International Journal of Engineering & Technology, 10 (2) (2021) 208-214

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Hybrid compression-encryption-watermarking image algorithm based on the quaternionic wavelets transform (QWT)

Abena Ndongo Hervé [1, 2] *, Eloundou Ebassa Bertrand Ledoux [3], Abena Malobe Paul [4], Noura Alexendre [4]

[1] *Energy, Signal, Imaging and Automatic Laboratory (LESIA), University of Ngaoundere, Cameroon*
[2] *National Higher School of Agro-Industrial Sciences (ENSAI), University of Ngaoundere, Cameroon*
[3] *Laboratory of Applied Technologies and Sciences (LTSA), University of Douala, Cameroun*
[4] *Departement of Physics, Faculty of Science, University of Ngaoundere, Cameroon*
**Corresponding author E-mail: herveabena@gmail.com*

Abstract

In this article, we present a robust new hybrid algorithm combining successive compression, chaotic encryption, and blind watermarking images based on the quaternionic wavelets transform (QWT) to ensure the fast, simple and secure transfer of digital data. The calculations of the various evaluation parameters were carried out with the aim of determining the robustness of our algorithm against certain attacks. The results obtained of the reconstructed images before and after attacks of the compressed-encrypted-watermarked images are appreciated by calculating the evaluation parameters values and by the human visual system. The application of this hybrid algorithm on CFA images al-lowed us to obtain a stand-alone transmission system and ensure the integrity of digital data.

Keywords: *Compression; Encryption; Blind Watermarking; Chaos; CFA Images; Quaternionic Wavelets Transform.*

1. Introduction

The digital revolution, the boom of communication networks and the ever-increasing public craze for new information technologies are yielding an increased manipulation (storage, exchange or processing) and increased circulation (broadcasting, duplicating, transforming, etc.) of digital data (images, videos, texts, sounds, etc.). The magnitude of these phenomena is such that fundamental questions now arise regarding the storage, control and protection of the data exchanged. To do this, several researchers have been interested in the transfer/storage and protection of digital data through different compression, encryption, watermarking techniques, etc. In front of all of these difficulties, the robust hybrid method combining successive compression-encryption-watermarking has very naturally emerged as an alternative or complementary solution to strengthen the security of those digital data [1, 2]. In the literature, several efficient images compression-encryption-watermarking methods have been developed and satisfy some conditions according to the problem be treated. The must contributions were made to grayscale images [3, 4] and even more to medical images [5, - 8]. However, to our knowledge, the CFA (Color Filter Array) images generated by digital photography [9] have not yet been compressed-encrypted-watermarked using quaternions. CFA images are important for image analysis because these raw images have not undergone any process (interpolation, demosaicking, etc.) that might alter their reliability [10], moreover the raw CFA images are regularly handled in our Laboratory (LESIA) as shown in the work of [11, - 15]. We will therefore be talking about developing and proposing a hybrid method combining successive compression, chaotic cryptography and blind watermarking for the rapid and secure transfer of this digital data. In the rest of this article, we will first present the properties of the quaternionic wavelets transform, then the proposed compression-encryption-watermarking methodology, and finally the presentation and analysis of the results obtained.

2. Quaternionic wavelets transform

2.1. Definition and properties of quaternions

Quaternions are extension of complex numbers [Lord William Hamilton in the 19th century] with a real part and three imaginary parts as follows:

$$q = a + ib + jc + kd, \text{ with } a, b, c, d \in \mathcal{R}, \text{and } i^2 = j^2 = k^2 = ijk = -1 \quad (1)$$

The multiplication of two those imaginary numbers i, j, k behaves like the vector product of orthogonal unit vectors:

$$\begin{cases} i * j = -j * i = k \\ j * k = -k * j = i \\ k * i = -i * k = j \end{cases} \quad (2)$$

The polar writing of a quaternion is analogous to the exponential complex: $q = |q|e^{i\varphi+j\theta+k\beta}$, giving access to the module/argument representation that allows us to separately represent the presence of local components in the image (amplitude), and their structures (phase). The conjugate and the standard of a quaternion are calculated in a similar way to complex numbers. The multiplication of quaternions is associative but not commutative. Quaternions can be represented as a linear combination, a vector of four coefficients, a scalar for the coefficient of the actual part and as a vector for the coefficients of the imaginary part [16 - 18].

2.2. Quaternionic structure of an image

The QWT incorporates the concept of phase into a decomposition into wavelets. Defined from an analytical quaternionic mother wavelet, the QWT provides qualitative coefficients in output, the phase of which accurately describes the coded structures. The power of description of the image already brought by the decomposition in sub-marks, is then supplemented by an even finer description thanks to the phase. The amplitude of a QWT coefficient $|q|$, invariant by translation of the image, quantifies the presence of a component, at any spatial position, in each frequency sub-mark. The phase, represented by three angles (φ, θ, β), provides a complete description of the structure of those components [19]. From a practical point of view, the mother wave is separable i.e., $\psi(x, y) = \psi_h(x)\psi_h(y)$, and considering Hilbert pairs $(\psi_h, \psi_g = \mathcal{H}\psi_h)$ (of wavelets) and $(\phi_h, \phi_g = \mathcal{H}\phi_h)$ (of scale functions), the analytical 2D wavelet is written in terms of separable products:

$$\begin{aligned} \phi &= \phi_h(x)\phi_h(y) + i\phi_g(x)\phi_h(y) + j\phi_h(x)\phi_g(y) + k\phi_g(x)\phi_g(y) \\ \psi^V &= \phi_h(x)\psi_h(y) + i\phi_g(x)\psi_h(y) + j\phi_h(x)\psi_g(y) + k\phi_g(x)\psi_g(y) \\ \psi^H &= \psi_h(x)\phi_h(y) + i\psi_g(x)\phi_h(y) + j\psi_h(x)\phi_g(y) + k\psi_g(x)\phi_g(y) \\ \psi^D &= \psi_h(x)\psi_h(y) + i\psi_g(x)\psi_h(y) + j\psi_h(x)\psi_g(y) + k\psi_g(x)\psi_g(y) \end{aligned} \quad (3)$$

Hence the following quaternionic matrix Q representing the scale function and the corresponding actual additives of the wave function:

$$Q = \begin{pmatrix} \phi_h(x)\phi_h(y) & \phi_h(x)\psi_h(y) & \psi_h(x)\phi_h(y) & \psi_h(x)\psi_h(y) \\ \phi_g(x)\phi_h(y) & \phi_g(x)\psi_h(y) & \psi_g(x)\phi_h(y) & \psi_g(x)\psi_h(y) \\ \phi_h(x)\phi_g(y) & \phi_h(x)\psi_g(y) & \psi_h(x)\phi_g(y) & \psi_h(x)\psi_g(y) \\ \phi_h(x)\phi_g(y) & \phi_g(x)\psi_g(y) & \psi_g(x)\phi_g(y) & \psi_g(x)\psi_g(y) \end{pmatrix} \quad (4)$$

We therefore obtain the matrix w of the different coefficients (a real LL part corresponding to the approximate component and three imaginary parts LH, HL, HH corresponding to the components of details) of the quaternionic wavelets transform:

$$w = \begin{pmatrix} LL_{\phi_h(x)\phi_h(y)} & LH_{\phi_h(x)\psi_h(y)} & HL_{\psi_h(x)\phi_h(y)} & HH_{\psi_h(x)\psi_h(y)} \\ LL_{\phi_g(x)\phi_h(y)} & LH_{\phi_g(x)\psi_h(y)} & HL_{\psi_g(x)\phi_h(y)} & HH_{\psi_g(x)\psi_h(y)} \\ LL_{\phi_h(x)\phi_g(y)} & LH_{\phi_h(x)\psi_g(y)} & HL_{\psi_h(x)\phi_g(y)} & HH_{\psi_h(x)\psi_g(y)} \\ LL_{\phi_h(x)\phi_g(y)} & LH_{\phi_g(x)\psi_g(y)} & HL_{\psi_g(x)\phi_g(y)} & HH_{\psi_g(x)\psi_g(y)} \end{pmatrix} \quad (5)$$

In order to display the image after being transformed into a quaternionic wavelet, we arrange the quaternionic coefficients of the matrix w as follows:

$$w_r = \begin{pmatrix} LL & LH \\ HL & HH \end{pmatrix} \quad (6)$$

3. Compression, chaotic cryptography and image watermarking

3.1. Compression

Image compression can be defined as reducing the size of an image file, while maintaining an acceptable level of quality. It reduces the redundancy of an image's data so that it can be stored without taking up a lot of space or transmitting it more quickly. The compression method used in this article is loss compression based on the quaternionic wavelets transform (QWT). Each quaternionic sub-mark (matrix w_r equation 6) being each made up of four components (columns of the matrix w equation 5): a real component ($LL_{\phi_h(x)\phi_h(y)}$) and three imaginary components depending on the angles φ, θ, et β ($LL_{\phi_g(x)\phi_h(y)}$, $LL_{\phi_h(x)\phi_g(y)}$ And $LL_{\phi_h(x)\phi_g(y)}$). Natural compression is done by simply removing the LH, HL and HH quaternionic sub-bands, in order to retain only the LL quaternionic sub-band with its four components ($LL_{\phi_h(x)\phi_h(y)}$, $LL_{\phi_h(x)\phi_g(y)}$, $LL_{\phi_g(x)\phi_h(y)}$ and $LL_{\phi_h(x)\phi_g(y)}$) because it contains almost all of the information of the original image [20]. Its module will be determined by the formula:

$$|LL| = \sqrt{LL_{\phi_h(x)\phi_h(y)}{}^2 + LL_{\phi_g(x)\phi_h(y)}{}^2 + LL_{\phi_h(x)\phi_g(y)}{}^2 + LL_{\phi_h(x)\phi_g(y)}{}^2} \quad (7)$$

Where |LL| represents the compressed image.
The matrix representation in order to obtain the reconstructed image is given by the matrix w_{rc} :

$$w_{rc} = \begin{pmatrix} LL_{\phi_h(x)\phi_h(y)} & LL_{\phi_g(x)\phi_h(y)} \\ LL_{\phi_h(x)\phi_g(y)} & LL_{\phi_h(x)\phi_g(y)} \end{pmatrix} \quad (8)$$

3.2. Chaotic cryptography

The cryptographic method used here is the chaotic symmetrical cryptography. The encryption key will still be used for decryption at the receiver level. The approach to the chaotic encryption technique applied here is simple and straightforward. It consists of mixing information with a chaotic sequence from a sender, usually described by a state representation with the state vector. Only the sender's output is transmitted to the receiver. The role of the receiver is to extract the original information from the signal received. The recovery of information is usually based on the synchronization of the sender and receiver states [21], [22].
We define a chaotic system as:

$$\begin{cases} \dot{x}_1 = x_3 \\ \dot{x}_2 = \varepsilon_1(x_3 - v) \\ \dot{x}_3 = \sigma(x_3 - x_2 - x_1) \\ \dot{v} = \varepsilon_2(x_2 - \gamma \sinh(v)) \end{cases} \quad (9)$$

Using chaotic sequences of system (9) the image is then encrypted in the following steps and the schematic diagram depicted in figure 1:

1) Select the initial values ($x_{10}, x_{20}, x_{30}, v_0, \varepsilon_1, \varepsilon_2, \sigma, \gamma$) system (9) to achieve chaotic state. This yields to four real sequences {X1}, {X2}, {X3} and {V};
2) Convert the real sequence X1, X2 and V to integer $X1 = \text{fix}(X1_i \times 10^{16} \bmod 256)$ as, $X2 = \text{fix}(X2_i \times 10^{16} \bmod 256)$ and $V = \text{fix}(V_i \times 10^{16} \bmod 256)$;
3) Read the original picture $I_0$with a size of $m * n * k$ pixels. Perform the confusion (permutation) of rows and column of the image respectively using the key sequences X1 and X2 to achieve the permuted image P;
4) Apply Bit-XORed based diffusion process on the permuted image P using the sequence X3 and V of the proposed chaotic system. The encrypted image is then achieved and shown on figure 1.

The decryption process is the reverse of this encryption scheme.

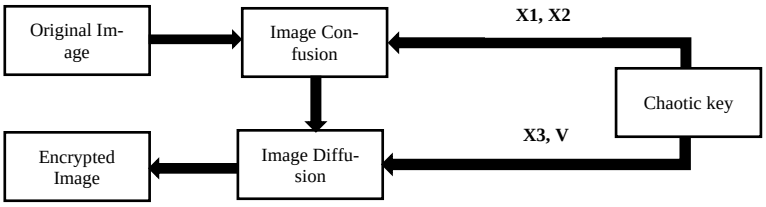

Fig. 1: Layout of the Encryption Scheme.

3.3. Blind watermarking of images

The watermarking algorithm used in this article is the substitution method in the frequency domain. The coefficients (pixels) of the mark (decryption key K) were inserted by replacing the coefficients of the compressed-encrypted image with those of the mark, using a secret key q. This key is to determine where the brand elements should be inserted. The extraction method used for this method is blind [15]. We only need the secret key q to extract the hidden mark (decryption key).

4. Proposed method of compression-encryption-watermarking

4.1. Tools used

The raw CFA images of size $512 * 512$ pixels used (Figure 2) in this work come from a color image obtained by 3CCD cameras [23, 24]. The algorithms were implemented using MATLAB software (version 8.3) installed on an 8GB RAM microcomputer, 1TB hard drive and 2.4GHz frequency with Windows 10 Professional Edition environment.

Fig. 2: CFA Raw Images.

4.2. Proposed robust hybrid compression-encryption-watermarking algorithm

We now present a new hybrid compression-encryption-watermarking algorithm combining successive compression technologies with losses, chaotic encryption and blind image watermarking. However, this algorithm can also be applied to grayscale and medical images. The proposed algorithm can be described in two stages: emission and reception of the image.

4.2.1. Emission process

Consider the original image I_0, a CFA image $m * n$ Pixels. The block diagram of the emission process is shown in Figure 3, and is summarized by the following steps:

1) Break down the original image I_0 quaternionic wavelets transform (QWT) in ℓ resolution levels. This results in a $(3\ell + 1)$ quaternionic sub-marks (LL, LH, HL, HH) and $(3\ell + 1) * 4$ elements that make up the matrix w of the QWT. We calculate the module of each sub-mark from the elements of the QWT in order to obtain the matrix w_r representing the standard format of the wavelets;
2) Eliminate the quaternionic sub-marks of details from the last level of resolution ℓ $(LH_\ell, HL_\ell, HH_\ell)$: calculating the quaternionic sub-mark module $|LL|$ which represents the compressed image;
3) Randomly generate using a chaotic generator, the encryption key K;
4) Encrypt with the encryption key K, the compressed image previously obtained;
5) Calculate the new matrix G that represents the subtraction of the compressed-encrypted image matrix (I_{cc}) and the encryption key K;
6) Set the secret key q from the matrix G to control the visibility of the watermarking. This key is defined here as an interval of thresholds;
7) Replace the coefficients of the compressed-encrypted image with those of the encryption key k using the secret key q. we then get our compressed-encrypted-watermarked image $\boldsymbol{I_{cct}}$.

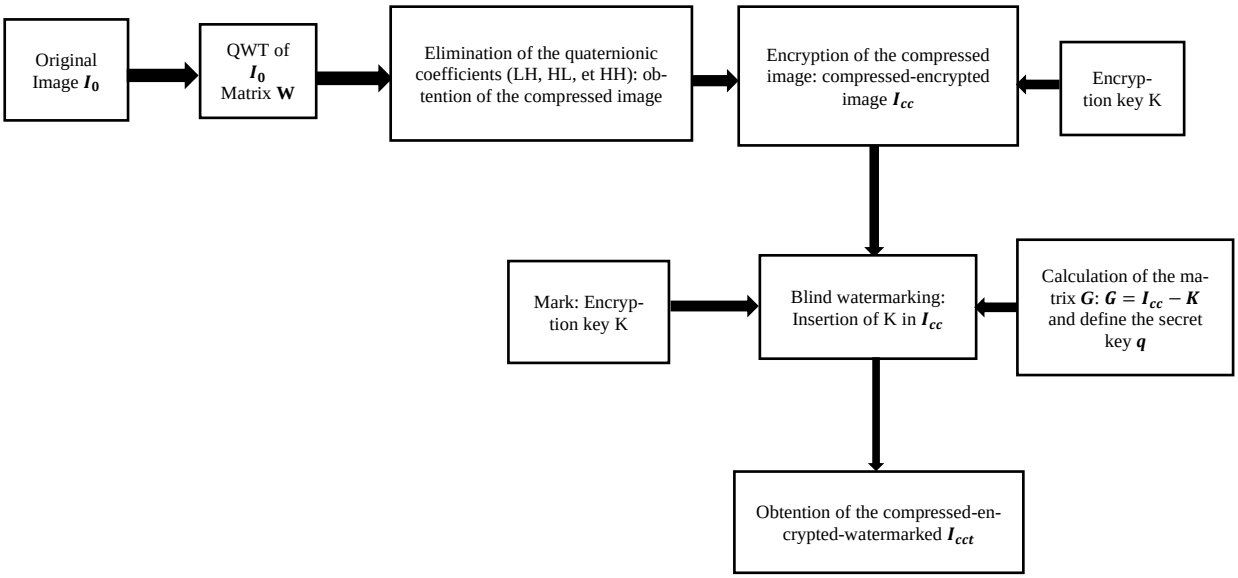

Fig. 3: Block Diagram of the Emission Process.

4.2.2. Reception process

At the reception, the return of the image is done by a series of opposite operations of the one proposed above. The block diagram of the reception process is illustrated in Figure 4, and is described by the following steps:

1) Extract the decryption key K in the compressed-encrypted-watermarked imageI_{cct} ;
2) Decipher the compressed-encrypted image from the decryption key K extracted in stage 1 of the receiving process;
3) Get the new value of the module$|LL|$based on the new values of the quaternionic components: We then get our image reconstructed I_r .

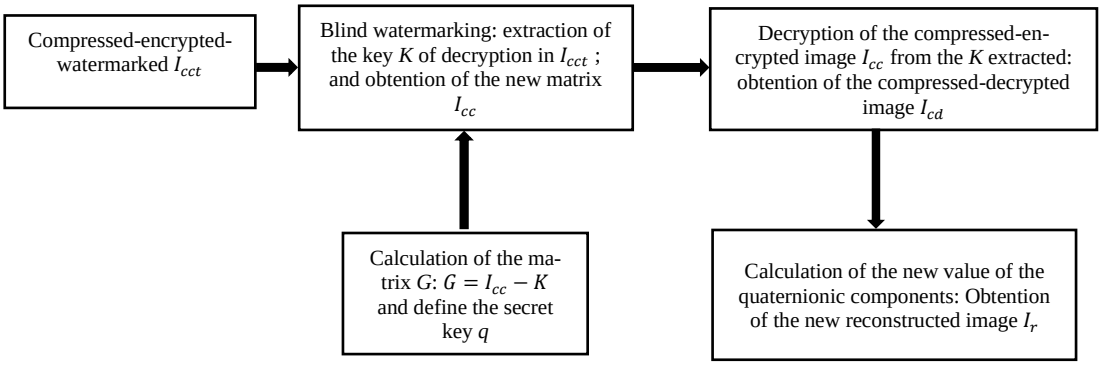

Fig. 4: Block Diagram of the Reception Process.

5. Results and discussions

Because encryption uses a symmetrical method, the encryption key will still be used for decryption at the receiver. To allow for a secure sharing of this session key, we hid it in the compressed-encrypted image to be sent. For this, we used a blind watermarking technique because of its robustness in the face of geometric attacks and erasure. The calculations of the various evaluation parameters (the Peak Signal to Noise Ratio (PSNR) and the Correlation Coefficient (CC)) were carried out with the aim of determining the robustness of our algorithm against certain attacks. The expressions of these different parameters are:

$$PSNR = 10\,log_{10}\left(\frac{max\,(max(I_o)^2)}{MSE}\right) \tag{10}$$

Where MSE is mean squared error between original and reconstructed images, which is defined as follow:

$$MSE = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{(I_o(i,j)-I_r(i,j))}{m*n} \tag{11}$$

$$CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(I_o(i,j)*I_r(i,j)}{\sqrt{(\sum_{i=1}^{m}\sum_{j=1}^{n}{I_o}^2(i,j)*\sum_{i=1}^{m}\sum_{j=1}^{n}{I_r}^2(i,j))}} \tag{12}$$

Generally, the CC value obtained between 0.7 and 1 is acceptable [1, 25, 26, 28]. It is important to mention that bigger the PSNR values more than obtains a high quality of reconstructed image. For PSNR=30dB, the quality of image is acceptable [1, 25, 26, 27].
To get information about statistical properties of compressed-encrypted-watermarked image, histogram analysis is a better way to obtain this information. Histogram of the compressed-encrypted-watermarked image gives the distribution of pixels. Figure 5 shows the histograms of the original image, reconstructed image and compressed-encrypted-watermarked image where we note a uniform distribution.
In the sequel, we will present an example of the application of this hybrid algorithm on image 1 described above (Figure 2).

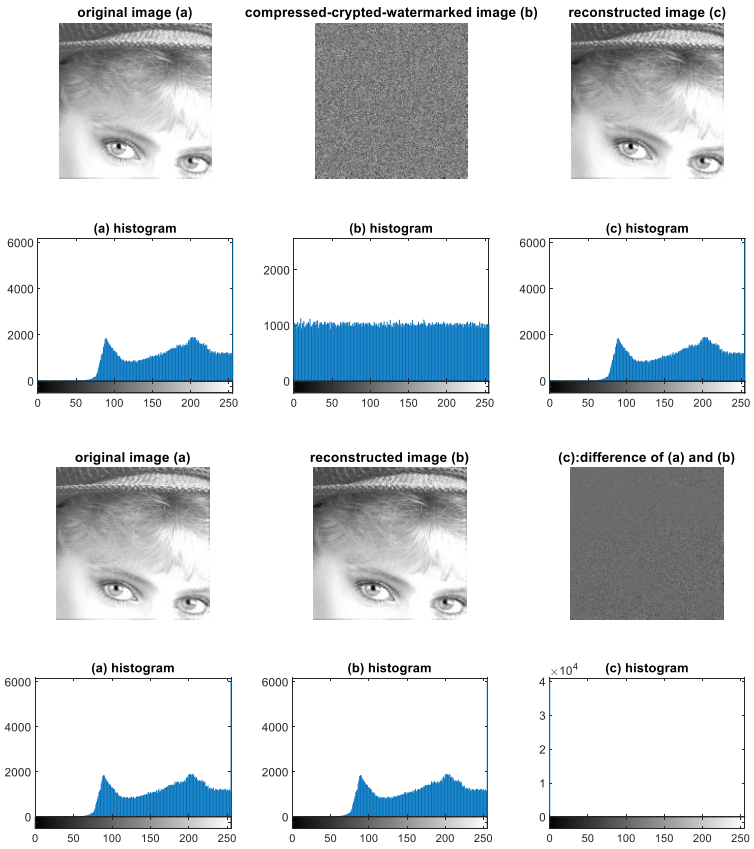

Fig. 5: Example of Application of the Compression-Encryption-Watermarking Algorithm of CFA Images.

Depending on the human visual system, we find that from this figure (Figure 5), that the reconstructed image (c) after compression-encryption-watermarking is difficult to differentiate the original image (a). Based on the calculated evaluation parameters, we find that the operation does not result in any loss of information equivalent to the CC=1.000 correlation coefficient and a peak noise signal ratio PSNR=185.2987dB.
In order to assess the robustness of our technique of blind crypto-watermarking of CFA images, several types of attacks existing in two classes, have been implanted. The first class consists of geometric attacks (Figure 6) aimed at sufficiently distorting the compressed-encrypted-watermarked image. While, the second class consists of erasure attacks (Figure 7) aimed at removing the decryption key in the compressed-encrypted-watermarked image.

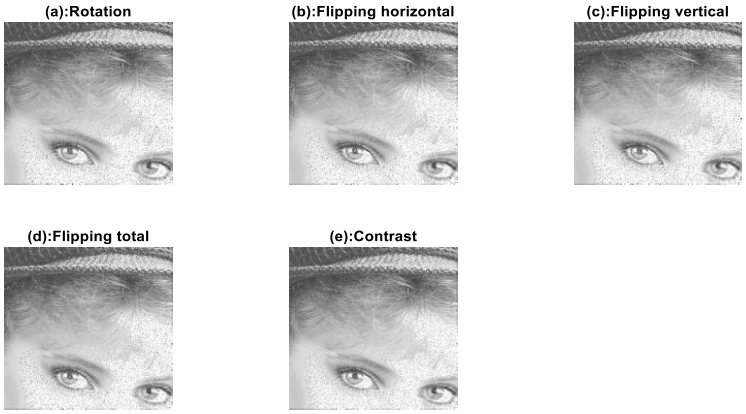

Fig. 6: Performance Against Geometric Attacks: Image Reconstructed from the Compressed-Encrypted-Watermarked and Attacked Image.

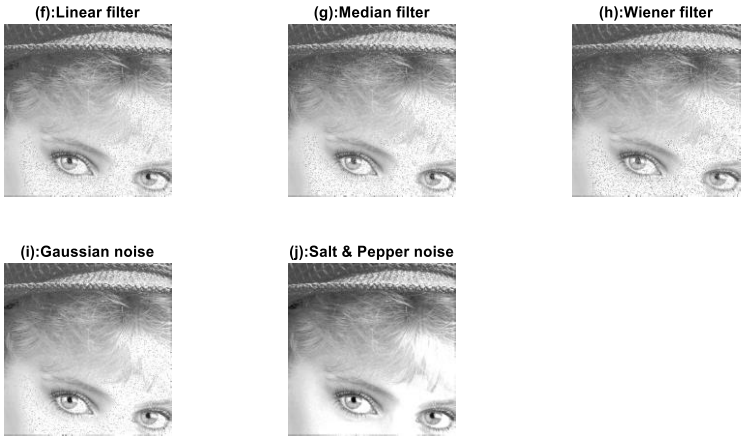

Fig. 7: Performance Against Erasure Attacks: Image Reconstructed from the Compressed-Encrypted-Watermarked and Attacked Image.

We find that from Figures 6 and 7, our robust hybrid method of compression-encryption-watermarking of CFA images resists geometric and erasure operations well. The images reconstructed after these operations are easily recognized by the human visual system despite the blackheads on the images.
The results obtained for the robust hybrid compression-encryption-watermarking method of CFA images on our various host images (Figure 2) are presented in the table below.

Table 1: Evaluation of the Parameters of Compression-Encryption-Watermarking of CFA Images

Designations		Image 1 PSNR (db)	CC	Image 2 PSNR (db)	CC	Image 3 PSNR (db)	CC	Image 4 PSNR (db)	CC	Picture 5 PSNR (db)	CC	Picture 6 PSNR (db)	CC
No attack	No attack	185.2987	1.0000	184.5975	1.0000	184.9743	1.0000	184.6742	1.0000	185.1343	1.0000	184.7194	1.0000
Geometric attacks	Rotation 10^0	33.4084	0.9877	31.4862	0.9770	32.3509	0.9820	32.2658	0.9837	32.9186	0.9854	32.0310	0.9814
	Contrast	34.1434	0.9913	32.0320	0.9822	32.9999	0.9868	33.0048	0.9886	33.6269	0.9896	32.6529	0.9862
	Horizontal Flipping	33.5231	0.9883	31.5889	0.9781	32.4791	0.9831	32.4104	0.9848	33.0230	0.9861	32.1025	0.9820
	Vertical Flipping	33.4953	0.9882	31.5459	0.9776	32.4115	0.9825	32.3743	0.9845	33.0140	0.9861	32.1381	0.9823
	Total Flipping	33.5177	0.9883	31.5771	0.9780	32.5049	0.9833	32.4219	0.9849	32.9966	0.9859	32.1026	0.9820
Erasure attacks	Linear filter	34.0921	0.9911	32.2645	0.9841	33.1510	0.9877	32.8093	0.9875	33.5023	0.9890	32.6620	0.9862
	Median filter	33.7691	0.9896	31.9904	0.9818	32.8170	0.9855	32.6945	0.9866	33.2771	0.9877	32.4304	0.9845
	Wiener filter	33.1305	0.9860	31.2864	0.9748	32.1859	0.9806	31.9438	0.9810	32.6064	0.9831	31.7455	0.9788
	De-debugging	47.6253	1.0000	46.3284	1.0000	45.2037	1.0000	46.1941	1.0000	46.4655	1.0000	47.2655	1.0000
	salt and peppers												
	Gaussian de-delusing	35.1166	0.9944	33.3263	0.9902	34.0350	0.9918	33.7671	0.9919	34.4250	0.9927	33.5427	0.9908

On table 1, we have good correlation coefficient (CC) values that allow us to judge the quality of the reconstructed image despite the various malicious operations performed on our compressed-encrypted-watermarked image. Experimental results show that our compression-encryption-watermarking method of CFA images maintains a good quality of reconstructed images and a good robustness against some conventional attacks.

6. Conclusion

At the end of our work, we were able to achieve our goal by developing a robust hybrid algorithm combining successive compression-encryption-watermarking of CFA images using quaternions. The proposed hybrid algorithm owes its simplicity to the QWT from which we performed our compression with losses by eliminating all quaternionic sub-marks of details while ensuring a quick transfer, and its robustness to the blind watermarking algorithm while ensuring a high level of security. So, we can say that our proposed robust hybrid algorithm ensures a fast, simple and secure transfer of CFA images in an unsecured environment where resources in terms of throughput and mark width are quite limited. Although the proposed approach is fairly effective, it is not sufficient to achieve completely safe protection. There are many ways to improve and develop new solutions. Our outlook now turns to establishing an intelligent hybrid algorithm from neural networks and monogenic wavelets.

References

[1] J. R. Marconi, « Secure transfer of images by combination of compression, encryption and tagging techniques ». Thesis, University of MONTPELLIER II. (October 31, 2006 edition).

[2] W. Puech, J.R. Marconi, « Crypto-Compression of medical images by selective encryption of DCT », In EUSIPCO'05, Antalya, Turkey, September. (2005)

[3] H. H. Ralaivao, P. A. Randriamitantsoa, T. Raminoson, « sécurisation des images par combinaison de tatouage et de cryptage », MADA-ETI, ISSN : 2220-0673, Vol.1, 2016.

[4] T. E. Rakotondraina, H. M. Ramafiarisona, A. A. Randriamitantsoa, « Transfert sécurisé d'images dans le domaine de la TFD », MADA-ETI, ISSN : 2220-0673, Vol.1, 2013.

[5] W. Puech, M. Dumas, « Transfert sécurisé d'images par combinaison de techniques de cryptographie et de tatouage », In Proc. 7th Colloque Compression et Représentation des Signaux Audiovisuels, CORESA'01, Dijon, France, novembre 2001.

[6] W. Puech, M. Dumas, J. C. Borie, M. Puech, « Tatouage d'images cryptées pour l'aide au Télédiagnostic », In Proc. 18th. Colloque Traitement du Signal et des Images, GRETSI'01, Toulouse, France, septembre 2001.

[7] J. R. Marconi, « Transfert sécurisé d'images par combinaison de techniques de compression, cryptage et marquage », Thèse de Doctorat, Université de MONTPELLIER II, Edition du 31 Octobre 2006.

[8] F. Autrusseau, J. P. Guedon, Y. Bizais, « Watermarking and cryptographic schemes for medical imaging », SPIE Medical Imaging, Image processing, vol. 5032-105, pp. 958-965, San Diego CA, USA, 15-20 February 2003.

[9] L. Rastislav et N. P. Konstantinos, « Color filter arrays: Design and performance analysis ». IEEE Transactions on Consumer Electronics, 51(4): 1260–1267, November 2005. https://doi.org/10.1109/TCE.2005.1561853.

[10] Y. Yang, « Contribution à l'évaluation objective de la qualité d'images couleur estimées par dématriçage ». Université des Sciences et Technologies de Lille, 2009.

[11] L. Bitjoka, B. Ousman, T. Dzudie, M.F. Carl, T. Emmanuel « Digital camera images processing of hard-to-cook beans ». Journal of Engineering and Technology Research 2(9), 177-188, 2010.

[12] B. Ousman, L. Bitjoka, G. Djaowé « Nondestructive determination of beans water absorption capacity using CFA images analysis for hard-to-cook evaluation ». International Journal of Electrical and Computer Engineering (IJECE), 3(3), 317–328, 2013.

[13] H. Abena, R. Barzina, B. Ousman, L. Bitjoka, « Comparaison des tatouages d'images CFA et couleur » dans le 2ème Atelier annuel sur la Cryptographie, Algèbre et Géométrie (CRAG 2), Pages : 113-120 du 03-07/12/2012 à l'Université de Ngaoundéré.

[14] D. Libouga, M. Otesteanu, I. O. Libouga, L. Bitjoka, G. D. Popa, « A Review on Image Segmentation Techniques and Performance Measures », International Journal of Computer and Information Engineering Vol.12(12), pp. 1107-1117, 2018.

[15] H. Abena, B. L. Eloundou, L. Bitjoka, D. Tieudjo, « Blind watermarking of CFA images based on quaternions », Far East Journal of Electronics and Communications, Volume 24, Number 1, 2021, Pages 67-80 ISSN: 0973-7006. https://doi.org/10.17654/EC024010067.

[16] N. L. Bihan : « Traitement quaternionique des images couleur », Colloques sur le Traitement du Signal et des Images, GRETSI (GRETSI, Groupe d'Etudes du Traitement du Signal et des Images), 2003.

[17] T. Bülow, « Hypercomplex Spectral Signal Representations for Image Processing and Analysis », Ph.D. thesis, Inst. f. Informatik u. Prakt. Math. Der Christian-Albrechts-Universität zu Kiel, 1999.

[18] N. Kingsbury, « Complex wavelets for shift in variant analysis and filtering of signals », Applied and Computational Harmonic Analysis, vol. 10, no.3, pp.234 –253, 2001. https://doi.org/10.1006/acha.2000.0343.

[19] R. Soulard, P. Carré, « Quaternionic wavelets for texture classification », In Proceedings of the 35th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), pages 4134–4137, Dallas (TX, USA), March 2010. https://doi.org/10.1109/ICASSP.2010.5495732.

[20] B. L. Eloundou, A. J. Oyobe, H. Abena, P. Ele, « Compression of medical images by quaternionic wavelet transform », International Journal of Engineering & Technology, 10 (2) (2021) 89-94. Website: www.sciencepubco.com/index.php/IJET. https://doi.org/10.14419/ijet.v10i2.31524.

[21] S. Boccaletti, J. Kurths, G. Osipov, D. L. Valladares and C. S. Zhou, « The synchronization of chaotic systems ». Physics Reports, Vol. 366, pp. 1-101, 2002 https://doi.org/10.1016/S0370-1573(02)00137-0.

[22] National Bureau of Standards, Data Encryption Standard, Federal Information Processing Standard, Publication 46, 1977.

[23] L. Zhang, X. Wu, A. Buades, and X. Li, « Color Demosaicking by Local Directional Interpolation and Non-local Adaptive Thresholding ». Journal of Electronic Imaging 20(2), 023016 (Apr-Jun 2011), https://doi.org/10.1117/1.3600632.

[24] X. Li, B. Gunturk, and L. Zhang, « Image Demosaicing: A Systematic Survey ». Proceedings of the SPIE-The International Society for Optical Engineering, 6822, no.1, Jan. 2008. https://doi.org/10.1117/12.766768.

[25] C. REY, « Tatouage d'image : Gain en robustesse et intégrité des images », Thèse, Université d'Avignon et des pays de Vaucluse. 14 février 2003.

[26] MANOURY, « Tatouage d'images numériques par paquets d'ondelettes », Thèse de Doctorat, Ecole Centrale de Nantes, Université de Nantes, France, 2001

[27] J. Mei, L. Sukangand, Xiaomei, A digital watermarking algorithm based on DCT and DWT, Proceedings of the International Symposium on Web Information Systems and Applications, may 22-24 2009:104-107, Nanchang, China 2009.

[28] B. L. Gunjal, S. N. Mali, "Secured color image watermarking technique in DWT-DCT domain" International Journal of Computer Science, Engineering and Information Technology (IJCSEIT) 1(3):36-44, 2011. https://doi.org/10.5815/ijitcs.2012.03.01.

[29] Noura, P. Ntsama, L. Bitjoka, « A robust biomedical images watermarking scheme based on chaos », International Journal of Computer Science and Security (IJCSS), volume (11): Issue (1): 2017.

[30] X. L. Long, C. C. Lin, S. M. Yuan. « Blind dual watermarking for color images authentication and copyright protection ». IEEE Transactions on Circuits and Systems for Video Technology, 28(5):1047{1055, 2016. https://doi.org/10.1109/TCSVT.2016.2633878.

[31] N. Tsafack, J. Kengne, A. E. Bassem, A. M. Iliyasu, K. Hirota, A. E. L. Ahmed, « Design and implementation of a simple dynamical 4-D chaotic circuit with applications in image encryption », Inf. Sciences, 515, pp. 191-217, 2020. https://doi.org/10.1016/j.ins.2019.10.070.