A Joint Encryption-Compression Technique for Images Based on Beta Chaotic Maps and SPIHT Coding

Najet Elkhalil *, Rim Zahmoul†, Ridha Ejbali‡, and Mourad Zaied§
* †‡§ Research Team in Intelligent Machines, National Engineering School of Gabes,
6072 Gabes, Tunisia
Email: najet.elkhalil@ieee.org rima.zahmoul@gmail.com ridha_ejbali@ieee.org mourad.zaied@ieee.org

***Abstract*—In this paper, we propose a new joint compression-encryption system based on Discrete Wavelet Technique (DWT) and Set Partitioning in Hierarchical Trees (SPIHT) coding for the compression part, and the chaotic standard system (Beta Chaotic Map) for the encryption process. Through the experimental results, the system proposed in this paper has an excellent statistical and cryptographic properties: it resists against common cryptanalytic attacks and provides high picture quality of the reconstructed image.**

Keywords–joint compression-encryption; SPIHT coding; Chaotic systems; Beta Chaotic Map.

I. INTRODUCTION

Recently, information storage and security have received a lot of attention. In image processing, for proving security to an image, several cryptography techniques are proposed. However, most of the Encryption techniques mask some quantity of knowledge to the source image that invariably will increase the dimensions of images, therefore, its storage and transmission time, and from that comes the necessity of data compression.

In literature, researchers try to propose new methods that guarantee the strength of the encryption process and preserve the quality of the compressed image. Arunkumar and Prabu [1] proposed a combination of the Rivest-Shamir-Adleman (RSA) encryption method and the lossless compression technique using SPIHT coding. This combination allows partial data access on the part of the decoder so it produces a better efficiency and less computational complexities. Ou et al. [2] developed an Image Compression Encryption Scheme using DWT, orthogonal wavelet family type Haar and Significance-Linked Connected Component Analysis encoder. For the encryption process, the AAdvanced Enceyption Standard (AES) method is used. The test results show that the reconstructed image has a high quality, and the method used for the encryption is efficient. Xiang et al. [3] proposed a Joint compression and selective encryption based on SPIHT (JCSE-SPIHT). The basic idea of the proposed approach is embedding encryption into SPIHT algorithm. The simulation results show that the proposed method has a high immunity against inherent attacks. To overcome the security issues in some previous works, we have proposed a novel joint Encryption-Compression algorithm.

This paper is organized as follows: Section 2 presented previous related works. In Section 3 DWT and SPIHT coding are described in detail. In Section 4 Beta chaotic map and the encryption process were detailed. Performance and security analysis are given in section 5. Finally, a brief conclusion is drawn in Section 6.

II. RELATED WORKS

In order to achieve better security level, chaos theory was frequently used in image cryptography combined with different compression algorithms. In what follows, some of those works were reviewed. Hamdi et al. [4] proposed a new selective encryption-compression scheme based on SPHIT coding and Chiricov Standard Maps. This scheme aims to integrate the encryption part into the compression one, so simultaneously they obtain an encrypted-compressed image. The approach was divided into three steps: The first step was generating three keys for the encryption process using the Chirikov Standard Map algorithm. The next step was to perform a DWT transformation. The third step is permutation after SPIHT coding. The Simulation results obtained in this approach are 99.91% the NPCR average and 33.51% UACI average. Gupta and Silakari [5] presented a chaos-based compression and encryption scheme using a cascading 3D cat map and standard map. The image is first compressed using curvelet transformation and then encrypted using the chaos 3D cat map. The simulation results show that the PSNR values are over 30dB, the NPCR average is over 99% and the UACI average is below 33%. Goel et al. [6] proposed a compression technique using Discrete Cosine Transform (DCT) and Huffman coding and symmetric cryptosystem technique using the Logistic Map. The experimental results of the proposed method. Also, the method has a high sensitivity key.

All this researches used chaotic maps and several compression techniques. We adopt this approach to create our new algorithm for joint image encryption-compression technique. Our scheme allows to improve image compression quality and security against different attacks.

III. COMPRESSION PART

To achieve better compression result, we combined the DWT and the SPIHT coding algorithm.

A. Discrete Wavelet Transform

The wavelet-based compression technique was created to beat the disadvantages of the discrete cosine transform [7]. The uses of DWT have become very popular within the image and video compression and it is a replacement standard for JPEG 2000 images compression [8][9]. The DWT transforms the plain text images into frequency bands, known as sub-bands LL, HL, LH and HH using filters. For one level decomposition, the DWT represents the image in the form of four sub-bands of lower resolution, one represents the approximation image and the three others show the details of the image with horizontal, vertical, and diagonal orientations as shown in the first part in

 ISBN: 978-1-61208-752-8

Figure 1, the other parts in the Figure show examples of other level decomposition.

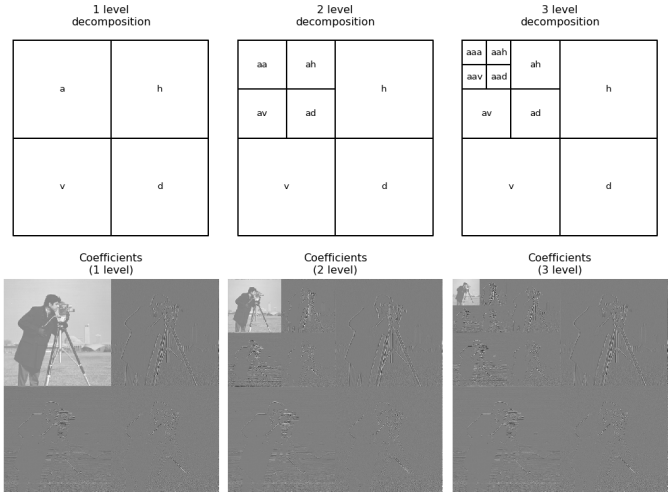

Figure 1. Wavelet Level Decomposition.

B. SPIHT Coding

Once the wavelet transform decomposition is done, several quantization algorithms are used. We decide to work with SPIHT coding because it is an efficient and computationally very fast technique for image compression [10]. The result of the SPIHT coding is an embedded bitstream from which the most effective images are reconstructed. The algorithm of SPIHT coding is defined by steps throughout every state is outlined by a bit-plane that contains an indication of wavelet coefficients that are quantified by the structure in a hierarchical tree. Every coefficient in all spatial orientation tree are then increasingly coded from the Most Significant Bit-plane (MSB) to the Least Significant Bit-plane (LSB), beginning with the coefficients possessing the highest magnitudes within the lowest pyramid levels [11][12]. In every bit-plane SPIHT coding computes a threshold Tp and assign it to one or more of the tree lists bellow:

- List of insignificant pixels (LIP): It contains all the coefficients that have a smaller magnitude than Tp(thresholds).
- List of significant pixels (LSP): It is a list of coefficients of pixels that have a grater magnitude than the Tp.
- List of insignificant sets(LIS): It contains groups (set) of coefficients that are defined by tree structures and they have magnitudes greater than Tp.

The steps of SPIHT coding are mentioned below:

1) Step 1: Initialization
   First of all, initialize the threshold Tp and order coefficients in LL sub-band to LIP, all the trees are moved to LIS and the LSP is empty.
2) Step 2: Sorting Pass
   This step aims to encode the important coefficient of the current bit. There are two main steps:
   a) Step1: verify the contained coefficients in List of significant pixels to check if they are significant coefficients:
      - If they are important, then output 1 and the sign bit of the wavelet coefficients are represented by 1 and 0 (positive or negative), and then remove the wavelet coefficient from LIP and add to the LSP.
      - If they are not important we do not need to remove them from the LIP and the output then will be"0".
   b) Step 2: Verify all the important set in the LIS.
3) Step 3: Refinement Pass
   The aim is output but not the improving position of important factor that was generated in the process of scanning. For all coefficient (i,j) in LSP, if (i,j) is not added in the scanning step, then $|i, j|$of the coefficient will be transmitted.
4) Step 4: Update the threshold
   Updating the threshold by decrements n by 1 and (back to step 2). Variable n defines the maximum number of bits needed to represent the largest coefficient in the spatial orientation tree : $n = |log_2 cmax|$,$cmax$ is the higher value of coefficient.

IV. Encryption Part

In this section, we will detail the chaotic encryption and clarify the steps of the Beta chaotic encryption.

A. Chaotic Encryption

We called Chaotic maps all nonlinear maps that display chaotic behavior, they generate pseudo-random sequences, which are used during the encryption process [13]. Many fundamental concepts in chaos theory, such as mixing and sensitivity to initial conditions and parameters are the same in cryptography. The only difference is that encryption operations are defined on limited sets of integers while chaos is defined on real numbers.

B. Beta Chaotic Encryption

In the recent years, chaotic maps have been used in different ways in cryptography, they have attracted the attention of many researchers and have been widely used in diverse applications [14][15], especially those related to security, in which they have shown excellent performance. The Chaotic system proposed, in the design of our new image compression-encryption algorithm, is based on the Beta Chaotic Map. The Beta Chaotic Maps discovered by professor Mourad Zaied, are inspired from the Beta function it is polynomial mapping and it reflects an example of how complex, chaotic behavior can appear from a simple non-linear dynamical equation [16]-[20]. It is chosen for its efficiency in front of different attacks and it is very suitable with the chosen image compression technique. The steps below describe the encryption process of our scheme:

- Step 1: Resizing the image
  In this step, we resize the chosen image into square dimension.
- Step 2: Generating the chaotic sequences

 ISBN: 978-1-61208-752-8

After making many combinations of Beta chaotic maps, generate two completely different pseudo-random sequences, the sensitivity of the beta chaotic maps to the simple variation of the initial condition gives us the possibility to generate several random sequences.

- Step 3: Permutation stage
  In this step, we shuffle the plaintext images rows and columns using the Beta random sequences (Q1 and Q2) generated in the previous step.
- Step 4: Substitution stage
  At this point, dividing the resulting matrix into four blocks of equal size. After that, translating each one to a random matrix W where each matrix will be transformed using the functions (1) (2) (3) (4)given below:

$$f_N(d) = T(d) mod G \tag{1}$$

$$f_R(d) = T\left\lfloor (\sqrt{d}) \right\rfloor mod G \tag{2}$$

$$f_S(d) = T(d^2) mod G \tag{3}$$

$$f_D(d) = T(2d) mod G \tag{4}$$

And the matrix function is given bellow:

$$W = \begin{bmatrix} \mathrm{f}_N(B_{1,1}) & \mathrm{f}_R(B_{1,2}) & \mathrm{f}_D(B_{1,3}) & \mathrm{f}_S(B_{1,4}) \\ \mathrm{f}_S(B_{2,1}) & \mathrm{f}_D(B_{2,2}) & \mathrm{f}_R(B_{2,3}) & \mathrm{f}_N(B_{2,4}) \\ \mathrm{f}_D(B_{3,1}) & \mathrm{f}_N(B_{3,2}) & \mathrm{f}_S(B_{3,3}) & \mathrm{f}_R(B_{3,4}) \\ \mathrm{f}_R(B_{4,1}) & \mathrm{f}_S(B_{4,2}) & \mathrm{f}_N(B_{4,3}) & \mathrm{f}_D(B_{4,4}) \end{bmatrix} \tag{5}$$

Function T: is a truncation of a decimal to form an integer for every number of the resulting matrix W. G: is the image type, (G=256) and (G=2) for respectively 8-bit gray image and binary image. Here we got a new random integer matrix I. So, we can now determine the encrypted image C using the following equation:

$$C = (P + I) mod G$$

And the decrypted image P by:

$$P = (C - I) mod G$$

- Step 5: Diffusion stage

The main idea of the diffusion stage is to disappear the redundancy in the statics and the information containing in the original image in the encrypted one. It is done by changing each pixel in the original image over the finite field GF(2^8).

To resume, the steps of our encryption-compression algorithm are presented in the flowchart Figure 2:

V. Simulations Results And Comparisons

In this section, different tests are made to evaluate the simulation results: statistical tests: histogram analysis and security tests against a differential attack including calculus of the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). Figures 3 and 4 represent the simulation experiment on Cameraman and Airplane image.

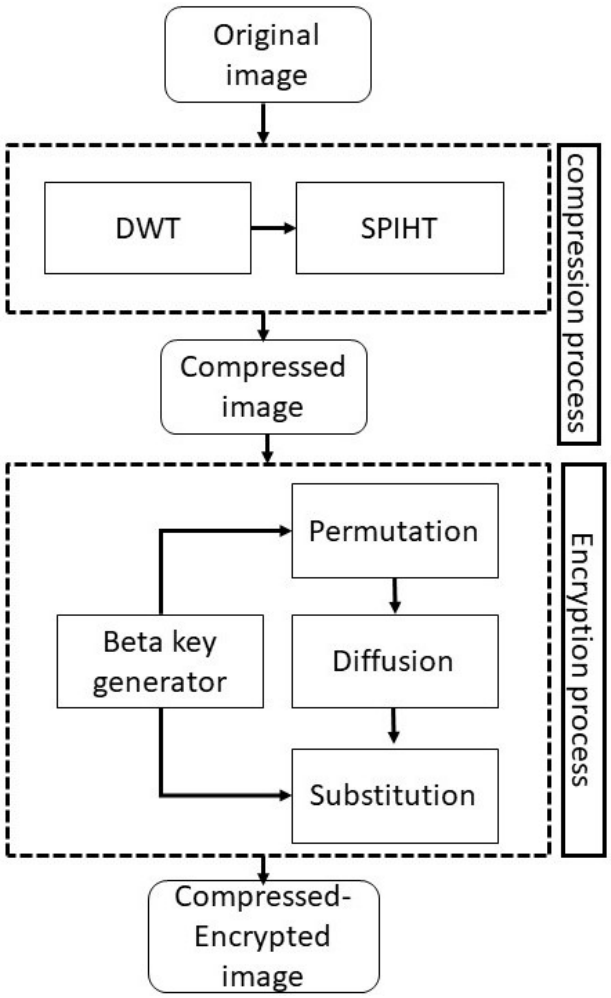

Figure 2. proposed scheme flowchart

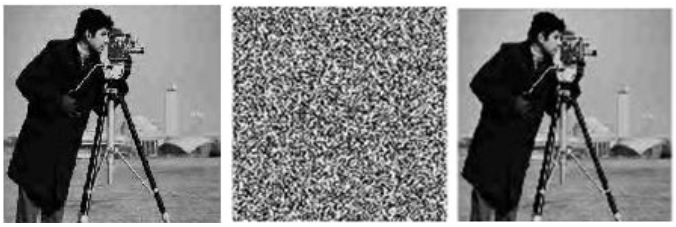

Figure 3. Images of simulation experiment on Cameraman: Cameraman original image, Cameraman compressed-encrypted image, cameraman decrypted image.

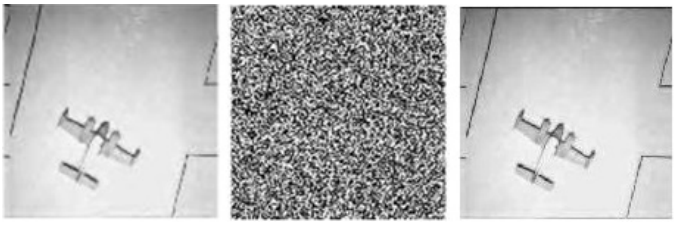

Figure 4. Images of simulation experiment on Airplane: Airplane original image, Airplane compressed-encrypted image, Airplane decrypted image.

 ISBN: 978-1-61208-752-8

A. Histogram Analysis

To avoid the access of data from attackers, it is very important to make sure that the encrypted and the original images are totally different and do not have any statistical similarities. We analyzed the histograms of many cyphered images also as their original images as shown in Figures 5 and 6. The histograms are totally different. The histogram of the

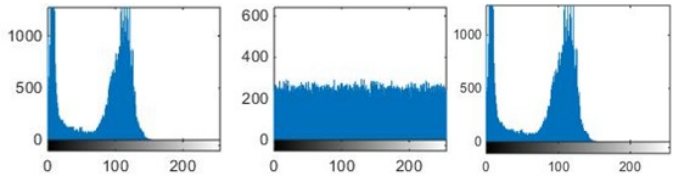

Figure 5. Histograms of experimental image Cameraman:Original image, Compressed-Encrypted image, The decrypted image.

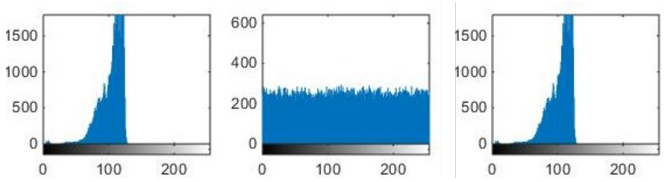

Figure 6. Histograms of experimental image Airplane: Original image, Compressed-Encrypted image, The decrypted image.

original image has massive spikes and its tilted. However, the histogram of the ciphered image is uniform, very flat, and bears no statistical resemblance to the plaintext image. Therefore, by comparison, the histograms of each encrypted-compressed and decrypted images, we tend to conclude that the encrypted images are random-like. Also, it does not give any chance to use any statistical attack on the proposed image encryption scheme.

B. NPCR And UACI Tests

In order to test the fact of one-pixel change on the original and the encrypted image, two measures can be done: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). The NPCR measures the percentage of different pixel numbers between the plaintext image and the cipher image however the UACI measures the average intensity of differences between them [21]. We obtained NPCR and UACI for a large variety of images by using our proposed algorithm and other algorithms, their testing results are shown in Tables 1,2 and 3. Also, we compared the NPCR and UACI of the proposed scheme and also the schemes in [4][22] in Table 2 and 3.

C. Mean Square Error

Mean Square Error (MSE) is the cumulative squared error between the encrypted and the original image. It is one of the error metrics used to evaluate the efficiency of various image encryption techniques. It is defined by the equation below:

$$MSE = \frac{1}{MN} \sum_{y=1}^{M} \sum_{x=1}^{N} [I(x,y) - I'(x,y)]^2$$

Where I(x, y) is the original image pixel, I(x, y) is the encrypted image pixel and M and N are the size of the original or the encrypted one. Our experimental results are shown in Table 4. In case of image encryption, MSE should be as high as possible which means more immunity to attacks.

D. Peak Signal To Noise Ratio Analysis

PSNR (Peak Signal to Noise Ratio) of encrypted image and original image is computed as in Table 4. It is defined by:

$$PSNR = 10_{10} \left[\frac{R^2}{MSE} \right]$$

TABLE I. NPCR AND UACI OF ENCRYPTED IMAGES USING OUR SCHEME.

Image name	NPCR	UACI
Lena (512x512)	99.5666	33.3384
Lena(256x256)	99.6368	33.3886
House	99.5910	33.4736
Boat(522x512)	99.6322	33.3720
Barbara	99.6368	33.5151
Lake	99.6337	33.3384

TABLE II. THE UACI OF ENCRYPTED IMAGES FOR OUR APPROACH AND ALGORITHMS IN [4,22].

Image name	UACI (our approach)	Ref[4]	Ref[22]
Lena (512x512)	33.33	33.51	33.36
Lena(256x256)	33.38	33.69	-
House	33.47	33.96	-
Boat(522x512)	33.37	33.73	-
Barbara	33.51	33.49	-
Lake	33.33	33.49	-

TABLE III. THE NPCR OF ENCRYPTED IMAGES FOR OUR APPROACH AND ALGORITHMS IN [4,22].

Image name	NPCR (our approach)	Ref[4]	Ref[22]
Lena (512x512)	99.56	99.91	99.61
Lena(256x256)	99.63	99.88	-
House	99.59	98.99	-
Boat(522x512)	99.63	99.61	-
Barbara	99.63	99.36	-
Lake	99.63	99.02	-

TABLE IV. MSE AND PSNR OF ENCRYPTED IMAGES USING OUR SCHEME.

Image name	MSE	PSNR
Lena (512x512)	10610.07	7.87
Lena(256x256)	11870.38	7.39
House	6986.46	9.69
Boat(522x512)	7648.06	9.30
Barbara	9645.17	8.29
Lake	9190.15	8.50

The high value of MSE and the low value of PSNR cause the resulting encrypted image more randomness.

VI. CONCLUSION

In this paper, we have proposed a high level secure system of image joint compression-encryption based on SPIHT coding and Beta Chaotic Map. As regards to diverse evaluation metrics, some performance and security analysis has been performed on our scheme. The results of the differential analysis indicate that the proposed encryption-compression algorithm is highly sensitive to small changes in original images. Therefore, it is very resistive against the differential attacks.

 ISBN: 978-1-61208-752-8

ACKNOWLEDGMENT

The authors would like to acknowledge the financial support of this work by grants from General Direction of Scientific Research (DGRST), Tunisia, under the ARUB program.

REFERENCES

[1] M. Arunkumar and S. Prabu, "Implementation of Encrypted Image Compression using Resolution Progressive Compression Scheme," International Journal of Computer Science and Mobile Computing (IJCSMC), vol. 3, no. 6, pp. 585590, 2014.

[2] S.-C. Ou, H.-Y. Chung, and W.-T. Sung, "Improving the compression and encryption of images using FPGA-based cryptosystems," Multimedia Tools and Applications, vol. 28, no. 1, pp. 522, Jan. 2006.

[3] T. Xiang, J. Qu, and D. Xiao, "Joint SPIHT Compression and Selective Encryption," Applied Soft Computing, vol. 21, pp. 159170, Aug. 2014.

[4] M. Hamdi, R. Rhouma, and S. Belghith, "A Selective Compression Encryption of Images Based on SPIHT Coding and Chirikov Standard Map," Signal Processing, vol. 131, pp. 514526, Feb. 2017.

[5] K. Gupta and S. Silakari, "Novel Approach for Fast Compressed Hybrid Color Image Cryptosystem," Advances in Engineering Software, vol. 49, no. 1, pp. 2942, Jul. 2012.

[6] N. Goel, B. Raman, and I. Gupta, "Chaos Based Joint Compression and Encryption Framework for End-to-End Communication Systems," Advances in Multimedia, vol. 2014, pp. 110, 2014.

[7] Z. Xiong, K. Ramchandran, M.T. Ochad, and Ya-Qin Zhang, "A Comparative Study of DC And Wavelet-Based Image Coding," IEEE Transactions on Circuits and System for Video Technology, vol. 9, no. 5, 1999.

[8] S. Grgic, K. Kers and M. Grgic, "Image Compression Using Wavelet," IEEE Transactions, ISIE99-Bled, Slovenia.

[9] M. Zaied, S. Said, O. Jemai, and C. Ben Amar, "A novel approach for face recognition based on fast learning algorithm and wavelet network theory," International Journal of Wavelets Multiresolution and Information Processing, 2011.

[10] E. Christophe, C. Mailhes, and P. Duhamel, "Hyperspectral image compression: adapting SPIHT and EZW to anisotropic 3-D wavelet coding," Image Processing: IEEE Transactions on, vol. 17, no. 12, pp. 2334-2346, 2008.

[11] A. Said and W.A. Pearlman, "A new, fast, and efficient image codec based on set partitioning in hierarchical trees, Circuits and Systems for Video Technology," IEEE Transactions on, vol. 6, no. 3, pp. 243-250, 1996.

[12] AG. Kadam and N. Pingle, "overview of spiht based image compression algorithm,": ijesrt,international journal of engineering sciences research technology, February, 2018.

[13] Y. Wang, et al., "A colour image encryption,algorithm using 4-pixel Feistel structure and multiple chaotic systems," Nonlinear Dynamics. vol. 81, no. 1, pp. 151-168.

[14] X. Wang, W. Zhang, W. Guo, and J. Zhang, "Secure chaotic system with application to chaotic ciphers,"Inform. Sci. vol. 221, no. 7, pp.555-570, 2013.

[15] W. Xu, Z. Geng, Q. Zhu, and X. Gu, "A piecewise linear chaotic map and sequential quadratic programming based robust hybrid particle swarm optimization," Inform. Sci. vol. 218, pp. 85-102, 2013.

[16] R. Zahmoul, R. Ejbali, and M. Zaied, "Image encryption based on new Beta chaotic maps," Optics and Lasers in Engineering vol. 96, pp. 39-49.

[17] R. Zahmoul and M. Zaied, "Toward new family beta maps for chaotic image encryption," 2016 IEEE International Conference on Systems, Man, and Cybernetics (SMC).

[18] M. Zaied, C. Ben Amar and A.M. Alimi, "Award a New Wavelet Based Beta Function,"Second International Conference on Signal,System, Decision and information technology IEEE, SSD03, pp. 185-191, Sousse-Tunisia Mars 2003.

[19] R. Zahmoul, A. Abbes, R. Ejbali, and M. Zaied, "A watermarking scheme based on DCT, SVD and BCM," International Joint Conference: 12th International Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)Optics and Lasers in Engineering, pp. 97-104, 2019.

[20] H. Souden, R. Ejbali, and M. Zaied, "Beta Chaotic Map Based Image Steganography," IEleventh International Conference on Machine Vision, (ICMV) , v. 11041, pp. 1104-1113, 2018.

[21] W. Yue, JP. Noonan, and S. Agaian, "NPCR and UACI randomness tests for image encryption,"Cyber J: Multidiscip J Sci Technol J Sel Areas Telecommun (JSAT) 2011:318.

[22] C. Fu, J.J. Chen, H. Zou, W.H. Meng, Y.F. Zhan and Y.W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," Optics Express. vol. 20, no.3, pp. 2363-2378, 2012.

 ISBN: 978-1-61208-752-8