Scientific Research Publishing

Journal of Information Security, 2022, 13, 244-256
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

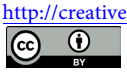
Hybrid Successive CFA Image Encryption-Watermarking Algorithm Based on the Quaternionic Wavelet Transform (QWT)

Hervé Abena Ndongo[1,2], Marcelin Vournone[2,3], Mireille Pouyap[1], Taya Ngakawa[2,3], Paul Abena Malobe[4]

[1]Energy, Signal, Imaging and Automatic Laboratory (LESIA), Department of Electrical and Industrial Automatic Engineering, National School of Agro-Industrial Sciences (ENSAI), University of Ngaoundere, Ngaoundere, Cameroon
[2]Mapping Production Division, Department of Data Collection, National Institute of Cartography, Yaounde, Cameroon
[3]Department of Physics, Higher Teacher Training College, University of Maroua, Maroua, Cameroon
[4]Department of Physics, Faculty of Science (FS), University of Ngaoundere, Ngaoundere, Cameroon
Email: pouyapmireille@gmail.com

How to cite this paper: Ndongo, H.A., Vournone, M., Pouyap, M., Ngakawa, T. and Malobe, P.A. (2022) Hybrid Successive CFA Image Encryption-Watermarking Algorithm Based on the Quaternionic Wavelet Transform (QWT). *Journal of Information Security*, **13**, 244-256.
https://doi.org/10.4236/jis.2022.134013

Received: July 12, 2022
Accepted: August 28, 2022
Published: August 31, 2022



Abstract

In this paper, we present a new robust hybrid algorithm combining successively chaotic encryption and blind watermarking of images based on the quaternionic wavelet transform (QWT) to ensure the secure transfer of digital data. The calculations of the different evaluation parameters have been performed in order to determine the robustness of our algorithm to certain attacks. The application of this hybrid algorithm on CFA (Color Filter Array) images, allowed us to guarantee the integrity of the digital data and to propose an autonomous transmission system. The results obtained after simulation of this successive hybrid algorithm of chaotic encryption and then blind watermarking are appreciated through the values of the evaluation parameters which are the peak signal-to-noise ratio (PSNR) and the correlation coefficient (CC), and by the visual observation of the extracted watermarks before and after attacks. The values of these parameters show that this successive hybrid algorithm is robust against some conventional attacks.

Keywords

Encryption, Blind Watermarking, Chaos, CFA Images, QWT

1. Introduction

The transfer or archiving of digital data is sometimes insecure. It is therefore essential to have secure systems for the transfer of these data and the protection of

the rights holders [1] [2]. For this purpose, several researchers have been interested in securing digital data through different simple protection techniques such as steganography, encryption, and watermarking; and even through different hybrid techniques such as steganography encryption and encryption-watermarking [3]-[16]. Faced with all these difficulties, the robust hybrid method combining successively encryption and watermarking has very naturally appeared as an alternative or complementary solution to strengthen the security of these digital data. Most contributions were made to grayscale images and even more medical images. However, to our knowledge, the CFA (Color Filter Array) images generated by digital photography [17] have not yet been successive encryption-watermarking based on the quaternionic wavelet transform (QWT). The successive hybrid method of encryption-watermarking is the one we will study in our work with the aim of ensuring the secure transfer of photographic images and obtaining a better compromise between invulnerability (robustness and security) and the amount of information to insert (capacity and imperceptibility). CFA images are important for image analysis because these raw images have not undergone any processing (interpolation, demosaicking, etc. [18] [19] [20]) that might alter their reliability [17] [21]. In the rest of this paper, we will introduce the properties of the quaternionic wavelet transform firstly, and then present the proposed successive encryption-watermarking methodology, the presentation of the results obtained after the simulation of this algorithm and finally the analysis, and discussion of our obtained results.

2. Quaternionic Wavelet Transform

2.1. Definition and Properties of Quaternions

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

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

The multiplication of two of these 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 [22] [23].

2.2. Quaternionic Structure of an Image

The QWT integrates the concept of phase in a break down 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 break down in sub-bands is then supplemented by an even keener 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-band. The phase, represented by three angles (φ, θ, β), provides a complete description of the structure of these components [24] [25]. From a practical point of view, the mother wavelet being separable *i.e.* $\psi(x,y) = \psi_h(x)\psi_h(y)$, and considering Hilbert's pairs $(\psi_h, \psi_g = \mathcal{H}\psi_h)$ (wavelets) and $(\phi_h, \phi_g = \mathcal{H}\phi_h)$ (scale functions), the 2D analytical wave is written in terms of separable products:

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

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

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

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 transformed into quaternionic wavelets [26] [27]:

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

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

$$w_r = \begin{pmatrix} LL & LH \\ HL & HH \end{pmatrix} \tag{6}$$

Two complementary filter banks, one using an even filter, the other an odd

filter, lead to four separable 2D filter banks [28], slightly offset from each other. These shifts correspond theoretically to the phase shifts of the 2D Hilbert transforms. One obtains a sub-pixel precision, translated indirectly in the notion of phase [24]. The original image I_0 is decomposed as shown in **Figure 1(A)** by a set of quaternion filter banks connected by operators $\downarrow 2$ of data subsampling (downsampling), low-pass (h_i) and high-pass (g_i) filters for the analysis (i taking the values 1 and 2) the signs of interpolation. Likewise, in order to reconstruct the filter banks and the decomposed image, we use the reconstruction structure (Synthesis) given by **Figure 1(B)**, a phase of dilation of the data with insertion of zeros (upsampling), obtained using of the operator $\uparrow 2$ and the low-pass ($\tilde{h}_i$) and high-pass ($\tilde{g}_i$) filtering operations. This allows us to obtain the quaternionic decomposition (Analysis) and reconstruction (Synthesis) structure of an image I_0 given by **Figure 1** below.

3. Chaotic Encryption and Blind Watermarking

3.1. Chaotic Encryption

The cryptographic method used here is the symmetrical chaotic cryptography.

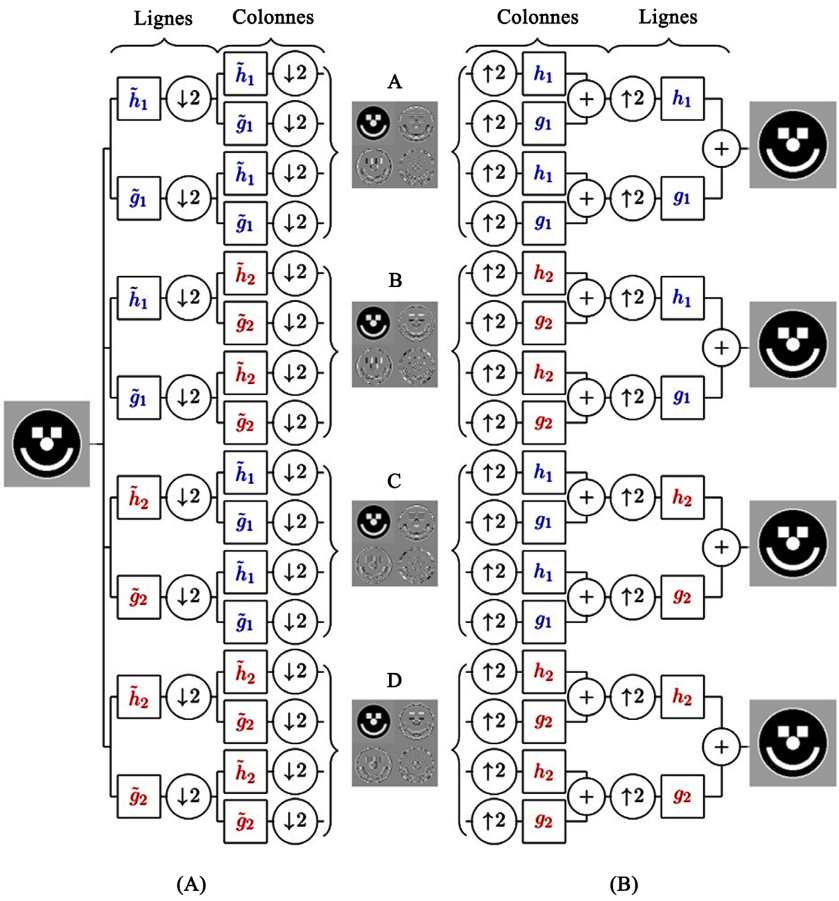


Figure 1. Decomposition and reconstruction structure of quaternion filter banks [24]. Where A, B, C and D are quaternionic coefficients or sub-bands. (A) Decomposition; (B) Reconstruction.

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 a 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 states of the sender and the states of the receiver [29] [30] [31].

3.2. Blind Watermarking

The watermarking algorithm used in this article is the substitution method in the frequency domain. The coefficients (pixels) of the watermark (tiers-person data, encryption key K, etc.) were embedded by replacing the coefficients of the host image (HH sub-mark) with those of the watermark, using a secret key q. This key is to determine where the watermark elements should be embedded. This method also requires a coefficient of strength in order to control the visibility of the watermark. The extraction method used for this method is blind. We only need the secret key to extract the hidden watermark [32].

4. Proposed Encryption-Watermarking Methodology

4.1. Tools Used

The raw CFA images of a size of 512 * 512 and 1024 * 1024 pixels used (**Figure 2**) in this work come from color images obtained by 3CCD cameras [18] [19]. The watermark image used of a size of 323 * 124 pixels (**Figure 2**) represents the tiers-person data. The algorithms were implemented using MATLAB software (version 8.3) installed on an 8 GB RAM microcomputer, 1 TB of hard drive and 2.4 GHz frequency with a Windows 10 Professional Edition environment.

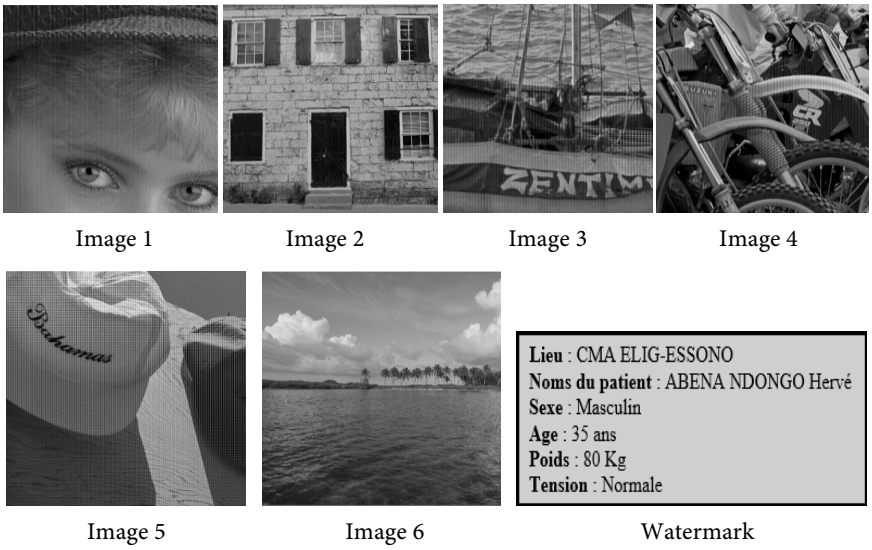


Image 1 Image 2 Image 3 Image 4

Image 5 Image 6 Watermark

Figure 2. Raw CFA images (image 1, …, image 6) and watermark image.

4.2. Proposed Hybrid Successive Image Encryption-Watermarking Algorithm

In this paper, we now present a new hybrid encryption-watermarking algorithm of CFA images successively combining the technologies of chaotic encryption and blind watermarking. However, this algorithm can also be applied to grayscale images. The proposed algorithm is described by the emission and the reception process. Consider the original image I_0, a CFA image of $m*n$ pixels and the watermark image M, a grayscale image of $k*l$ pixels. The block diagram of the emission process is shown in Figure 3, and is summarized by the following steps:

1) Define a chaotic system and the encryption key k [4];

2) Encrypt (confuse and broadcast) the original image using the key k: encrypted image I_c;

3) Break down the encrypted image I_c through the quaternionic wavelets transform (QWT) in ℓ resolution levels. This results in a $(3\ell+1)$ quaternionic sub-bands (LL, LH, HL, and HH) and $(3\ell+1)*4$ elements that make up the matrix w of the QWT. We calculate the module of each sub-band from the elements of the QWT in order to obtain the matrix w_r representing the standard format of the wavelets transforms;

4) Embedded using the key q, the watermark M into one of the quaternionic sub-bands of details of the last level of resolution ℓ ($LH_\ell, HL_\ell, HH_\ell$);

5) Calculate the inverse quaternionic wavelet transform (IQWT) of the elements of the new matrix w' from the matrix w'_r modified selected sub-bands and other remaining sub-bands. We then obtain our encrypted-watermarked image I_{ct}.

The reception process is the reverse of this emission process scheme to obtain reconstructed image I_r.

5. Results and Discussion

The objective of our work was therefore to develop a robust algorithm combining successively encryption and watermarking of digital photography images using quaternions allowing the secure transfer of CFA images. The results obtained

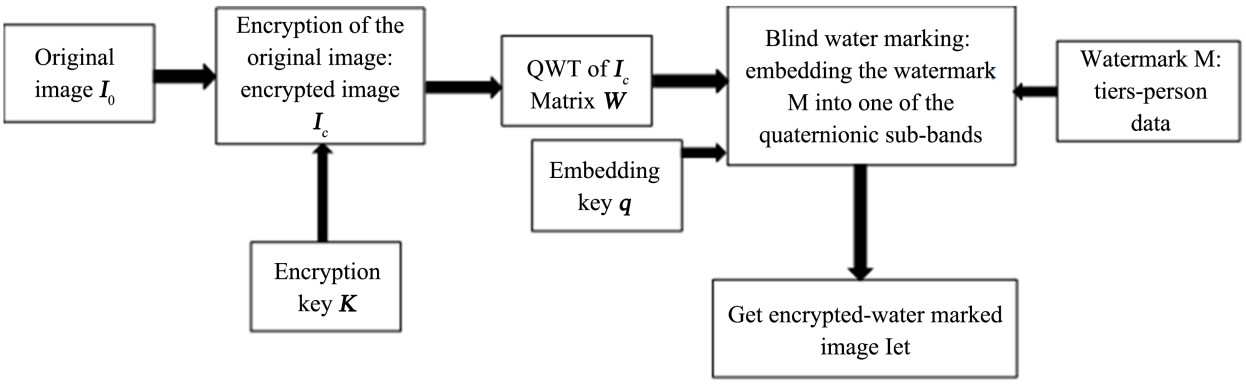


Figure 3. Block diagram of the emission process of the hybrid encryption and watermarking algorithm.

after execution of our program on MATLAB of the successive hybrid algorithm of encryption-watermarking (defined above **Figure 3**) on the original CFA image will be presented below. 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 some attacks. These two parameters are the most commonly used distortion measures in image processing to measure the absolute quality (or degree of degradation) of an image. This measure is based on the comparison of pixels between the original image and the modified image (encrypted-watermarked image, reconstructed image, etc.) giving an indication of the degradation introduced at a pixel level. The expressions of these different parameters are:

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\max\left(\max\left(I_o\right)^2\right)}{\mathrm{MSE}}\right) \tag{7}$$

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

$$\mathrm{MSE} = \sum_{i=1}^{m}\sum_{j=1}^{n}\frac{\left(I_o(i,j) - I_r(i,j)\right)^2}{m*n} \tag{8}$$

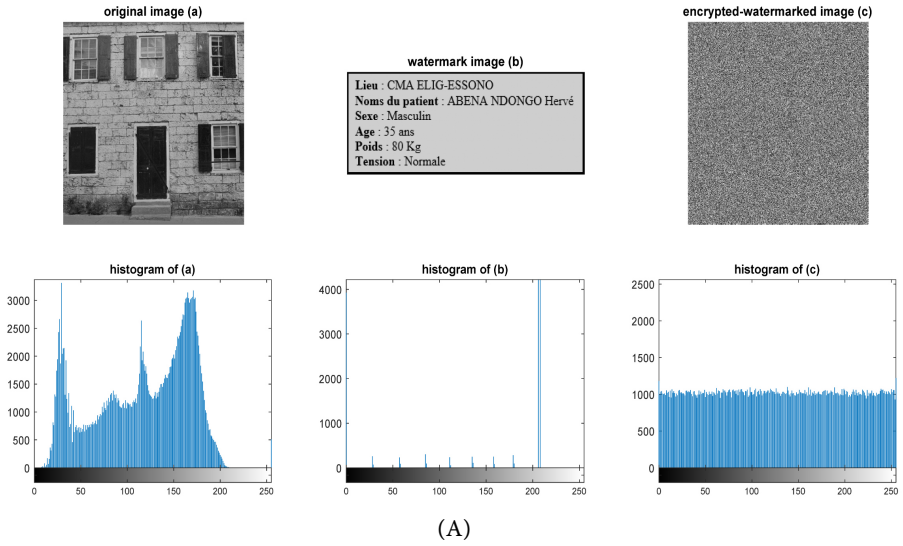
$$\mathrm{CC} = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(I_o(i,j)*I_r(i,j)\right)}{\sqrt{\sum_{i=1}^{m}\sum_{j=1}^{n}I_o^2(i,j)*\sum_{i=1}^{m}\sum_{j=1}^{n}I_r^2(i,j)}} \tag{9}$$

Generally, the CC value obtained between 0.7 and 1 is acceptable [1] [2] [3] [33]. It is important to mention that bigger the PSNR values more than obtain a high quality of reconstructed image. For PSNR = 30 dB, the quality of image is acceptable [2] [3] [6] [33].

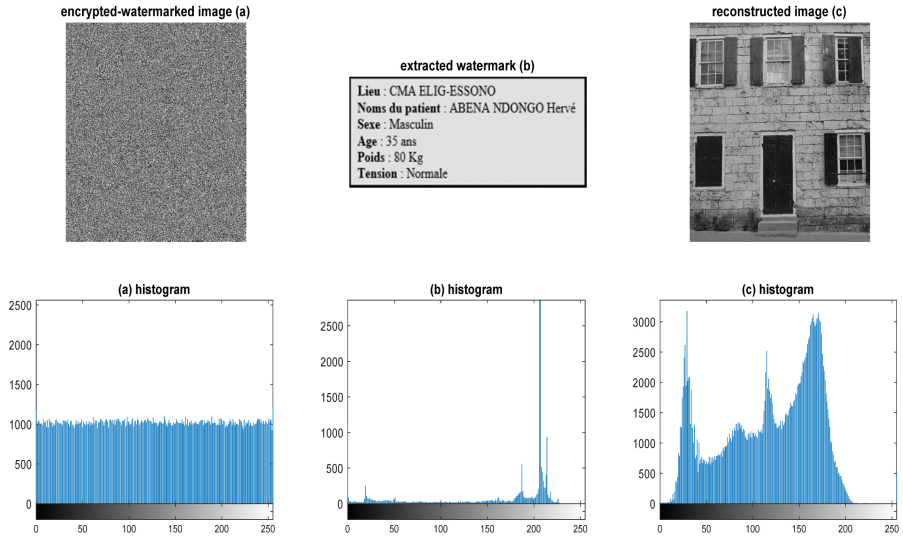
In the next, we will present an example of the application of this hybrid algorithm on image 2 illustrated above **Figure 2**.

According to the human visual system, we note that from **Figure 4**, that it is difficult to differentiate the original image from the reconstructed image and the same to the watermark from the extracted watermark after encryption and then watermarking. According to the calculated evaluation parameters, we find that the operation generates an information loss equivalent to the correlation coefficient CC = 0.9996 (with CC ≈ 1) and a peak signal-to-noise ratio PSNR = 42.4562 dB (already > 30 dB). So, we can say that our algorithm for successive encryption-watermarking of CFA images was successful depending on the standards described in the literature.

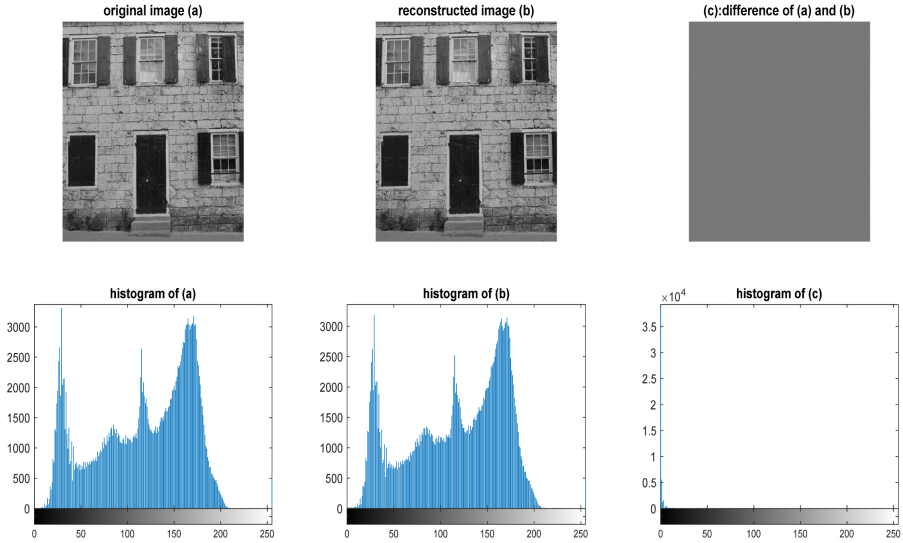
In order to evaluate the robustness of our hybrid algorithm of successive CFA image encryption, several types of attacks existing in two classes, have been implemented. The first class consists of geometric attacks (**Figure 5**) which aims to sufficiently distort the encrypted-watermarked image. While, the second class consists of erasure attacks (**Figure 6**) aimed extracted watermark in the encrypted-watermarked image.


original image (a)
watermark image (b)
Lieu : CMA ELIG-ESSONO
Noms du patient : ABENA NDONGO Hervé
Sexe : Masculin
Age : 35 ans
Poids : 80 Kg
Tension : Normale
encrypted-watermarked image (c)
histogram of (a)
histogram of (b)
histogram of (c)

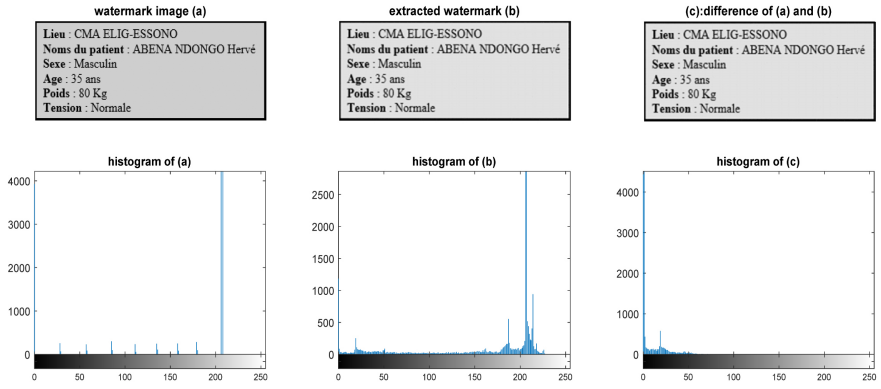
(A)


encrypted-watermarked image (a)
extracted watermark (b)
Lieu : CMA ELIG-ESSONO
Noms du patient : ABENA NDONGO Hervé
Sexe : Masculin
Age : 35 ans
Poids : 80 Kg
Tension : Normale
reconstructed image (c)
(a) histogram
(b) histogram
(c) histogram

(B)

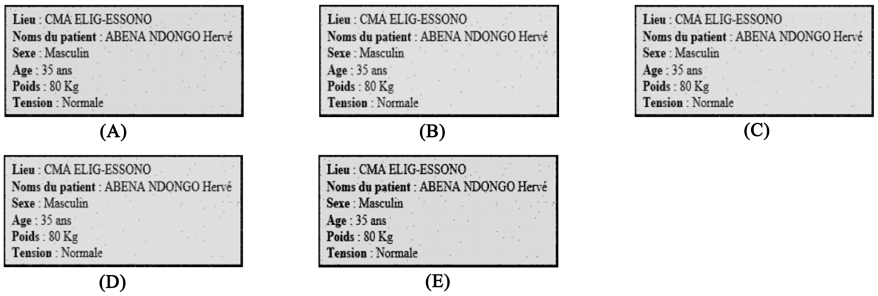

original image (a)
reconstructed image (b)
(c):difference of (a) and (b)
histogram of (a)
histogram of (b)
histogram of (c)

(C)



(D)

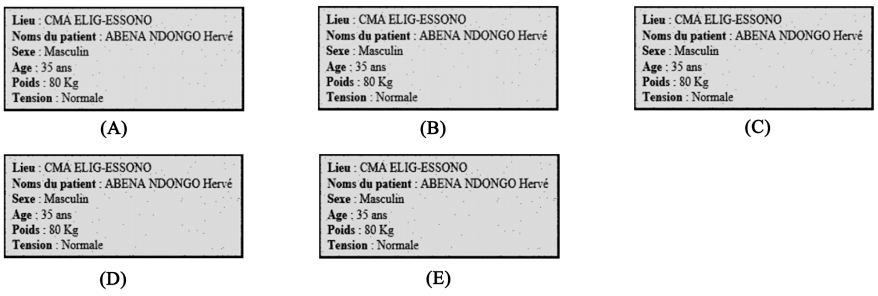
Figure 4. Example of applying the successive hybrid algorithm for encryption then watermarking of CFA images. (A) Emission process; (B) Reception process; (C) Difference between the original image and the reconstructed image; (D) Difference between the watermark and the extracted watermark.



(A) (B) (C)

(D) (E)

Figure 5. Performance against geometric attacks: watermarks extracted from encrypted then watermarked images and attacked. (A) Rotation; (B) Flipping horizontal; (C) Flpping vertical; (D) Fipping total; (E) Contrast.



(A) (B) (C)

(D) (E)

Figure 6. Performance against erasure attacks: watermarks extracted from encrypted then watermarked images and attacked. (A) Linear filter; (B) Median filter; (C) Wiener filter; (D) Gaussian noise; (E) Salt & Pepper noise.

We find that from **Figure 5** and **Figure 6**, our successively implemented hybrid CFA image encryption-watermarking algorithm is well resilient to geometric and erasure operations, as the watermarks extracted after these operations are easily recognized by the human visual system. The values of different evaluation parameters for the hybrid successive encryption-watermarking algorithm are presented in **Table 1** below.

The results obtained after simulation (presented in Table 1) show that our successive CFA image encryption-watermarking algorithm maintains a good quality of the extracted watermarks and good robustness against some conventional attacks which is acceptable.

We compare our results obtained by our hybrid successive encryption then watermarking algorithm with those of the works of A. Khalfallah *et al.* [34], W. Puech *et al.* [35] and Mohamed *et al.* [36]. The results obtained are presented in Table 2 below:

We can see from Table 2 that our results are better on the quality of the reconstructed image since our value (in bold) of PSNR is largely above theirs.

Table 1. Evaluation parameters for the hybrid method successive encryption-watermarking of CFA images.

DESIGNATIONS		Image 1		Image 2		Image 3		Image 4		Image 5		Image 6	
		PSNR (dB)	CC	PSNR (dB)	CC	PSNR (dB)	CC	PSNR (dB)	CC	PSNR (dB)	CC	PSNR (dB)	CC
No attack	No attack	41.8956	0.9993	42.4562	0.9996	41.9432	0.9994	42.1124	0.9992	41.8772	0.9996	42.7459	0.9996
Geometric attacks	Rotation 100	37.0250	0.9983	35.9579	0.9963	35.5676	0.9963	37.5729	0.9983	37.5633	0.9983	35.9805	0.9964
	Contrast	36.7605	0.9981	35.6735	0.9958	35.2846	0.9958	37.3469	0.9981	37.3233	0.9981	35.7079	0.9959
	Horizontal Flipping	36.8662	0.9981	35.9289	0.9963	35.4782	0.9961	37.4171	0.9981	37.3962	0.9981	35.8939	0.9962
	Vertical Flipping	36.8777	0.9981	35.9019	0.9962	35.5003	0.9962	37.4025	0.9981	37.4221	0.9981	35.8953	0.9962
	Total Flipping	36.8624	0.9981	35.9002	0.9962	35.4704	0.9961	37.4207	0.9981	37.4200	0.9981	35.8877	0.9962
Erasure attacks	Linear filter	33.8101	0.9923	33.2677	0.9875	32.8930	0.9875	34.3502	0.9924	34.3466	0.9924	33.2945	0.9876
	Median filter	37.1101	0.9984	36.0053	0.9964	35.6075	0.9964	37.6702	0.9984	37.6596	0.9984	36.0271	0.9965
	Wiener filter	36.9526	0.9982	35.8476	0.9962	35.4661	0.9962	37.5276	0.9983	37.5081	0.9983	35.8730	0.9962
	De-debugging salt and peppers	36.7606	0.9981	35.6737	0.9958	35.2848	0.9958	37.3470	0.9981	37.3235	0.9981	35.7079	0.9959
	Gaussian de-debugging	36.7606	0.9981	35.6736	0.9958	35.2848	0.9958	37.3471	0.9981	37.3234	0.9981	35.7079	0.9959

Table 2. Comparison of the quality of the reconstructed image without attacks of the encrypted-watermarked image.

Authors	A. Khalfallah *et al.* (2006)	W. Puech *et al.* (2008)	Mohamed *et al.* (2019)	Proposed method
Calculed parameters	PSNR (dB)	PSNR (dB)	PSNR (dB)	PSNR (dB)
No attack	34.2500	38.7500	33.0119	**42.4562**

6. Conclusion

At the end of our work, we were able to achieve our goal by developing a hybrid successive, reversible, and robust encryption-watermarking algorithm applied to CFA images using quaternions. The combination of chaotic encryption and blind watermarking techniques has enabled the secure and simple transfer of CFA images in an insecure environment, and where throughput and bandwidth resources are quite restricted. The use of the Quaternionic Wavelet Transform (QWT) optimizes the trade-off between robustness and the amount of information to be embedded during blind watermarking. The different results we have just presented show a good quality of the reconstructed image despite the attacks suffered by our encrypted-watermarked image. So, we can say that our algorithm of successive encryption-watermarking of CFA images was successful. There are still many avenues to be discovered in order to improve and develop new solutions. Our perspectives now turn to the establishment of an intelligent hybrid algorithm based on neural networks and monogenic wavelets.

Acknowledgements

The authors would like to thank the journal editor and all organizations that provided data for this research.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Rey, C. (2003) Tatouage d'image: Gain en robustesse et intégrité des images. Thèse, Université d'Avignon et des pays de Vaucluse, Avignon.

[2] Manoury, A. (2001) Tatouage d'images numériques par paquets d'ondelettes. Thèse de Doctorat, Ecole Centrale de Nantes, Université de Nantes, Nantes.

[3] Anstett, F. (2005) Les systems dynamiques chaotiques pour le chiffrement: Synthèse et cryptanalyse. Centre de Recherche en Automatique de Nancy (CRAN), Nancy.

[4] Nkapkop, J.D., Effa, J.Y., Borda, M., Ciprian, A., Bitjoka, L. and Alidou, M. (2016) Efficient Chaos-Based Cryptosystem for Real Time Applications. *Acta Technica Napocensis Electronics and Telecommunications*, **57**, 5-10.

[5] Tsafack, N., Sankar, S., Bassem, A.E., Kengne, J., Jithin, K.C., Belazi, A., Mehmood, I., Bashir, A., Song, O.Y., and Ahmed, A.E.L. (2016) A New Chaotic Map with Dynamic Analysis and Encryption Application in Internet of Health Things. *IEEE Access*, **8**, 137731-137744. https://doi.org/10.1109/ACCESS.2020.3010794

[6] Gunjal, B.L. and Mali, S.N. (2011) Secured Color Image Watermarking Technique in DWT-DCT Domain. *International Journal of Computer Science*, *Engineering and Information Technology* (*IJCSEIT*), **1**, 36-44.

[7] Mei, J., *et al.* (2009) A Digital Watermarking Algorithm Based on DCT and DWT. *Proceedings of the International Symposium on Web Information Systems and Applications*, Nanchang, 22-24 May 2009, 104-107.

[8] Petitcolas, F.A. (2000) Watermarking Schemes Evaluation. *IEEE Signal Processing*,

17, 58-64. https://doi.org/10.1109/79.879339

[9] Liu, X.-L., Lin, C.-C. and Yuan, S.-M. (2016) Blind Dual Watermarking for Color Images Authentication and Copyright Protection. *IEEE Transactions on Circuits and Systems for Video Technology*, **28**, 1047-1055. https://doi.org/10.1109/TCSVT.2016.2633878

[10] Ralaivao, H.H., Randriamitantsoa, P.A. and Raminoson, T. (2016) Sécurisation des images par combinaison de tatouage et de cryptage. MADA-ETI, Vol. 1. https://www.madarevues.gov.mg

[11] Rakotondraina, T.E., Ramafiarisona, H.M. and Randriamitantsoa, A.A. (2016) Transfert sécurisé d'images dans le domaine de la TFD. MADA-ETI, Vol. 1. https://www.madarevues.gov.mg

[12] Autrusseau, F., Guedon, J.P. and Bizais, Y. (2003) Watermarking and Cryptographic Schemes for Medical Imaging. *SPIE Medical Imaging*, *Image Processing*, Vol. 5032, 958-965.

[13] Puech, W., Dumas, M., Borie, J.C. and Puech, M. (2001) Tatouage d'images cryptées pour l'aide au Télédiagnostic. *Proceedings* 18*th Colloque Traitement du Signal et des Images*, *GRETSI*'01, Toulouse, Septembre 2001.

[14] Sunjay, B. and Raman, A. (2011) Chaos-Based Robust Watermarking Algorithm for Rightful Ownership Protection. *International Journal of Image and Graphics*, **11**, 471-493. https://doi.org/10.1142/S0219467811004263

[15] Noura, A., Ntsama, P. and Bitjoka, L. (2017) A Robust Biomedical Images Watermarking Scheme Based on Chaos. *International Journal of Computer Science and Security* (*IJCSS*), **11**, 1-18.

[16] Puech, W. and Marconi, J.R. (2005) Crypto-Compression of Medical Images by Selective Encryption of DCT. *EUSIPCO*'05, Antalya, September 2005, 1-10. https://hal-lirmm.ccsd.cnrs.fr/lirmm-00106485

[17] Rastislav, L. and Konstantinos, N.P. (2005) Color Filter Arrays: Design and Performance Analysis. *IEEE Transactions on Consumer Electronics*, **51**, 1260-1267. https://doi.org/10.1109/TCE.2005.1561853

[18] Zhang, L., Wu, X., Buades, A. and Li, X. (2011) Color Demosaicking by Local Directional Interpolation and Non-Local Adaptive Thresholding. *Journal of Electronic Imaging*, **20**, Article ID: 023016. https://doi.org/10.1117/1.3600632

[19] Li, X., Gunturk, B. and Zhang, L. (2008) Image Demosaicing: A Systematic Survey. *Proceedings of the SPIE—The International Society for Optical Engineering*, Vol. 6822, 68221J. https://doi.org/10.1117/12.766768

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

[21] Rastislav, L. and Konstantinos, N.P. (2007) Single-Sensor Camera Image Processing et Color Image Processing: Methods and Applications. CRC Press, London, 363-392. https://doi.org/10.1201/9781420009781.ch16

[22] Bülow, T. (1999) Hypercomplex Spectral Signal Representations for Image Processing and Analysis. Ph.D. Thesis, Inst. f. Informatik u. Prakt. Math. Der Christian-Albrechts-Universität zu Kiel, Kiel.

[23] Le Bihan, N. (2003) Traitement quaternionique des images couleur. Colloques sur le Traitement du Signal et des Images, GRETSI (Groupe d'Etudes du Traitement du Signal et des Images).

[24] Soulard, R. and Carré, P. (2010) Quaternionic Wavelets for Texture Classification. *Proceedings of the* 35*th IEEE International Conference on Acoustics*, *Speech and*

Signal Processing (*ICASSP* 2010), Dallas, 15-19 March 2010, 4134-4137. https://doi.org/10.1109/ICASSP.2010.5495732

[25] Chan, W.L., Choi, H.H. and Baraniuk, R.G. (2008) Coherent Multiscale Image Processing Using Dual-Tree Quaternion Wavelets. *IEEE Transactions on Image Processing*, **17**, 1069-1082. https://doi.org/10.1109/TIP.2008.924282

[26] Abena Ndongo, H., Eloundou Ebassa, B.L., Bitjoka, L. and Tieudjo, D. (2021) Securing CFA Images through the Simultaneous Hybrid Encryption-Watermarking Method Using Quaternions. *Journal of Image Processing & Pattern Recognition Progress*, **8**, 17-28. http://computers.stmjournals.com/index.php?journal=JoIPPRP&page=index

[27] Madhu, C. and Anant Shankar, E. (2017) Image Compression Using Quaternion Wavelet Transform. *Helix*, **8**, 2691-2695. https://doi.org/10.29042/2018-2691-2695

[28] Kingsbury, N. (2001) Complex Wavelets for Shift in Variant Analysis and Filtering of Signals. *Applied and Computational Harmonic Analysis*, **10**, 234-253. https://doi.org/10.1006/acha.2000.0343

[29] Boccaletti, S., Kurths, J., Osipov, G., Valladares, D.L. and Zhou, C.S. (2002) The Synchronization of Chaotic Systems. *Physics Reports*, **366**, 1-101. https://doi.org/10.1016/S0370-1573(02)00137-0

[30] National Bureau of Standards (1977) Data Encryption Standard, Federal Information Processing Standard.

[31] Tsafack, N., Kengne, J., Abd-El-Atty, B., Iliyasu, A.M., Hirota, K., and Abd EL-Latif, A.A. (2020) Design and Implementation of a Simple Dynamical 4-D Chaotic Circuit with Applications in Image Encryption. *Informing Science*, **515**, 191-217. https://doi.org/10.1016/j.ins.2019.10.070

[32] Abena, H., Eloundou, B.L., Bitjoka, L. and Tieudjo, D. (2021) Blind Watermarking of CFA Images Based on Quaternions. *Far East Journal of Electronics and Communications*, **24**, 67-80. https://doi.org/10.17654/EC024010067

[33] Marconi, J.R. (2006) Transfert sécurisé d'images par combinaison de techniques de compression, cryptage et marquage. Thèse, Université de Montpellier II, Montpellier.

[34] Khalfallah, A., Kammoun, F., Salim, M.B. and Christian, O. (2006) Evaluation du crypto-tatouage sémi-aveugle par le chaos dans le domaine multiresolution à base d'ondelette 9/7. 9ième *Conférence Maghrébine sur les technologies de l'information*, *MCSEAI*'06, Agadir, Hermes-Lavoisier, Traité IC2, 269-298. https://hal-lirmm.ccsd.cnrs.fr/lirmm-00129595

[35] Puech, W. and Coatrieux, G. (2008) Hybrid Coding: Encryption-Watermarking-Compression for Medical Information Security. Version 1, Chapitre d'ouvrage.

[36] Mohamed, B.A., Esam, A.H., El-Sayed, E.A., Mohamed, M.A. and Moustafa, A.H. (2019) Image Encryption and Watermarking Combined Dynamic Chaotic Hopping Pattern with Double Random Phase Encoding DRPE. *Optical and Quantum Electronics*, **51**, Article No. 246. https://doi.org/10.1007/s11082-019-1961-2