International Journal of Computer Theory and Engineering, Vol. 1, No.2, June 2009
1793-8201

DWT-AES Processor for a Reconfigurable Secure Image Coding

D. Dia, M. Zeghid, M. Atri, B. Bouallegue, M. Machhout and R. Tourki

***Abstract*—In this paper, we proposed a reconfigurable secure image codec based on the Discrete Wavelet Transformation (DWT) and the Advanced Encryption Standard (AES) processor. Either, use of image coding with DWT or encryption using AES is well known. However, linking these two designs to achieve secure image coding is leading. The prominent feature of this method is a partial encryption of bass frequency (LL bands) by AES-128 (128-bit keys), or AES-192 or AES-256. Our approach provides considerable levels of security (key size, partial encryption, encryption mode), and has very limited adverse impact on the compression efficiency. The proposed codec can provide up to 9 cipher schemes within a reasonable software cost. Correlation, PSNR and compression rate results from these codec are analyzed**

***Index Terms*—AES, Band LL, DWT, Partial Encryption, Security Levels.**

I. INTRODUCTION

In the digital world nowadays, the security of digital images/videos becomes more and more important since the communications of digital products over network occur more and more frequently. Since digital video transmission system usually includes a compression module that aims to reduce the transmitted bit rate, the cryptography techniques have to be carefully designed to avoid potential adverse impact on the compression efficiency, and on the functionalities that the compression format provides.

The past decade, several efforts have developed image-video encryption schemes for secure information transfer. These techniques can be classified into three types according to the target data selected from compression stages. The first one is named "Spatial Domain" schemes, which apply encryption to the original information directly like [1]. The second scheme is named "Bitstream Domain", which encrypts the code words of compressed Bitstream like [2]. To reduce the amount of processing overhead, the third schemes as know "Frequency Domain" has been proposed, which utilize the results of DCT or DWT transformation and quantization stages of compression process [3].

To deal with the amount of codec performance and intensive computation given by security mechanisms, this paper proposes a secure image codec configurable. We have proposed our codec by synthesis of the JPEG200 codec and the JPEG Codec.

Manuscript received March 30, 2009.

The authors are with the Electronics and Microelectronics Laboratory, Faculty of Sciences Monastir, 5000 Tunisia (corresponding author Medien. Zeghid: +216-73 501 785; fax: +216-73 501 785).

Our codec present the bloc DWT of JPEG2000 and the bloc Huffman coding of JPEG. So, the sensibility of the Human Visual System (HVS) to DCT based image processing cause a lot error [4]. From this point of view the discrete wavelet transform (DWT) is a very attractive version of the frequency models for the HVS. The Huffman coding presents an advantage to be less complex and few calculations than EBCOT. The JPEG and JPEG2000 codec are presented and compared in [4]. Furthermore, we combine the compression and encryption into single process upon user need. We improved an approach called band LL encryption to reduce encryption and decryption time in image communication and processing. The encryption-decryption effects are achieved by the AES algorithm [5]. In our approach, AES is aim to encrypt group of LL bands. The prominent feature of this method is an encryption of LL bands by AES-128 (128-bit keys), or AES-192 (192-bit keys), or AES-256 (256-bit keys). Instead, we focus on a method that implements partial encryption of LL bands. Our codec can provide up to 9 cipher band LL encryption schemes. Using a security vector, the user can allot a precise security service of his application (security or no, encryption or decryption, key-length, full encryption or LLi band encryption, ECB or CBC mode). Our unified software design can run both our proposed image codec and the extended image codec as know secure image codec.

The rest of this paper is organized as follows. Section 2 introduces our proposed image codec scheme and present results compression comparison of our codec with JPEG2000 and JPEG. In section 3, some blocs of our proposed secure images codec are presented. The first part of this section presents the AES algorithm and some necessary considerations concerning security levels of the cryptosystems. Another part presents the detailed description of the image encryption scheme. Also, the controller module is defined. The illustration of the performances and the efficiency of the proposed secure image codec through analysis security by statistical approach are described in section 4 and 5. Conclusions are drawn in section 6.

II. PROPOSED IMAGE CODEC

Our codec (figure 1) is hybrid, present the bloc DWT of JPEG2000 and the bloc Huffman coding of JPEG. This codec combines the advantages of these both norms. The wavelet transform has emerged as a cutting edge technology, within the field of image compression. Wavelet-based coding provides substantial improvements in picture quality at higher compression ratios [6]. Over the past few years, a

variety of powerful and sophisticated wavelet-based schemes for image compression have been developed and implemented. JPEG 2000, the new ISO/ITU-T standard for still image coding, is wavelet-based compression technique [7]. JPEG is very well known ISO/ITU-T standard created in the late 1980s. There are several mode defined for JPEG, including baseline, lossless, progressive and hierarchical. Baseline mode is the most popular and supports lossy coding only. It is based on the 8x8 block DCT, zig-zag scanning, uniform scalar quantization and Huffman coding. The lossless mode is based on a predictive scheme and Huffman coding.

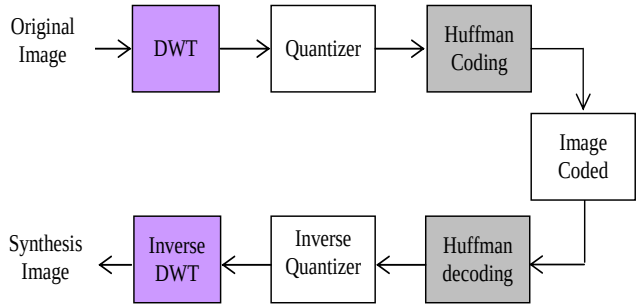

Fig. 1: Bloc diagram of our proposed image codec

A. Discrete Wavelet Transform

The lifting scheme is an algorithm used for implementation of DWT developed in [9] and [10]. It is constituted by predictions and updating steps. We have four steps, two primary lifting steps (predictions) and two others dual lifting steps (updating) for 9/7 filter. However, 5/3 filter based on one prediction and one updating. The result of the wavelet transformation of image is low frequencies coefficients (LL band) and high frequencies coefficients (HH band). The LH and HL bands present the low and high coefficients.

B. Huffman Coding

David Huffman developed a form of encoding that creates the most efficient set of prefix codes for a given text. The ease with which Huffman codes can be created and used makes this still an extremely popular tool for compression code. The Huffman coding is used in popular standards codec like JPEG.

C. Compression Comparison Results

It is well known that the compression performance of an image codec is determined both by the statistical characteristics of the input image and by the capability of the coding algorithm to explore these characteristics. The quality of synthesis image was calculated by Peak Signal to Noise Ratio (PSNR) in decibels (dB) according to the equation (1):

$$PSNR = 10Log_{10}\frac{255^2}{MSE} \qquad (1)$$

Where image coded in 8 bits and MSE the cost function named Mean Squared Error (MSE) given by:

$$MSE = \frac{1}{N \times M}\sum_{i=0}^{N-1}\sum_{j=0}^{M-1}\left(C_{ij} - R_{ij}\right)^2 \qquad (2)$$

Where N×M, is the size of the macro block, C_{ij} and R_{ij} are the pixels being compared in current macro block and reference macro block respectively.

In table I, we compare our lossless compression codec with JPEG2000 and JPEG.

TABLE I LOSSLESS COMPRESSION COMPARISON

Parameter			Our 5/3	JPEG2000	JPEG
Images	Size	Cratio	PSNR	PSNR	PSNR
Bretagne	480x640x3	11.29	46,58	44.25	37
Akiyo	144x176x3	10.91	46,70	46.67	40,8
foreman	144x176x3	9,47	46,65	40,56	32,2
diskus	288x352	11.40	46,55	44,23	42,9

We remark JPEG codec have less PSNR than our lossless codec and JPEG2000. Considering various test images, we obtained better PSNR values for our lossless compression codec at same compression ration (Cratio).

Table II shows performance comparison in terms of PSNR and Compression ratio of our lossy compression codec with JPEG2000 and JPEG codec. In this case JPEG2000 codec perform PSNR than our lossy codec compression. JPEG present less PSNR than two others. Our lossy compression presents better quality (PSNR) synthesis all tests images than JPEG.

TABLE II LOSSY COMPRESSION COMPARISON

Parameter			Our 9/7	JPEG2000	JPEG
Images	Size	Cratio	PSNR	PSNR	PSNR
Bretagne	480x640x3	10.72	40.21	44.25	37
Akiyo	144x176x3	10.50	43.50	46.67	40,8
foreman	144x176x3	08,87	39,24	40,56	32,2
diskus	288x352	10,75	43,29	44,23	42,9

In conclusion our codec present the lossless compression and lossy compression in single process upon the user need. Our lossless compressions perform all test images than they famous software codec, JPEG2000 and JPEG. Therefore our lossy compression, present better quality synthesis images than JPEG and less than JPEG2000.

III. PROPOSED IMAGE SECURE CODEC

This section presents the overflow of our secure image codec. This codec can perform the proposed image codec and the extended codec as know secure image codec upon the user need. The top level view of the secure codec is shown in figure 2.

Our goal is to provide up to 9 cipher schemes: full encryption, LL band encrypted, LL2 band encrypted (6,25% of transformed data is encrypted). The encryption-decryption effects are achieved by the AES algorithm. The flow data through the secure codec is through DWT module and then the AES module while the controller take cares of reading the instructions.

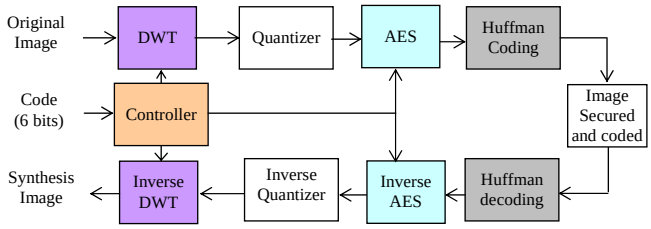

Fig. 2: Design of the secure image codec

A. AES Algorithm

AES is a block cipher with variable key length (128-bit, 192-bit, and 256-bit respectively) and block size of 128-bit. Our design has covered the three versions [11]. The only differences are the number of rounds performed (Nr) and round keys needed. In our case of variable key size, Nr equals 10, 12 or 14. Its key setup time is excellent, and its key agility is good. AES very low memory requirements make it very well suited for restricted-space environments, in which it also demonstrates excellent performance.

The defense community has classified the information into different levels of trust and sensitivity. These levels represent the well-known security classifications, namely, Low, Medium, and High security. The U.S National Security Agency (NSA) has conducted a review of the AES encryption algorithm and its applicability to the protection of national security information. In June 2003, the NSA review determined that the design and the strength of all three AES key lengths are sufficient to protect classified U.S government information up to the 'SECRET' level. Their review concluded that only the AES 256-bit key length was strong enough to protect classified information at the "High security" level (top level security). Furthermore, the key length in AES could be used as a variable of security vector.

B. Controller module

The controller is a module needed for optimizing applications security requirements based on a variable system resources. Conceptually, it is an engine or security-critical real-time system to achieve a high system performance in terms of quality of security. The input of the controller is a security service attribute-value vectors specified by users, and the output is an array of selective values for each required security service. The most important abstraction in our controller module is security levels, which is used to indicate how strength is a particular security service?

Users can define their security requirements for a particular security service by specifying a security range. Figure 3 illustrates the structure of the security vector, which consists of 6 bits. The first bit of vector is the security service, when the user choice to encrypt the image data, this bit = '1'. The second bit defines the category of the cryptographic operation (encryption or decryption). Subsequently, there are 2 bits of cryptographic modes. Currently, ECB and CBC modes are implemented in our processor. Also, an extension to other cryptographic modes is expected. Two other fields in the security vector are indicated by Key Pointer (KP) and Protocol Pointer (PP). They refer to the length of the key and the data must be encrypted (full encryption, partial encryption), respectively. As depicted in figure 3 (b), the control AES identify the encryption or decryption scheme.

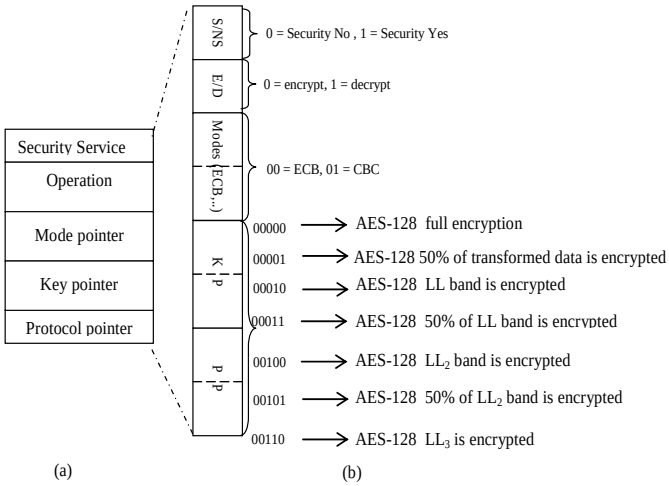

Fig. 3: Security vector: (a) General format; (b) Definition

IV. Security Analysis by Statistical Approach

Shannon suggested two methods of diffusion and confusion in order to frustrate the powerful attacks based on statistical analysis [12]. Statistical analysis has been performed on the proposed secure image coding, demonstrating its superior confusion and diffusion properties which strongly defend against statistical attacks. This is shown by a test on the histograms of the ciphered image and on the correlation of adjacent pixels in the ciphered image. We choose two typical classes of images. The first class of visual data discussed is typical still image data and the test image is Lena at resolution 256x256 pixels. Since this special type of visual data is usually encoded in lossy mode (9/7 filter), the Lena image is lossy transformed in our experiments before encrypted. The coefficients of 9/7 filter are float; therefore based on AES characteristics data; we encrypt only the floor of their coefficients. The second type of digital visual data, as know medical images represent an application class where lossless coding is important (5/3 filter). Heart test image at resolution 256x256 pixels is used in this case.

A. Full Encryption Results

- Histograms

In this case all transformed image is encrypted. Then, we select several grey-scale images having different contents, and we shown their histograms. Two typical examples among them as know Lena and Heart image are shown in figure 4.

We can see that the histograms of the ciphered images are fairly uniform and are significantly different from that of the originals images. 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 and compress/decompress steps.

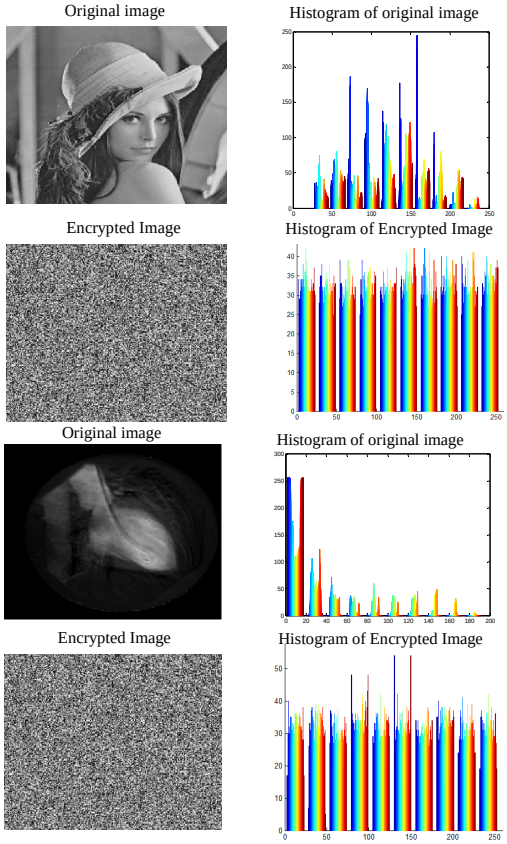

Fig. 4: Histograms of the plain and ciphered images:Lena and Heat

ü Correlation Results

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

$$Cov(x, y) = E[(x - E(x)).(y - E(y))] \quad (3)$$

Where E (.); is the mathematical expectation, x and y are grey-scale values of two adjacent pixels of the image. The horizontal correlation coefficients of original and ciphered Lena image are 0.93 and 0.04 respectively, which are very different. Same results are obtained for Heart image (table III).

TABLE III CORRELATION COEFFICIENTS OF TWO ADJACENT PIXELS IN tested images

Images	Horizontal Correlation	Vertical Correlation
Lena	0.93	0.95
Ciphered Lena	0.0494	0.0513
Heart	1	1
Ciphered Heart	0.0592	0.0625

B. Partial Encryption (LL band encrypted)

Our goal is to enough of the significant information (LLi band), so that it is difficult for the cryptanalyst to determine the meaning of each unencrypted bit. LL bands encryption of transformed images is examined in this subsection. The relative size of the important part and the security of each scheme are then analyzed.

ü Histograms

The histograms of test images used in this experiment are shown in figure 5. Therefore, only 25% (band LL) of transformed data is encrypted. From figure 5, we can see that the histograms of the encrypted images are significantly different from that of the originals images. Therefore, it does not provide any indication to employ any statistical attack on the image under consideration.

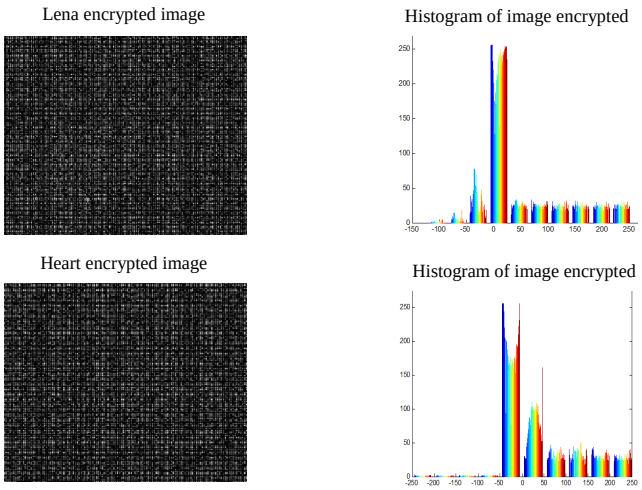

Fig. 5 Histograms of ciphered image (LL band encrypted)

ü Correlation Results

Figure 6 show the correlation distribution of two horizontally adjacent pixels in the plain-image and that in the ciphered image (LL is encrypted):

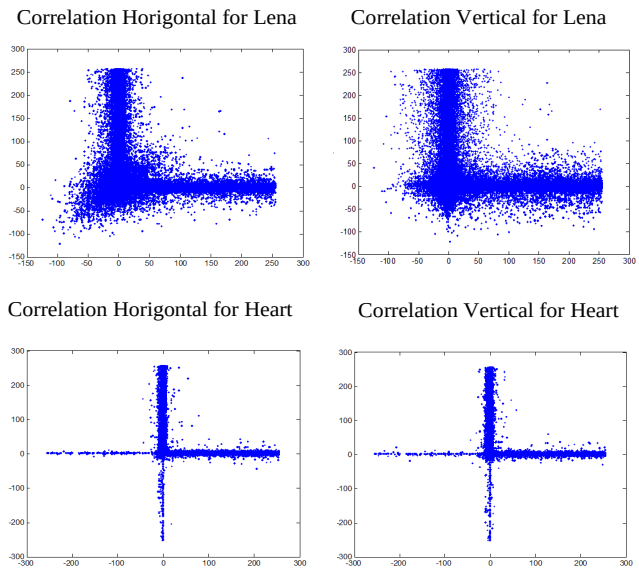

Fig. 6: Correlation of two horizontally and vertically adjacent pixels in the Lena and Heart encrypted LL band

For the both images; the horizontal correlation is approximately identical to the correlation vertical. Therefore the encrypted is uniform in the two directions.

V. SECURE IMAGE CODEC PERFORMANCES

Various experiments have been done to exam the performance of the proposed secure codec. The test images were decomposed into 6-level DWT. The proposed codec use the propriety of multi-resolution analysis of wavelet to achieve various purposes of selective encryption. The decomposition multi-resolution of low frequency coefficients allow us to encrypt the essential information that expressed as a frame percentage.

A. *Correlation* sensitivity

Figure 7 and figure 8 shows the horizontal and vertical correlation, for Lena and Heart test image respectively, as a function of the image percentage which is encrypted.

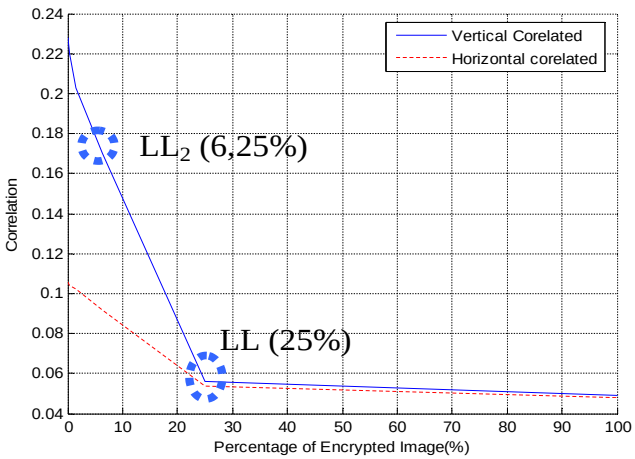

Fig. 7: Correlation sensitive tests: Lena ciphered image

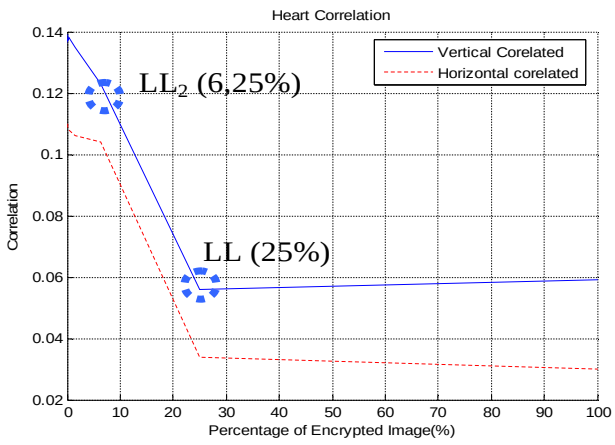

Fig. 8: Correlation sensitive tests: Heart ciphered image

From figure 7 and 8, the following comments can be drawn:

- Design of all AES ciphers schemes (AES-full encryption, AES-band LL_i encryption) took from 0,04 (for AES-128 full encryption) to 0,06 (for AES-128 LL encryption) of the total correlation (0,93). It means that when the frame percentage encrypted is changed from 100% to 25% the correlation becomes slightly different.
- LL bands encryption approach can not be blindly applied to any LL_i bands. We can see, the correlation exceed 0,1 when the frame percentage encrypted is less 6,25% (LL_2). In order to improve safety the encryption performance of this approach (LL_2 band encrypted) against the statistical analysis, CBC mode for AES is configured.

B. *PSNR sensitivit*

The quality of encryption is also expressed in Peak Signal Noise to Ratio (PSNR) of the encrypted image. Figure 9, figure 10 shows the PSNR for Lena and heart tests images respectively, as a function in percentage of encrypted transformed image.

We can see that the PSNR decrease according to the percentage of the quantity of encrypted information for both ciphered images. For lena test image the PSNR is less than 11 dB (PSNR = 6 dB if the lenna is full encrypted) and less than 15 dB for heart test image. This fact shows the high security of the both ciphered images.

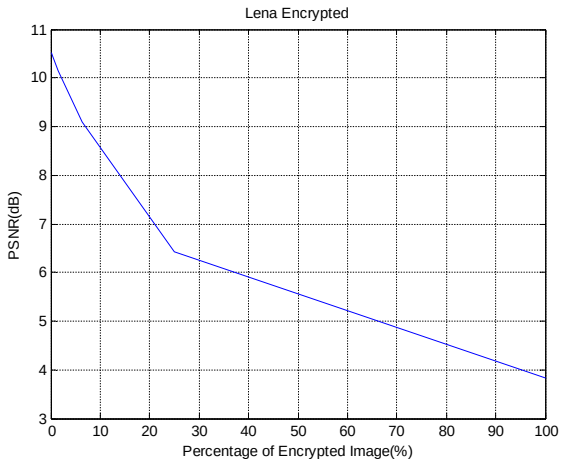

Fig. 9: PSNR sensitive tests: Lena ciphered image

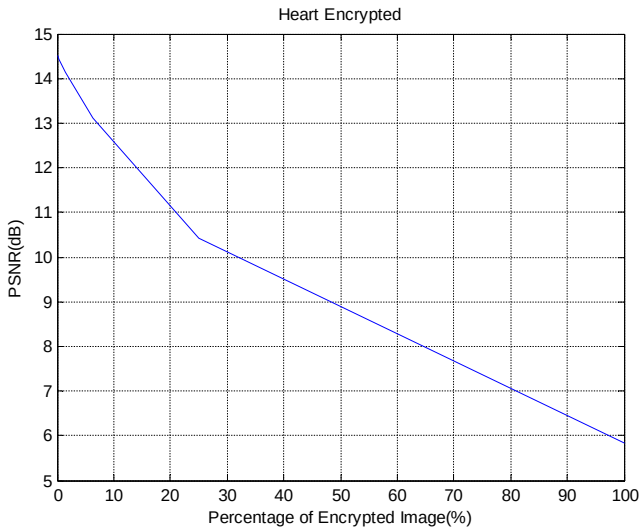

Fig. 10: PSNR sensitive tests: Heart ciphered image

C. *Compression* Ration sensitivity

Compression ratio and PSNR of reconstituted test images in terms of encryption scheme (full encryption, LL_i band encrypted) are presented in table IV, table V and table VI.

From table IV (full encryption), the codec developed in this work provide the same quality of synthesis images (PSNR) if the security service is configured or not (table I and table II). However the compression ratio decrease in

average to 6,63 and 6,04 respectively for lossless and lossy compression.

TABLE IV COMPRESSION RATIO AND PSNR RESULTS: FULL ENCRYPTION

Parameter		Our 5/3		Our 9/7	
Images	Size	Cratio	PSNR	Cratio	PSNR
Bretagne	480x640x3	8,98	46,58	8,98	40.21
Akiyo	144x176x3	8,84	46,70	8,84	43.50
foreman	144x176x3	8,84	46,65	8,02	39,24
Diskus	288x352	8,78	46,55	8,96	43,29

From table V (LL band encrypted), the loss of compression ration is less than full encryption (table IV). It decrease in average to 0,85 and 1,2 respectively for lossless and lossy compression without security. As can be see, hat in almost cases the best performance is obtained by our secure codec in term PSNR of synthesis images.

TABLE V COMPRESSION RATIO AND PSNR RESULTS: LL BAND ENCRYPTION

Parameter		Our 5/3		Our 9/7	
Images	Size	Cratio	PSNR	Cratio	PSNR
Bretagne	480x640x3	9,93	46,58	10,40	40.21
Akiyo	144x176x3	10,15	46,70	9,10	43.50
foreman	144x176x3	8,85	46,65	8,05	39,24
Diskus	288x352	10,73	46,55	10,10	43,29

Table VI present compressions ratios and PSNR for tests images when LL2 band was encrypted. The quality of reconstructed images is similar in the codec without security. The compressions ratios decrease in average to 0,31 for lossless compression and 1,04 for lossy compression compared at our codec without security.

TABLE VI COMPRESSION RATIO AND PSNR RESULTS: LL2 BAND ENCRYPTION

Parameter		Our 5/3		Our 9/7	
Images	Size	ratio	PSNR	ratio	PSNR
Bretagne	480x640x3	10,96	46,58	10,50	40.21
Akiyo	144x176x3	10,64	46,70	9,40	43.50
foreman	144x176x3	9,10	46,65	8,10	39,24
Diskus	288x352	11,13	46,55	10,30	43,29

The Huffman coding is based on the probability of pixels presence, therefore dependent of the percentage of the encrypted image, the coder provides us compression ratios about those of the JPEG2000, to see higher for lossless compression.

Finally, we have found two classes off LL bands encryption schemes for our codec (see figure 11): first class (full encryption, 50% transformed data is encrypted, LL1) requires the largest security and the medium time encryption; second group (LL1 is encrypted, 12,5% transformed data is encrypted, LL2 is encrypted) requires the medium from low security and the low time encryption.

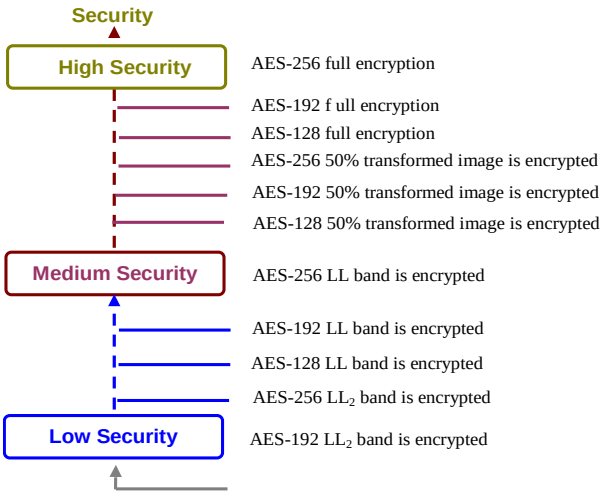

Fig. 11: Secure codec sensitivity performance: security levels

VI. CONCLUSION

In this work we have proposed an image codec with multi level of security based on DWT and AES processor. We extended the AES algorithm and applied it toward the cryptography of continuous image streams. To express the tradeoffs between security and real-time application requirements, we have proposed and developed an AES processor with respect two parameters; security and requirements. We have proposed a partial encryption technique based on AES-128 or AES-192 or AES-256. Taking advantage of the DWT in our codec, one may choose to encrypt LL band with security level goes from low to high. Increased protection is traded off against more encryption time. The percentage of data subjected to encryption while maintaining medium confidentiality is significantly reduced as compared to full encryption, the encryption of 6,25% (LL2 band) data already delivers a satisfying secure result. The actual applicability of the presented approach depends on the scenario in which it is to be used (key size, encryption protocol). Experimental results demonstrate that the proposed secure codec is fast and is well suited to provide high security communication and high compression ratio with low latencies.

REFERENCES

[1] P. Melih and D. Vadi, "A MPEG-2-transparent scrambling technology", IEEE Transactions on Consumer Electronics, 48 (2002), pp.345–355.

[2] L. Qiao and K. Nahrstedt, "Comparison of MPEG encryption algorithms", International Journal on Computer and Graphics, Special Issue on Data Security in Image Communication and Network, 22 (1998), pp.437–448.

[3] G.Liu, T.Ikenaga, S.Goto and T.Baba, "A Selective Video Encryption Scheme for MPEG Compression Standard", in IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 89 (2006), pp. 194-202.

[4] D.Santa-Cruz and T.Ebrahimi, "A study of JPEG 2000 still image coding versus other standards", X European Signal Processing Conference, Tampere, Finland, September 2000.

[5] M. Zeghid, M. Machhout, L. Khriji, A. Baganne and R. Tourki, "A Modified AES Based Algorithm for Image Encryption", International Journal of Computer Science and Engineering,1(2007), pp.70-75.

[6] M. Vetterl Mand and J. Kovacevic, "Wavelets and Subband Coding", Englewood Cliffs, New Jersey, Prentice Hall, 1995, Reissued by authors 2007, http://cm.bell-labs.com/who/jelena/Book/home .html.
[7] ISO/IEC/JTC1/SC29/WG1 N390R, JPEG 2000 Image Coding System, Mars. 2000, http://www.jpeg.org/public/fcd15444-1.pdf.
[8] Information and Communication Theory group, http://ict.ewi.tudelft.nl/index.php, Delft University of technology, last updated 21 July 2005.
[9] D. Dia, M. Atri, R. Tourki, "A Improved Fast Motion Block Matching for Wavelet Video Coding", IEE International Symposium on Signal Processing and Information Technology, Cairo, Egypt, 2007.
[10] D. Dia, M. Atri, R. Tourki, "Improved Fast Motion Block Matching Based Adaptive Rood Pattern Search", 6th International Conference on System Science and Simulation in Engineering, Venice, Italy, November, 2007.
[11] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)", Federal Information Processing Standards Publications (FIPS PUBS) 197-26 (2001).
[12] C.-E. Shannon, "Communication theory of secrecy system", Bell systems Tech journal, 28(1949), 656–715.

interoperability and performance evaluation. He is working in collaboration with LESTER Laboratory, Lorient Cedex France.

Mohsen 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.

Dhaha Dia received his M. S degree in Automatic and Signal Processing from ENIT University of Tunis, Tunisia in 2003. He is currently a member of the Laboratory of Electronics & Micro-electronics. His research includes Image Processing, Compression, and Video Coding.

Medien Zeghid received his M.S. degree in Electronic Materials and Devices from the Science Faculty of Monastir, Tunisia, in 2005. 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.

Mohamed Atri born in 1971, received his Ph.D Degree in Micro-electronics from the Science Faculty of Monastir in 2001. He is currently a member of the Laboratory of Electronics & Micro-electronics. His research includes Circuit and System Design, Image Processing, IPs and SoCs.

Belgacem Bouallegue received his MSc in Physic Microelectronic and his DEA in Electronic Materials and Dispositifs from the Science Faculty of Monastir, Tunisia, in 1998 and 2000, respectively. Currently, he is a PhD student. His research interests include High Speed Networks, Multimedia Application, Network on Chip: NoC, flow and congestion control.

Rached Tourki was born in 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 research includes IP design, Image and Video Processing, cryptography and SoCs.