Meteosat Images Encryption based on AES and RSA Algorithms

Meteosat Image Encryption

[1]Boukhatem Mohammed Belkaid
Laboratoire d'Analyse et Modélisation des Phénomènes Aléatoires, UMMTO, BP 17 RP, 15000, Tizi-Ouzou, Algérie

[2]Lahdir Mourad
Laboratoire d'Analyse et Modélisation des Phénomènes Aléatoires, UMMTO, BP 17 RP, 15000, Tizi-Ouzou, Algérie

[3]Cherifi Mehdi
Laboratoire d'Analyse et Modélisation des Phénomènes Aléatoires, UMMTO, BP 17 RP, 15000, Tizi-Ouzou, Algérie

***Abstract*—Satellite image Security is playing a vital role in the field of communication system and Internet. This work is interested in securing transmission of Meteosat images on the Internet, in public or local networks. To enhance the security of Meteosat transmission in network communication, a hybrid encryption algorithm based on Advanced Encryption Standard (AES) and Rivest Shamir Adleman (RSA) algorithms is proposed. AES algorithm is used for data transmission because of its higher efficiency in block encryption and RSA algorithm is used for the encryption of the key of the AES because of its management advantages in key cipher. Our encryption system generates a unique password every new session of encryption. Cryptanalysis and various experiments have been carried out and the results were reported in this paper, which demonstrate the feasibility and flexibility of the proposed scheme.**

***Keywords*—AES; RSA; MSG; satellite; encryption; keys**

I. INTRODUCTION

The amount of satellite image has increased rapidly on the Internet, in public or local networks. Meteosat image security becomes increasingly important for many applications, e.g., confidential transmission, multispectral imaging for providing electronic images of clouds, land and sea surfaces, analysis of air masses to monitor the thermodynamic state in the lower part of the atmosphere and environment data collection and relay transmitted by automatic platforms (marine beacons, land and airborne ...)[1]. The unlawful, unofficial, and unauthorized access and illegal use of Meteosat imagery increases the importance of information security to keep the critical and confidential imagery and transmission process secure, dependable, trustworthy, and reliable. Cryptography is the most widely accepted information security technique employed to make the Meteosat image transmission processes reliable and secure from unauthorized access and illegal use [2-3]. Cryptographic techniques can be divided into symmetric (with a secret key) and asymmetric encryption (with private and public keys). In symmetric cryptosystems, the same key is used for the encryption or decryption and this key need to be secure and must be shared between the transmitter and the receiver. These cryptosystems are very fast and easy to use. Many image encryption algorithms have been developed in last year's. Among them, we find, the public symmetric AES algorithm, which has proven its robustness against different types of attacks nowadays [4-9], the asymmetric RSA [10-12] algorithm and the IDEA algorithm. Using these algorithms allow separately kind of luxurious ensure confidentiality. For this reason, a hybrid cryptosystem based on both AES and RSA is proposed. The Advanced Encryption Standard (AES) and the Rivest Shamir Adleman (RSA) algorithms are the two popular encryption algorithms that vouch confidentiality, integrity and authenticity over an insecure communication network and Internet.AES algorithm which contain iterative rounds. AES algorithm support several cipher modes of operation such as ECB (Electronic Code Book), CBC (Cipher Block chaining), OFB (Output Feedback), CFB (Cipher Feedback) and CTR (Counter) [13-15]. In our system, privacy is ensured by AES algorithm using five modes of operation and the RSA algorithm is used to transmit the keys. The cryptosystem also check the integrity of images using a simple process based on correlation between the pixels of Meteosat images. The rest of the paper is organized as follow. Section 2 discusses the proposed hybrid cryptosystem scheme. Section 3 and 4 shows some numerical results. Finally, section 5 concludes the paper.

II. THE CRYPTOSYSTEM PROPOSED

In this work a communication system based on AES and RSA algorithms is realized. The global scheme of the proposed system for private communications is shown in Fig.1. Note that the transmission channel is a public one. Consequently, any hacker has a free access to information passing through the channel which is considered perfect in our works. The cryptosystem is designed to protect MSG images transmitted over the channel of transmission against any attack.

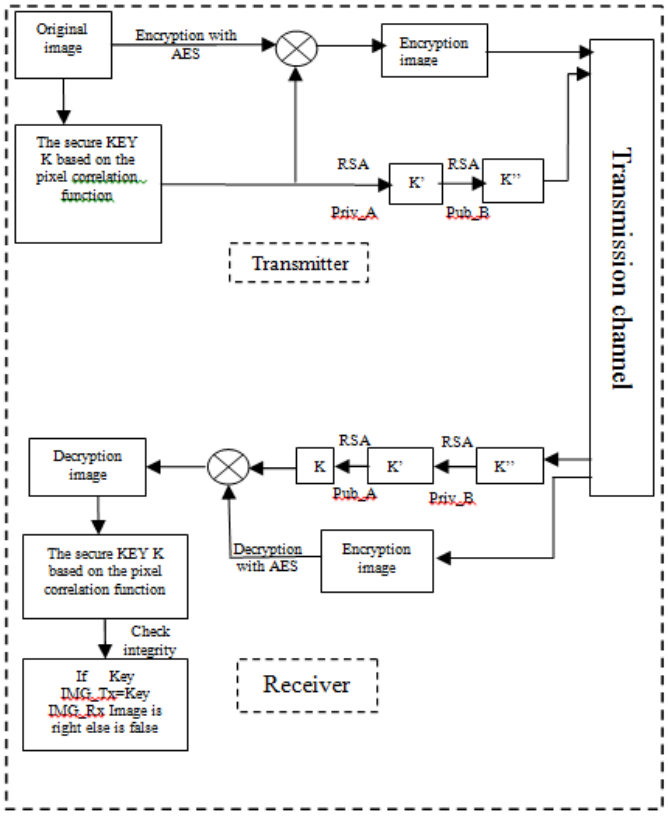

Fig. 1. Transmission chain based on AES and RSA

A. Transmission block

1) AES algorithm structure

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001. The figure 2 shows the AES cipher in detail,

Indicating the sequence of transformations in each round and showing the corresponding decryption function. Four different stages are used, one of permutation: ShiftRows, and three of substitution: (1) Substitute bytes, (2) MixColumns, (3) AddRoundKey, and is fast in both software and hardware.

AES is a variant of Rijndael which has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits. By contrast, the Rijndael specification per se is specified with block and key sizes that may be any multiple of 32 bits, both with a minimum of 128 and a maximum of 256 bits.

2) Cipher operation block

A mode of operation is a technique for adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream. Five modes of operation have been defined by NIST (SP 800-38A) are used. A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream. The five modes are intended to cover a wide variety of applications of encryption for which a block cipher could be used.

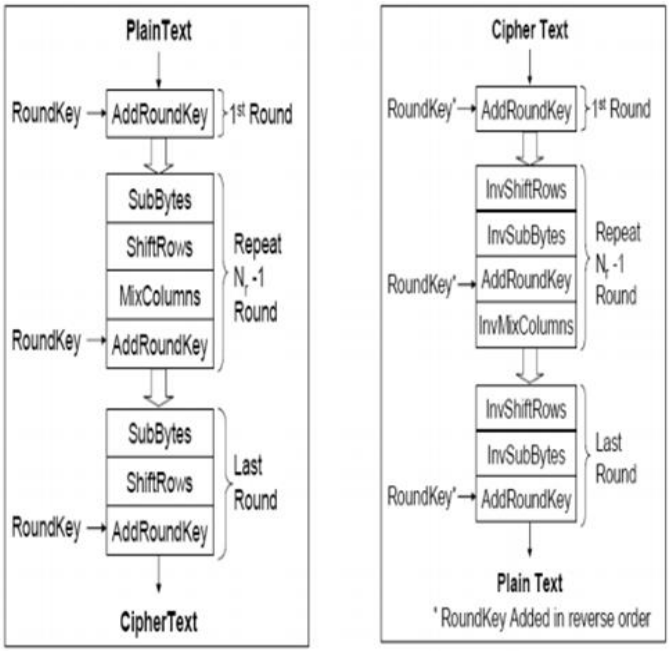

Fig. 2. AES encryption and decryption algorithm

These modes are intended for use with any symmetric block cipher, including triple Data Encryption Standard (DES) [16-17] and AES.

- Electronic codebook (ECB)

Encryption:

$$C_j = E(K, P_j) \qquad j = 1, \ldots, N \qquad (1)$$

Decryption:

$$P_j = D(K, C_j) \quad j = 1, \ldots, N \qquad (2)$$

- Cipher block chaining (CBC)

Encryption:

$$C_j = E\big(K, [C_{j-1} \oplus P_j]\big) \qquad (3)$$

Decryption:

$$D(K, C_j) = D\left(K, E\big(K, [C_{j-1} \oplus P_j]\big)\right)$$
$$D(K, C_j) = C_{j-1} \oplus P_j \qquad (4)$$
$$C_{j-1} \oplus D(K, C_j) = C_{j-1} \oplus C_{j-1} \oplus P_j = P_j$$

- Cipher feedback (CFB)

Encryption:

$$I_1 = IV$$
$$I_j = LSB_{b-s}(I_{j-1}) // C_{j-1} \; j = 2, \ldots, N \qquad (5)$$
$$I_j = E(K, I_j) \; j = 1, \ldots, N$$
$$C_j = P_j \oplus MSB_s(O_j) \quad j = 1, \ldots, N$$

Decryption:

$$\left.\begin{aligned} I_1 &= IV \\ I_j &= LSB_{b-s}(I_{j-1}) // C_{j-1}\ j = 2, \dots, N \\ O_j &= E(K, I_j)\ j = 1, \dots, N \\ P_j &= C_j \oplus MSB_s(O_j)\ \ j = 1, \dots, N \end{aligned}\right\} \quad (6)$$

- Output feedback (OFB)

Encryption:

$$C_j = P_j \oplus E(K, [C_{j-1} \oplus P_{j-1}]) \quad (7)$$

Decryption:

$$C_j = C_j \oplus E(K, [C_{j-1} \oplus P_{j-1}]) \quad (8)$$

- Counter (CTR)

Encryption:

$$\left.\begin{aligned} I_1 &= Nonce \\ I_j &= O_{j-1}\ \ j = 2, \dots, N \\ O_j &= C_j \oplus E(K, I_j)\ \ j = 1, \dots, N \\ O_j &= E(K, I_j)\ \ j = 1, \dots, N \\ C_j &= P_j \oplus E(K, I_j)\ \ j = 1, \dots, N-1 \end{aligned}\right\} \quad (9)$$

Decryption:

$$\left.\begin{aligned} I_1 &= Nonce \\ I_j &= LSB_{b-s}(I_{j-1}) // C_{j-1}\ j = 2, \dots, N \\ O_j &= C_j \oplus E(K, I_j)\ \ j = 1, \dots, N \\ P_j &= C_j \oplus O_j\ \ j = 1, \dots, N-1 \\ P_N^* &= C_N^* \oplus MSB_u(O_N) \end{aligned}\right\} \quad (10)$$

3) RSA asymmetric algorithm

The RSA algorithm was publicly described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The RSA algorithm is the most popular and proven asymmetric key cryptographic algorithm. The RSA algorithm is based on the mathematical fact that it is easy to find and multiply large prime numbers together, but it is extremely difficult to factor their product. The private and public keys in the RSA are based on very large (made up of 100 or more digits) prime numbers [10-12]. In such a cryptosystem, the encryption key is public and differs from the decryption key which is kept secret. In RSA, this asymmetry is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem. To transmit the key K, the transmitter can encrypt this key using the RSA asymmetric algorithm .The transmitter have the public and private key, $Pub_E(b_x,n_x)$, $Priv_E(u_x,n_x)$, and the receiver have the public and private key $Pub_R(b_y,n_y)$, $Priv_R(u_y,n_y)$.

The transmitter signs the key K with the RSA algorithm using the private key of the sender $priv_E$ to obtain a signed key K' such that:

$$K' = K^{Ux} \bmod (n_x) \quad (11)$$

The key K' is encrypted for the second time using the RSA public key Pub receiver to generate the key K":

$$K'' = K'^{by} \bmod (n_y) \quad (12)$$

B. Reception block

Inverse functions are used to reconstruct the same sent image. Here the function of correlation between adjacent pixels is used to verify integrity. The cryptosystem developed can detect in the reception if a change affects the image in the transmission channel, using the correlation function in the block verification of integrity.

III. Numerical Results

In this study, a Meteosat image database is used. Meteosat images used recorded by the Meteosat Second Generation (MSG) on twelve visible and infrared channels are provided by the meteorological station of the National Meteorology Office (ONM) Dar El Beida, Algeria. Figure 3 shows all MSG images used for our various tests.

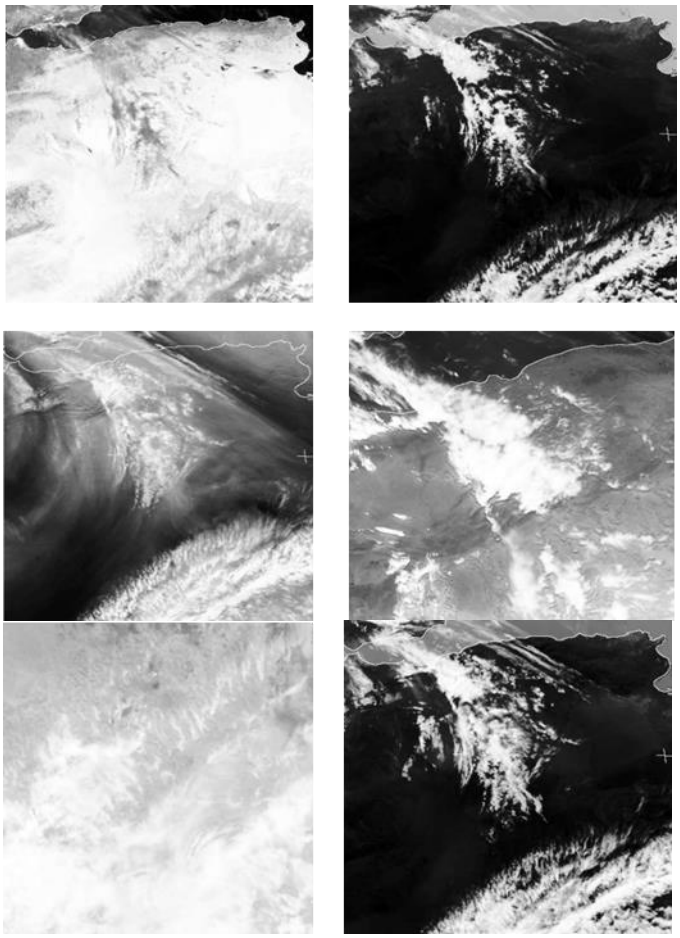

Fig. 3. MSG images in different channels

An ordinary computed Meteosat image, as shown in Figure 4, having a size of 262 144 bytes and a resolution of 512 × 512, is used for the experiments and analysis.

The encrypted and decrypted images aregiven in Figures 5 and 6, respectively, to prove the robustness and quality of the encryption results. The encrypted Meteosat image is totally

scrambled and highly secure from unauthorized access and illegal use. The decrypted Meteosat image is the same as the original image, with no changes and/or alterations.

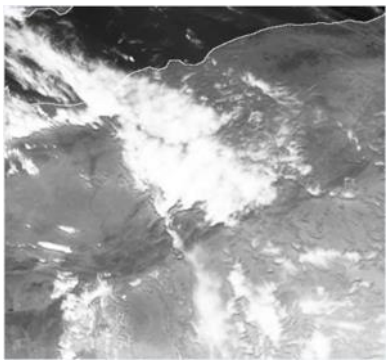

Fig. 4. Original image

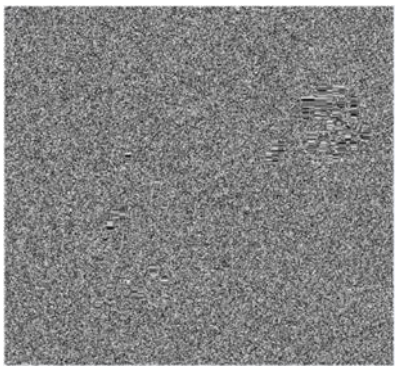

Fig. 5. ECB image encrypted

Fig. 6. Decrypted image

IV. Security Analysis

The security of the above-described encryption scheme is now analyzed by studying various tests: histogram analysis, correlation coefficients analysis and key space analysis.

A. Histogram Analysis

Figs. 7, 8 and 9 show histograms of an original image and encrypted images for two modes of operation ECB and OFB. The experiment results show that the histogram of the encrypted Meteosat images is fairly uniform and different from the original image.

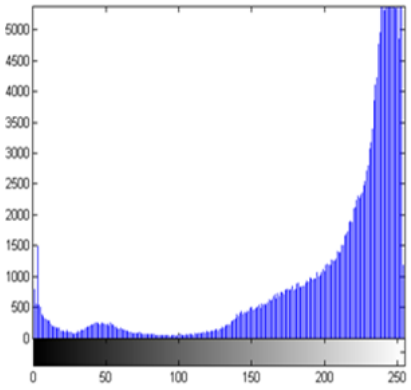

Fig. 7. Histogram of original image

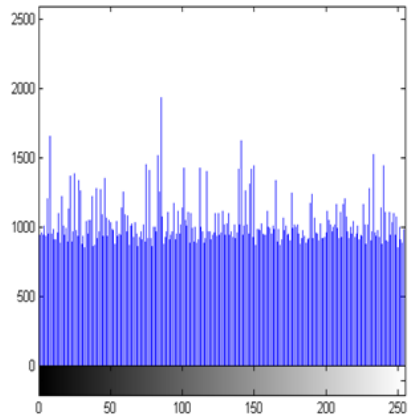

Fig. 8. Histogram of ECB image encrypted

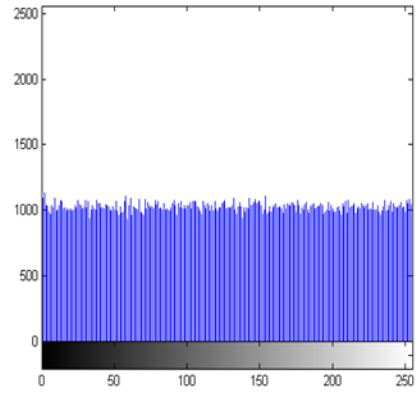

Fig. 9. Histogram of OFB image encrypted

B. Correlationciefficients analysis

Figure 10 shows the correlation coefficients for the encrypted Meteosat images for the five modes. It is clear from computed experimental results of these figures that there is negligible correlation between these images. We note that the performance of CBC and CTR modes because they have a lower correlation coefficient. ECB mode has the highest coefficient.

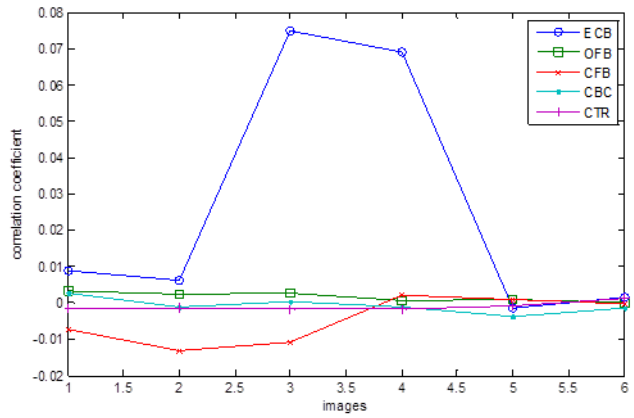

Fig. 10. Correlation coefficients of encrypted images

C. Keysensitivity

Security keys are extremely important to an image encryption algorithm for ensuring the security of protected images in against the differential and brute force attacks. Generally speaking, the security of an image encryption algorithm depends on its security key design. An encryption algorithm should contain a sufficiently large key space and should be strongly sensitive to the change of security keys. Here, the sensitivity tests performance of the encryption and decryption processes as shown in Fig. 11.

As can be seen in Fig. 11 that the five modes have low correlation, except the ECB mode, which the pixels are higher correlated than the others modes.

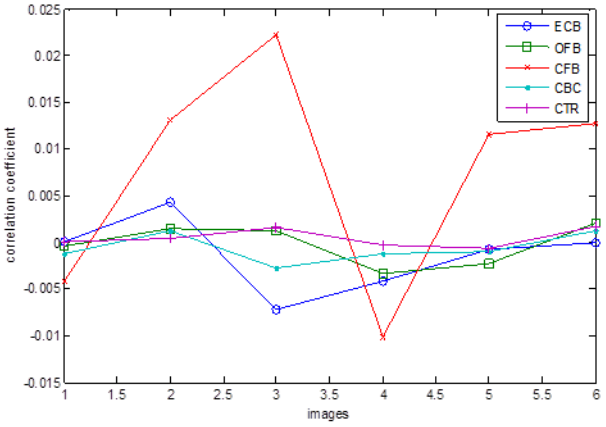

Fig. 11. The sensitivity of Key

D. Integrity Check

For this test, the emission and reception footprint are calculated for the six Meteosat images in CTR mode. The obtained results show in the Table I.

From Table I, the problem of integrity is checked when the image change in the transmission channel because the image of the cryptographic decrypted footprint is different from that of the original images.

TABLE I. INTEGRITY RESULTANT

MSG Images	Footprint emission	Footprint reception
1	16964897393897	14203735824732
2	87151338539745	96443232263919
3	19947467820021	98621115981365
4	19026974966893	16175845459547
5	22994972443810	12356287082727
6	03660222107272	87780179090053

V. CONCLUSION

In this paper, to overcome security, performance, privacy and reliability issues of satellite MSG imagery, a new cryptosystem based on AES and RSA algorithms has been proposed.

Experiment results indicate that the pixel value distribution in the encrypted Meteosat images is even and uniform. The results have been analyzed thoroughly to study the strength of the confusion and diffusion properties, security and resistance level against some known attacks. Compared with other similar encryption schemes [18-20], our algorithm described above has higher security and can resist all kinds of known attacks

The proposed system is not just limited to this area, but can also be widely applied in the secure storage and transmission of confidential MSG images over the Internet and/or any shared network environment.

The tests have done in this study, and the obtained results are encouraged to focus the future research on new methods of integrity in the following areas of security to control integrity:

The marking (watermarking) as regards the insertion of a mark (watermark).

The IDC-hiding (hiding data) which is marked with a large amount of data.

The fingerprint is a form of marking where each object receives a known and unique identification number.

The digital signature is also a brand that simultaneously depends on the information obtained from the clear document and from hash functions.

REFERENCES

[1] Su-Yin Tan, “Meteorological Satellite Systems, Springer Briefs in Space Development,” 125 pp., 2014.

[2] W. Stallings, ‘’Cryptography and Network Security: Principles and Practice’’, 4th ed., Prentice Hall, 2011.

[3] Jonathan Katz, Yehuda Lindell, “Introduction to Modern Cryptography: Principles and Protocols”, ISBN: 978-1-58488-551-1, 2008.

[4] J. Daemen and V. Rijmen, “AES Proposal: The Rijndael Block Cipher,” tech. rep., Proton World Int.l, KatholiekeUniversiteit Leuven, ESAT-COSIC, Belgium, 2002.

[5] J. Daemen, V. Rijmen, “ the Design of Rijndael,” Springer Verlag, New York, Inc. Secaucus, NJ, USA, 2002.

[6] Wen, “AES encryption algorithm analysis and security stupy,” Computer Applications of Petroleum, Vol. 16 No.2, 2008.

[7] A. A. Shtewi, B. E. M. Hasan, A. El Fatah and A. Hegazy, "An Efficient Modified Advanced Encryption Standard (MAES) Adapted for Image Cryptosystems," IJCSNS International Journal of Computer Science and Network Security, Vol.10 No.2,pp.226-232 February 2010.

[8] B. Manoj andN Haribar Manula "Image Encryption and Decryption usingAES" International Journal of Engineering and Advanced Technology(IJEAT) ISSN: 2249 – 8958, Vol. 1, Issue5, June 2012.

[9] H. hamiche, M. lahdir , M. tahanout and S. djennoune , "masking digital image using a novel technique based on a transmission chaotic system and spiht coding algorithm" international journal of advanced computer science and applications (IJACSA), 3(12), 2012.

[10] W. Di-e, M. E. Hellman, "New Directions in Cryptography. IEEE Transactions on Information Theory," IT-22(6):644-654, 1976.

[11] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, 21:120-126, 1978.

[12] S. Ammarah, V. Kaul, "Security Enhancement Algorithm for Data Transmission using Elliptic Curve Diffie - Hellman Key Exchange," International Conference & workshop on Advanced Computing 2014 (ICWAC 2014) – www.ijais.org.

[13] M. Dworkin, "Recommendation for Block Cipher Modes of Operation," NIST Special Publication 800-38A, 2001 Edition.

[14] W. Stallings, "cryptography and network security principles and practice," Prentice Hall Press Upper Saddle River, NJ, USA, 744 pp., 2011.

[15] R.Chakraborty, S. Agarwal, "Triple SV: A Bit Level Symmetric Block Cipher Having High Avalanche Effect,"nternational Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011.

[16] B. Parsharamulun, R. V. Krishnaiah, "A New Design of Algorithm for Enhancing Security in Bluetooth Communication with Triple DES," International Journal of Science and Research (IJSR), Volume 2 Issue 9, September 2013.

[17] S. Singh, S.K. Maakar, "A Performance Analysis of DES and RSA Cryptography," nternational Journal of Emerging Trends & Technology in Computer Science, Volume 2, Issue 3 May – June 2013.

[18] H. T. Panduranga and S. K. Naveen Kumar. "Hybrid approach for image encryption using SCAN patterns and Carrier Images." International Journal on Computer Science and Engineering 2.02 (2010): 297-300.

[19] J. Gao, ''.New Chaotic Image Encryption Algorithm Based on Hybrid Feedback''. Computer Application, 2008,28(2):434..436.

[20] G. Singh &S. Kinger,"Integrating AES, DES, and 3-DES Encryption Algorithms for Enhanced Data Security." International Journal of Scientific & Engineering Research 4.7 (2013): 2058.

AUTHOR PROFILE

Mohammed Belkaid Boukhatem was born in Algeria in 1987. He received his engineering degree in telecommunication from the the national institute of telecommunication and new technologies of information and communication Oran in 2010 and Magister degree in Electronics Remote Sensing from Mouloud Mammeri University of Tizi-Ouzou (Algeria) in 2015. He is currently pursuing his PhD thesis in LAMPA laboratory at Faculty of Electrical Engineering and Computing. His current research interests include image processing, signal processing and Meteosat image coding. His main application domain is cryptography.

Mourad Lahdir was born in Algeria in 1969. He received his Magister degree in Electronic from the Mouloud MAMMERI University of Tizi-Ouzou (Algeria) in 1999 and Ph.D. degree in Electronics Remote Sensing from the Mouloud MAMMERI University of Tizi-Ouzou in 2007. His research activities are image processing, Meteosat and hyperspectral image compression, wavelet and fractal image application, progressive data transmission and watermarking.

Mehdi Cherifi was born in Algeria in 1985. He received his engineering degree in Electronic from the Mouloud Mammeri University of Tizi-Ouzou in 2010 and Magister degree in Electronics Remote Sensing from Mouloud Mammeri University of Tizi-Ouzou (Algeria) in 2015.He is currently pursuing his PhD thesis in LAMPA laboratory at Faculty of Electrical Engineering and Computing. His current research interests include image processing, signal processing, Meteosat image compression.