Volume 57, Number 2, 2016

ACTA TECHNICA NAPOCENSIS
Electronics and Telecommunications

COMPARATIVE ANALYSIS OF DIFFERENT STRUCTURES OF CHAOS-BASED CRYPTOSYSTEMS: A SURVEY

Joseph Yves EFFA[1)], Jean De Dieu NKAPKOP[1)], Mihaela CISLARIU[2)], Monica BORDA[2)]
[1)]The University of Ngaoundéré, Faculty of Science, P.O. Box 454 Ngaoundéré, Cameroon
[2]Technical University of Cluj-Napoca, 26-28 Baritiu Street, 400027, Cluj-Napoca, Romania
Email:Monica.Borda@com.utcluj.ro

Abstract: In recent years the interest for image encryption based on chaotic maps has become a major concern. In this paper, we evaluate each step of the process used in image encryption based on chaotic maps. In an attempt to give an answer to each of the issues raised, we perform experiments and we analyze performances of a few chaos-based cryptosystems by using common analytical criterions like entropy analysis, correlation coefficients, key space, key sensitivity, number of rounds, etc. By evaluating the results, the study shows that majority of schemes that rely on converting chaotic values in real numbers are time consuming. For real-time applications, it is important to improve image encryption schemes by reducing the cyclic digitization of chaotic numbers in the generation of permutation and diffusion keys.

Keywords: *Image encryption, permutation only, diffusion, permutation-diffusion, combining permutation and diffusion*

I. INTRODUCTION

The image encryption is a technique that provides security for images by converting the original image into an image which is difficult to understand [1]. The image encryption techniques can be divided into two groups based on the approach used to construct the encryption scheme: chaos-based methods and conventional methods. However, conventional methods such as DES, AES, IDEA and RSA are not suitable for image encryption due to some intrinsic properties of the images such as bulky data capacity and high redundancy, which are generally difficult to handle by using these traditional techniques [2]. These methods therefore cannot be good candidates, especially for rapid communication applications.

Unlike the conventional cryptographic algorithms which are mainly based on discrete mathematics, chaos-based cryptography relies on the complex dynamics of nonlinear systems or maps which are deterministic but simple. The distinct properties of chaos, such as ergodicity, quasi-randomness, sensitivity dependence on initial conditions and system parameters, make chaos a good alternative for image encryption. Indeed, there are similarities between chaos and cryptography. These similarities are listed in Ref. [3].

The basic principle of image encryption using chaos is therefore based on the ability of some dynamic systems to produce sequence of numbers that are random in nature. There are many architectures using chaos-based image encryption [1,2,4]. Depending on the type of key used in the encryption algorithms, chaos-based cryptosystems are either symmetric or asymmetric. Symmetric encryption, in which the decryption key is identical to the encryption key, is the oldest method in cryptology and is still used today. By contrast, asymmetric cryptosystems use different keys for decryption and encryption [5]. We focus here on image cryptosystem based on the permutation and diffusion operations (symmetric encryption). This architecture includes two important operations, permutation operation and diffusion operation. The first one permutes the plain-image, instead of changing the value of pixel. The last one changes the value of pixel, instead of altering the position of pixel. This architecture became the general architecture for chaos-based image encryption the most used in literature [5].

Although many studies have been done in the field of chaos-based image encryption, in this paper, an attempt is made to analyze different structures of chaos-based cryptosystems in order for the researchers to choose the best operation to encrypt an image. The comparisons are made using the current fastest encryption schemes.

II. STRUCTURES OF CHAOS-BASED CRYPTOSYSTEMS

There are many structures of chaos-based cryptosystems encountered in the literature. In this paper, we are discussing architectures which could generalize all these cryptosystems. According to their architecture, the chaos-based cryptosystems can be therefore classified into four categories. These categories are: confusion-only, diffusion-only, image cryptosystem based on the permutation and diffusion operations, and image cryptosystem combining the permutation-diffusion architecture.

The major core of these systems consists of one or several chaotic maps serving the purpose of either just encrypting the image or shuffling the image and subsequently encrypting the resulting shuffled image.

There are a large number of chaotic maps used in these architectures, for example Logistic map, Tent map, Standard chaotic map, Cat chaotic map, generalized Baker chaotic map, Chen's chaotic system, Lorenz chaotic system and so on [6]. These chaotic maps represent the key stream

Manuscript received May 25, 2016; revised May 31, 2016

generators for all the existing chaos-based cryptosystems.

II.1. Confusion step

For an ordinary image, each pixel is usually highly correlated with its neighboring adjacent pixels either in horizontal, vertical or diagonal directions. The confusion stage is therefore used to reduce the correlation between pixels. This stage is the pixel permutation where the positions of the pixels are scrambled over the entire image without disturbing the values of the pixels. With this stage the image becomes unrecognizable. The pixel positions are swapped in the ordinary image or in blocks of images, by means of a secret key called permutation key. The control parameter and the initial conditions of chaotic system which represent the encryption key must be well chosen to get a pseudo-random sequence.

In this stage, the correlation coefficients of the shuffled image are too low compared with those of the ordinary image. Thus, it satisfies zero co-correlation property. The shuffled image also has a high sensitivity to slightest changes to the permutation key. However, it is not very secure to have only the permutation stage since it may be broken by any attack. Indeed, the histograms in the confusion step are not uniformly distributed and are the same from those of the original images.

Many strategies to do the permutation process have been used in the literature. The comparison of a few of them will be made hereafter.

II.2. Diffusion step

The diffusion stage is used to confuse the relationship between cipher image and ordinary image. Instead of permuting the entire image, the pixel values are sequentially modified and the modification made to a pixel usually depends on the accumulated effect of all the previous pixel values, so that a slight change in one pixel could be spread out to almost all the subsequent pixels. Chaotic map is used as generation of key stream for substitution and the substitution is often one of simple operations such as XOR, XNOR, shift, add, and subtract or a combination of these simple operations.

Compared to permutation, diffusion significantly enhances the security of the cryptosystem. The Histograms in the diffusion step consist of spikes that are almost uniformly distributed and significantly different from those of the original images. Therefore these histograms bear no statistically resemblance to those of the original images and they do not provide any clue to employ any statistical attack. However, in general, diffusion is time consuming. For conventional chaos cipher images, overall 3 to 4 rounds are needed usually to achieve a satisfactory diffusion performance.

II.3. Confusion-diffusion architecture

The crucial measure for the quality of a cryptosystem is its capability to withstand the attempts of an unauthorized participant, or an opponent, to gain knowledge about the unencrypted information. A good cryptosystem should resist all kinds of known attacks. For this purpose, Fridrich [7] has suggested that a chaos-based image encryption scheme should compose the iterations of two processes: permutation and diffusion.

The typical block diagram of the permutation-diffusion architecture is depicted in Figure 1. This architecture forms the basic structure of a number of chaos-based cryptosystems recently proposed in the literature [5, 6]. It includes two important operations: permutation operation and diffusion operation which are two separate and iterative stages. In general, separate keys are used for permutation and diffusion stage of the encryption process for enhancing the security of the algorithm. However, for a number of chaos-based cryptosystems, to achieve a satisfactory level of security by using this architecture the confusion-diffusion operation is repeated a number of times.

For image encryption, it is more suitable to use confusion-diffusion operation in this order since the reverse order (diffusion-confusion) showed that it is the worst method for key sensitivity [6].

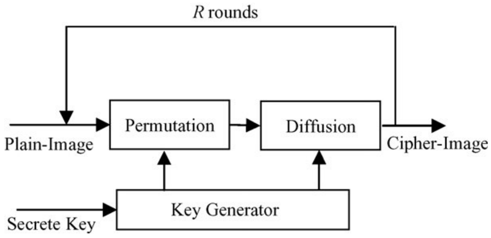

Figure 1. Image cryptosystem based on the permutation and diffusion operations.

II.4. Combining the confusion-diffusion architecture

Another approach is to consider that separate confusion and diffusion leads to an effort which is actually duplicated. This effort may be avoided if the permutation and diffusion operations can be combined via changing the values of the pixels while relocating them. The general architecture of this kind of strategy is depicted in Figure 2. For this kind of strategy, the image only is scanned once so that the encryption speed and efficiency can be significantly improved.

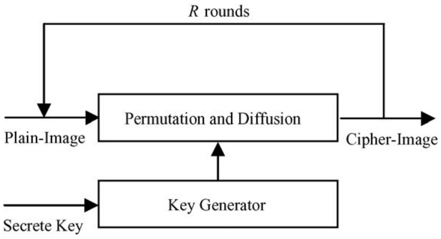

Figure 2. Image cryptosystem combining the permutation–diffusion architecture.

To use this architecture, the key stream must be generated by the complex chaos-based pseudo-random key stream generators. At the same time, the use of complex chaotic systems can make the rise of runtime of chaos-based image encryption. Indeed, to design fast image encryption architecture, some authors do not recommend the use of complex chaotic maps [6].

III. EXPERIMENTS AND PERFORMANCE ANALYSIS OF CRYPTOSYSTEMS

All the architectures of chaos-based cryptosystems represented above raised some open questions. In an attempt to give an answer to each of the issues raised, we perform here experiments and we analyze performances of a few chaos-based cryptosystems by using common analytical criterions.

III.1. Chaotic maps

Chaotic maps often occur in the study of dynamical systems. For a discrete time index set, $T = \{0, 1, 2,...\}$, consider a time series $\{n, n\in T\}$. Assume that x_0 is an initial condition. Discrete maps usually take the form of iterated functions as follows:

$$x_{n+1} = F\left(x_n\right) \tag{1}$$

where F is a nonlinear function.

Chaotic map is an effective technique for image encryption. The initial condition and parameters of the map can be taken as secret keys. The traditional approach to extracting pseudorandom numbers from the output of a chaotic system involves iterating Eq. (1) and then extracting a value from its current state variable. These two operations are performed repeatedly until sufficient pseudorandom numbers are obtained. We then obtain the chaotic sequences X=[x_1, x_2, x_3...] usable for the generation of a pseudorandom keystream.

III.2. The permutation analysis of a few cryptosystems

In their paper [8], Chong Fu et al. proposed to use Chirikov standard map to shuffle the pixel positions of the plain image. However, the state value of a chaotic map is a floating-point number. For a use in cryptography, an integer is usually required. This means that the conversion from floating-points to integers cannot be avoided in practical applications. Unfortunately, such a conversion is time consuming. In order to incorporate Chirikov standard map into image encryption that operated on a finite set, they must then discretize. Its application to a grayscale test image with 512×512 size is shown in Figure 3.

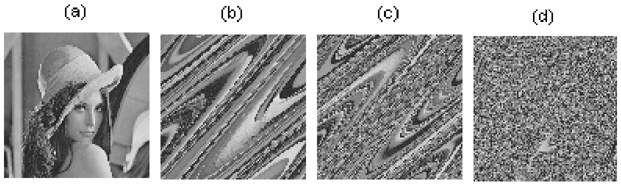

Figure 3. (a) The plain image with 512×512 size. (b) The test image after applying the Chirikov standard map once. (c) The test image after applying the Chirikov standard map three times. (d) The test image after applying the Chirikov standard map five times.

As a result, to get the image completely unrecognizable this permutation needs five rounds of iterations. The methods which are based on this approach suffer from a problem. Due to the finite computing precision, orbits of temporal discrete chaotic systems can eventually become periodic and thus produce a low level of security.

In the paper by Fouda et al. [9], the technique used for the permutation of pixels is based on the ascending or descending sorting of a chaotic sequence. By the chaotic scheme of the values in a generated sequence, they obtain a pseudorandom distribution of the positions (indices) of these values as shown in Figure 4. The permutation key is then defined as a distribution of indices derived from the sorting.

As a result, this method allows to easily achieve high performance of pseudorandom permutation through any type of chaotic systems using the true precision of the computer.

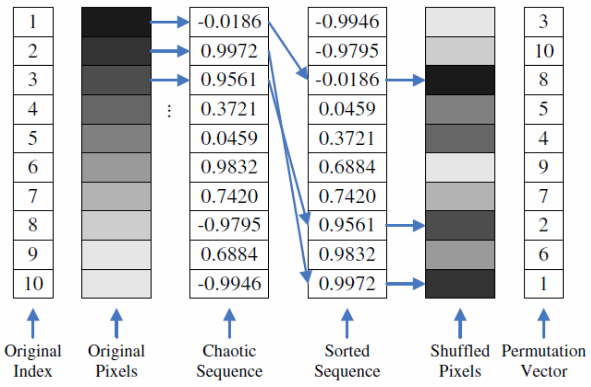

Figure 4. Permutation based on chaotic sequence sorting.

In their paper, Fouda et al. [10] proposed a novel permutation strategy which significantly accelerated the permutation step of their previous work [9]. In this previous work, the initialization phase was not dynamic to increase the complexity of the algorithm. Indeed, the generation of large permutation from the chaotic system was extremely time-consuming, due to the large amount of integrations/iterations. As a consequence, it was necessary to make more than one round for the previous cipher to be of a higher level of security. To overcome this, they proposed a new technique for the fast generation of large permutation keys, by combining chaotic system with Linear Diophantine Equation (LDE). In this scheme, chaotic numbers are generated using a chaotic system. Then these numbers are used to generate the coefficients of the LDE. The solutions of LDE are used to generate the permutation key for encryption. The high security and low computational complexity are achieved not only by using large permutation based on the sorting of the solutions of LDE but also by generating only one permutation from the sorting of the solutions of the LDE, then by dynamically updating d number of integers ($d > 2$) in the permutation.

In another paper of Chong Fu et al. [11], the chaos-based bit-level permutation scheme is proposed for digital image encryption to overcome the drawbacks of conventional permutation-only type image cipher. The scheme introduced a significant diffusion effect in the permutation procedure through a two-stage bit-level shuffling algorithm. The two-stage permutation operations are realized by chaotic sequence sorting algorithm and Arnold Cat map, respectively. In this scheme, a grayscale image is decomposed into 8 bit-planes and each bit-plane is shuffled separately by using Arnold Cat map, thus a certain diffusion effect is introduced in permutation stage. As a result, the histogram of the cipher-image is fairly uniform and comparable with that of permutation–diffusion scheme owing to the significant diffusion effect introduced in the shuffling process as shown in Figure 5.

All the permutation strategies discussed here are representative for all the others. They use different security analysis to validate the good performance and the

Table1. Comparison of different permutation steps

Reference		**Permutation with a discretized map [8]**	**Permutation with the chaotic sequence sorting [9]**	**Permutation with the chaotic sequence sorting+LDE [10]**	**Permutation with diffusion effect [11]**
Entropy		7.4456	7.4456	7.4456	7.9880
NPCR		99.3931	99.3954	99.3435	-
UACI		21.6319	21.5115	21.4312	-
Correlation coefficients of permuted image	Horizontal	0.0491	-0.000017	-0.0028	0.0368
	vertical	0.0511	-0.0029	-0.000787	-0.0392
	diagonal	0.0310	0.00068	-0.0020	0.0068
Round number of permutation		5	1	1	2
Key space		9.2×10^{18}	2.27×10^{57}	2.27×10^{57}	2^{153}
Key sensitivity		96.99 percent difference	99.3839 percent difference	99.42 percent difference	99.61 percent difference

robustness. All the security analysis details are concluded in the form of table as shown in Table 1. The plain-image of Lena of size 512×512 is used in all the experiments. From this table, an analysis can be made of each permutation method used for image encryption using chaos theory.

For the above values, we can find that all the permutation schemes are key sensitive; except reference [8] which has low key space, the key space of the others references is very large to resist brute force attack; the correlation coefficients are low so all the pixels are decorrelated. However, as conventional permutation operation shuffles only the pixel positions without changing its value, entropy of the three others permutation types are near to that of the original image and the histogram of the shuffled image is the same as that of the plain-image. The permutation with diffusion effect method shows a competitive performance as permutation encryption scheme compared to the others. However, in order to incorporate generalized chaotic Cat map into image encryption that operated on a finite set, it has to be discretized. And we told that this operation is time consuming. Indeed due to the discretization of chaotic maps, at least two rounds of the permutation process are used to obtain satisfactory performance. By using permutation with a discretized map, due to the finite computing precision, orbits of temporal discrete chaotic systems will eventually become periodic and the encryption scheme could be weak to resist all kind of attacks. The use of chaotic sequence sorting allows taking advantage of the true accuracy of the computer for the fast generation of chaotic sequences. The method also presented the advantage that it could be combined with any type of chaotic system.

III.2. The performance analysis of the whole chaos-based encryption algorithm

We have previously shown that the permutation-only type image cipher is superior in the aspect of efficiency due to its lowest computational complexity. It only shuffles the position of each pixel in a secret order while it does not alter its value. Here, we are focusing only on the whole chaos-based encryption algorithm as it already includes the diffusion aspect. Indeed, in all the chaos-based encryption algorithms, the image cipher introduces a substitution module which alters the pixel values sequentially in order to significantly enhance the security of the cryptosystem.

To perform our study we consider the two most important structures of chaos-based encryption schemes namely the separated permutation and diffusion stages and the combined permutation and diffusion stages.

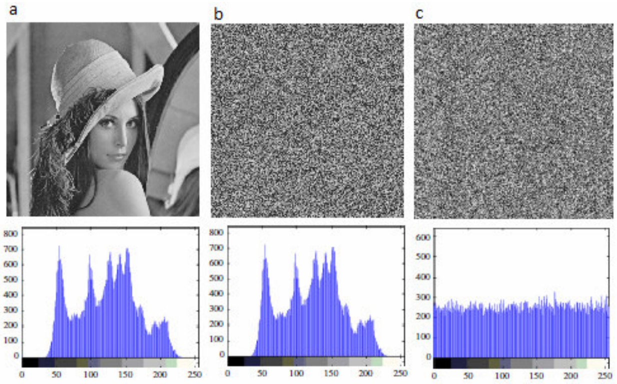

Figure 5. The histogram of the permuted image. (a) Plain-image. (b) Permutation with the chaotic sequence sorting+LDE. (c) Permutation with diffusion effect.

In the encryption schemes which use the permutation-diffusion technique, many methods have been often used to obtain a good cipher image. To cite a few, we have:

- The cipher image can be obtained by XORing the shuffled image binary sequence with the key stream;
- The cipher image is obtained by XORing each pixels of confused image with the diffused image;
- The cipher image is obtained by XORing each pixels of confused image with the diffusion key;
- by XORing the permuted pixel array and the chaotic sequence an intermediate cipher is generated. This intermediate cipher image is shuffled to get the final cipher array. The resultant cipher array is transformed to get the final cipher.
- The cipher image is obtained by XORing each pixels of confused image with the diffusion key and the previously masked pixel. This diffusion process is subsequently more secure by XORing the cipher image with the key stream;

Another technique is to combine the permutation and diffusion stages, instead to separate them as previously. Some of them are presented below:

- Some algorithms decompose input images into bit-planes, randomly swaps bit-blocks among different bit-planes, and conducts XOR operation between the scrambled images and secret matrix;
- The image is partitioned into blocks of pixels. Then, a chaotic pseudorandom sequence is employed to shuffle the blocks and, at the same time, to change the pixel values. The technique used for the generation of pseudorandom numbers from spatiotemporal chaos avoids time-consuming operations such as multiplication and conversion from floating points to integers.

Table2. Comparison of different chaos-based encryption algorithm

		The permutation-diffusion			**Combining the permutation-diffusion**		
Reference		[8]	[9]	[10]	[2]	[4]	[11]
Entropy		7.9902	7,9993	7.9992	7.9994	7.9992	7.9880
NPCR		99.61	99,603	99.6201	99.639	-	-
UACI		33.48	33,456	33.4006	33.554	-	-
Correlation coefficients of permuted image	Horizontal	0.0088	-0,0010	0.0026	0.000707	-0.0155	0.0368
	vertical	-0.0087	-0,0016	0.0034	0.002165	0.0199	-0.0392
	diagonal	-0.0060	0,0010	-0.0019	0.014886	0.0244	0.0068
Number of rounds		1	10	1	2	-	2
Key space		2^{167}	2.27×10^{57}	2.27×10^{57}	-	2^{451}	2^{153}
Key sensitivity		99.62 percent difference	99,628 percent difference	99.61 percent difference	99.622 percent difference	high	99.61 percent difference

In all the presented schemes, the decryption process is the reverse operation of encryption.

The chaos-based encryption schemes discussed here are representative off all the others. They use different security analysis to validate the good performance and the robustness. All the security analysis details are concluded in the form of table as shown in Table 2. The comparisons are made using the current fastest encryption schemes and the plain-image of Lena of size 512×512 is used in all the experiments.

From the Table 2, we can find that all the studied encryption schemes have exhibit a high rate of security. Indeed, all the schemes have entropy close to 8; an expected value of NPCR which is around 99.609%; an expected value of UACI which is around 33.464%; the correlation coefficients close to zero; a large key space to resist brute force attack and a high key sensitivity to resist differential attack. When the security requirement is fulfilled, the running speed becomes an important factor for practical applications. In references [2, 9, 11] at least two rounds of the substitution diffusion process are used to obtain satisfactory performance. Chong Fu et al. proposed a single round architecture for image encryption by introducing a bidirectional diffusion scheme which accelerates the spreading process is used [8]. Although this reduces the number of rounds, the single round itself takes longer. Indeed their scheme leads to a longer processing time in a single round because the permutation is time consuming. According to the number of rounds to obtain high level of security while preserving the speed, the scheme proposed in [10] could guarantee real-time encryption.

This study also point out that most of the existing chaos-based encryption algorithm demands a huge amount of computational time due to repeating process of shuffling and quantization of real values sequence of chaotic numbers into binary representation. Although we cannot currently avoid the discretization of chaotic values in the diffusion phase, the study shows that we should continue to improve the image encryption without cyclic digitization of chaotic numbers in the generation of permutation and diffusion keys.

For the experiments, the following formulas which assess the quality of the good cipher have been used.

Correlation of adjacent pixels

There is a very good correlation among adjacent pixels in the digital image. Eq. (2) is used to study the correlation between two adjacent pixels in horizontal, vertical and diagonal orientations.

$$r_{xy} = \frac{\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})(y_i - \bar{y})}{\sqrt{\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{x})^2\right)\left(\frac{1}{N}\sum_{i=1}^{N}(x_i - \bar{y})^2\right)}} \qquad (2)$$

$$\bar{x} = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (3)$$

$$\bar{y} = \frac{1}{N}\sum_{i=1}^{N} y_i \qquad (4)$$

where x_i and y_i are greyscale values of *i-th* pair of adjacent pixels, and N denotes the total numbers of samples.

Information entropy analysis

In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. It is well known that the entropy $H(m)$ of a message source m can be measured by:

$$H = -\sum_{i=1}^{2^M} p(m_i)\log_2\left(p(m_i)\right) \tag{5}$$

where M is the number of bits to represent a symbol; $p(m_i)$ represents the probability of occurrence of symbol m_i and *log* denotes the base 2 logarithm so that the entropy is expressed in bits. For a purely random source emitting 2^8 symbols, the entropy is $H(m)$ = 8 bits.

Differential attack analysis

The diffusion performance is commonly measured by means of two criteria, namely, the number of pixel change rate (NPCR) and the unified average changing intensity (UACI). NPCR is used to measure the percentage of different pixel numbers between two images. The NPCR between two ciphered images *A* and *B* of size m×n is:

$$NPCR_{AB} = \frac{\sum_{i=1}^{m}\sum_{j}^{n} D(i,j)}{m\times n}\times 100 \tag{6}$$

where

$$D(i,j) = \begin{cases} 1 & A(i,j) \neq B(i,j) \\ 0 & otherwise \end{cases} \tag{7}$$

The NPCR value for two random images, which is an expected estimate for a good image cryptosystem, is given by:

$$NPCR_{\text{expected}} = \left(1 - \frac{1}{2^{\log_2(N)}}\right)\times 100 \tag{8}$$

where N is the gray levels of the image. For instance, the expected NPCR for two random images with 256 gray levels is 99.609%.

The second criterion, UACI is used to measure the average intensity of differences between the two images. It is defined as:

$$UACI_{AB} = \frac{100}{m\times n}\sum_{1}^{m}\sum_{1}^{n}\frac{\left|A(i,j)-B(i,j)\right|}{255} \tag{9}$$

The UACI value for two random images is given by

$$UACI_{\text{expected}} = \frac{1}{N^2}\left(\frac{\sum_{i=1}^{N-1} i(i+1)}{N-1}\right)\times 100 \tag{10}$$

IV. CONCLUSION

The paper proposes comparative analysis of different structures of chaos-based cryptosystems. According to their architecture, we classified the cryptosystems into four categories. After that we discused and analyzed each encryption scheme. We use different security analysis to evaluate the most popular permutation strategies that are representative off all the others. Then we employ the same method to evaluate the most important structures of chaos-based image encryption schemes: the permutation-diffusion and the combining permutation and diffusion. The comparisons are made using the current fastest encryption schemes. The study points out that most of the existing chaos-based encryption algorithm demands a huge amount of computational time due to repeating process of shuffling and quantization of real values sequence of chaotic numbers into binary representation. The use of chaotic sequence sorting allows taking advantage of the true accuracy of the computer for the generation of fast permutation and diffusion keys. Thus, coupled with the diffusion process, this scheme achieves high level of security while preserving the speed.

ACKNOWLEDGEMENTS

The work described in this paper was supported under the Postdoctoral Fellowships Program "Eugen Ionescu" granted by Romania government and managed by the "Agence universitaire de la Francophonie (AUF) ". J.Y. Effa would like to thanks the AUF for their financial support.

REFERENCES

[1] P.R. Sankpal and P.A. Vijaya, "Image Encryption using Chaotic Maps: A Survey", in *IEEE Proceedings Fifth International Conference on Signal and Image Processing,* pp.102-107, 2014. DOI: 10.1109/ICSIP.2014.80

[2] Y. Wang, K-W. Wong, X. Liao and G. Chen, "A new chaos-based fast image encryption algorithm", Applied Soft Computing, vol. 11, pp.514–522, 2011.

[3] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems", International Journal of Bifurcation and Chaos, vol. 16, pp.2129-2151, 2006.

[4] Z. Tang, J. Song, X. Zhang and R. Sun, "Multiple-image encryption with bit-plane decomposition and chaotic maps", Optics and Lasers in Engineering, vol. 80, pp.1–11, 2016.

[5] J.D.D. Nkapkop, J.Y. Effa, M. Borda and R. Terebes, "A Novel Fast and Secure Chaos-Based Algorithm for Image Encryption" In: I. Bica et al. (eds.), Innovative Security Solutions for Information Technology and Communications, Lecture Note in Computer Science, Springer, Switzerland, vol. 9522, pp.87-101, 2015

[6] B. Wang, Y. Xie, C. Zhou, S. Zhou and X. Zheng, "Evaluating the permutation and diffusion operations used in image encryption based on chaotic maps", Optik, vol. 127, pp.3541–3545, 2016.

[7] J. Fridrich, "Symmetric ciphers based on two dimensional chaotic maps", International Journal of Bifurcation and Chaos, vol. 8, pp.1259-1284, 1998.

[8] C. Fu, J.J. Chen, H. Zou, W.H. Meng, and Y.F. Zhan, A "chaos-based digital image encryption scheme with an improved diffusion strategy", Optics Express, vol. 20, pp.2363-2378, 2012.

[9] J.S.A. Eyebe Fouda, J.Y. Effa, B. Bodo and M. Ali, "Efficient Cryptosystem Based on Chaotic Sequences Sorting", American Journal of Signal Processing, vol. 2, pp.15-22, 2012.

[10] J.S.A. Eyebe Fouda, J.Y. Effa, S.L. Sabat and M. Ali, "A fast chaotic block cipher for image encryption", Communications in Nonlinear Science and Numerical Simulation, vol. 19, pp.578–588, 2014.

[11] C. Fu, B.-B. Lin, Y.-S. Miao, X. Liu and J.-J. Chen, "A novel chaos-based bit-level permutation scheme for digital image encryption", Optics Communication, vol.284, pp.5415–5423, 2011.