A ROBUST CHAOTIC AND FAST WALSH TRANSFORM ENCRYPTION FOR GRAY SCALE BIOMEDICAL IMAGE TRANSMISSION

Adélaïde Nicole Kengnou Telem[1], Daniel Tchiotsop[1], Thomas Kanaa[2], Hilaire B. Fotsin[3], Didier Wolf[4]

[1]Laboratoire d'Automatique et d'Informatique Appliquée (LAIA), Department of Electrical Engineering, IUT FV, University of Dschang, P.O. Box 134 Bandjoun – Cameroon.
[2]Laboratoire d'Electronique, Electrotechnique, Automatique et Télécommunications, Université de Douala, B.P. 1872 Douala.
[3]Laboratory of Electronics and Signal Processing, Faculty of Science, University of Dschang, P.O Box. 067 Dschang, Cameroon.
[4]Centre de Recherche en Automatique de Nancy (CRAN) UMR CNRS 7039, ENSEM Université de Lorraine, Nancy, France.

ABSTRACT

In this work, a new scheme of image encryption based on chaos and Fast Walsh Transform (FWT) has been proposed. We used two chaotic logistic maps and combined chaotic encryption methods to the two-dimensional FWT of images. The encryption process involves two steps: firstly, chaotic sequences generated by the chaotic logistic maps are used to permute and mask the intermediate results or array of FWT, the next step consist in changing the chaotic sequences or the initial conditions of chaotic logistic maps among two intermediate results of the same row or column. Changing the encryption key several times on the same row or column makes the cipher more robust against any attack. We tested our algorithms on many biomedical images. We also used images from data bases to compare our algorithm to those in literature. It comes out from statistical analysis and key sensitivity tests that our proposed image encryption scheme provides an efficient and secure way for real-time encryption and transmission biomedical images.

KEYWORDS

Image Encryption, Chaotic Logistic Map, Fast Walsh Transform, Telemedicine

1. INTRODUCTION

The fascinating developments in digital image processing and network communications during the past decade have created a great demand for real-time secure image transmission over the Internet and through wireless networks. In the past decade, images had been coded using orthogonal transform techniques such as Fourier transform coding [1-4], Hadamard Transform image coding and Walsh Hadamard Transform image. coding [5-9]. Fast algorithms have been designed to improve the speed of those techniques. They are known as Fast Fourier Transform coding (FFT) and Fast Hadamard Transform (FHT). Some variants of FHT are the Fast Walsh Hadamard Transform (FWHT) and Fast Walsh Transform (FWT). PRATT et al [10] has investigated a combination of Hadamard Transform to uniform quantization. Fundamental properties of the Hadamard transform have been discussed in conjunction with image coding application. It has been shown that the Hadamard Transform is better than the Fourier transform for image coding [10]. The Hadamard Transform has

several interesting properties. The most important properties from the standpoint of image coding are dynamic range, conservation of energy, and entropy. Hadamard Transform is faster than Fourier Transform [10]. All these transforms have the disadvantage that the coded image can be easily decoded by just applying the inverse transformation. So, the security of information is not guaranteed by using only these techniques.

Image encryption is the most useful technique to retain the confidentiality when images are stored or transmitted. Telemedicine for instance uses telecommunications technology to transmit medical images of a patient to a doctor who is at a distance. The confidentiality of medical information being essential, these images must be secured before, during and after transmission. Digital images, as it is known from the bibliography, have some very important features such as, bulk data capacity, strong correlation among adjacent pixels, redundancy of data, being less sensitive compared to the text data and existence of patterns and background [11]. So, concerning the above mentioned features, traditional ciphers like Data Encryption Standard (DES), Advanced Encryption Standard (AES), International Data Encryption Algorithm (IDEA) and Rivest-Shamir-Adleman (RSA), are not suitable for real time image encryption as these ciphers require a large computational time and high computing power. Nowadays, the position permutation, which is used in a great number of conventional image encryption algorithms, has the advantage to be fast. However, the security of these methods depends on the security of the algorithm, which does not satisfy the basic requirement of a modern encryption scheme.

In recent years, chaos based methods has been used for image encryption. Chaos is suitable for image encryption, as it is closely related to some dynamics of its own characteristics and refers to unpredictability. The behavior of the chaos system, under certain conditions, results phenomena which are characterized by sensitivities to the initial conditions and to the system parameters. Through the sensitivities, the system responses act to be random. The main advantages of the chaotic encryption approach include: high flexibility in the encryption system design, good privacy due to both nonstandard approach and vast number of variants of chaotic systems, large, complex and numerous possible encryption keys and simpler design.

I.S.I. Abuhaiba and M.A.S. Hassan proposed in [12] and improved encryption method based on two dimensional Fourier Transform, crossover operation and the use of a keyed mutation function. In [13], B.K. Shreyamshakumar et al showed that, image cryptosystem usually manipulates an entire data set without any presumption about compression at later time; consequently, the secure transmission of image has become more costly in term of time, bandwidth and complexity. A novel image encryption technique that conserves the compression ratio is proposed. The algorithm is embedded as a part of JPEG image encoding scheme. Firstly, fuzzy PN sequence is used to confuse the modified Direct Cosine Transform (DCT) blocks. Then the DCT coefficients of each modified (DCT) block are converted to unique uncorrelated symbols, which are confused by another fuzzy PN sequence. Finally, the variable length encoded bits are encrypted by chaotic stream cipher. To overcome the weakness of some cryptosystem, Anil Kumar and M.K. Ghose in [14] used chaotic standard map and linear feedback shift register to extend substitution- diffusion stage in cryptosystem. The number of round depends on pseudo-random sequence and original image. Vinod Patidar et al [15] used a secret key of 161-bits to provide a novel and robust chaos based pseudo random permutation - substitution scheme for image encryption. The key gives the fix number of rounds. Preliminary permutation, substitution and main permutation are done row-by-row and column-by-column instead of pixel-by-pixel. An efficient permutation – diffusion mechanism is used by Ruisong Ye [16]. A generalized Arnold map and Bernoulli shift map are employed in permutation and diffusion process. One chaotic orbit from Arnold map is used to get two index order sequences for the permutation. The two generalized maps are used to provide two pseudo-random gray value sequences for a two-way diffusion of gray values. Lin Teng and Xingyuan Wang in [17] proposed a bit-level image encryption algorithm based on spatiotemporal chaotic system which is self adaptive. The ciphered images depend on the plain image. The execution time is reduced by using a bit-level encryption. M. Khan and T. Shah in [18] used fractional Rössler chaotic system to product nonlinear component which can be used as block cipher with strong cryptographic properties.

In [19], Xiaoling Huang and Guodong Ye replace traditional chaotic confusion-diffusion architectures by a non linear traverse on the plain image. They used dependent diffusion and reverse 2 dimensional map. J.S. Armand Eyebe Fouda et al [20] proposes a method to overcome the time–consuming of image encryption based on chaos. This algorithm uses a one round encryption scheme for the fast generation of large permutation and diffusion keys based on the sorting of the solution of Linear Diophantine Equation (LDE). But the LDE is too complex compared to the simple chaotic logistic map. The hybrid scheme that combines a chaos-based

watermarking algorithm is proposed by E.Chrysochos et al in [21]. Two different watermarks and chaos are used. The first one is embedded in frequency domain combined with a two dimensional chaotic function. The second one is embedded in luminosity histogram of the image. In [22], Osama S. suggests a modification on the standard map and used it for confusion-diffusion mechanism in chaotic image cryptosystem. The plain image is firstly shuffled by a modification of standard chaotic map for many rounds. Then, the shuffled image is diffused by Henon chaotic map. Several rounds are necessary to achieve the goal of encryption. Jun-xin Chen et al in [23] used a dynamic state variables selection mechanism to accelerate the encryption, enhance the security and promote the efficiency of chaos based image cryptosystem. Two chaotic state variables are used to encrypt one plain pixel, this make the encryption not fast. Quan Liu et al, in [24] used the couple map lattice based on the chaos with Markov properties as a key stream generator to construct a novel image encryption algorithm.

Narendra Singh and Aloka Sinha [25] proposed a new method for image encryption using fractional Fourier transform and chaos theory. Random phase masks are generated using iterative chaos function. Heba M. et al in [26] improves the security of scrambling: scrambling blocks instead of individual pixels reduce the computation time; scrambling in another domain in order to overcome the drawbacks of spatial-domain scrambling; making such that the key stream depends on the plain image in order to resist the chosen-plaintext and known-plaintext attacks. They used three different modes of cipher operation block chain, cipher feedback and output feedback to implement 2D chaotic Baker map for scrambling in the Fractional Fourier Transform domain on digital images. The initialization vector works as the main key. In [27], a single channel color image encryption has been proposed based on iterative fraction Fourier transform and two-coupled logistic map by L. Sui and B. Gao. But fast Fourier transform is not as fast as Fast Walsh Hadamard transform. Zhang Ya-hong et al [28] proposed a binary image encryption algorithm based on chaos map and discrete Walsh transform is proposed. Firstly, chaos sequence is used to encrypt the image, and then the encryption image is scrambled by the discrete Walsh transform, which can achieve high-strength encryption. The chaotic operations are taken out before discrete Walsh transforms and his algorithm is applied on binary images.

In this work, our aim is to highly secure a coded image using chaos and FWT. Our method is very different from the scheme in [28]. We do apply the chaotic image encryption techniques during the FWT process, and we can use both binary and gray scale images. We combine a two- dimensional FWT and chaos methods encryption to produce a new image encryption system. We use two logistic chaotic maps, an external secret key to chaotic permutation and substitution in FWT of the image. The computation of the FWT of image needs several intermediate steps; when changing the position of pixels in the intermediate step results by using chaotic permutation. The pixel values are also change by XOR convolution with chaotic sequences. This acts to secure and hide information better than a simple FWT. The new cryptosystem is simple, efficient and robust. The results show the effectiveness of the algorithm.

In the rest of the paper, we describe the preliminary notions of FWT and logistic map in section 2, section 3 contains the description of our encryption system and section 4 presents the experimental results and security analysis. A conclusion ends the paper.

2. WALSH HADAMARD TRANSFORM AND LOGISTIC MAP

2.1 Walsh Hadamard matrices

The binary orthogonal Walsh functions are defined in the space of real numbers. These functions do take only two values: +1 and -1. A Walsh function is characterized by its position or by its sequence s. The sequence (s) is the number of zero crossings of waveform. It therefore increases with the number of time that the waveform alternates in sign. We can notice that the difference between Walsh matrix and Hadamard matrix is the order of sequence appearance. In Walsh matrix, sequences appear in decimal order.

The discrete Walsh functions are periodic with period N, where N is an integral power of two ($N = 2^p$). Thus a complete orthogonal set will have N distinct functions. These functions designated $wal(m,n)$ are described by equations (1) and (2) as proved in [29].

$wal(0,n) = 1;$ for n=0,1,2,…..N-1.

$$wal(1,n)=\begin{cases}1 & for \quad n=0,1,....(\frac{N}{2}-1)\\ -1 & for \quad n=\frac{N}{2},\frac{N}{2}+1,...N-1\end{cases} \tag{1}$$

$$wal(m,n)=wal(\left[\frac{m}{2}\right],2n).wal(m-2\left[\frac{m}{2}\right],n) \tag{2}$$

Where $\left[\frac{m}{2}\right]$ indicates the integer part of $\frac{m}{2}$

2.2 The Fast Walsh Transform (FWT)

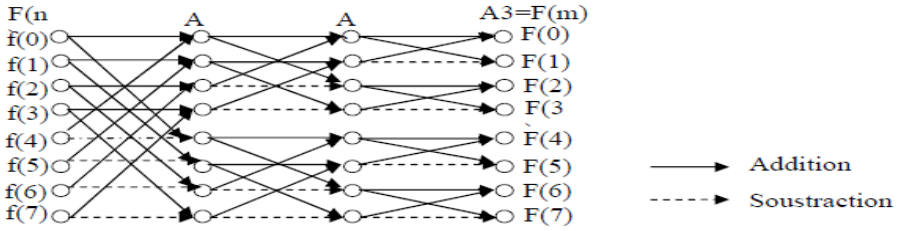

Figure1: Flow graph for the 8-length Walsh transform [29]

Given an N-length real array f(n), we can define the Walsh transform as [29] :

$$F(m)=\sum_{n=0}^{N-1}f(n)wal(m,n) \quad ; \text{m=0, 1, . . . N-1.} \tag{3}$$

Similarly, the inverse transform is

$$f(n)=\frac{1}{N}\sum_{n=0}^{N-1}F(m)wal(n,m) \quad ; \text{n=0, 1, ...N-1} \tag{4}$$

In [29], *JOHN L. SHANKS* describes a computation algorithm analogous to the cooley-Tukey algorithm. The computation of (3) and (4) requires no multiplication. The algorithm requires $NLog_2N$ summation to compute a complete Walsh transform rather than N^2 as indicated by equation (3). Figure 1 shows the flow graph for the 8-lenght Walsh transform.

A1 and A2 are intermediate steps before the final result A3 or F (m). For the general case when $N=2^p$, the intermediate Walsh transform arrays are defined by:

$$A_l(j_0,j_1,...j_{l-1},k_{p-l-1},....,k_0)=\sum_{k_{p-l}=0}^{1}A_{l-1}(j_0,j_1,...j_{l-2},k_{p-l-1},....,k_0)(-1)^{j_{l-1}k_{p-l}} \tag{5}$$

Where $l=1,2,....p$ and

$$A_0(k_{p-1},k_{p-2},...k_0)=f(k_{p-1},k_{p-2},...k_0) \tag{6}$$

The general equation for the $N=2^p$ - length discrete Walsh function is then

$$wal(j_{p-1},j_{p-2},...j_0;k_{p-1},k_{p-2},....k_0)=\prod_{i=0}^{p-1}(-1)^{j_{p-1-ik_i}} \tag{7}$$

Since $wal(n,m) = wal(m,n)$, the inverse Walsh transform is identical to the Walsh transform with the difference that all the values are divided by N. As $N = 2^p$, we have p-2 intermediate Walsh transform arrays [29].

2.3 Walsh transformation of images

Let the array $f(x, y)$ representing the intensity samples of an original image over an array of N^2 points. The two-dimensional Hadamard transform, $F(u,v)$ as proved in [27], of $f(x, y)$ is given by matrix product [10] of equation (8).

$$[F(u,v)] = [H(u,v)][f(x,y)][H(u,v)] \tag{8}$$

Where $[H(u,v)]$ is an N order symmetric Hadamard matrix. The inverse two-dimensional Hadamard transform, $f(x, y)$, of $F(u,v)$ is also given by the matrix product of equation (9).

$$[f(x,y)] = \frac{1}{N^2}[H(u,v)][F(u,v)][H(u,v)] \tag{9}$$

As a Walsh matrix is the sequence ordered Hamard matrix, we can compute the two-dimensional Walsh transform by using (8) where Hadamard matrix is replaced by ordered Walsh matrix. *PRATT et al* have given in [10] the series form of the two-dimensional Walsh Hadamard transform as expressed in (10).

$$F(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)(-1)^{p(x,y,u,v)} \tag{10}$$

Where $p(x, y, u, v) = \sum_{i=0}^{n-1}(u_i x_i + v_i y_i)$

The items u_i , v_i, x_i and y_i are the binary representations of u, v, x, and y respectively.

The walsh matrix which is the Hadamard "ordered" such that the sequence s of each row is larger than the sequence of the preceding row, can be written as in (11).

$$F(u,v) = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)(-1)^{q(x,y,u,v)} \tag{11}$$

Where $q(x, y, u, v) = \sum_{i=0}^{n-1}(\rho_i(u)x_i + \rho_i(v)y_i)$

$\rho_0(u) = u_{n-1}$; $\rho_1(u) = u_{n-1} + u_{n-2}$; $\rho_2(u) = u_{n-2} + u_{n-3}$; . . . $\rho_{n-1}(u) = u_1 + u_0$

2.4 Logistic chaotic map

The typical chaotic dynamical systems, such as logistic map and Lorenz system can be used for image encryption. The logistic map has been widely used because of its simplicity and its efficiency. It is mathematically expressed by equation (12) in [30].

$$X_{k+1} = \mu X_k (1 - X_k) \tag{12}$$

Where $0 < \mu \leq 4$ is called bifurcation parameter and X_k is a real number in the range [0, 1]. The status of the system depends on μ . The bifurcation diagram of the logistic is shown in figure 2.

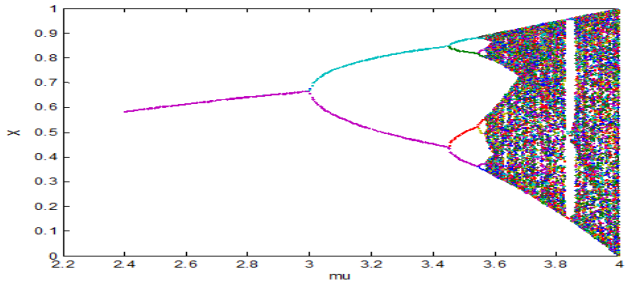

Figure 2: bifurcation diagramme of logistic map

We can see in the diagram that for 3.569955672 <m <= 4, the mapping has a chaotic form. With different initial conditions X_o , the generated sequences X_k are non-correlated, non periodic and non-converging. The system is very sensitive to the initial condition X_o . In image encryption; this characteristic is used to generate different sequences only by changing the initial condition X_o .Those sequences are easy to generate and seem to be like white noise. They are used in permutation-diffusion process of encryption.

The probability density function of logistic map which is shown in Figure 3 can be described as follows.

$$\rho(x) = \begin{cases} \dfrac{1}{\pi\sqrt{1-x^2}} & -1 < x < 1 \\ 0 & otherwise \end{cases} \tag{13}$$

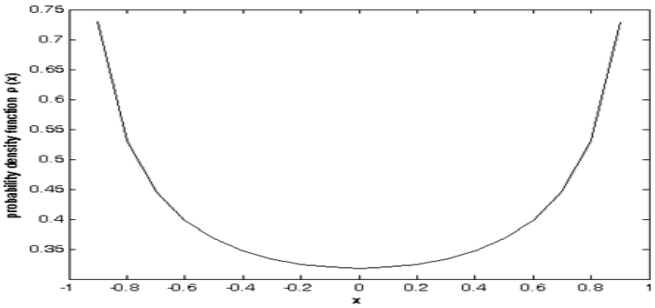

Figure 3: Probability density of Logistic map

It comes from figure 3 that the probability density of a Logistic map is symmetric; ρ(x) does not depend on the initial value X_0, indicating that the chaos system is ergodic.

3. THE CHAOTIC-FWT IMAGE ENCRYPTION ALGORITHM

Our proposed encryption scheme of gray-scale image, which has been implemented in MATLAB, is presented in detail in this section. We use an external secret key, two chaotic logistic maps and the FWT to achieve the goal of the encryption. Two basis of image encryption processes are used: the permutation and the substitution. For image encryption methods based on chaos, those processes are applied directly on the pixel values of images. In [28], those processes are used to encrypt the image and then the encryption image is scrambled by the discrete Walsh transform. Thus, image encryption through chaos and the discrete Walsh transform are performed separately.

In this work, we realize image encryption performing chaos and the discrete Walsh transform simultaneously. Figure 4 illustrates our image encryption scheme. In the following paragraph, different steps of the scheme as well as the complete description of our encryption algorithm are discussed.

3.1 An external secret key

The proposed algorithm uses an external secret key of thirty two hexadecimal numbers. Let « **ABCDEFGHIJKLMNOPRSTUVWαβγηθλξρτφ** » be an external key, the 32 hexadecimal numbers will be distributed as follows:

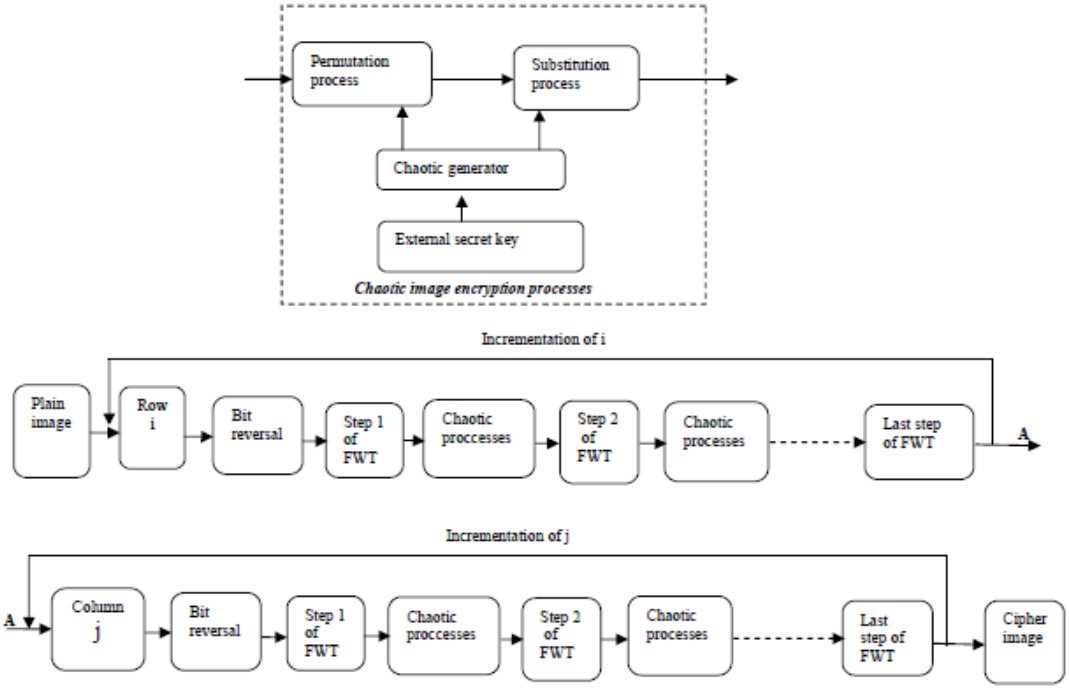

Figure 4: image encryption scheme

- **ABCDE** and **RSTUV** are used to calculate the parameters **μ** of the chaotic logistic maps ;
- **FGHIJ** and **Wαβγη** give the initial conditions of the chaotic logistic maps ;
- **KLM** and **θλξ** refer to the variation of the initial conditions of the chaotic logistic maps among two rows or two columns respectively ;
- **NOP** and **ρτφ** give the variation of the initial conditions of the chaotic logistic maps among two step of FWT;

3.2 Chaotic generators

In the algorithm, two chaotic logistic maps are used to generate those chaotic sequences. They are given by (14) and (15).

- $X_{n+1} = \mu_x x_n (1 - x_n)$; (14)
- $Y_{n+1} = \mu_y y_n (1 - y_n)$. (15)

Where μ_x , μ_y and the initial conditions x_0, y_0 are obtained from an external secret key as shown in Figure 5.

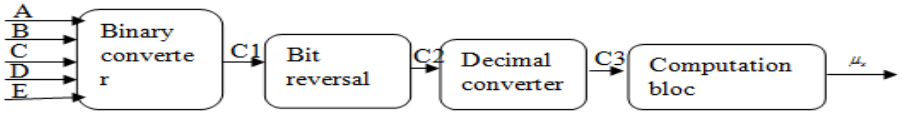

Figure 5: Bifurcation parameter of chaotic logistic map processing.

The hexadecimal numbers A,B,C,D and E coming from external secret key are converted into their corresponding binary representation to obtain a code C1.The bit reversal operation is apply to C1 to obtain a code C2 which is converted into a decimal code to compute the bifurcation parameter μ_x *as indicated in equation (16).*

The parameter μ_x is determined as follow:

- Use the code **ABCDE** from the external secret key and convert each hexadecimal numbers **A, B, C, D and E** into their corresponding binary number of 4 bits long and obtain a code **C1** having 20 bits long.
- Apply "bit reversal" on the code C1 to obtain the code C2.
- Convert C2 into decimal number called C3.

Then $\mu_x = 3.9 + \frac{C_3}{2^{24}}$ (16)

As μ_x , μ_y is calculate by using **RSTUV** from the external secret key.

$$\mu_y = 3.8 + \frac{C_3}{2^{24}} \quad (17)$$

The initial conditions of the chaotic logistic maps are determined as the parameter μ . We use **FGHIJ** and **Wαβγη,** respectively for X_o and Y_o and calculate as follow.

$$X_o = \frac{C_3}{2^{24}} \quad (18)$$

$$Y_o = \frac{C_3}{2^{24}} \quad (19)$$

3.3 Pixel Substitutions

During the encryption process, we have to change the values of pixels. We use equations (14) and (15) to generate the chaotic sequences. As the numbers generated from those equations are not integers, the chaotic sequences are transform into integer sequences as follow:

$$x = (x \times 1000) \bmod 256 \quad (20)$$

3.4 The chaotic FWT process

The computation of the FWT is performed in two steps. Let the array $f(x, y)$ being the intensity samples values of an image $I_{M \times N}$.

Firstly, a one-dimensional Walsh transform is taken along each row of the array $f(x, y)$. Here, the first chaotic logistic map is used. For the first row, the initial condition x_0 comes directly from an external secret key. For other rows, the procedure to obtain an initial condition is presented in figure 6.

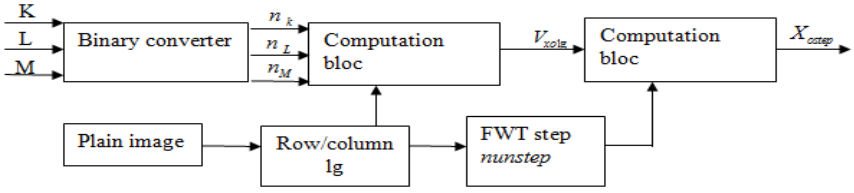

Figure 6: *Initial condition* X_o *of chaotic logistic map processing. We extract K, L and M from an external secret key and convert each of them into their corresponding binary representation* n_k , n_L , n_M . *From the plain image, we take* l_g *which is the index number of the row or the column.* n_k , n_L , n_M *and* l_g *are used to compute* V_{x0lg} . *To change chaotic sequences from one intermediate step of FWT to another one, we use the index number of the intermediate step*

called " $nunstep$ *" and* $V_{x0\lg}$ *to calculate the initial condition* X_{0step} *of the corresponding intermediate step of FWT.*

We determine the initial condition X_0 as follow:

- Use the code **KLM** from an external secret key and convert each hexadecimal number into their corresponding binary numbers **Kb, Lb** and **Mb** of 4 bits long each**.**
- Let n_k, n_L and n_M be the total number of bit '1' in the binary representation of K,L and M. The variation of the initial condition on row 'lg' is given by

$$V_{xo\lg} = \frac{\left(\frac{K}{2^{n_k}} + \frac{L}{2^{n_L}} + \frac{M}{2^{n_M}}\right)}{2^{(\lg + n_k + n_L + n_M)}}$$

where $\lg \neq 1$ (21)

- Then the initial condition used on the row 'lg' is given by

$$X_{o\lg} = X_O + V_{x0\lg} \quad (22)$$

As we can see in figure 1, each FWT process of an image of size M ($M = 2^p$), need $p-2$ intermediate steps before the result. We start by bit reversal on the position of the pixel in the row. Equation (5) is used to calculate the array A1 of the reversal row. This is the first step of FWT. Having a corresponding initial condition of the chaotic logistic map of the row; we use equation (14) to generate the chaotic sequence of the first step A1. We sort this sequence in "ascending" order and use it to permute the position of the element in A1 to obtain $A_1^{'}$. We use equation (20) to transform the chaotic sequence into integer chaotic sequence. The values of the element in $A_1^{'}$ are substituted by its "xored" with an integer chaotic sequence to obtain $A_1^{''}$. From $A_1^{''}$ we compute the next step of FWT called A2.The same operation is done on A2 as on A1 with different initial condition obtain as follow:

$$X_{Ostep} = X_{0\lg} + \frac{(V_{x0\lg} \times nunstep)}{10} \quad (23)$$

Where $nunstep$ is the number of step and $nunstep \neq 1$.

The procedure is repeated for all the rows of the whole image.

Then a second one-dimensional Walsh transform is taken along each column. We use the second chaotic logistic map and the procedure is similar.

3.5 The proposed encryption algorithm

Let $I_{M\times N}$ be an original image. We can describe our encryption algorithm as follow:

- *Generate an external secret key;*
- *Use an external secret key to calculate* μ_x *and* X_0 *;*
- *Generate the masking and permutation chaotic sequence;*
- *For each row*
  - *Reverse the bit on the position of each element of the row;*
  - *Compute the first step of FWT on the row ;*
  - *Apply chaotic permutation and substitution on the first array* A_1 *by using the sequence generate directly from an external secret key ;*
  - *For the other step* $A_2 \ldots\ldots A_{p-1}$
    - *Change the initial condition* X_{0step} *;*
    - *Compute the array* A_i *;*

- *Apply chaotic permutation and substitution ;*

- *Use an external secret key to calculate* μ_y *and* Y_0 *;*
- *Generate the masking and permutation chaotic sequence;*
- *For each column*
  - *Reverse the bit on the position of each element of the column;*
  - *Compute the first step of FWT on the column ;*
  - *Apply chaotic permutation and substitution on the first array* A_1 *by using the sequence generate directly from an external secret key ;*
  - *For the other step* $A_2 \ldots\ldots A_{p-1}$
    - *Change the initial condition* X_{0step} *;*
    - *Compute the array* A_i *;*
    - *Apply chaotic permutation and substitution ;*

As we can see on figure 7, the process of decryption is completely inverse to the encryption process described above, except that, on step 9 and 18 , each value should be divided respectively by N and M as indicate on inverse FWT. The decryption algorithm is described below:

- *Generate an external secret key;*
- *Use an external secret key to calculate* μ_x *and* X_0 *;*
- *Generate the masking and permutation chaotic sequence;*
- *For each column*
  - *Reverse the bit on the position of each element of the column;*
  - *Compute the first step of FWT on the column ;*
  - *Apply chaotic permutation and substitution on the first array* A_1 *by using the sequence generate directly from an external secret key ;*
  - *For the other step* $A_2 \ldots\ldots A_{p-1}$
    - *Change the initial condition* X_{0step} *;*
    - *Comput the array* A_i *;*
    - *Apply chaotic substitution and permutation;*
    - *Divide each element of the final result by N*
- *Use an external secret key to calculate* μ_y *and* Y_0 *;*
- *Generate the masking and permutation chaotic sequence;*
- *For each row*
  - *Reverse the bit on the position of each element of the row;*
  - *Compute the first step of FWT on the row ;*
  - *Apply chaotic permutation and substitution on the first array* A_1 *by using the sequence generate directly from an external secret key ;*
  - *For the other step* $A_2 \ldots\ldots A_{p-1}$
    - *Change the initial condition* X_{0step} *;*
    - *Compute the array* A_i *;*
    - *Apply chaotic permutation and substitution ;*
    - *Dived each element of the final result by M*

3.6 Evaluation metrics

To evaluate the encryption quality, many evaluation metrics are considered.

3.6.1 Correlation coefficient

For the evaluation of encryption quality, the correlation coefficient (Co) is used as follow:

$$Co = \frac{N_p \sum_{j=1}^{N_p} (x_j \times y_j) - \sum_{j=1}^{N_p} x_j \times \sum_{j=1}^{N_p} y_j}{\sqrt{N_p \sum_{j=1}^{N_p} x_j^2 - (\sum_{j=1}^{N_p} x_j)^2 \times (N_p \sum_{j=1}^{N_p} y_j^2 - (\sum_{j=1}^{N_p} y_j)^2)}} \quad (24)$$

Where x and y are gray scale pixel values of the original and encrypted images, and N_p is total number if pixels. Correlation between plain and cipher images must be close to zero to prove a good encryption quality.

3.6.2 Security analysis

A good encryption scheme should be robust against all kinds of known attacks such as cryptanalytic, statistical and brute-force attacks.

For a secure image cipher, the key space should be large enough to make the brute force attack infeasible. According to Shannon's theory, it is possible to solve many kinds of ciphers by statistical analysis. Confusion and diffusion are introduced to increase the difficulty of statistical analysis. The histogram of the cipher images and the correlations of adjacent pixel in the cipher image are the two primary measurements to statistical property. A cipher image coming from a good image encryption scheme should have a uniform histogram. Each pixel of any image has a high correlation with its adjacent pixels either in horizontal, vertical or diagonal directions.

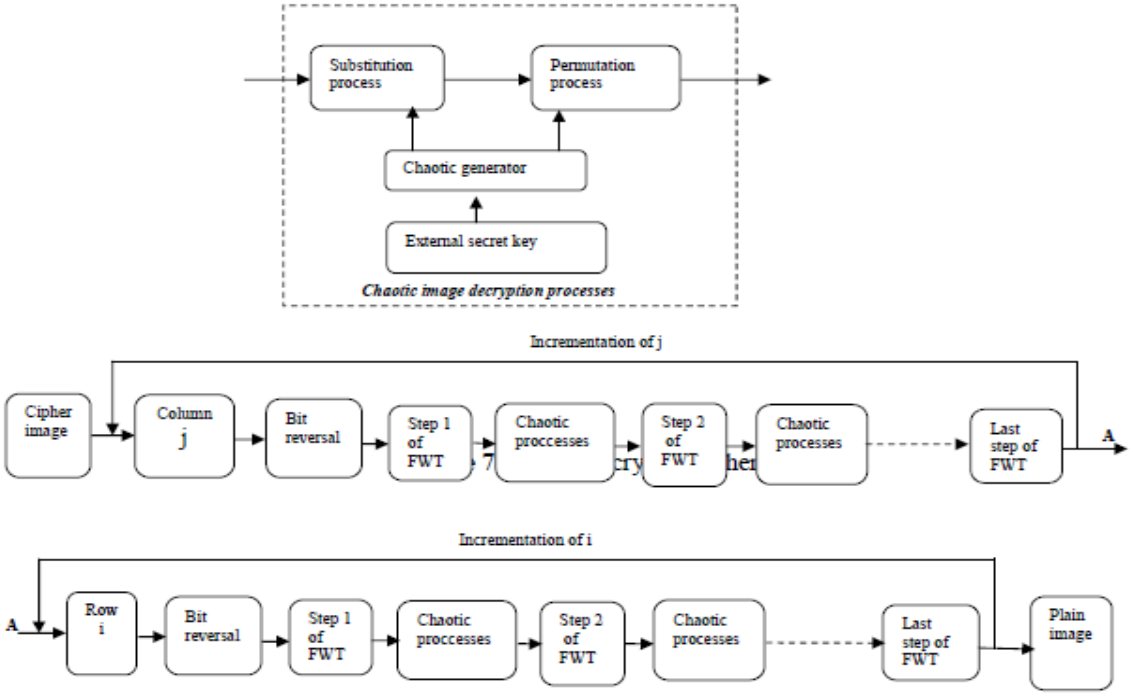

Figure 7: Image Decryption scheme

For testing the correlation in a plain and encrypted image respectively, the correlation coefficient γ of each pair of pixels was calculated using the following formula.

$$E(x) = \frac{1}{N_{ap}} \sum_{i=1}^{N_{ap}} x_i \tag{25}$$

$$D(x) = \frac{1}{N_{ap}} \sum_{i=1}^{N_{ap}} [x_i - E(x)]^2 \tag{26}$$

$$\mathrm{cov}(x, y) = \frac{1}{N_{ap}} \sum_{i=1}^{N_{ap}} [x_i - E(x)][y_i - E(y)] \tag{27}$$

$$\gamma(x, y) = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}} \tag{28}$$

In equations (25)-(28) x and y are the gray values of two adjacent pixels in the image and N_{ap} is the total number of adjacent pairs of pixels.

The information entropy, introduced by Shannon, is one of the most important features of randomness. Information entropy $H(s)$ is calculated by the following formula

$$H(s) = -\sum_{i=0}^{N_{gl}-1} P(s_i) \log_2 (\frac{1}{p(s_i)}) \tag{29}$$

Where N_{gl} is the number of gray level in the image and $P(s_i)$ shows the probability of appearance of the symbol s_i.

3.6.3 Differential attacks

Two common measures, Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) are used to test the influence of changing a single pixel in the original image on the whole image encrypted by the proposed algorithm. Therefore, if $A(i, j)$ and $B(i, j)$ are the pixels in row i and column j of the encrypted images A and B, with only one pixel difference between the respective plain images, then the NPCR is calculated by using the following formula:

$$NPCR = \frac{\sum_{i,j} D(i, j)}{W \times H} \times 100\% \tag{30}$$

Where W and H are the width and height of A or B. $D(i, j)$ is produced as follow:

$$D(i, j) = \begin{cases} 1 & if \quad A(i, j) = B(i, j) \\ 0 & otherwise \end{cases} \tag{31}$$

The second number (UACI) is calculated by the following formula.

$$UACI(A, B) = \frac{1}{W \times H} \left[\sum_{i,j} \frac{|A(i, j) - B(i, j)|}{255} \right] \times 100\%$$

4 EXPERIMENTAL RESULTS AND SECURITY ANALYSIS

4.1 Experimental Results

Figure 8 shows the visual test of our encryption scheme on several medical gray scale images. An external secret key used for this encryption is « **5A9FE86248A78612327A9E2339AB8C12** ». As one can see in Figure 8, there

is not visual similarity between cipher and original images. We tested many images and all the results were conclusive. Looking at cipher images (figure8 (b, e and h)), it's impossible to imagine which images have been encrypted because the cipher images do not give any clue of original images. Visual test confirm that cipher images is not like original one. From Figure 8 c, f and i, we notice the similarity between original and decrypted images. The cipher images have been successful decrypted. Different external key were used and we obtained the same results. Mathematically, we confirmed the test by checking many evaluations metrics.

4.1.2 Correlation test and entropy information analysis

An evaluation metric which tests the similarity between cipher and original images is correlation coefficient (Co). Table 1 presents the Co values of several medical gray scale images of [31].

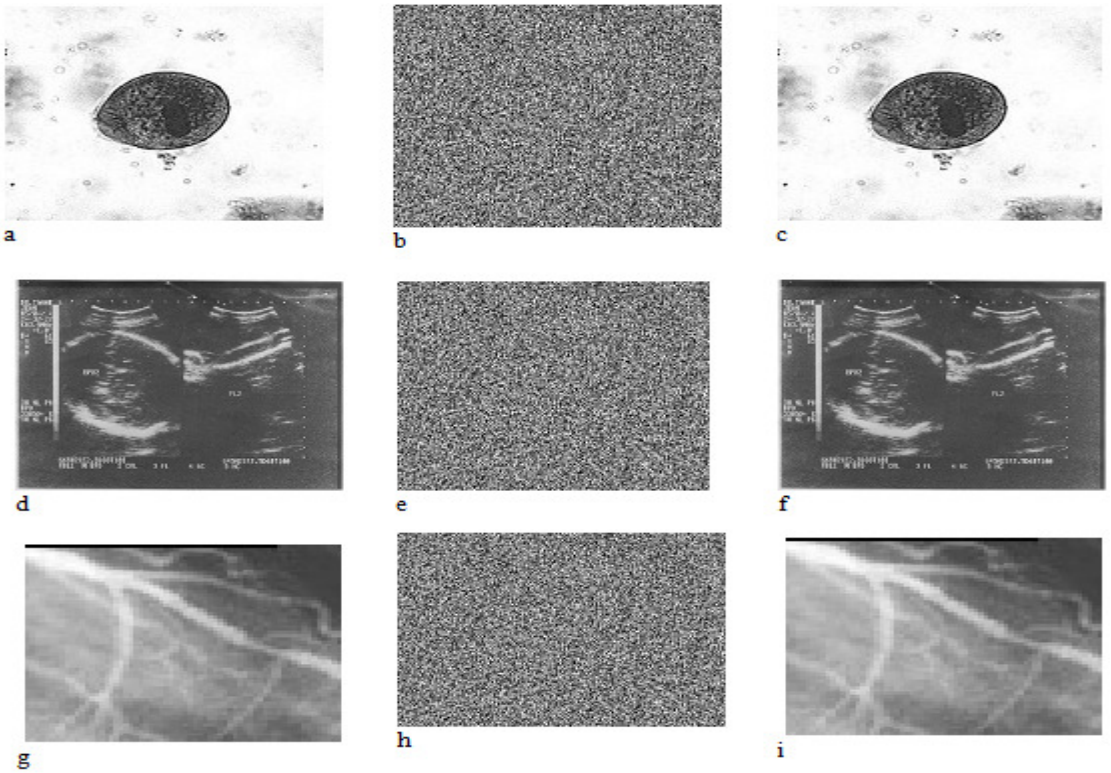

Figure 8: Visual test on some biomedical images using the secret key « **5A9FE86248A78612327A9E2339AB8C12** »: Frame (a), (b) and (c) show a plain image "Entamoeba Coli trophozoite " and its corresponding cipher and decrypted image respectively. Frame (d) ,(e) and (f) show a plain image "echopelv" and its corresponding cipher and decrypted image respectively. Frame (g), (h) and (i) show a plain image "angio" and its corresponding cipher and decrypted image respectively.

The greater is the value Co, the more similar are the compared images. When the compared images are identical, we obtain the maximum and critical correlation value which is one. We can see from table 1 that all Co are very closed to zero for ciphers, meaning that cipher images are not correlated with the original. The highest value obtained using this key is 0.0064 for the Entamoeba hitolytica trophozoite_redim2. In the contrary, the decrypted and the original images are always identical since all the corresponding correlations are one. In the case of 256 gray-scale images, truly random image entropy is equal to eight [20], which is the ideal value. As shown in table 1, we notice that the values obtained in the proposed scheme are very close to 8. The highest value is 7.9994 and the smallest one is 7.9970. The plain images and the decrypted images have the same entropy information which is, in all cases, as we can from table 1, smaller than the entropy information of cipher images. This indicates that the chaotic FWT has hidden information randomly and information leakage in encryption process is negligible. We also conclude the effectiveness of the algorithm because of the highest value of entropy information.

Table 1: Correlation coefficients an entropy information of some medical images from [31].

Image Name	size	Cipher Image		Decrypted Image	
		Correlation coefficients	Entropy information	Correlation coefficients	Entropy information
ANTAMOEBACOLI	398x407	-6.1021e-004	7.9993	1	5.9299
article_oeuf_taeniaC2	200x200	0.0024	7.9973	1	7.1138
Balantidium Coli cyst	200x200	0.0038	7.9975	1	6.6781
Balantidium coli_trophozoite	200x200	0.0046	7.9972	1	5.5143
DICROCOELIUM	400x341	0.0014	7.9993	1	6.1649
Entamoeba Coli trophozoite	200x200	-0.0022	7.9969	1	6.8476
Entamoeba Histolytica cyst	200x200	-0.0010	7.9971	1	5.6970
Entamoeba histolytica -cyst-Gini	130x130	-7.2972e-004	7.9994	1	5.7185
Entamoeba hitolytica trophozoite	200x200	0.0014	7.9970	1	7.3585
Entamoeba hitolytica trophozoite_redim	120x120	0.0022	7.9972	1	7.3494
Entamoeba hitolytica trophozoite_redim2	172x160	0.0064	7.9974	1	7.4079
oeuf_ascarisc	266x200	-0.0014	7.9993	1	6.6170
S- Hematobium egg	400x300	-0.0022	7.9993	1	6.7551
S- Mansoni egg	400x300	-0.0025	7.9993	1	6.3052
tropho_entamoeba_histolytica2	332x213	-3.0008e-004	7.9993	1	3.9022
tropho_iodamoeba_butschlii	200x200	-0.0022	7.9972	1	5.9442
angioF	64x64	3.3850e-006	7.9971	1	7.2376
angio	64x64	4.9866e-004	7.9972	1	7.2563
node2	64x64	0.0033	7.9972	1	6.8732
Ossify	64x64	-0.0019	7.9976	1	6.9989
CTpancratitis	64x64	0.0030	7.9975	1	6.4541
echo1	64x64	8.9342e-004	7.9972	1	6.3281
I1_200	64x64	5.3473e-004	7.9979	1	6.4746
k_bw	64x64	0.0050	7.9971	1	6.1897
lung16	64x64	-1.1081e-004	7.9976	1	6.1142
Pelvis	64x64	0.0013	7.9974	1	6.4653
ribs	64x64	-3.6710e-004	7.9973	1	6.2298
DisLocElbow	64x64	0.0034	7.9971	1	5.5326
echopelv	373x453	0.0026	7.9993	1	6.5896

To prove the effectiveness of the algorithm on any type of image, we apply it on various other non medical images. We have used the USC-SIPI image database which is a collection of digitized image available and maintained by the University of Southern California [32]. We have chosen miscellaneous volume to measure the correlation coefficient of several USC-SIPI image databases. Table 2 shows the results of those images. The same as for medical images, correlations Co of images in table 2 are near to zero and the entropy information is near to eight. The maximum value of Co is 0.0036. It is very low compared to the critical value 1. The entropy information of plain image and decrypted image is also small than the decrypted one. Our algorithm is then efficient not only on medical images but also on all types of images.

4.2 Security analysis

We discuss here the security analysis of the proposed image encryption algorithm such as key space analysis, statistical analysis and various attacks.

Table 2: Correlation coefficients and entropy information of the USC-SIPI image database

Filename	Description	Size	Type	Cipher Images		Decrypted Images	
				Correlation coefficients	Entropy information	Correlation coefficients	Entropy information
4.1.01	Girl	256	color	0.0021	7.9974	1	7.0525
4.1.02	Couple	256	color	7.6609e-004	7.9973	1	6.4207
4.1.03	Girl	256	color	6.0843e-004	7.9971	1	5.5939
4.1.04	Girl	256	color	2.4958e-005	7.9974	1	7.2575
4.1.05	House	256	color	0.0059	7.9971	1	6.4961
4.1.06	Tree	256	color	-0.0019	7.9969	1	7.3103
4.1.07	Jelly beans	256	color	0.0016	7.9968	1	5.7286
4.1.08	Jelly beans	256	color	0.0018	7.9968	1	6.2430
4.2.01	Splash	512	color	-3.3974e-004	7.9993	1	7.2533
4.2.02	Girl (Tiffany)	512	color	-0.0014	7.9993	1	6.6009
4.2.03	Mandrill (a.k.a. Baboon)	512	color	6.0137e-004	7.9993	1	7.3583
4.2.04	Girl (Lena, or Lenna)	512	color	-7.4253e-004	7.9993	1	7.4451
4.2.05	Airplane (F-16)	512	color	7.2430e-004	7.9993	1	6.7025
4.2.06	Sailboat on lake	512	color	6.5275e-004	7.9993	1	7.4842
4.2.07	Peppers	512	color	-4.5261e-004	7.9993	1	7.5937
5.1.09	Moon surface	256	Gray	-0.0036	7.9972	1	6.7093
5.1.10	Aerial	256	Gray	-0.0035	7.9974	1	7.3118
5.1.11	Airplane	256	Gray	-0.0017	7.9972	1	6.4523
5.1.12	Clock	256	Gray	0.0031	7.9974	1	6.7057
5.1.13	Resolution chart	256	Gray	4.9859e-004	7.9971	1	1.5483
5.1.14	Chemical plant	256	Gray	-0.0032	7.9972	1	7.3424
5.2.08	Couple	512	Gray	0.0014	7.9994	1	7.2010
5.2.09	Aerial	512	Gray	-2.7959e-004	7.9994	1	6.9940
5.2.10	Stream and bridge	512	Gray	-1.3095e-004	7.9993	1	5.7056
7.1.01	Truck	512	Gray	8.9836e-006	7.9993	1	6.0274
7.1.02	Airplane	512	Gray	0.0023	7.9993	1	4.0045
7.1.03	Tank	512	Gray	-0.0011	7.9993	1	5.4957
7.1.04	Car and APCs	512	Gray	0.0012	7.9993	1	6.1074
7.1.05	Truck and APCs	512	Gray	9.0072e-004	7.9993	1	6.5632
7.1.06	Truck and APCs	512	Gray	0.0016	7.9994	1	6.6953
7.1.07	Tank	512	Gray	0.0012	7.9993	1	5.9916
7.1.08	APC	512	Gray	-8.9170e-004	7.9994	1	5.0534
7.1.09	Tank	512	Gray	5.0805e-004	7.9994	1	6.1898
7.1.10	Car and APCs	512	Gray	-2.6314e-004	7.9994	1	5.9088
boat.512	Fishing Boat	512	Gray	4.5354e-004	7.9994	1	7.1914
elaine.512	Girl (Elaine)	512	Gray	-4.5148e-005	7.9993	1	7.5060
house	House	512	color	-4.6406e-004	7.9993	1	7.2334
gray21.512	21 level step wedge	512	Gray	-2.9650e-004	7.9993	1	4.3923
numbers.512	256 level test pattern	512	Gray	-5.0912e-004	7.9994	1	7.7292

4.2.1 Key space analysis

4.2.1.1 Key space

Our proposed image cipher has 2^{128} different combinations of the secret key. Even if one knows the combination of the secret key, it is not easy to imagine the signification of each bit. As chaotic logistic maps are sensitive to the initial condition, it is not possible to generate the same sequences with different initial conditions.

4.2.1.2 Key sensitivity test

An ideal image cipher should be extremely sensitive with respect to the key used in the algorithm. A single change as small as possible in the key should not decrypted the cipher image successfully. We have tested the sensitivity with respect to the key for several images. To this end, the encrypted image corresponding to plain image is decrypted with a slightly different key from the original one. Further, we calculate correlation coefficient between the encrypted image and the image decrypted using a slightly different key. Some examples are discussed below.

a) The encrypted image (Fig.8 (b)) is decrypted with another key « 5A**8**FE86248A78612327A9E2339AB8C12 » which is different to the original key « 5A**9**FE86248A78612327A9E2339AB8C12 ». The difference between these keys in this case changes the parameter μ of the first chaotic logistic map that introduces a change of a single bit. The resultant encrypted image is shown in Fig.9 (a).

b) The encrypted image (Fig.8 (b)) is decrypted by making a slight modification in the original key « 5A9FE862**5**8A78612327A9E2339AB8C12 », once again, only a single bit is changed in the initial condition X_0 .The resultant of the decrypted image is shown in Fig.9 (b).

c) We changed the variation of the initial conditions of the chaotic logistic maps among two columns and decrypted the encrypted image (Fig.8 (b)) with « 5A9FE86248A78612327A9E2339**8**B8C12 ». Fig.9 (c) shows the resultant decrypted image which is not correlated with the original image.

d) In figure 9.(d) , the variation of the initial conditions of the second chaotic logistic maps among two step of FWT has been changed to decrypt the encrypted image (Fig.8 (b)) . The key used is in this case « 5A9FE86248A78612327A9E2339AB8**D**12 ».

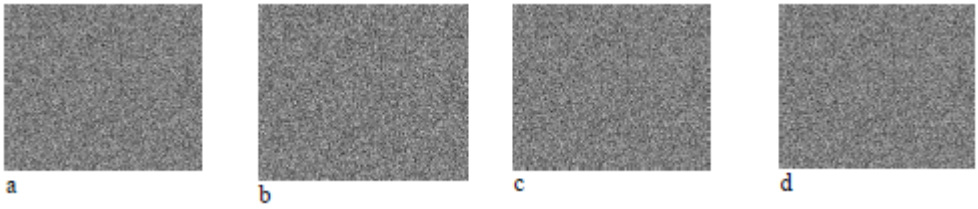

Figure 9: Frame (a)-(d) show the decrypted images from the encrypted image of Fig.8 (b) using slightly different keys than the key used for encryption.

With a slight change in the key, one is unable to find any clue about the original image from the decrypted image. To compare the decrypted images, we have calculated the correlation coefficient among the decrypted images. Table 3 gives us the results of this comparison. The Co between various decrypted images is close to zero. This means that, without an exact key we cannot succeed on decryption process. We conclude from table 3 that one cannot find any clue about the plain image even if there is a little change in the key. The correlation coefficient is negligible. This confirms the effectiveness and the key sensitivity of the proposed algorithm.

Table 3: Correlation coefficients between various decrypted images show in Fig. 9

Figure	Correlation coefficients
Fig.9 (a) and fig.9(b)	0.0011
Fig.9 (a) and fig.9(c)	0.0019
Fig.9 (a) and fig.9(d)	-0.0058
Fig.9 (b) and fig.9(c)	-6.4778e-004
Fig.9 (b) and fig.9(d)	-0.0029
Fig.9 (c) and fig.9(d)	-2.5939e-004

4.2.2 Statistical analysis

4.2.2.1 Histograms of encryption images

The histograms of the plain and encrypted images which are obtained by the proposed method are shown in Figure 10.

Comparing the histograms, we can see a uniform distribution of gray-scale values of the encrypted image, which testify the toughness of the method over any statistical attack, on the other hand, the histogram of the plain image has a discrete shape. This shows that the encrypted image is secured with our encryption scheme and will resist to any statistical attack.

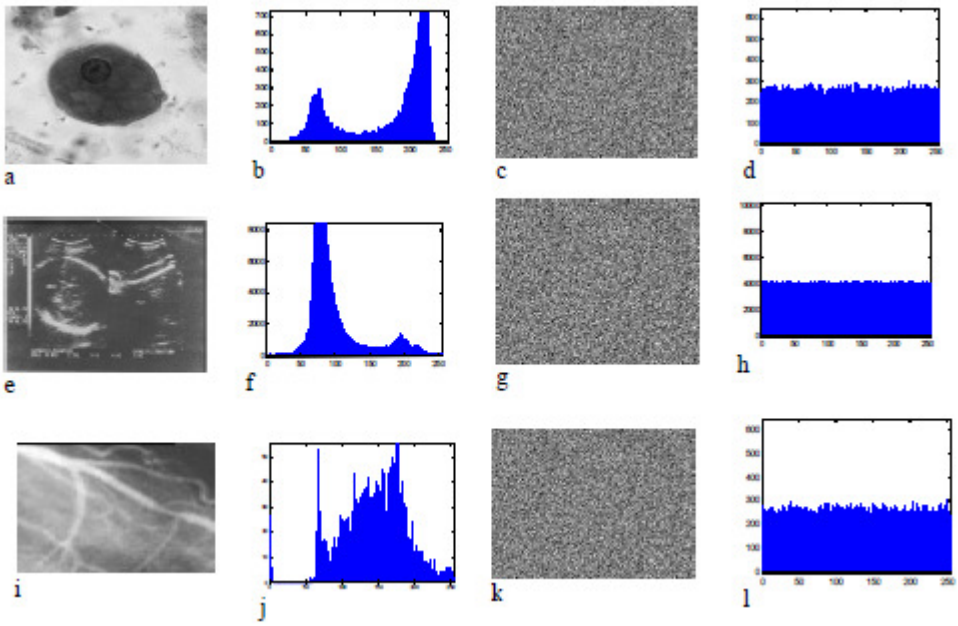

Figure 10: Histogram analysis plain and cipher images using the secret key « **5A9FE86248A78612327A9E2339AB8C12** » : Frame (a) ,(b) , (c) and (d) shows a plain image "Entamoeba Coli trophozoite " and its corresponding histogram, cipher image and cipher image histogram respectively. Frame (e), (f), (g) and (h) shows a plain image "echopelv » and its corresponding histogram, cipher image and cipher image histogram respectively. Frame (i), (j), (k) and (l) shows a plain image "angio » and its corresponding histogram, cipher image and cipher image histogram respectively.

4.2.2.2 Correlation of two adjacent pixels

Table 4 and 5 show the correlation coefficients of the encrypted image which are significantly small.

Image Name	size	vertical Correlation	Horizontal Correlation	diagonal Correlation
ANTAMOEBACOLI	398x407	-9.9620e-004	-0.0021	4.6031e-004
article_oeuf_taeniaC2	200x200	0.0032	5.8918e-004	2.5862e-004
Balantidium Coli cyst	200x200	0.0043	0.0017	0.0011
Balantidium coli_trophozoite	200x200	0.0039	0.0067	0.0103
DICROCOELIUM	400x341	-7.4781e-004	1.7493e-004	6.0780e-005
Entamoeba Coli trophozoite	200x200	-0.0011	-0.0053	0.0014
Entamoeba Histolytica cyst	200x200	-0.0080	-0.0044	0.0010
Entamoeba histolytica -cyst-Gini	130x130	5.7690e-005	-0.0037	-0.0094
Entamoeba hitolytica trophozoite	200x200	0.0071	4.3757e-005	0.0168
Entamoeba hitolytica trophozoite_redim	120x120	-0.0072	-0.0044	-0.0181
Entamoeba hitolytica trophozoite_redim2	172x160	-0.0062	-0.0036	-7.5165e-004
oeuf_ascarisc	266x200	-0.0037	-0.0034	-0.0098
S- Hematobium egg	400x300	-9.0690e-004	-0.0012	0.0030
S- Mansoni egg	400x300	-0.0042	-0.0051	-0.0027
tropho_entamoeba_histolytica2	332x213	0.0011	0.0027	0.0037
tropho_iodamoeba_butschlii	200x200	-0.0024	-0.0034	0.0017
angioF	64x64	0.0019	4.6372e-004	-0.0189
angio	64x64	0.0043	0.0018	-0.0019
node2	64x64	2.6963e-004	0.0062	0.00127
Ossify	64x64	-0.0019	-0.0026	-0.0054
CTpancratitis	64x64	-1.4781e-004	1.7493e-004	2.8270e-004
echo1	64x64	-0.0015	-0.0019	-0.0010
I1_200	64x64	-0.0041	0.0021	-0.0077
k_bw	64x64	-7.7958e-004	0.0060	0.0019

lung16	64x64	0.0032	-1.2543e-004	-0.0045
Pelvist	64x64	0.0032	7.4269e-004	0.0059
ribs	64x64	-0.0029	0.0016	5.8551e-004
DisLocElbow	64x64	0.0030	0.0067	0.0012
echopelv	373x453	0.0029	9.8533e-004	-0.0013

Table 5 : Vertical Correlation, horizontal correlation and diagonal correlation in original and encrypted images from databases.

Description	**Size**	**Type**	**vertical Correlation**	**Horizontal Correlation**	**diagonal Correlation**
Girl	256	color	-3.0267e-004	0.0030	0.0025
Couple	256	color	9.6135e-005	-5.1245e-004	2.9248e-005
Girl	256	color	-0.0021	8.7873e-004	0.0064
Girl	256	color	0.0049	-0.0010	0.0075
House	256	color	0.0068	0.0050	0.0091
Tree	256	color	-0.0018	-1.0421e-004	0.0042
Jelly beans	256	color	4.4661e-004	0.0027	-0.0149
Jelly beans	256	color	0.0043	0.0024	-0.0130
Splash	512	color	-6.6091e-004	2.0623e-004	0.0030
Girl (Tiffany)	512	color	-3.5130e-004	0.0020	-4.0162e-005
Mandrill (a.k.a. Baboon)	512	color	-1.4749e-004	0.0026	0.0026
Girl (Lena, or Lenna)	512	color	-0.0012	-5.0917e-004	9.3274e-004
Airplane (F-16)	512	color	-2.5210e-004	4.2253e-004	0.0020
Sailboat on lake	512	color	4.5260e-004	6.7865e-004	0.0050
Peppers	512	color	-0.0013	-5.9019e-004	0.0013
Moon surface	256	Gray	-0.0027	-0.0015	0.0028
Aerial	256	Gray	-0.0039	-0.0033	-0.0131
Airplane	256	Gray	-3.8301e-004	-2.9019e-004	0.0040
Clock	256	Gray	-0.0016	-0.0044	-1.1211e-005
Resolution chart	256	Gray	-0.006	0.005	0.0040
Chemical plant	256	Gray	-0.0031	-0.0041	0.0032
Couple	512	Gray	0.0015	0.0021	-8.3758e-004
Aerial	512	Gray	-5.8159e-004	0.0015	-0.0017
Stream and bridge	512	Gray	-2.8863e-004	1.4263e-004	1.9218e-004
Truck	512	Gray	8.0192e-005	-0.0017	-0.0033
Airplane	512	Gray	4.7223e-004	-1.0775e-004	0.0044
Tank	512	Gray	0.0015	-9.1835e-004	0.0024
Car and APCs	512	Gray	5.6711e-004	0.0025	0.0040
Truck and APCs	512	Gray	8.4519e-004	0.0017	-0.0016
Truck and APCs	512	Gray	0.0010	0.0015	-0.0018
Tank	512	Gray	0.0014	0.0018	0.0038
APC	512	Gray	-4.8602e-004	-0.0030	0.0065
Tank	512	Gray	9.5672e-004	-5.2212e-005	-0.0048
Car and APCs	512	Gray	-6.6662e-004	7.9005e-004	-4.1089e-004
Fishing Boat	512	Gray	4.3259e-004-	2.4145e-004	-0.0011
Girl (Elaine)	512	Gray	-6.4632e-004	-3.4630e-004	-0.0023
House	512	color	-0.0012	-0.0011	3.9412e-004
21 level step wedge	512	Gray	-4.2585e-004	-2.0421e-004	-5.0421e-004
256 level test pattern	512	Gray	1.8902e-004	-6.4185e-004	-1.7506e-004

In table 1 and 2 we used Co value to confirm general relationship between cipher and original images. Horizontal correlation (HC), vertical correlation (VC) and diagonal correlation (DC) are also evaluated to prove no correlation between cipher and original images. HC, VC and DC are all smaller than one as well for medical images as for the others. The maximum value is 0.018, compare to critical value, this is negligible.

Hence, correlation tests let to conclude that there is no correlation between cipher and original images. The proposed encryption effects are rather well. The results shown above demonstrate that our cipher image has good statistical property through confusion and diffusion stage.

4.2.3 Differential attacks

To test the influence of changing a single pixel in the original image, on the whole image encrypted by the proposed algorithm, NPCR and UACI of many images have been calculated and presented in table 6. For a gray-scale image, the NPCR is close to 99.6093% and the UACI is close to 33.33%.

Table 6: Values of NPCR and UACI of many medical images

Image Name	size	Corr(A,B)	NCPR	UACI
ANTAMOEBACOLI	398x407	-0.0031	99.6147	33.5323
article_oeuf_taeniaC2	200x200	-0.0021	99.5621	33.5172
Balantidium Coli cyst	200x200	-0.0068	99.6048	33.5938
Balantidium coli_trophozoite	200x200	-0.0013	99.6155	33.4818
DICROCOELIUM	400x341	0.0028	99.5972	33.4172
Entamoeba Coli trophozoite	200x200	0.0089	99.5819	33.2297
Entamoeba Histolytica cyst	200x200	-0.0058	99.6124	33.5771
Entamoeba histolytica -cyst-Gini	130x130	-0.0054	99.5987	33.5897
Entamoeba hitolytica trophozoite	200x200	0.0052	99.6017	33.2815
Entamoeba hitolytica trophozoite_redim	120x120	-0.0012	99.6094	33.5018
Entamoeba hitolytica trophozoite_redim2	172x160	-0.0018	99.6231	33.5405
oeuf_ascarisc	266x200	-0.0015	99.6132	33.5091
S- Hematobium egg	400x300	0.0042	99.5876	33.3906
S- Mansoni egg	400x300	0.0042	99.6056	33.3705
tropho_entamoeba_histolytica2	332x213	2.2082e-004	99.6078	33.4721
tropho_iodamoeba_butschlii	200x200	-0.0043	99.6170	33.5577
angioF	64x64	0.0032	99.6384	33.4193
angio	64x64	0.0075	99.5911	33.2566
node2	64x64	0.0031	99.5804	33.3958
Ossify	64x64	-0.0013	99.6307	33.4322
CTpancratitis	64x64	-2.7335e-004	99.6185	33.4818
echo1	64x64	0.0040	99.5667	33.3026
I1_200	64x64	-0.0025	99.6063	33.5109
k_bw.thumb	64x64	0.0033	99.6429	33.4121
lung16thumb	64x64	8.6350e-004	99.6094	33.4520
Pelvisthumb	64x64	0.0014	99.5804	33.4501
ribsthumb	64x64	0.0017	99.6048	33.4636
DisLocElbowthumb	64x64	0.0021	99.6063	33.4122
echopelv	373x453	0.0013	99.5941	33.4013

We found NPCR close to 99.6 % in all the cases tested. This proves that encryption scheme is very sensitive with respect to a small percentage of pixels changes in the plain image. The UACI, in all the cases, is found close to 33% indicating that the rate of influence due to one-pixel change in plain image is very high. The result of these two tests shows that the proposed cipher is sensitive to a minor change in plain image. In order to compare our algorithm to the existing schemes, we tested it on images usually used in the literature. The comparative results are presented in table 7.

Table 7: comparison of results

Evaluation metrics	Images / References	Lena	Mandrill	Airplane
Vertical correlation	Ref [18]	0.0034	-0.0019	-0.0036
	Ref [31]	-0.0016		
	Ref [15]	-0.0194		
	ours	**-0.0012**	**-0.00014**	**-0.00038**
Horizontal correlation	Ref [18]	0.0026	-0.0014	-0.0017
	Ref [31]	0.0031		
	Ref [15]	0.0241		
	ours	**-0.00050**	**0.0026**	**-0.00029**

Diagonal correlation	Ref [18]	-0.0019	-0.0013	-0.0020
	Ref [31]	0.0067		
	Ref [15]	0.0243		
	ours	**0.00090**	**0.0026**	**-0.0040**
Entropy	Ref [18]	7.9992	7.9991	7.9990
	Ref [31]	7.9952		
	Ref [15]	7.9974		
	ours	**7.9993**	**7.9993**	**7.9993**
NCPR	Ref [18]	99.6201	99.6109	99.6178
	Ref [31]	>96		
	Ref [15]	93.6768		
	ours	**99.6109**	**99.6475**	**99.6034**
UACI	Ref [18]	33.4006	33.4757	33.5370
	Ref [31]	31.79		
	Ref [15]	33.3364		
	ours	**33.4953**	**33.4980**	**33.3312**

In [20], Linear Diophantine Equation (LDE), whose coefficients are integers and dynamically generated from chaotic system, is used to encrypt images. The procedure to generate sequences used in permutation –diffusion process is too complex. We used a simple logistic map and FWT to obtain better results than [20] as we can see in table 7. In [33], chaos is not used in the encryption process. Comparison shows our encryption scheme provides better results. In [17], a bit-level image encryption based on spatiotemporal chaotic system is used. Our chaotic FWT image encryption has better results. The same observation is done in [26] where the generalized Arnold and Bernoulli shift map are employed. According to table 7, the results obtained from our chaotic FWT encryption scheme are the best.

5. CONCLUSIONS

In this work, a new scheme of image encryption based on chaos and FWT has been proposed to secure biomedical images. This utilizes two chaotic logistic maps, an external secret key of 128 bits long and a two-dimensional FWT. The parameter and the initial conditions for two logistic maps are derived using an external secret key. It has been shown that it is possible to apply chaotic methods encryptions to the two-dimensional Fast Walsh Transform of images. We have carried out statistical analysis, key sensitivity analysis to demonstrate the security and the effectiveness of the new image encryption system. The main features of the proposed encryption scheme are its simplicity, its efficiency, the high speed and high order of security. Our method also has better confusion, diffusion and security. The method is robust against brute-force attacks because of the changing of the initial conditions of the chaotic logistic maps during the process of rows and columns of the chaotic FWT. Our algorithm is easy to implement and could be use in real time transmission of secured biomedical images in telemedicine.

REFERENCES

[1] B.M Hennelly and J.T Sheridan,"Image encryption and the fractional Fourier transform", Optik-International Journal for light and Electron optics, vol.114, 2003, pp.251-265.

[2] H. C. Andrews and W. K. Pratt, "Fourier transform coding of images", Presented at the 1968 Hawaii International Conf. on System Sciences, Jan. 671-619, 1968.

[3] H. C. Andrews and W. K. Pratt, "Television bandwidth reduction by Fourier image coding", presented at the Soc. of Motion Picture and Television Engrs., 103 Tech. Conf., May 1968.

[4] E. 0. Brigham and R. E. Morrow, "The fast Fourier transform " , IEEE Spectrum, vol. 4, Dec. 1967, pp. 63-70.

[5] J. L. Walsh, "A closed set of orthogonal functions," Am. J. Math., vol. 45, 1923 pp. 5-24,

[6] N. J. Fine, "On the Walsh functions", Trans. Am. Math. Soc., vol. 65, 1949, pp. 372-414.

[7] N. J. Fine, "The generalized Walsh functions", Trans. Am. Math. Soc., vol. 69, 1950, pp. 66-77.

[8] G. W. Morgenthaler, "On Walsh-Fourier series", Trans. Am. Math. Soc., vol. 84, 1957, pp. 472-507.

[9] K. W. Henderson, "Some notes on the Walsh functions", IEEE Trans. Electronic Computers (Correspondence), vol. EC-13, Feb. 1964, pp.50-52.

[10] PRATT et al, "Hadamard Transform Image Coding", Proceedings of the IEEE, VOL. 57, No.1, Jan. 1969, pp. 58-67.

[11] M. S.Murty, D. Veeraiah and A. S. Rao "Digital signature and watermark methods for image authentication using cryptography analysis", Signal & Image processing: an International Journal, vol. 2, No 2, June 2011, pp. 170-179.

[12] I. S. I. Abuhaiba and M. A. S. Hassan, "Image encryption using differential evolution approach in frequency domain", Signal & Image processing: An International Journal, Vol. 2, No 1, March 2011, pp. 51-69.
[13] B.K.Shreyamshakumar and C. R. Patil, " JPEG image encryption using fuzzy PN sequences ", Signal, Image and Video Processing, Vol.4, Issue4, 2010, pp. 419-427.
[14] A. Kumar and M.K.Ghose, "Extended substitution-diffusion based image cipher using chaotic standard map", Commun. Nonlinear Sci.Num. Simul., Vol.16, 2011, pp. 372 - 382.
[15] V. Patidar, N.K. Pareek, G. Purohit and K.K Sud, "A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption", Optic Commun., Vol. 284, 2011, pp.4331-4339.
[16] R. Ye, "A novel chaos-based image encryption scheme with an efficient permutation-diffusion mechanism", Optic Commun., Vol. 284, 2011, pp. 5290-5298.
[17] L. Teng and X. Wang, "A bit-level image encryption algorithm based on spatiotemporal chaotic system and self-adaptive", Optics Commun., Vol. 285, 2012,pp. 4048-4054.
[18] M. Khan and T. Shah, "An efficient construction of substitution box with fractional chaotic system", Signal, Image and Video Processing, 2013.
[19] W. Zhang, K.Wong, H. Yu and Z. Zhu, "An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion", Commun. Nonlinear Sci. Num. Simul., Vol. 18, 2013, pp. 2066-2080.
[20] J.S. Eyebe Fouda, J.Yves Effa, L. Samrat, and A. Maaruf, "A fast chaotic block cipher for image encryption", Commun. Nonlinear Sci.Num. Simul., vol. 19, 2013, pp. 578-588.
[21] E.Chrysochos, V.Fotopoulos,M.Xenos and A.N.Skodras, " Hybrid watermarking based on chaos and histogram modification ", Signal, Image and Video Processing, Vol.8,Issue5, 2014, pp. 843-857.
[22] O. S. Faragallah, "Efficient confusion – diffusion chaotic image cryptosystem using enhanced standard map", Signal, Image and Video Processing, 2014; doi: 101007/s11760-014-0683-y
[23] J-X. Chen, Z-l. Zhu, C. Fu, H. Yu and L-B. Zhang, "A fast chaos-based image encryption scheme with a dynamic state variable selection mechanism", Commun. Nonlinear Sci.Num. Simul., Vol. 20, 2015, pp. 846-860.
[24] Q. Liu, P-Y. Li, M-C. Zhang, Y-X. Sui and H-J. Yang, "A novel image encryption algorithm based on chaos maps with Markov properties", Commun. Nonlinear Sci.Num. Simul., Vol. 20, 2015,pp. 506-515.
[25] N. Singh, and A. Sinha, "Optical image encryption using fractional Fourier transform and chaos", Optics and Lasers in Engineering 46, 2008, pp .117-123.
[26] H. M.Elhoseny, H. E.H.ahmed, A. M.Abbas et al, " chaotic encryption of images in the fractional Fourier Transform domain using different modes of operation ", Signal, Image and Video Processing, vol. 9, 2015, pp. 611-622
[27] L. Sui, B. Gao, "Single- channel color image encryption based on iterative fractional Fourier transform and chaos", Optics & Laser Technology 48, 2013, pp. 117-127.
[28] Z. Ya-hong, L. Xin-wei, and C. Hui., "Binary Image Encryption Algorithm Based on Chaos and Walsh Transform" [J], 2011, Issue 3, pp.60-62, Doi:10.3969/j.issn;1006-2475.2011.03.016.
[29] J. L. SHANKS, "Computation of the Fast Walsh-Fourier Transform", IEEE Transaction on Computers, Short Notes, may 1969, pp. 457-459.
[30] X. Wang, J.Zhao and H. Liu, "A new image encryption algorithm based on chaos", Optic Communication, 2012, Vol. 285, pp.562-566.
[31] Medical image database, available on : http:// imagemedical Data-Base-htm.
[32] Natural image database, available on : http://sipi.usc.edu/database/.
[33] K.Narendra, V.Patidar, and K.S. Krishan, "Diffusion-substitution based gray image encryption scheme", Digital Signal Processing, Vol.23 n.3, pp. 894-901, May, 2013.

AUTHORS

Kengnou Telem Adelaide Nicole was born 1977 in Dschang - Cameroon. In 2003, she was graduated at the Advanced Teacher's Training College for Technical Education (ENSET) – University of Douala, with DIPET 1 (Bachelor in Electrical and Electronics Engineering). In 2005, she obtained the DIPET 2 at the same institution. She obtained the Master degree in Electronics in 2012 at the faculty of Science of the University of Dschang. She is currently a Technical High School teacher in electronics engineering. In parallel to her job, Mrs. KENGNOU is doing studies and research for a PhD thesis. Her research interests are telemedicine, secure transmission of physiological signals and images, wireless communication and image processing. Mrs. KENGNOU Adelaide is member of both the Laboratory of Electronics and Signal Processing (LETS) of the faculty of science of the University of Dschang and the Laboratory of Automatic and Applied Informatics (LAIA) of FOTSO Victor University Institute of Technology – University of Dschang.

Tchiotsop Daniel was born in 1965 in Tombel - Cameroon. He graduated in Electromechanical engineering from the Ecole Nationale Supérieure Polytechnique (ENSP) of Yaoundé-Cameroon in 1990, he obtained a MS degree in Solid Physics in 1992 from the Faculty of Science of the University of Yaoundé I, a MS degree in Electrical Engineering and Telecommunication in 2003 from ENSP-Yaoundé and a PhD at INPL (Institut National Polytechnique de Lorraine), Nancy–France, in 2007. Dr TCHIOTSOP teaches in the Department of Electrical Engineering of the FOTSO Victor University Institute of Technology – University of Dschang since 1999 where he is actually the Head of

Department. He is with the Laboratoire d'Automatique et d'Informatique Appliquée (LAIA) where his main items of research include Biomedical Engineering, Biomedical signal and image processing, Telemedicine and intelligent systems.Dr TCHIOTSOP is partner with the Centre de Recherche en Automatique de Nancy (CRAN) – Université de Lorraine, France, Laboratoire d'Electronique et du Traitement de Signal (LETS) – ENSP, University of Yaoundé 1, and Laboratoire d'Electronique et du Traitement du Signal 'LETS) – Faculty of Science, University of Dschang.

Thomas F. N. was born in Douala - Cameroon in 1964. He received a Diploma in Electromechanical Engineering from Ecole Nationale Supérieure Polytechnique (ENSP) - Yaoundé - Cameroon in 1990, his Master Degree in Electronics and Signal Processing in 2000, and his Ph.D. Degree in Engineering Sciences, on Electrical and Telecommunications Engineering from the University of Yaoundé I - Cameroon in 2006, carried out simultaneously in Ecole Nationale Supérieure des Télécommunications (ENST) of Bretagne, Brest, France. Since 1997, he is a Lecturer in the Cameroon State Universities in Electronics, Automation, Signal and Image Processing. He has been with the Ecole Nationale Supérieure d'Enseignement Technique, University of Douala from 1997 to 2009; with the Ecole Normale Supérieure Annexe Bambili (ENSAB), University of Yaoundé I from 2009 to 2011; with the Higher Technical Teacher Training College (HTTTC), University of Bamenda since 2011 where he acts both as Head of Department and Assistant Director. His research interests are in remote sensing, signal and image processing for applied sciences. Actually, his research is dedicated to oil slick detection, atmospheric pollution, malaria detection, biometry, roughness detection.

H.B. Fotsin was born in 1967. He obtained the degree of "Doctorat de Troisième Cycle" in 2000 and the degree of "Doctorat d'Etat" in 2005, both from the University of Yaoundé I, Cameroon. He is currently Associate Professor of Physics and Head of the Electronics and Signal Processing Laboratory at the Faculty of Science, University of Dschang, Cameroon. Dr Fotsin is author and co-author of more than 40 scientific articles mostly in the field of nonlinear dynamics and chaos control and synchronization in electronic circuits.

Didier wolf is a professor at the University of Lorraine and runs the Research Center for Automatic Control of Nancy (UMR CNRS 7039). His research focuses on signal and image processing applied to health (cancer and neurology).