Journal of Information Sciences and Computing Technologies ISSN 2394-9066

SCITECH RESEARCH ORGANISATION| Volume 1, Issue 1 January, 2015|

Journal of Information Sciences and Computing Technologies
www.scitecresearch.com

Performances analysis of image encryption for medical applications

Sammoud Ali, Cherif Adnen
Signal processing Laboratory, Science Faculty of Tunis, UTM 1060 Tunis.
Email: sammoudali@yahoo.fr , adnen2fr@yahoo.fr

Abstract

This work is interested in securing transmission of digital images on the Internet, in public or local networks such as medical images, military or biometrics (authentication retina or fingerprint). We will implement three famous algorithms which are the RSA, DES and AES. The first one uses an asymmetric method for generating the keys (public and private) hence the second and the third algorithms are symmetric cipher block and use only private key for ciphering and deciphering. The simulation results will be presented and discussed in function of two main security parameters which are the length of the information blocks and the key length. Finally, a comparative study between the three techniques is conducted in order to classify everyone by the best performances of robustness especially with the presence of different kinds of attacks.

Keywords: Encryption data; image; RSA; DES; AES.

1-Introduction

Today, the data transmission on the remote networks suffers from severe changes (access to credit cards, e-commerce transactions, espionage of secret information on military, attacks on the net). Therefore, encryption can provide solutions to these problems by minimizing the risk of access to information and databases. Cryptography is a necessary tool that can be used in the protection of privacy, intellectual property, business and financial information, public security and social as well as the practice of e-commerce transactions and anonymous payments. It secures passwords, files, signature authentication, mobile phones and smart cards (R. Norcen, M. Podesser, A. Pommer, H.P.Schmidt, A. Uhl, 2003).

In fact, since 1970 appeared the data encryption standard (DES) as a robust block cipher algorithm especially used for data encryption. In 1997, this algorithm was replaced by the advanced encryption standard (AES). Another kind of asymmetric algorithm called RSA, was created in 1977 by A. Rivest, A.Shamir and L.Adelman. These algorithms are more suitable to text and data encryption than digital encryption, due to their intensive computational process unless accelerated by hardware implementations (A.Cheddad , J.Condell, K.Curran and P. McKevitt, 2010). Sinha and Singh (G. Alvareza , S. Lib, L. Hernandeza, 2007) proposed a new technique to encrypt an image for secure image transmission. This technique consists in adding to the encoded version of the original image, by using an error-correcting code. The tests and stimulated attacks on this version proved that the cryptosystem proposed by Sinha and Singh is insecure. The weakness lies on the small size of the keys and in the redundant properties of the BCH codes.

Another famous encryption algorithm called Blowfish cipher block was introduced in 2004. The original image was divided into blocks, which were rearranged into a transformed image using a transformation algorithm. The results show that increasing the number of blocks by using smaller block sizes led to lower pixel correlation and higher entropy (F. Saeed and M. Rashid, 2010).

2. Image encryption with RSA algorithm

2.1. Principle

The RSA algorithm is an asymmetric algorithm that was created in 1977 and named by the names of its inventors A. Rivest, A.Shamir and L.Adelman (W. Puech, J.M.Rodriguez, 2004). This encryption uses two different keys: a public

key(e) that can encrypt documents and the other private key (d) which is intended to decrypt the message. The principle of ciphering is illustrated by figure 3.

After computing the public and the private keys respectively (e) and (d), the encrypted block (MC) is obtained as:

$$MC = M \wedge e \mod (n)$$

Where:

M : is the original block

N= p *q

p,q : are integer numbers verifying PGCD(p,q) = 1.

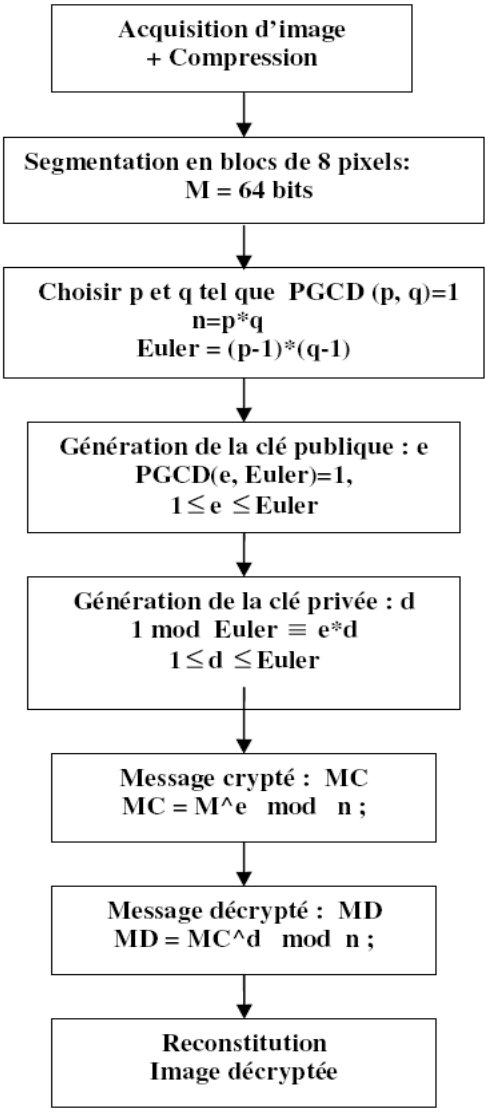

Fig. 1 : The RSA algorithm

2.2.Simulation results

Figures 2 represent the original and encrypted image with RSA algorithm with N=128 bits and L= 64 bits. Their respective histograms are illustrated in figures 3 and 4.

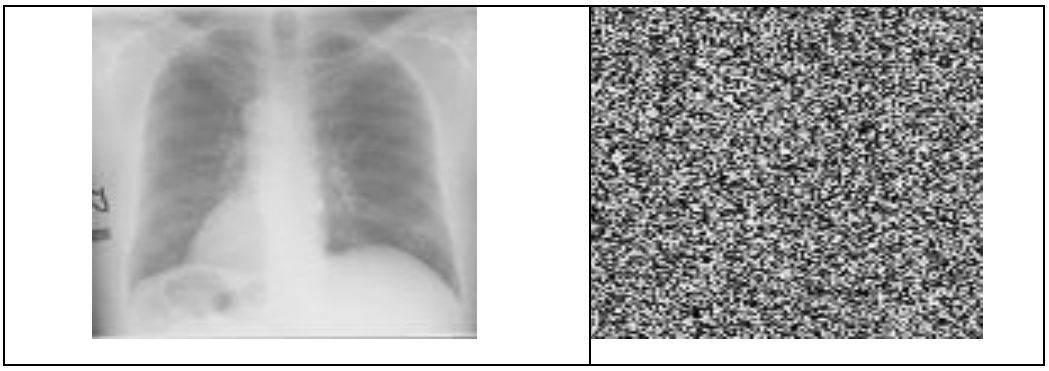

Fig. 2 : Original and encrypted image with RSA algorithm

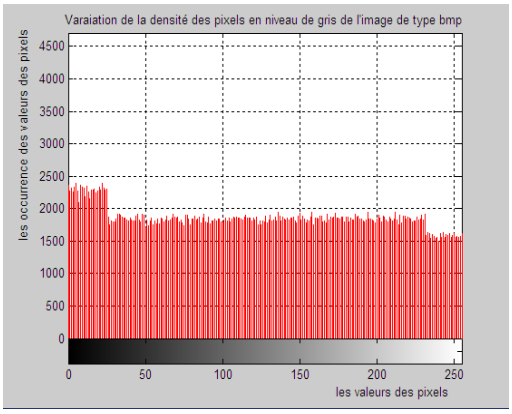

Fig. 3: Histogram of the original image

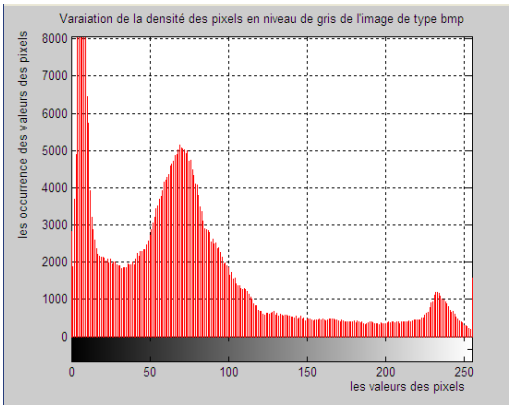

Fig. 4: Histogram of the encrypted image

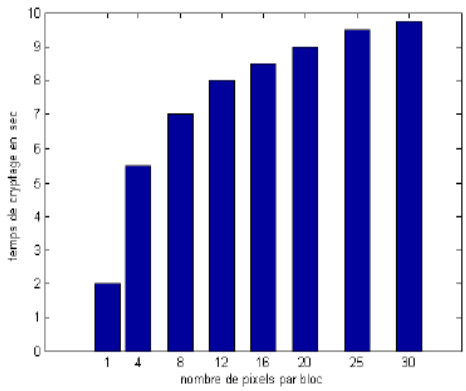

Fig. 5 :computing time vs block length

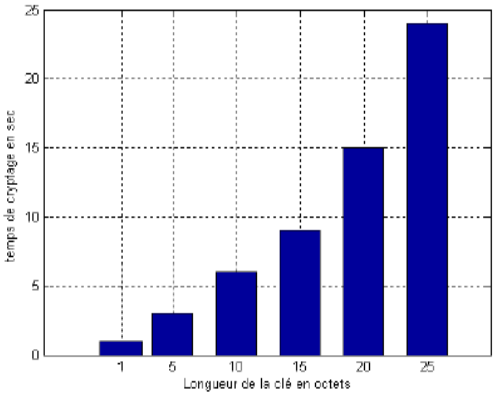

Fig. 6 :computing time vs key length

We can deduce that the encryption time increases significantly with the key length (N) and the ciphering block length (L). A compromise is necessary in this case, and the optimum solution is to adopt L = 8-12 pixels as length of image blocks and N = 512 to 1024 bits for the key. The table in Figure 8 shows the results of encrypted and decrypted blocks with blocks of L = 8 pixels and a key length N = 1024 bits.

3. Image encryption with DES algorithm

3.1. DES principle

DES (Data Encryption Standard) is a global standard for over 35 years. Although it is a little older, it was very resistant to cryptanalysis between 1970 and 2000, and remains a very safe algorithm but actually is replaced by the AES algorithm. The principle of the DES algorithm is to divide a text into blocks of 64 bits (8 octets), then we make an initial block permutation, we cut the blocks into two parts left and right, called G and D, after is carried out a step of permutation and substitution repeated 16 times (called rounds). Finally, we concatenate the left and right sides and then perform an inverse initial permutation. The secret key therefore serves both to encrypt and to decrypt the message. The key has a length of 64 bits (8 characters) but only 56 bits are used. Figure 7 illustrates the encryption algorithm that gives us the appearance of this symmetrical method.

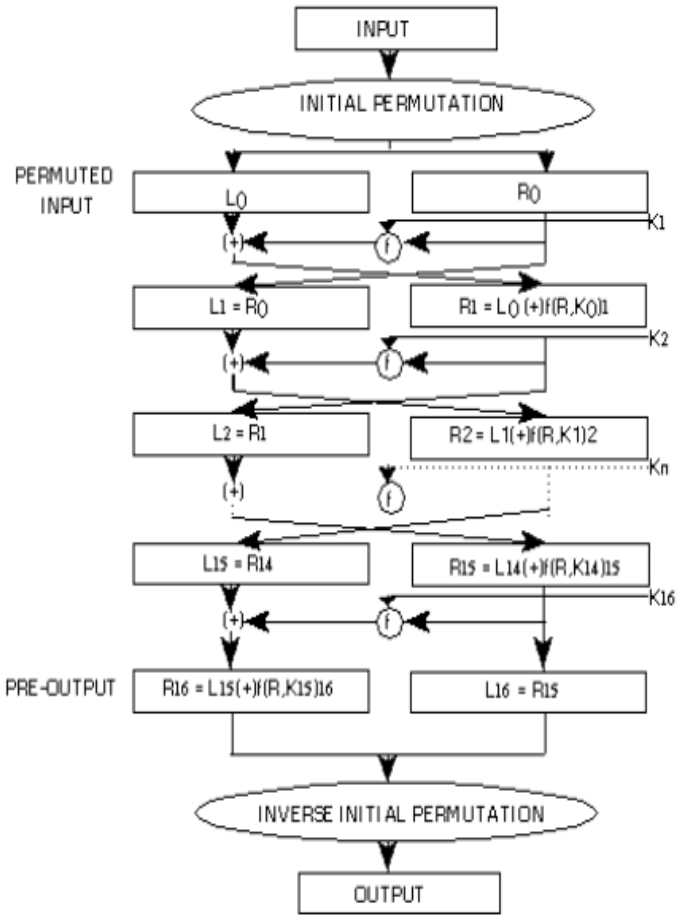

Fig. 7. DES Algorithm

Indeed, the security of DES with 16 rounds is high and resists in all linear attacks, differential or correlated keys. The great security relies on its tables of very effective non linear substitutions to dilute information. Furthermore, the number of keys is high and can easily be increased by changing the number of bits taken into account. But, its main problem is the high computing time and the difficulty of its real time implementation.

3.2. Simulation

To watch the difference between encryption algorithms, we illustrated in the following figures 8 and 9 an example of DES ciphering algorithm.

Fig.8. Original image

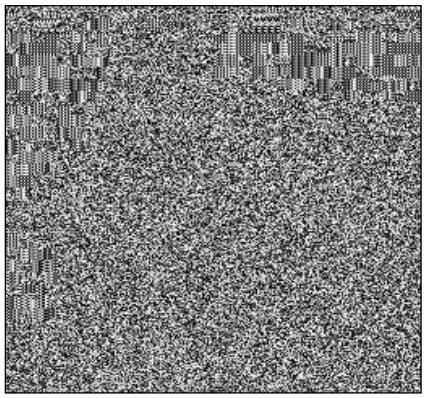

Fig.9. DES : block=64 bits, key= 64 bits

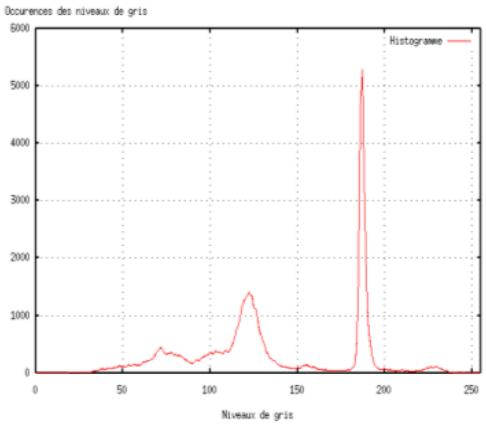

Fig.10: Histogram of the original image

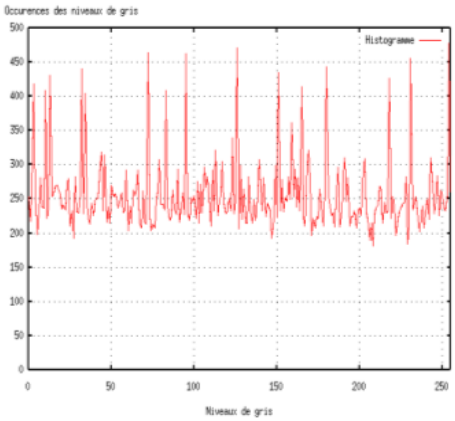

Fig.11: Histogram of the encrypted image

3.3- Encrypting time

The encryption times of the algorithms (DES, TEA, RSA) depend on the size of the picture, we can deduce that the DES is slower and cannot function in a real time mode without hardware implementation (Fig.12).

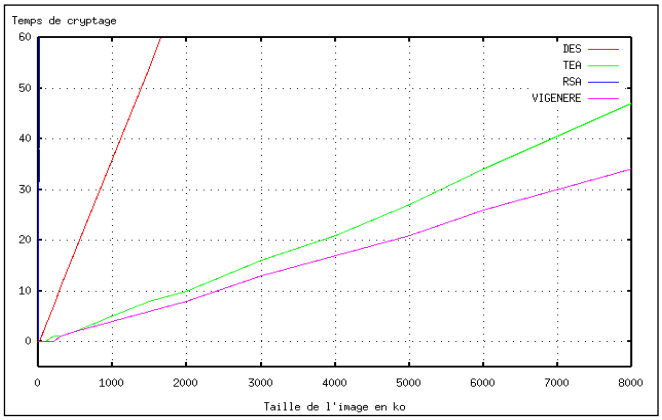

Fig.12: Encryption and computing time for several ciphering algorithms

4. Image encryption with AES algorithm

4.1. AES principle

AES algorithm was developed by NIST (the National Institute of Standards and Technology) in 1997 to replace the DES (Data Encryption Standard) which has become too low by current attacks. AES is a recent symmetric block cipher which is going to replace the Data Encryption Standard (DES) in all applications: it supports different combinations of key length and message block size. AES operates on 128-bit blocks of data and uses 128, 196, or 256 bit keys (Diaa Salam.A, H. M. Abdual-Kader, and M. M. Hadhoud. 2010).

Table 1 : AES parameters

Algorithm	Key length (Nk words)	Block Size (Nb words)	Number of rounds (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

AES allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array organized as a 4x4 matrix called the state. The algorithm begins with an Add round key stage followed by nine rounds of four stages and a tenth round of three stages which applies for both encryption and decryption algorithm. These rounds are organized by the following four stages (Manoj. B, Manjula N Harihar, 2012):

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key.

The tenth round Mix columns stage is not included. The first nine rounds of the decryption algorithm are governed by the following four stages:

- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

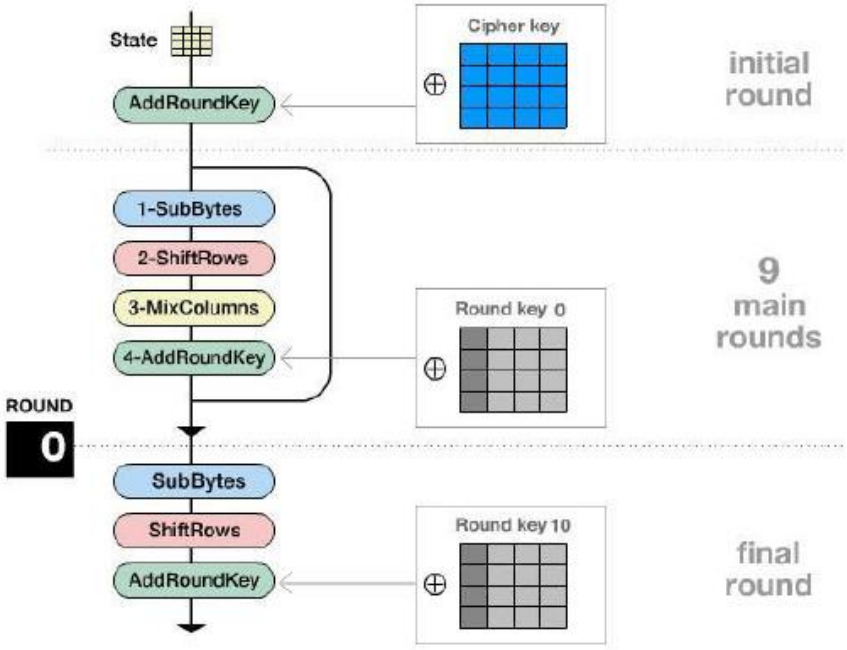

Fig.13 : AES Algorithm

AES operates in three modes:

-The first one is the Electronic Codebook Mode (ECB) which encrypts a block of plaintext data to the corresponding block of cipher text data.

- The second mode is the Cipher Block Chaining (CBC) in which a block of plaintext is encrypted in dependence of the preceding block of cipher text.

- The third mode is the Cipher FeedBack (CFB). The key stream is obtained by encrypting the previous cipher text block. FBC is a stream cipher. Its main interest is that it requires an encryption function, which simplifies its soft or hard implementation and conception.

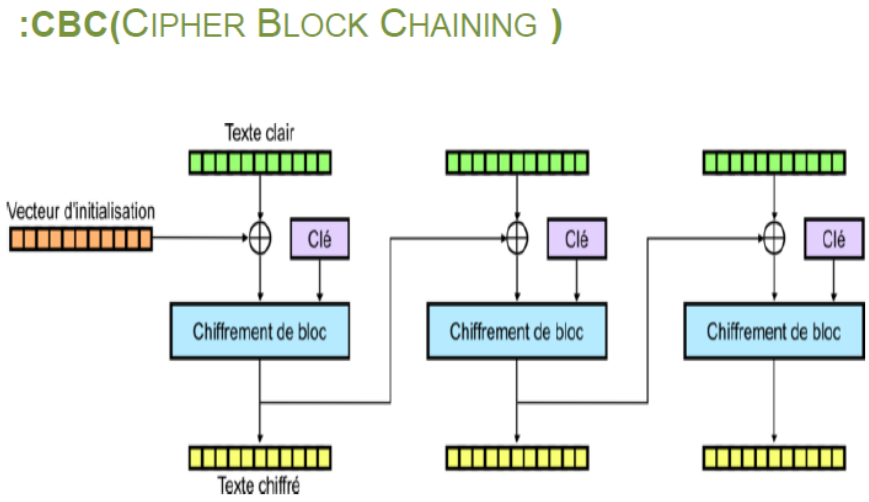

Fig.14 : AES Algorithm in CBC mode

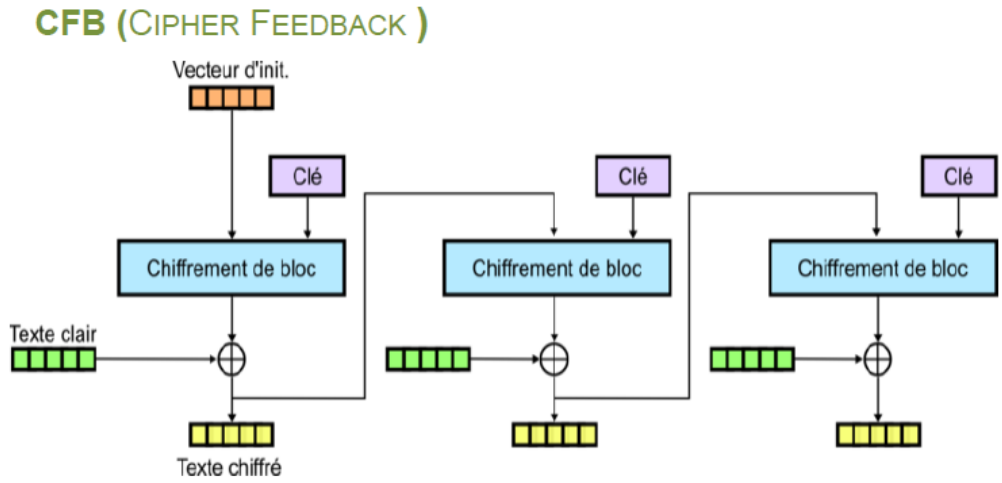

Fig.15 : AES Algorithm in CFB mode

4.2. Simulation results

Figures 16, 17 and 18 represent an example of a encrypted medical image without and with jpeg compression. We can observe that for a based mode offering a key size of 128 bits, the encrypting and decrytng times vary between 70 ms and 89ms hence for the extended mode with a key of 256 bits, the times are about 83ms to 102 ms. Tables 2 and 2, confirm these results and demonstrate that EBC mode gives the optimum values.

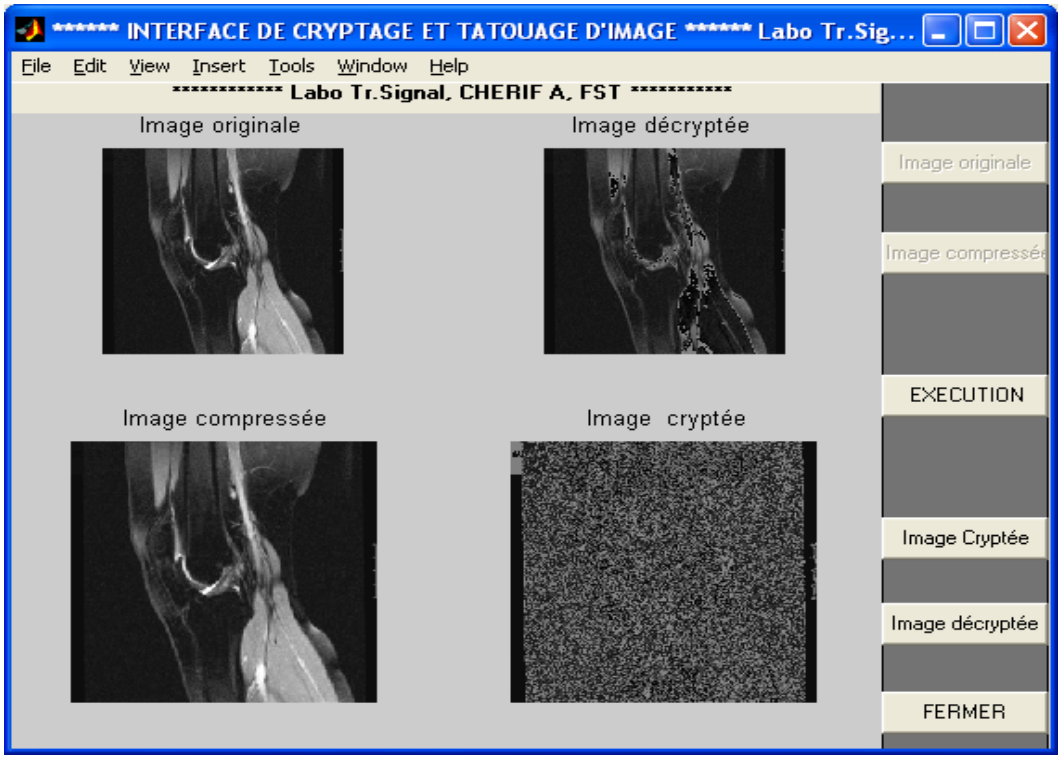

Fig.16 : Original, compressed and encrypted image with AES Algorithm

Table 2. Encrypting and decrypting times in function of the AES mode and the block length

Modes	Temps de chiffrement (ms)	Temps de déchiffrement (ms)	Taille (ko)
EBC	87	83	765
CBC	102	93	765
EBC	44	56	250
CBC	86	59	250

Table 3. Encrypting and decrypting times in function of the AES mode and the key length

Modes	Temps de chiffrement (ms)	Temps de déchiffrement (ms)	Taille de la clé (bits)
EBC	90	82	256
CBC	102	94	256
EBC	78	82	192
CBC	95	87	192
EBC	74	70	128
CBC	89	84	128

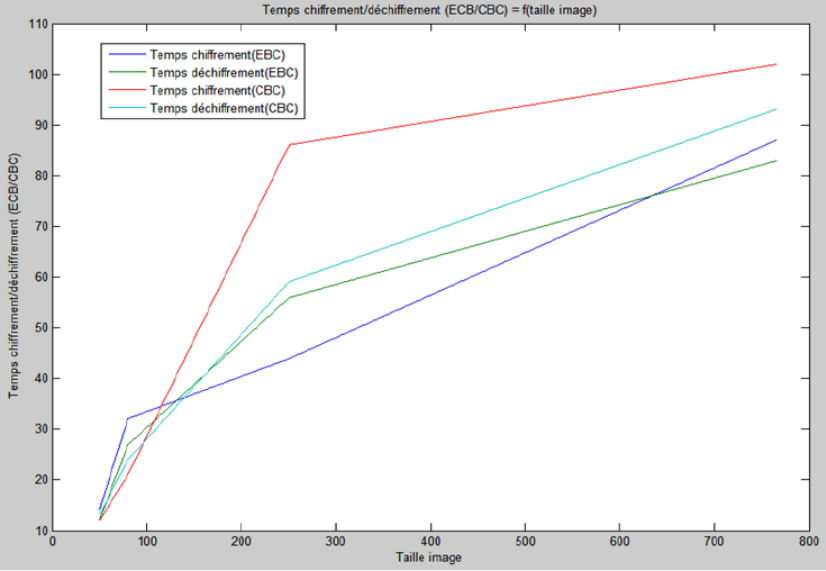

Fig.17. Encrypting time in function of the image size (in Ko)

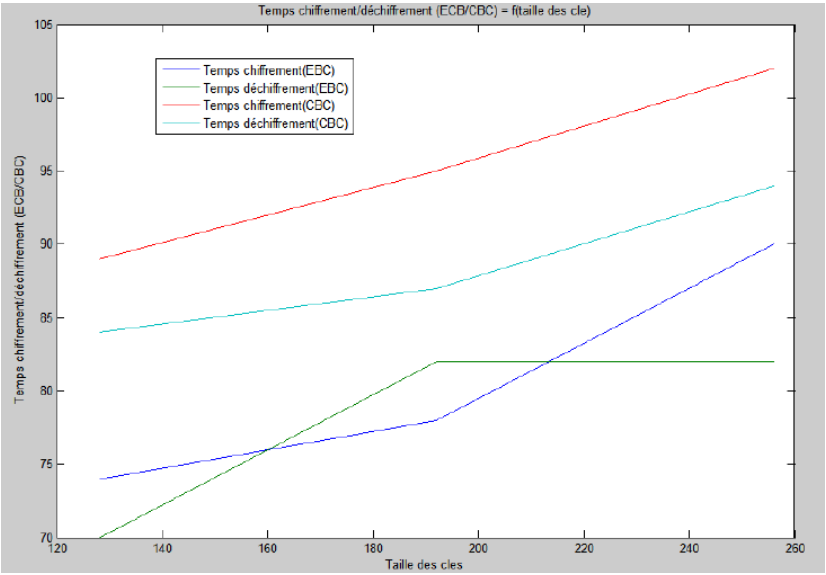

Fig.18. Encrypting time in function of the key size (in bits)

5. Conclusion

In this work, we have implemented three encryption algorithms for digital images transmission based on DES, AES and RSA algorithms under MATLAB environment. For the RSA algorithm we are confronted with the problems of time and real-time computing constraints. Its implementation demonstrates that the optimal results were obtained for a key length of 512 or 1024 bits and a block length of 8 pixels=64 bits. However, for the AES-128 algorithm, the computing times are reduced to 50 ms (for a key size of 128 bits and a block length of 16 pixels) and conduct to a real time functioning of the ciphering system. We note that these times can be considerably reduced by hardware implementation (DSP or FPGA) with using a compiled language such as the code composer studio, C++ or VHDL programming.

References

[1] R. Norcen, M. Podesser, A. Pommer, H.P.Schmidt, A. Uhl, (2003). Confidential storage and transmission of medical image data. Computers in Biology and Medicine 33, 277–292, Pergamon.

[2] Abbas Cheddad , Joan Condell, Kevin Curran, Paul McKevitt, (2010).A hash-based image encryption algorithm Optics Communications 283, 879–893, Elsevier.

[3] Gonzalo Alvareza , Shujun Lib, Luis Hernandeza, (2007). Analysis of security problems in a medical image encryption system. Computers in Biology and Medicine 37, 424 – 427, Elsevier.

[4] Fauzan Saeed and Mustafa Rashid, (2010). Integrating Classical Encryption with Modern Technique IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.5.

[5] William PUECH José, Marconi RODRIGUES, (2004). Sécurisation d'image par crypto-tatouage , CORESA'2004 conference, Lille, France.

[6] Diaa Salama Abdul Minaam, Hatem M. Abdual-Kader, and Mohiy Mohamed Hadhoud. (2010). Evaluating the effects of Symmetric Cryptography Algorithms on Power Consumption for Different Data Types. International Journal of Network Security, Vol.11, No.2, 78-87.

[7] Manoj. B, Manjula N Harihar, (2012). Image Encryption and Decryption using AES International Journal of Engineering and Advanced Technology, Volume-1, Issue 5.

[8] L.H. Encinas, A. P. Domınguez, (2006). Comments on a technique for image encryption using digital signature. Optics Communications 268, 261–265, Elsevier.

[9] G. H. Karimian, B. Rashidi, and A.farmani, (2012). A High Speed and Low Power Image Encryption with 128-Bit AES Algorithm International Journal of Computer and Electrical Engineering, Vol. 4, No. 3.

Authors biograhy

A.Sammoud

He is a researcher member in the Signal Processing Laboratory at the Science Faculty of Tunis. He received in 2006 the Bachelor from Science Faculty of Monastir in Informatics. In 2008, He obtained his Master degree in Electronics from FST- Tunisia. Actually, he prepares his doctorate thesis in the field of image encryption and watermarking.

A.Cherif

He received his engineering diploma from the High Engineering Institute of Tunis in 1987 and his Ph.D. in electrical engineering and electronics from The National Engineering School of Tunis (ENIT) in 1996. Actually he is a Senior professor at the Science Faculty of Tunis, responsible for the Signal Processing Laboratory. He participated in several research and cooperation projects, and he is the author of more than 100 international communications and publications.