Proceedings of Engineering & Technology (PET)
pp. 107-113

Symmetric encryption algorithm image for wireless multimedia sensor network

Amina Msolli, Abdelhamid Helali,
Laboratory of Micro-Optoelectronics and Nanostructures (LMON),
Faculty of Sciences
Monastir University, Tunisia
amina.msolli@yahoo.fr

Hassen Maaref
Laboratory of Micro-Optoelectronics and Nanostructures (LMON),
Faculty of Sciences
Monastir, Tunisia
Abdelhamid.helali@isimm.rnu.tn

***Abstract*—The need for security with multimedia applications becomes increasingly important for protected personal life. This need appears mandatory in the wireless sensor network for secure data transmission due to the hostile deployment environment. Thus the material constraint sensor nodes orients us to optimize the standard encryption technique that consumes more time and materials. In this paper, we have focused on symmetric AES encryption algorithm and we have intervened to make it compatible with the sensor node nature and increase the lifetime of the wireless sensor network. Our used algorithm was to encrypt the image in real time while reducing the execution time. Measuring the performance of encryption and decryption on the execution time, the histogram and the entropy of the image.**

Keywords—AES; WSN; wireless multimedia sensor network (WMSN); image;

I. INTRODUCTION

Spouses renovations of microelectronics and wireless transmission technologies have been produced at reasonable cost micro-sensors. These micro-sensors are appointed sensor nodes. They are deployed in a random manner in a field corresponding to the grounds of interest to collect and transmit environmental data to one or more collection points through wireless links and autonomously, form a Wireless Sensor Network (WSN). The data collected by the nodes are routed through a multi-hop routing to a node considered as a "collection point", known as sink. The latter can be connected to the network user (via Internet, satellite, etc.).

A sensor node includes a sensor unit responsible for capturing physical parameters (heat, humidity, vibrations, radiation ...) and transforming them into digital quantities, in an acquisition unit. Along with a data processing and storage unit and a wireless transmission one. A battery powers these three units.

The field of sensor network applications is increasingly expanded thanks to technical developments facing the fields of electronics and telecommunications. These changes include the reduction of size and cost of the sensors, as well as the expansion of product available sensors lines (movement, temperature ...) and the evolution of wireless communication media. In addition to civilian applications (environmental, building, industrial, transportation, medical, commercial, etc.). Indeed, sensor networks applications may be used in the military field (intrusion detection, combatants localization, enemy position, vehicles, weapons, etc. on a battlefield, underwater, in space, on the ground…). For applications based on the image, such as still images, video and audio streams, we use wireless sensor network in which nodes are equipped with multimedia devices such as cameras, wireless microphones. Hence the Wireless Multimedia Sensor Network (WMSN) [1, 2, 3].

Often, in harsh environments and power limitation are factors that make them very vulnerable wireless sensor networks and subject of several types of attacks. Where security in WSN is of crucial importance. Therefore, symmetric encryption algorithm with low energy consumption key is required for this type of network. Unlike Public-key encryption algorithm which is a fundamental technology which is worldwide used. But it has its physical limitations such as memory and battery power, so it is not applied to sensor networks [4].

In this paper, we have investigated the AES algorithm which is a symmetrical encryption algorithm and we have worked on it to make it compatible with the sensor node nature and to increase the lifespan of the wireless sensor network. The algorithm used to encrypt the real time image while reducing the execution time. In addition, we have measured encryption and decryption performance on the execution time, the histogram and the entropy of the image.

The rest of the paper is organized as follows. In Section II, we have studied the Advanced Encryption Standard (AES) algorithm. Then, our implementation of cryptographic algorithm AES symmetric key change is briefly described in section III; in addition, a discussion of the measurement results of the encryption and decryption performance of the image on the execution time, the histogram and entropy. Finally, Section IV concludes the paper.

II. ADVANCED ENCRYPTION STANDARD (AES)

AES (Advanced Encryption Standard) [5], [6] is a new standard for symmetric encryption block established to change the old Data Encryption Standard (DES), which was published

ISSN: 2356-5608

by the National Institute of Standards and Technology (NIST) the United States as Federal Information Processing Standard Pub 197 (FIPS 197) on November 26, 2001. After a standardization of five years process, NIST adopted the Rijndael algorithm as AES. AES is an encryption algorithm that is used to protect electronic data. Since AES has special features tailored for WSN applications [7, 8], the secure AES implementation can greatly affect the very limited resources of network nodes.

Key Expansion

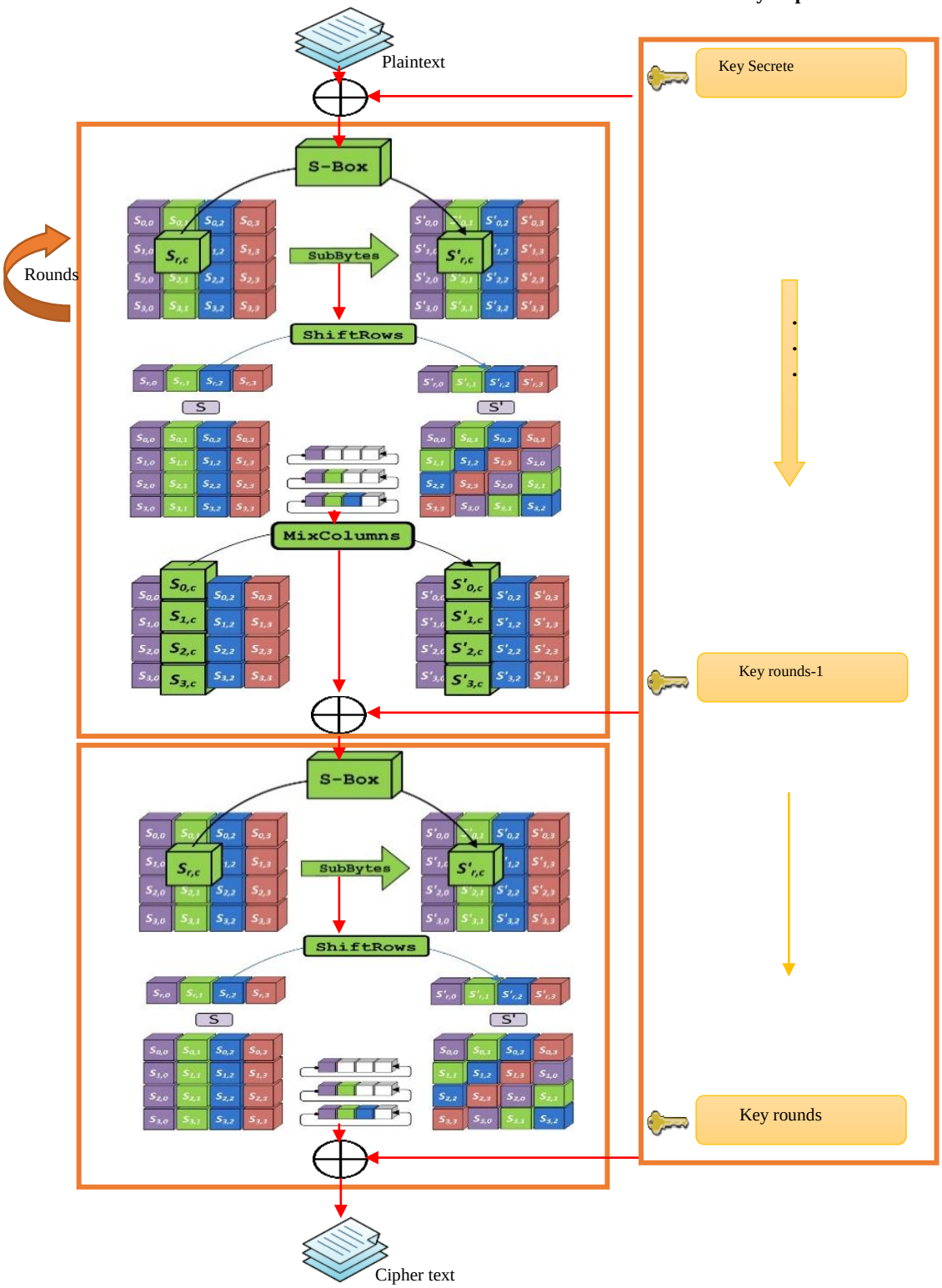


Fig. 1. AES algorithm structure

The AES algorithm is composed of three main parts: encryption, decryption, and key extension. Key expansion generates a schedule Key derived from the secret key, which is used in the encryption and decryption procedure. The AES algorithm is capable of using cryptographic keys of 128, 192 and 256 bits to encrypt and decrypt data in blocks of 128 bits operates. The number of revolutions depends on the cryptographic keys 10, 12 and 14 respectively.

AES is based on a 4x4 bytes matrix (referred to as "state"). The algorithm is made to perform simple four different transformations applied consecutively on the bit data blocks, in a number of iterations, called rounds. These transformations are: Sub Bytes, Shift Rows, Mix Columns and Add Round Key, as shown in Figure 1.

A. *SubByte*

SubByte is a non-linear byte substitution function. Each byte of the state is replaced by another one with a substitution table (S-box). S-box, which is derived from a multiplicative inverse of a finite field.

B. *ShiftRows*

ShiftRows is a permutation function. An offset equal to the line number shifts each row of the state to the left.

C. *MixColumns*

MixColumns is a mixing function. This transformation operates on the State column by column; the four bytes of each column of the state are combined using an invertible linear transformation. The MixColumns function is responsible for multiplying a constant matrix with the state.

D. *AddRoundKey*

AddRoundKey is an XOR function. For each round, a sub-key is derived from the main key using Rijndael key schedule, XORed with state matrix.

During decryption, the algorithm AES reverses the encryption by performing the inverse transformations. Taking the 128-bit block of ciphertext and converting it into plain text by applying the inverse of the four operations. AddRoundKey is the same for encryption and decryption. However, the other three have inverse functions used in the decryption process: reverse SubBytes (InvSubBytes), inverse ShiftRows (InvShiftRows), and inverse MixColumns (InvMixColumns).

III. IMPLEMENTATION AND PERFORMANCE MEASUREMENT

The materials and environmental constraints sensor nodes deployment influences the way to use such a standard algorithm and forces them to adapt according to the constraints. The great interest in the wireless sensor network is to reduce the energy consumption of sensor nodes to increase network lifetime. It has been shown in [9] that the decrease in the number of encryption rounds results in less energy consumption. For this, the idea of encryption process consists of only five rounds for the AES-128 and seven rounds for the AES-192 and AES-256.

A. *Evaluation parameters*

The evaluation of the algorithm was performed by some well-known criteria.

1) Run time: The running time is a critical parameter in the development of an encryption algorithm. It is the overall time required to encrypt and decrypt the image.

2) Histogram of the image: Histogram of the image is a recently used parameter. It shows the random distribution of encrypted image pixels. Compared histogram encrypted and original images, the total change in the pixel intensities of the images.

3) Image entropy: Digital images are a combination of discrete values of pixels, combined together to form a visual perception of the image. It can analyze the randomness in the encrypted image. entropy measures the difference between the entropy of the original image and the encrypted one. we have the best encryption if the entropie has more than one change. The entropy of an image can be calculated by equation (1).

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

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

B. *Experimental Results*

1) Run time:

In this section, we will evaluate the performance of our simulation results. We have improved the Advanced Encryption Standard algorithm in the wireless sensor network. MATLAB is used to implement the simulation of different standard images. Images are encrypted and decrypted (Fig. 2, 3, 4, 5) with a very short execution time. This analysis is introduced from a measuring different sizes of image as shown in Figure 6.

2) Histogram of the image:

Histogram is a very useful way to analyze the encryption effect on the image. The ideal resulting histogram after encryption must be flat. Our program shows quite adequate results, however, for the histograms of images Lena and Cameraman have shown a total change of the intensity distribution of the original image. The results for the selected images are exihibited in figures 7, 8, 9 and 10.

3) Image entropy:

The entropy measures the information content of the data, the more the data content is random the harder to be recognized after encryption. The entropy change for different images with different extensions (png and jpg) and different dimension is shown in Table 1. On average 10.55% of the entropy change is observed.

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors).*

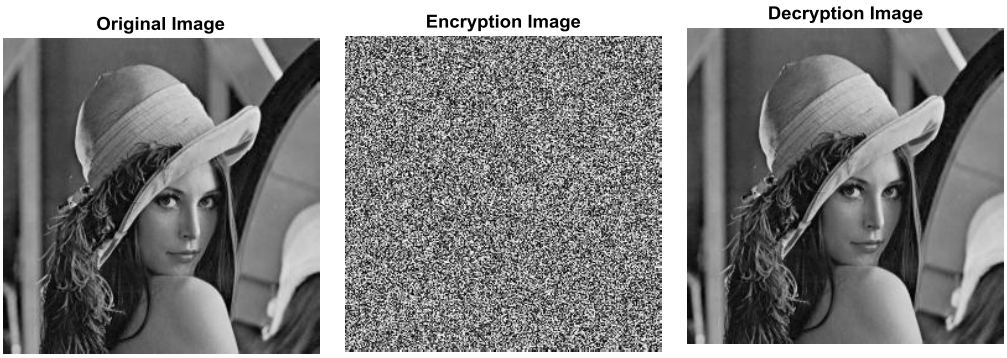


Fig. 2. Encryption and decryption Lena image.jpg 256x256

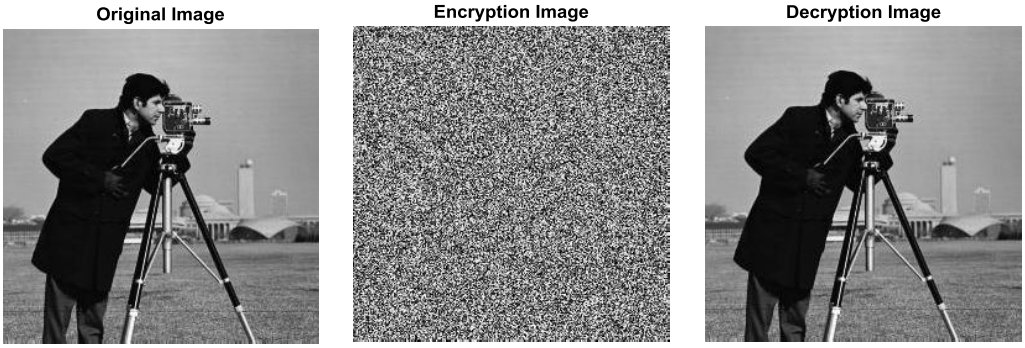


Fig. 3. Encryption and decryption Cameraman image.jpg 256x256.

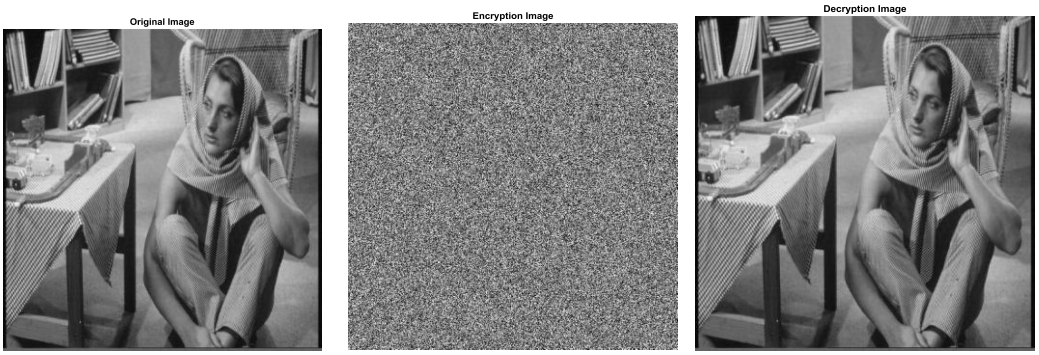


Fig. 4. Encryption and decryption woman image.jpg 512x512.

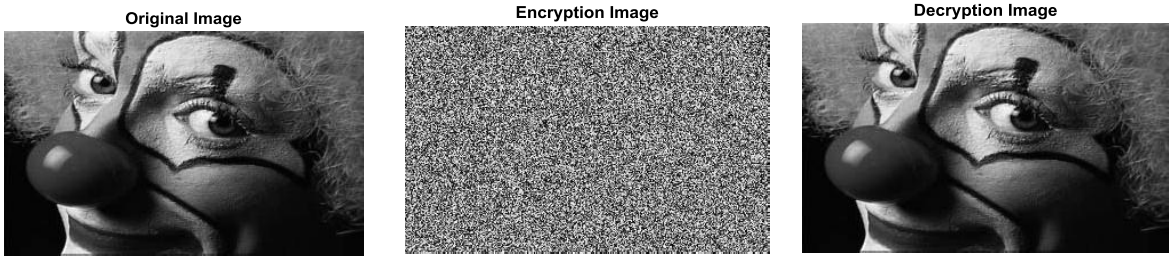
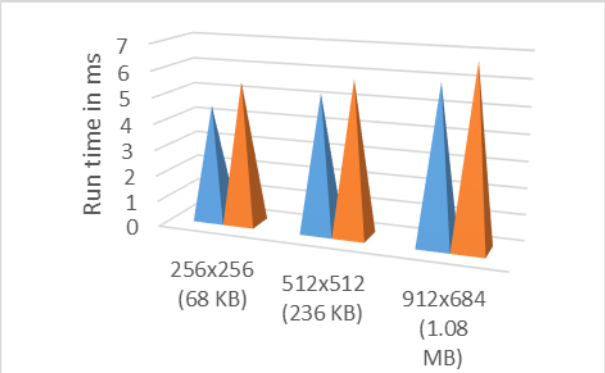


Fig. 5. Encryption and decryption clown image. png 200x320.



	256x256 (68 KB)	512x512 (236 KB)	912x684 (1.08 MB)
Encryption run time in ms	4,5	5,3	6
Decryption run time in ms	5,5	5,9	6,8

Fig. 6. execution times for different size images.

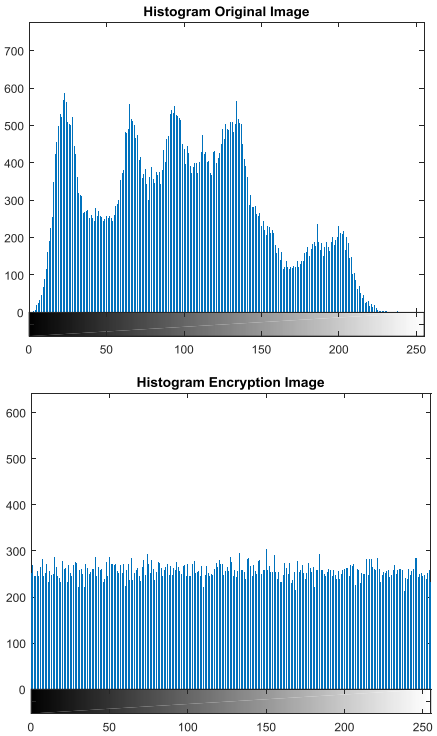


Fig. 7. Lena image Histogram of origin and encrypted.

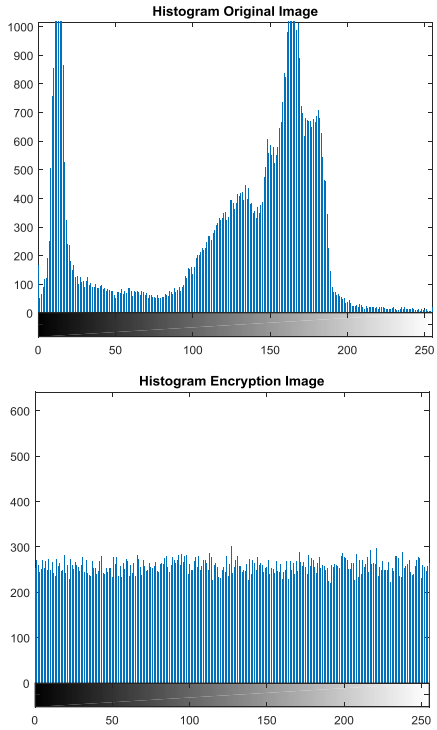


Fig. 8. Cameraman image Histogram of origin and encrypted.

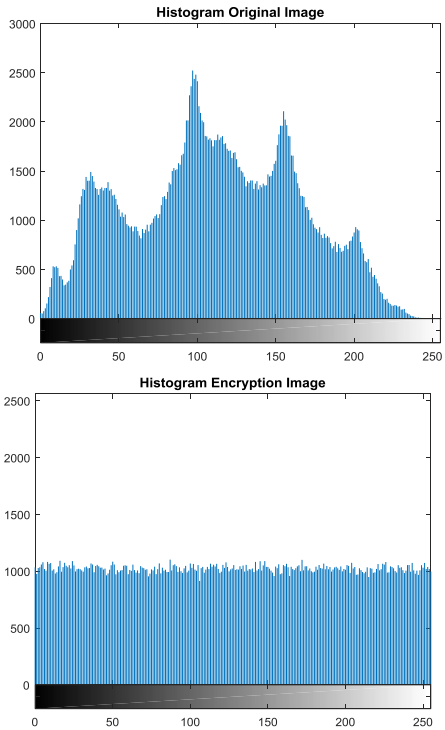
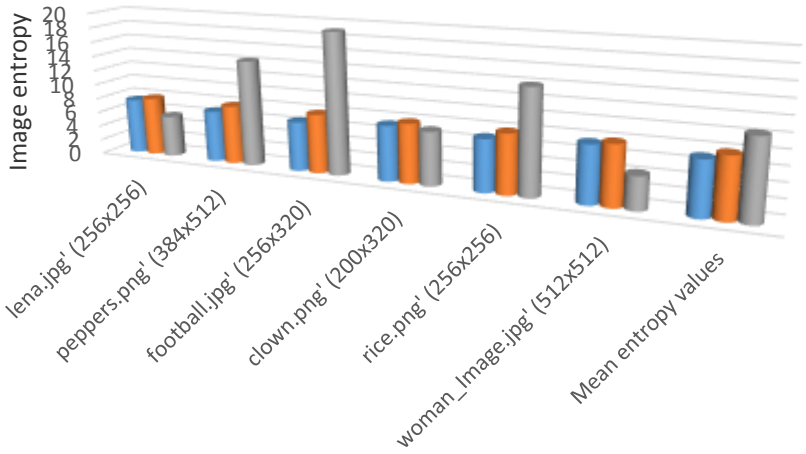


Fig. 9. Woman image Histogram of origin and encrypted.

TABLE I. IMAGE ENTROPY



	lena.jpg' (256x256)	peppers.png' (384x512)	football.jpg' (256x320)	clown.png' (200x320)	rice.png' (256x256)	woman_Image.jpg' (512x512)	Mean entropy values
original entropy	7,5691	6,991	6,7134	7,4585	7,0115	7,6631	7,2344
encryption entropy	7,9971	7,9991	7,998	7,9972	7,9968	7,9994	7,9979
Percent change	5,65	14,4	19,13	7,22	14,05	4,38	10,55

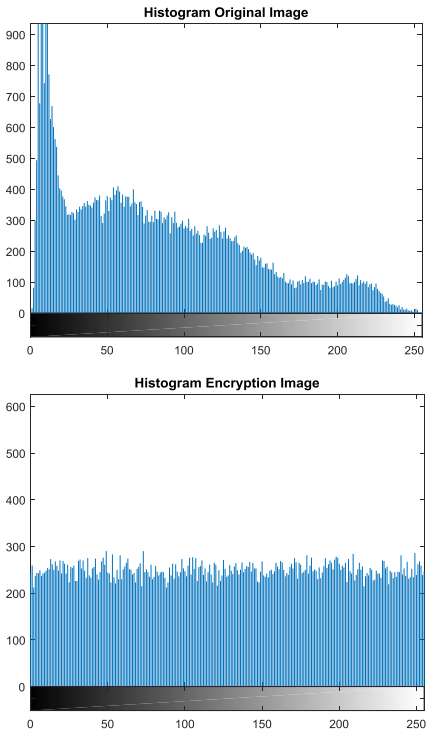


Fig. 10. Clown image Histogram of origin and encrypted.

IV. CONCLUSION

In this article, we have presented the analysis of AES algorithm performance changes applied to wireless multimedia sensor network; at execution time, entropy and a histogram of the various standard images. Simulation results show that the modified algorithm is more adapted to wireless sensor network, since it admitted the best execution time. Therefore, the modified algorithm increases the network lifetime.

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

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

[7] 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.

[8] 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.

[9] R. Chandramouli, S. Bapatla, K. P. Subbalakshmi, "Battery power-aware encryption", ACM Transactions on Information and System Security, vol. 9, no. 2, pp. 162-180, May 2006.