5. Comparison of execution time in ms between AES and Shift-AES for different image sizes on disk.

Furthermore, to evaluate the performance of the similarity between the energy consumption and the safety. Simulations are made between the different key sizes of security and the execution time for a standard image Lena of size 256x256. The simulation (Fig. 6) gives an execution time at the Lena image encryption of approximately 7 ms, 8 ms and 10 ms for key size 128 bits, 192 bits and 256 bits respectively, for the AES algorithm while in the Shift-AES approach the run time is approximately 1.3 ms, 1.4 ms and 1.5 ms. Fig. 7 specifies that the proposed approach called Shift-AES consumes less energy than that AES. Hence this approach increases the lifetime of the wireless multimedia sensor network.

TABLE. V. CHOICE OF SHIFT PARAMETERS FOR COLUMNS

	α=0, η=1,(low) β=2, γ=3	**α=1, η=3,(low) β=1, γ=3**	**α=1,(low) η=2,(up) β=3,(low) γ=1(up)**	**α=3, η=2,(low) β=1, γ=0**	**α=0, η=2,(low) β=0, γ=2**	**α=1,(up) η=2,(up) β=2,(low) γ=1(low)**
Entropy (cipher image)	7.7758	7.7572	7.7490	**7.7829**	7.7671	7.7566
NPCR (%) UACI (%)	99.55 **29.88**	99.48 30.84	99.53 31.15	**99.79** 31.51	99.72 30.70	99.68 32
horizontal Correlation (cipher image)	0.6116	**0.1870**	0.3854	0.3034	0.4641	0.4219

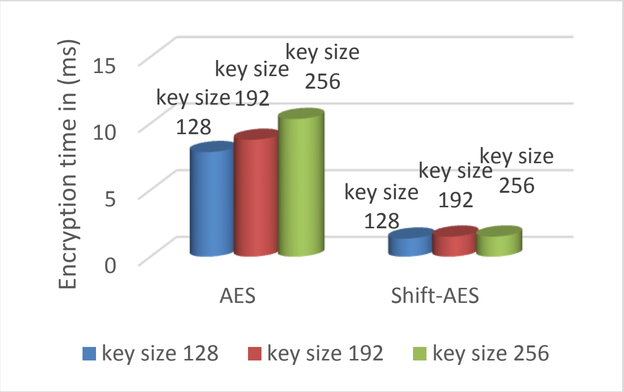


Fig. 6. Comparison encryption time between AES and AES-Shift for the different key sizes.

Throughput: The throughput is another parameter that can examine the performance of the approach. The throughput is similar at the speed of encryption and decryption. The throughput is the division between the global data size to be encrypted and the time total execution of encryption so of deciphering, it is expressed in megabytes per second.

Fig. 7 explains the evolution of throughput according to the size of images. Shift-AES appeared better to favor that the AES algorithm especially for the large data size, because if the throughput increases then the energy consumption reduces.

VI. CONCLUSION

This paper proposes a new approach named Shift-AES with simple operations for the real-time applications in wireless multimedia sensor network. An experimental performance is defined to verify the results of the analysis and prove the effectiveness of the proposed Shift-AES approach. The simulation of several standard image tests of different size and dimension allows us to observe:

5) A total invisibility in the encrypted image.

6) A difference in the content of pixel intensity between the original image and encrypted, in the histogram.

7) A percentage average value of the entropy of the images is about 12.13%, expresses the resistance against the attacks statistics.

8) A random distribution of correlation coefficients of two adjacent pixels in the encrypted image.

9) The robustness against the differential attacks appeared to the NPCR = 99.63% and UACI=30.71% .

10) A rapidity of execution equal to 1.3 ms instead of 7 ms compared with the standard algorithm.

11) And an increase of throughput and speed of transmission.

This rapidity and increase of throughput allow to decrease the energy consumption. Consequently, increase the lifetime of the network. More energy high efficiency, a high level of security and robustness against statistics and differential attacks.

These results are quite adequate to conclude that Shift-AES is a very satisfying and ideal algorithm for the wireless multimedia sensor network.

Future works focus to apply this new approach in various modes of encryption known to have the safest mode and implement the proposed approach on sensors nodes to estimate the energy consumption.

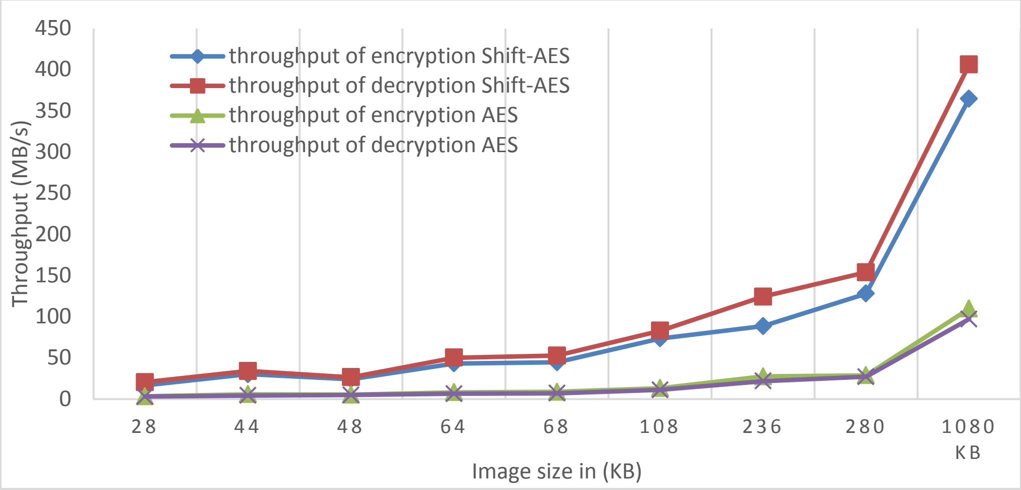


Fig. 7. Comparison of throughput between AES and Shift-AES.

References

[1] Ian F. Akyildiz, Tommaso Melodia, Kaushik R. Chowdhury, "A Survey On Wireless Multimedia Sensor Networks", Computer Networks (ELSEVIER), Vol 51, Pages 921-960, 2007.

[2] K.Kalaivani, B.R. Sivakumar, "Surey On Multimedia Data Security", International Jounal Of Modeling and Optimization, Vol 2, February 2012.

[3] Viral Patel, Krunal Panchal, "Survey on Security in Multimedia Traffic in Wireless Sensor Network", International Journal of Engineering Development and Research (IJEDR), vol. 2, pp. 3906-3910, Dec 2014.

[4] Yun Zhou, Yuguang Fang, Yanchao Zhang , "Securing wireless sensor network s: a survey," IEEE Communications Surveys and Tutorials, vol. 10, No.3, 3rd Quarter, 2008.

[5] Standard, Data Encryption. "Data encryption standard." Federal Information Processing Standards Publication, 1999.

[6] DataEncryptionStandard(DES).Available:http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[7] W.Stallings, "Cryptography and Network Security 4th Ed," Prentice Hall, PP. 58-309, 2005

[8] Coppersmith, D. "The Data Encryption Standard (DES) and Its Strength against Attacks."I BM Journal of Research and Development, pp. 243 -250 May 1994

[9] FIP 197: Announ cing the Advanced Encryption Standard , Nov . 26,. 200 I. http://csrc.nist.gov/publications/fips/fipsI97/fips-197.pdf

[10] J. Daemen and V. Rijmen , "AES Proposal : Rijndael, AES Algorithm", Submission, September 3, 1999.

[11] Schneier, B., "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings (Dec. 1993), Lecture Notes in Computer Science (LNCS), Springer-Verlag, Vol. 809, pp. 191-204, 1993, ISBN 3-540-58108-1.

[12] X. Lai and J. Massey, "A proposal for a new block encryption standard", In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, 1990.

[13] R.L. pavan, M.J.B. Robshaw, R.Sidney, and Y.L. Yin. "The RC6 Block Cipher". Ver 1.1, August 1998.

[14] Wheeler, D.J., & Needham, R.J, "TEA, a tiny encryption algorithm", In Fast Software Encryption – Proceedings of the 2nd International Workshop,1008, (1994)

[15] Abdelfatah A. Yahya and Ayman M. Abdalla, "A Shuffle Image-Encryption Algorithm", Journal of Computer Science, Vol 4, p. 999-1002, 2008

[16] Ankit Srivastava, Dr. N. Revathi Venkataraman, "AES-128 Performance in Tinyos with CBC Algorithm (WSN) ," International Journal of Engineering Research and Development, vol. 7, pp. 40-49, June 2013.

[17] Ortega Otero, Tse.J, Manohar.R. , "AES Hardware-Software Co-design in WSN," Asynchronous Circuits and Systems (ASYNC), 2015 21st IEEE International Symposium on, pp. 85 – 92, May 2015.

[18] P.D. Khambre,S.S.Sambhare, P.S. Chavan, "Secure Data in Wireless Sensor Network via AES (Advanced Encryption Standard)", International Journal of Computer Science and Information Technologies, vol. 3, 2012.

[19] Hyeopgeon Lee, Kyounghwa Lee, Yongtae Shin, "Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs", Advanced Communication Technology (ICACT), 2010 The 12th International Conference on (Volume:1), pp. 243 – 248, Feb 2010.

[20] Abdulkarim Amer Shtewi, Bahaa Eldin M. Hasan, Abd El Fatah .A. Hegazy," An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems", International Journal of Computer Science and Network Security, Vol 10(2), Pages 226-232, February 2010.

[21] Yue Wu, Joseph P. Noonan, , and Sos Agaian, "NPCR and UACI Randomness Tests for Image Encryption", Journal of Selected Areas in Telecommunications (JSAT),pp.31-38, April 2011.