A Modified AES Based Algorithm for Image Encryption

M. Zeghid, M. Machhout, L. Khriji, A. Baganne, and R. Tourki

***Abstract*—**With the fast evolution of digital data exchange, security information becomes much important in data storage and transmission. Due to the increasing use of images in industrial process, it is essential to protect the confidential image data from unauthorized access. In this paper, we analyze the Advanced Encryption Standard (AES), and we add a key stream generator (A5/1, W7) to AES to ensure improving the encryption performance; mainly for images characterised by reduced entropy. The implementation of both techniques has been realized for experimental purposes. Detailed results in terms of security analysis and implementation are given. Comparative study with traditional encryption algorithms is shown the superiority of the modified algorithm.

***Keywords*—**Cryptography, Encryption, Advanced Encryption Standard (AES), ECB mode, statistical analysis, key stream generator.

I. Introduction

ENCRYPTION is a common technique to uphold image security. Image and video encryption have applications in various fields including internet communication, multimedia systems, medical imaging, Tele-medicine and military communication.

Many image-protection techniques are using vector quantization (VQ) as encryption technique (Chang et al., 2001; Chen and Chang, 2001). In Chang et al. (2001), VQ decomposes an image into vectors, which are then encoded and decoded vector-by-vector. Alternatively, Chen and Chang (2001) use VQ to divide desired images for encryption into a large number of shadows that are guaranteed undetectable to illegal users. Image and text cryptography has been achieved using chaotic algorithms (Fridrich, 1997; Sobhy and Shehata, 2001, Haojiang, Yisheng, Shuyun and Dequn Li 2005). A symmetric block encryption algorithm creates a chaotic map (Fridrich, 1997) for permuting and diffusing image data. For thorough encryption, the chaotic map is applied to the image, iteratively, multiple times. The chaotic algorithm of Sobhy and Shehata (2001) is based on the Lorenz system of equations. Both image and text data are encrypted successfully, but knowledge of the system allows devising an optimization routine that discovers the key by output minimization. Phase encoding techniques exist for encrypting image data (Zhang and Karim, 1999; Park et al., 2001). Color image data is regarded in Zhang and Karim (1999), where a double-phase technique is utilized. Color images are encrypted from an indexed image and thereby decrypted back to its color format. The work of Wu and Kuo (2001) describes selective encryption based on a digital coefficients table. It was shown its limitation due to a less intelligible recovered image. Color and gray-scale images were considered in Koga and Yamamoto (1998), where a lattice-based extension to Visual Secret Sharing Scheme (VSSS) (Naor and Shamir, 1994) was developed. A hashing approach to image cryptography is taken in Venkatesan et al. (2000); wavelet representations of images are obtained, and a new randomized strategy for hashing is introduced. Several cryptosystems exist like as data encryption [3], steganography [14], digital signature (Aloka Sinha, Kehar Singh, 2003) and SCAN (S.S. Maniccama, N.G. Bourbakis 2004) have been proposed to increase the security of secret images. However, one common defect of these techniques is their policy of centralized storage, in that an entire protected image is usually maintained in a single information carrier. If a cracker detects an abnormality in the information carrier in which the protected image resides, he or she may intercept it, attempt to decipher the secret inside or simply ruin the entire information carrier (and once the information carrier is destroyed, the secret image is also lost forever). Another method is to encrypt image data, e.g., using DES (Data Encryption Standard). DES, however, is very complicated and involves large computations. A software DES implementation is not fast enough to process the vast amount of data generated by multimedia applications and a hardware DES implementation (a set-top box) adds extra costs both to broadcasters and to receivers. In order to tackle these problems systems based on advanced encryption standard (AES) where proposed. AES is very fast symmetric block algorithm especially by hardware implementation [7, 11, 12, 15]. The AES algorithm is used in some applications that require fast processing such as smart cards, cellular phones and image-video encryption. However, a central consideration for any cryptographic system is its susceptibility to possible attacks against the encryption algorithm such as statistical attack, differential attack, and various brute attacks. Block cipher symmetric algorithms; allow different ciphering mode [17]. Electronic CodeBook (ECB) is the most obvious mode; ciphered blocks is a function of the corresponding plaintext block, the algorithm and the

Manuscript received March 4, 2007. This work was supported by Tunisian/French CMCU project and Sultan Qaboos University, Oman.

M. Zeghid, M. Machhout, and R. Tourki are with the Electronics and Micro-Electronic Laboratory (LEME), Monastir, Tunisia.

L. Khriji is with the Department of Electrical and Computer Engineering, Sultan Qaboos University, Muscat, Oman. He is on leave from the Institut Supérieur des Sciences Appliquées et de Technologie de Sousse (ISSATS), Tunisia (e-mail: lazhar@squ.edu.om).

A. Baganne is with LESTER-University of South Brittany, Lorient, France.

secret key. Consequently a same data will be ciphered to the same value; which is the main security weakness of that mode [1, 15, 19, 20]. CBC mode provides improved security since each encrypted block depends also on the previous plaintext block. Its use proves limited in an encryption image due to the processing time. There are two levels of security for digital image encryption: low-level security encryption and high-level security encryption. In low-level security encryption, the encrypted image has degraded visual quality compared to that of the original one, but the content of the image is still visible and understandable to the viewers. In the high-level security case, the content is completely scrambled and the image just looks like random noise. In this case, the image is not understandable at all to the viewers. This paper proposes new encryption schemes as a modification of AES algorithm. The modification is done by adding a key stream generator, such as (A5/1, W7), to the AES image encryption algorithm in order to increase the image security and in turn the encryption performance.

This paper is organized as follows. Section 2, gives a brief survey of AES techniques. Section 3 evaluates the performance of AES algorithm with respect to the security in image encryption. Section 4 announces the proposed encryption algorithm and describes its hardware implementation. Experimental results are shown in section 5, and discuss the efficiency of the proposed algorithm scheme. The last section concludes the paper.

II. AES Algorithm

Rijndael is a block cipher developed by Joan Daemen and Vincent Rijmen. The algorithm is flexible in supporting any combination of data and key size of 128, 192, and 256 bits. However, AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4×4 matrix that is called the state. For full encryption, the data is passed through Nr rounds (Nr = 10, 12, 14) [4, 6]. These rounds are governed by the following transformations:

(i) *Bytesub transformation:* Is a non linear byte Substitution, using a substation table (s-box), which is constructed by multiplicative inverse and affine transformation. The Fig.1 shows the step of the Bytesub transformation.

(ii) *Shiftrows transformation:* Is a simple byte transposition, the bytes in the last three rows of the state are cyclically shifted; the offset of the left shift varies from one to three bytes.

(iii) *Mixcolumns transformation:* Is equivalent to a matrix multiplication of columns of the states. Each column vector is multiplied by a fixed matrix. It should be noted that the bytes are treated as polynomials rather than numbers.

(iv) *Addroundkey transformation:* Is a simple XOR between the working state and the roundkey. This transformation is its own inverse.

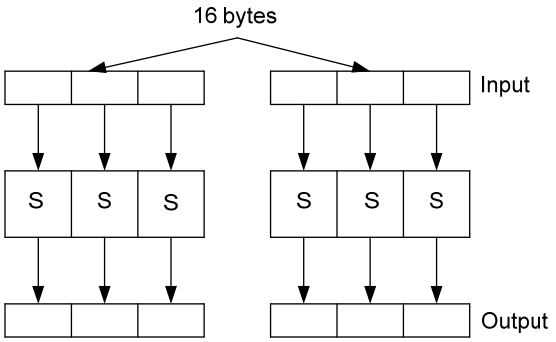


Fig. 1 Block diagrams for Substitution

The encryption procedure consists of several steps as shown by Fig. 2. After an initial addroundkey, a round function is applied to the data block (consisting of bytesub, shiftrows, mixcolumns and addroundkey transformation, respectively). It is performed iteratively (N_r times) depending on the key length. The decryption structure has exactly the same sequence of transformations as the one in the encryption structure. The transformations Inv-Bytesub, the Inv-Shiftrows, the Inv-Mixcolumns, and the Addroundkey allow the form of the key schedules to be identical for encryption and decryption.

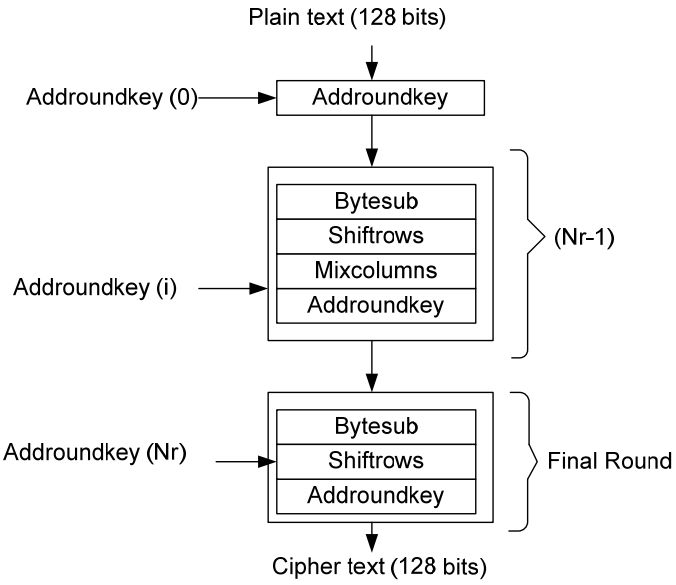


Fig. 2 AES algorithm- Encryption Structure

III. Security Analysis by Statistical Approach

A good encryption scheme should resist all kinds of known attacks, such as known-plain-text attack, cipher-text attack, statistical attack, differential attack, and various brute-force attacks. Some security analysis techniques perform on the AES image encryption scheme, including the statistical analysis and key space analysis.

1) Statistical Analysis

Shannon suggested two methods of diffusion and confusion in order to frustrate the powerful attacks based on

statistical analysis [18]. Statistical analysis has been performed on the AES, demonstrating its superior confusion and diffusion properties which strongly defend against statistical attacks. This is shown by a test on the histograms of the enciphered image and on the correlation of adjacent pixels in the ciphered image.

a) Histograms of Encrypted Images

We select several grey-scale images (256×256) having different contents, and we calculate their histograms. One typical example among them is shown in Fig. 3. We can see that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration. Moreover, there is no loss of image quality after performing the encryption/decryption steps [9].

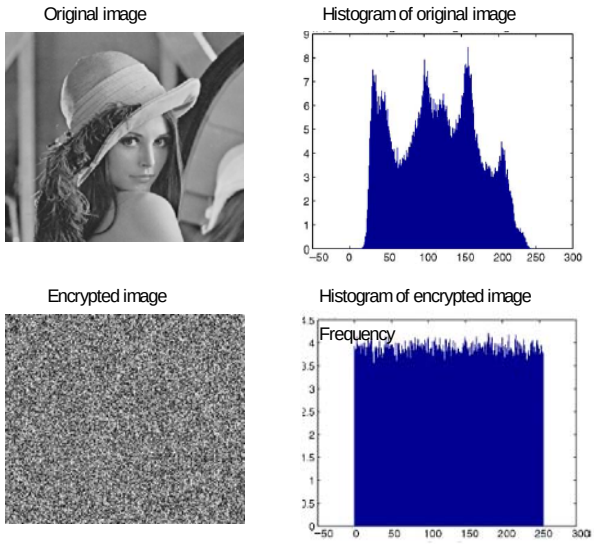


Fig. 3 Histograms of the plain image and ciphered image

b) Correlation of Two Adjacent Pixels

We test the correlation between two vertically adjacent pixels, and two horizontally adjacent pixels respectively, in a ciphered image. First, we randomly select n pairs of two adjacent pixels from an image. Then, we calculate the correlation coefficient of each pair by using the following formula.

$$cov(x,y) = E(x - E(x))(y - E(y)) \quad (1)$$

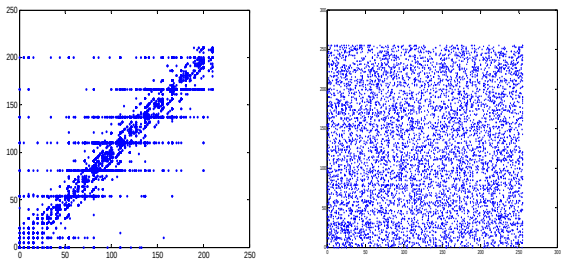
Where x and y are grey-scale values of two adjacent pixels in the image. Figs. 4(a)-(b) show the correlation distribution of two horizontally adjacent pixels in the plain-image and in the ciphered image, respectively. Simulation results for horizontal and vertical directions were illustrated in Table I.

2) Key Space Analysis

A good encryption scheme should be sensitive to the secret keys, and the key space should be large enough to make brute-force attacks infeasible [16, 5, 10]. In our case, the key space size is 10^{128}. It is large enough to resist at all type of brute-force attacks. The experimental results also demonstrate that AES is very sensitive to the secret key. Table I illustrates the sensitivity of AES to the secret key k_i. Fig. 4(a) shows Lena-image encrypted using different k_i. As can be seen when the secret key k_i is changed slightly the encrypted image becomes absolutely different. Similar results can be obtained for correlation coefficients as shown in Table II. As we can see, the sensitivity to key which is the main characterization of AES algorithm guarantees the security of our scheme. Undoubtedly, the secret keys are secure enough even when a chosen plaintext/ciphertext attack is adopted.

TABLE I
CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN TWO IMAGES (LENA TEST IMAGE ENCRYPTED USING DIFFERENT K_i)

Correlation	horizontal	vertical
Plain image	0,93	0,95
Image encrypted by k_1	0,058	0,051
Image encrypted by k_2	0,036	0,035
Image encrypted by k_3	0,047	0,044
Image encrypted by k_4	0,06	0,054



(a) (b)

Fig. 4 Correlation of two horizontally adjacent pixels; (a) in the plain-image, and (b) in the ciphered-image

The AES image encryption system is analyzed thoroughly in this section. By studying the strengths of the confusion and diffusion properties, and its security against statistical attack, AES ensures a high security for ciphered image. But the security of the scheme is based on the complexity of AES and the image proprieties. In Electronic CodeBook (ECB) mode; ciphered block is a function of the corresponding plaintext block, the algorithm and the secret key. Consequently a same data will be ciphered to the same value; which is the main security weakness of that mode and the image scheme encryption. In fact, if the image contains homogeneous zones, all the same blocks remain also the same after ciphering. In this case encrypted image will also contain textured zones and the entropy of the image is not maximal. One typical example among them is shown in Fig. 5.

A number of different objective measures can be utilized for quantitative comparison of the performance of the different algorithms. These criteria provide some measure of closeness between two digital images by exploiting the

differences in the statistical distributions of the pixel values. In our study the following metrics have been used.

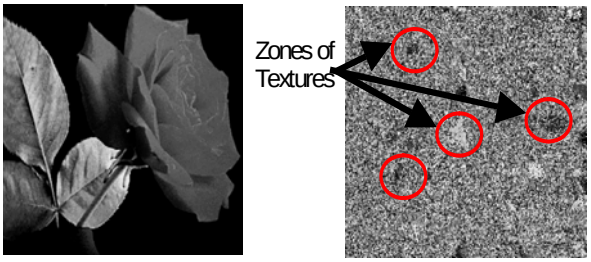


Fig. 5 Rose encryption - Appearance of textures zones

- Entropy and correlation: Let A be an image of size N. The entropy of A is written as,

$$H(A) = -\sum_{i=0}^{255} p(x_i) log_2(p(x_i)); \quad (2)$$

Where $p(x_i) = n/N$ is the correlation of the pixel xi, and n is the number of grey levels that repeat themselves.

TABLE II
CORRELATION AND ENTROPY RESULTS

Test image = Lena	Plain image	Ciphered image
horizontal Correlation	0,92	0,066
vertical Correlation	0,93	0,077
Entropy	4,604	7,91

- The PSNR measure quantifies the difference between the original image and the smoothed one. The PSNR value related to the test image is PSNR = 6.88 (db).

In order to improve safety the encryption performance of the proposed method against the statistical analysis, key stream generator is added to AES image encryption.

IV. MODIFIED AES ALGORITHM

The new image encryption scheme is a modified AES algorithm. It is formed by the AES algorithm and a key stream generator as shown in Fig. 6. The latter has two different forms; (i) A5/1 key stream generator and (ii) W7 key stream generator.

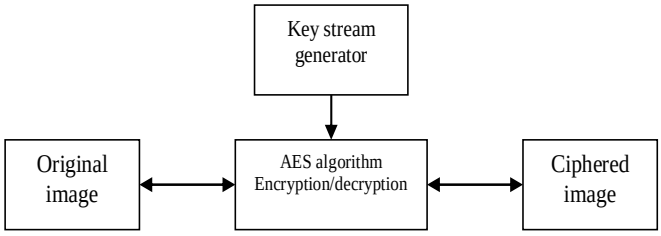


Fig. 6 New AES image encryption scheme

1) A5/1 Key Stream Generator

The A5/1 cipher is composed by three Linear Feedback Shift Registers (LFSRs); *R1*, *R2*, and *R3* of length 19, 22, and 23 bits, respectively. Each LFSR is shifted, using clock cycles that are determined by a majority function. The majority function uses three bits; C1, C2, and C3. The 64 bits of the key map to the LFSR's initial state as: R1(19 bits): $x^{19} + x^5 + x^2 + x + 1$, R2(22 bits): $x^{22} + x + 1$,R3(23 bits): $x^{23} + x^{15} + x^2 + x + 1$. At each clock cycle, after the initialization phase, the last bits of each LFSR are XORed to produce one output bit [2, 8].

2) W7 Key Stream Generator

The W7 algorithm is a byte-wide, synchronous stream cipher optimized for efficient hardware implementation at very high data rates. It is a symmetric key algorithm supporting key lengths of 128 bits. W7 cipher contains eight similar models; C1, C2,…., C8. Each model consists of three LFSR's and one majority function. W7 architecture is composed by a control unit and a function unit [8]. The function unit is responsible of the key stream generation. The proposed architecture for the hardware implementation of one cell is presented in Fig. 7. Each cell has two inputs and one output. The one input is the key and it is the same for all the cells. The other input consists of control signals. Finally, the output is of 1-bit long. The outputs of each cell form the key stream byte.

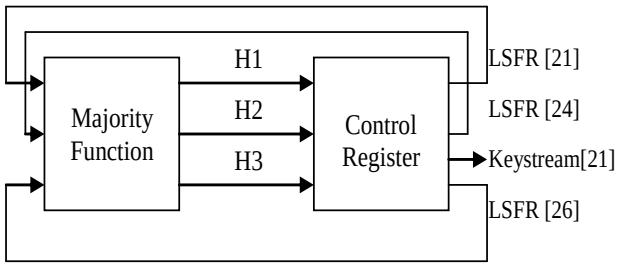


Fig. 7 W7 key stream generator proposed architecture

V. EXPERIMENTAL RESULTS

First, the AES image encryption algorithm is tested and evaluated based on software and hardware simulation. The results are obtained from a xilinx Virtex_II FPGA. Different standard images have been used "lena," "lisaw," "mouse," "cheetah" and "rose" (greyscale format) in the simulations which are performed with three existing image encryption algorithms; "VC", "MIE", "N/KC" in addition to our proposed scheme which includes AES. Table III shows the average time required by AES for each image. Table IV examines quantitatively the encryption time of the MIE, the VC, the N/KC and the AES algorithms. We can note clearly that AES algorithm is much faster then its counterpart.

TABLE III
AVERAGE TIME REQUIRED BY AES FOR DIFFERENT IMAGES

Image (Size)	**Encryption time**
Lisaw (256×256)	31.75 ms
Lena(256×256)	31.75 ms
Cheetah(200×320)	29,25 ms
Clown (200×320)	29,25 ms
Rose (200×320)	29,25 ms
Mouse (200×320)	29,25 ms

TABLE IV
ENCRYPTION TIME USING DIFFERENT ALGORITHMS WITH LENA AS TEST IMAGE

Algorithm	Encryption (s)
MIE	0,27
VC	1,98
N/KC	0,15
AES	0,03175

The following experimentation compares the AES algorithm and the AES with key stream generator. Results are given in Table V. When evaluating a given implementation, the throughput of the implementation and the hardware resources required to achieve this throughput are usually considered as the most critical parameters. All the designs were synthesized in a xilinx Virtex_II, for having a common hardware device for the comparison. For sequential design in ECB mode, the implementation occupies 52 % of area. The data blocks are accepted after each 10 clock cycles and similarly, the output blocks appear after each 10 clock cycles. The design uses a system clock of 129 MHz. Therefore, the data is processed at a rate of 1651 Mbits/sec. As illustrated in Table V, the A5/1 key stream generator has minimal area since its architecture is quite simple. We notice, in spite of the addition of A5/1 or W7, the throughput of the AES remains unaltered.

TABLE V
CIPHER PERFORMANCE AND AREA COMPARISON

Cipher	Area en %	Frequency (Mhz)	Throughput (Mbps)
A5/1	8,64	269.2	-
W7	14.16	176.9	-
AES+A5/1	62.81	128.6	**1646**
AES+W7	59.75	128.6	**1646**
AES	52.8	129	**1651**

This experimentation discusses the security issues. Table VI compares our newly image encryption scheme with AES image encryption in terms of correlation, entropy and PSNR.

TABLE VI
COMPARATIVE RESULTS IN TERMS OF CORRELATION, ENTROPY AND PSNR

Encryption algorithm	AES	AES+A5/1	AES+W7
Correlation vertical	0,066	0,077	**0,03**
Correlation Horizontal	**0,046**	**0,056**	**0,02**
PSNR	6,88	6,83	**6,77**
Entropy	7,91	7,96	**~8**

The correlation passes from 0,056 for A5/1 as generator of keys to 0.02 for W7. The W7 key stream generator improves the security of the AES algorithm. However, the entropy of the image becomes closer to the maximum value (which is 8). Moreover, the use of key stream generator for all types of images (either textured or not) improves the encryption security. We can see clearly at Fig. 8 that the noisy points are disappeared from the textures zones.

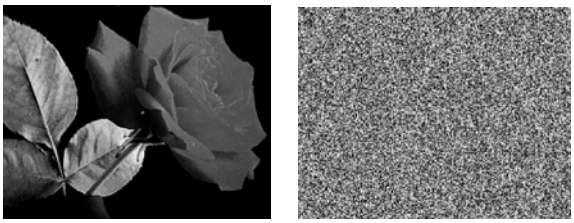


Fig. 8 Disappearance of texture zones

VI. CONCLUSION

In this paper a new modified version of AES, to design a secure symmetric image encryption technique, has been proposed. The AES is extended to support a key stream generator for image encryption which can overcome the problem of textured zones existing in other known encryption algorithms. Detailed analysis has shown that the new scheme offers high security, and can be realized easily in both hardware and software. The key stream generator has an important influence on the encryption performance. We have shown that W7 gives better encryption results in terms of security against statistical analysis attacks.

REFERENCES

[1] N. Bourbakis, A. Dollas, Scan-based compression-encryption hiding for video on demand. *IEEE Multimedia Mag*. 10, 79–87, 2003.

[2] A. Canteaut and E. Filiol, "Ciphertext Only Reconstruction of LFSR-based Stream Ciphers ", Institut national de recherche en informatique et en automatique (INRIA), Technical report No 3887, Feb. 2000 Theme 2.

[3] H. Cheng, L. Xiaobo, Partial encryption of compressed images and videos. *IEEE Trans. Signal Process*. 48 (8), 2439–2451, 2000.

[4] J. Daemen, V. Rijmen, "The block cipher Rijindael", *Proceedings of the Third International Conference on smart card Research and Applications, CARDIS'98*, Lecture Notes in computer Science, vol.1820, Springer, Berlin, 2000, pp.277_284.

[5] N. Ferguson, J. Kelsey, S. Lucks, B. Schneier, M. Stay, D. Wagner, D. Wagner, and D. Whiting. Improved cryptanalysis of Rijndael. In Bruce Schneier, editor, *Proceedings of Fast Software Encryption – FSE'00*, number 1978 in Lecture Notes in Computer Science, pages 213–230. Springer-Verlag, 2000.

[6] Federal Information Processing Standards Publications (FIPS 197), "Advanced Encryption Standard (AES) ", 26 Nov. 2001.

[7] K. Gaj, P.Chodowiec, "Fast implementation and fair comparison of the final candidates for advanced encryption standard using field programmable gate arrays", in : *CT-RSA 2001,* pp.84-99.

[8] M.D. Galanis, P. Kitsos, G. Kostopoulos, N. Sklavos, O. Koufopavlou, and C.E. Goutis, "Comparison of the hardware architectures and FPGA implementations of stream ciphers" in *Proceedings of 11th IEEE International Conference on Electronics, Circuits and Systems (ICECS'04)*, Dec. 13-15, 2004.

[9] J.J. Amador, R. W.Green "Symmetric-Key Block Cipher for Image and Text Cryptography": International Journal of Imaging Systems and Technology, No. 3, 2005, pp. 178-188.

[10] H. Gilbert, M. Minier. A collision attack on 7 rounds of Rijndael. In *The third Advanced Encryption Standard Candidate Conference*, pages 230–241, NIST, April 2000. See http://www.nist.gov/aes.
[11] A. Hodjat, I. Verbauwhede, "A 21.54 Gbits/s Fully Pipelined AES Processor on FPGA". *Proceedings of the 12th Annual IEEE Symposium on Field-Programmable Custom Computing Machines (FCCM'04)*.
[12] K. Janvinen, M. Tominisko, J. Skytta, "A fully pipelined memorlyess 17, 8 Gpbs AES-128 encryptor", in *International symposium of Field programmable Gate arrays*, 2003, pp.207-215.
[13] S.S. Maniccama, N.G. Bourbakis, "Image and video encryption using SCAN patterns", in *Pattern Recognition 37* (2004), pp 725 – 737.
[14] L.M. Marvel, G.G. Boncelet, C.T. Retter, Spread spectrum image steganography, *IEEE Trans. Image Process*, 8 (8), 1075–1083, 1999.
[15] M. Mclone, J.V. McCanny, "Rijindael FPGA implementations utilizing look-up tables", *J.VLSI signal process*, syst. 34(3)(2003)261-275.
[16] R. C.-W. Phan, "Impossible differential cryptanalysis of 7-round Advanced Encryption Standard (AES)", *Information processing letters 91(2004) 33-38*.
[17] B. Schneier, Applied Cryptography: Protocols, Algorithms and Source Code in C. John Wiley and Sons, 1996.
[18] C.E. Shannon, "Communication theory of secrecy system", Bell syst Tech,, 1949; 28; 656-715.
[19] L. Shiguo, S. Jinsheny, W. Zhiquan, "A block cipher based a suitable of the chaotic standard map", *chaos, solutions and fractals 26(2005) 117-129*.
[20] L. Shujun, Z. Xuan, M. Xuanqin, C. Yuanlong, "chaotic encryption scheme for real time digital video", SPIE vol.4666,p.149-160, *Real-Time Imaging*, March 2002.

M. Zeghid received his M.S. degree in Materiaux et Dispositif pour l'electronique from the Science Faculty of Monastir, Tunisia, in 2005, respectively. Currently, he is a PhD student. His research interests include Security Networks, implementation of standard cryptography algorithm, Multimedia Application, Network on Chip: NoC. He is working in collaboration with LESTER Laboratory, Lorient, France.

M. Machhout was born in Jerba, on January 31 1966. He received MS and PhD degrees in electrical engineering from University of Tunis II, Tunisia, in 1994 and 2000 respectively. Dr Machhout is currently Assistant Professor at University of Monastir, Tunisia. His research interests include implementation of standard cryptography algorithm, key stream generator and electronic signature on FPGA.

Lazhar Khriji received his BS degree in electronics, and his MS and PhD degrees in electrical engineering from University of Tunis II, Tunisia, in 1990, 1992 and 1999, respectively. In 2002, he received the Doctor of Technology degree in Information Technology from Signal Processing Institute, Tampere University of Technology, Finland. Dr. Khriji is currently Associate Professor at University of Sousse, Tunisia. From 2002, he is in sabbatical leave with Sultan Qaboos University, Oman. From 1997 to 1999 he was a research scientist with the Research Institute for Information Technology, Tampere, Finland. His research interests include Signal and image processing and analysis, nonlinear filtering, Adaptive filtering, Image coding, Image encryption, Genetic algorithms, Fuzzy logic, Hardware implementation of DSP algorithms.

A. Baganne born in 1968 is presently an Associate Professor at the UBS University and member of the LESTER Lab. He received his Ph.D. degree in Signal Processing and Telecommunications at the University of Rennes, France,in 1997 and the Engineer degree in Electronics from the National Superior Engineering School in Angers (ESEO), France, in 1993. His research interests include communication synthesis, codesign, co-simulation, computer architecture, VLSI design and CAD tools.

R. Tourki was born in Tunis, on May 13 1948. He received the B.S. degree in Physics (Electronics option) from Tunis University, in 1970; the M.S. and the Doctorat de 3eme cycle in Electronics from Institut d'Electronique d'Orsay, Paris south University in 1971 and 1973 respectively. From 1973 to 1974 he served as microelectronics engineer in Thomson CSF. He received the Doctorat d'etat in Physics from Nice University in 1979. Since this date he has been professor in Microelectronics and Microprocessors with the physics department, Faculte des Sciences de Monastir. His current research interests include: Digital signal processing and hardware software codesign for rapid prototyping in telecommunications.