

## Research Article

# A New Chaos-Based Image-Encryption and Compression Algorithm

Somaya Al-Maadeed,<sup>1</sup> Afnan Al-Ali,<sup>2</sup> and Turki Abdalla<sup>2</sup>

<sup>1</sup>Department of Computer Science and Engineering, Qatar University, P.O. Box 2713, Doha, Qatar

<sup>2</sup>Department of Computer Engineering, College of Engineering, University of Basrah, B.P. 49, Basrah, Iraq

Correspondence should be addressed to Somaya Al-Maadeed, s.alali@qu.edu.qa

Received 1 September 2011; Revised 20 December 2011; Accepted 17 January 2012

Academic Editor: Ahmed Bouridane

Copyright © 2012 Somaya Al-Maadeed et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We propose a new and efficient method to develop secure image-encryption techniques. The new algorithm combines two techniques: encryption and compression. In this technique, a wavelet transform was used to decompose the image and decorrelate its pixels into approximation and detail components. The more important component (the approximation component) is encrypted using a chaos-based encryption algorithm. This algorithm produces a cipher of the test image that has good diffusion and confusion properties. The remaining components (the detail components) are compressed using a wavelet transform. This proposed algorithm was verified to provide a high security level. A complete specification for the new algorithm is provided. Several test images are used to demonstrate the validity of the proposed algorithm. The results of several experiments show that the proposed algorithm for image cryptosystems provides an efficient and secure approach to real-time image encryption and transmission.

## 1. Introduction

An increasing amount of information is being transmitted over the Internet, including not only text but also audio, image, and other multimedia files. Images are widely used in daily life, and, as a result, the security of image data is an important requirement [1]. In addition, when either communication bandwidth or storage is limited, data are often compressed. In particular, when a wireless communication network is used, low-bit-rate compression algorithms are needed as a result of bandwidth limitations. Encryption is also performed when it is necessary to protect user privacy [2]. Image-encryption algorithms are used to provide this security; for our purposes, these algorithms can be divided into two groups with respect to the approach used to construct the encryption scheme: chaos-based methods and nonchaos-based methods. Image encryption can also be divided into full encryption and partial encryption (also called selective encryption) schemes according to the percentage of the data that is encrypted. Encryption schemes can also be classified as either combined-compression methods or noncompression methods.

Several reviews have been published on image and video encryption, including selective (or partial encryption) methods, providing a fairly complete overview of the techniques developed to date [3]. Kunkelmann [4] and Qiao and Nahrstedt [5] provide overviews, comparisons, and assessments of classical encryption schemes for visual data, with an emphasis on MPEG. Bhargava et al. [6] review four MPEG-encryption algorithms published by the authors themselves from 1997 to 1999. More recent MPEG encryption surveys are provided by But [7] (in which the suitability of available MPEG-1 ciphers for streaming video is assessed). Other data formats have also been discussed with respect to selective encryption. Coding schemes based on wavelets [8], quad trees [9, 10], iterated function systems (fractal coding) [11], and vector quantization [12] have been used to create selective encryption schemes.

In 1997, two kinds of schemes based on higher-dimensional chaotic maps were proposed in which a discretized chaotic map of the pixels in an image is permuted by several rounds of shuffling operations [2]. Between every two adjacent rounds of permutations, a diffusion process is performed, which can significantly change the distribution of

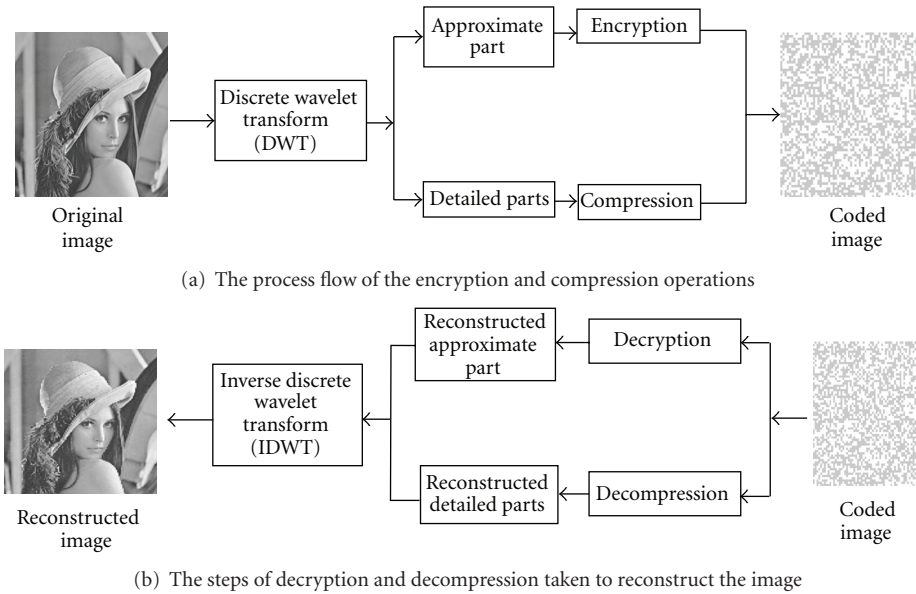


FIGURE 1: The processes of the new algorithm.

the image histogram, thereby making a statistical decryption attack impossible. Empirical testing and cryptanalysis have both demonstrated that the chaotic Baker and Cat maps are good candidates for this kind of image encryption. Similar ideas have also appeared, including a 1998 paper [13], in which a rapid bulk-data encryption scheme was designed by combining chaotic, Kolmogorov flows with an adaptation of a very fast shift-register-based pseudorandom number generator [14]. Recently, a Feed-Back Chaotic Synchronization (FCS) for designing a real-time secure symmetric encryption scheme has been implemented in hardware [15–17].

The basic principle of encryption with chaos is based on the ability of some dynamic systems to produce sequence of numbers that are random in nature. This sequence is used to encrypt messages. For decryption, the sequence of random numbers is highly dependent on the initial condition used for generating this sequence. A very minute deviation in the initial condition will result in a totally different sequence. This sensitivity to initial condition makes chaotic systems ideal for encryption.

In this paper, we present an approach for encrypting images, our approach is based on chaotic maps, where we suggest to use the wavelet transform for image decomposition as we will discuss later and then we propose to use one, two, or three external encryption keys to encrypt the important part using one-dimensional chaotic map. We will provide a comparison in terms of the correlation between the original image and the encrypted image for all the three cases of encryption by the multiple keys when the number of external encryption keys increases in each time.

Next section is an overview of our proposed method of selective encryption of an image. The rest of this paper is organized as follows: Sections 3 and 4 give a brief discussion to the wavelet transform and chaos theory, respectively: Test, verification, and efficiency of the proposed new encryption

algorithm are given in Section 5. Finally, Section 6 concludes this paper.

## 2. System Overview

In this paper, we propose an efficient, selective chaos-based image-encryption and compression algorithm. The block diagram of this algorithm is shown in Figure 1. The encryption and compression operations is shown in Figure 1(a). First, we have set the chaotic map parameters (the initial values) as well as to select the external encryption keys. The chaos-based encryption algorithm is as follows: after wavelet transformation, an amount of 25% (in case of one-level decomposition) or 6.25% (in case of two-level decomposition) of the original image, which corresponds to the important part, is transformed into one-dimensional vector with a dimension equal to the important part size, let us call it  $W$ . The chaotic map will be run for  $W$  iterations and generate a vector of ones and zeros of dimension equal to  $W$  too; it will be called a *threshold vector*, then the pixels of the image vector will be encrypted with one, two, or three external encryption keys according to that threshold vector.

From Figure 1(b), the secret image of size  $(128 \times 128)$  pixels is decomposed using discrete wavelet transform (DWT). In practice, this process of decomposition usually repeated  $n$  times, and it is repeated just on the LL-sub band as mentioned for octave-band decomposition. Here in this work, the decomposition will be for one-level or two-level decomposition in order to compare different amounts of encrypted data and examine their effect on security. The image is decomposed into four subimages: the approximation component (LL) and three detail components (horizontal, vertical, and diagonal). The most important component, the LL component, is then encrypted using a chaos-based

image-encryption algorithm, and the other three components are subsequently compressed using wavelet analysis. The implementation of the algorithm achieves high encryption rates, as discussed in Section 5. The steps of decryption and decompression taken to reconstruct the image are described at Figure 1(b).

### 3. Wavelet Transform

A wavelet is a small wave with its energy concentrated in time, providing a tool for the analysis of time-varying phenomena. A wavelet not only has an oscillating characteristic but also has the ability to allow for simultaneous time and frequency analyses with a flexible mathematical foundation. The first step of a general image-compression technique is the wavelet transform, which is designed to distinguish between the visually important information and unimportant information. The transform is also intended to reduce the statistical dependence between coefficients so that the source coding will be more efficient.

The important of wavelet as a multiresolution technique comes from its decomposition of the image into multilevel of the independent information with changing the scale-like geographical map, in which the image has nonredundant information due to the changing of the scale. In this way, every image will be transformed in each level of decomposition to a one low information image and three details image in horizontal, vertical, and diagonal axis image, also the low information image can be decomposed into another four images. These approaches of decomposition process provide us a number of unrealizable features in the original image, which appear in their levels after the application of transformation [18].

There are different types of wavelet transforms, including continuous wavelet transform (CWT) and the discrete Wavelet Transform (DWT). The CWT is used for signals that are continuous in time, and the DWT is used when a signal is being sampled, such as during digital signal processing or digital image processing [19]. In this work, discrete wavelet transform is used. In a discrete wavelet transform, an image can be analyzed by passing it through an analysis filter bank, which consists of a low-pass and high-pass filter at each decomposition stage. When a signal passes through these filters, it is split into two bands. The low-pass filter, which corresponds to averaging operation, extracts the coarse information of the signal. The high-pass filter, which corresponds to a differencing operation, extracts the detail information of the signal. The output of the filtering operations is decimated by 2. A two-dimensional transform can be accomplished by performing two separate one-dimensional transforms. First, the image is filtered along the  $x$ -dimension using low pass and high pass analysis filters and decimated by 2. Low pass filtered coefficients are stored on the left part of the matrix and high pass filtered on the right. Because of decimation, the total size of the transformed image is same as the original image. Then, it is followed by filtering the subimage along the  $y$ -dimension and decimated by 2. Finally, the image has been split into four bands denoted by LL, HL, LH, and HH,

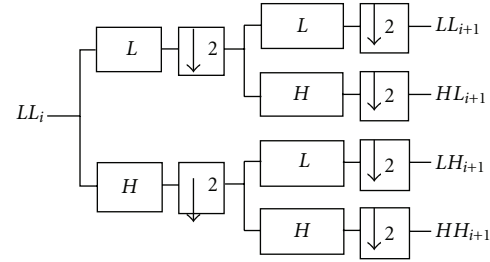


FIGURE 2: Splitting of subband into next higher Level four subbands.

after one-level decomposition. The LL band is again subject to the same procedure. The reconstruction of the image can be carried out by reversing the above procedure, and it is repeated until the image is fully reconstructed [18, 19]. This procedure of wavelet splitting is shown in Figure 2.

### 4. Image Encoding Using 1D-Discrete Chaotic Maps

In mathematics and physics, chaos theory describes the behavior of certain nonlinear dynamical systems that, under certain conditions, exhibit dynamics that are highly sensitive to initial conditions. As a result of this sensitivity, the behavior of chaotic systems appears to be random as a result of the exponential growth of errors in the initial conditions. This apparently chaotic behavior occurs even though these systems are deterministic in the sense that their future dynamics are well defined by their initial conditions, and there are no random elements involved. A chaotic dynamical system is a deterministic system that exhibits seemingly random behavior as a result of its sensitive dependence on its initial conditions and can never be specified with infinite precision. The behavior of a chaotic system is unpredictable; therefore, it resembles noise [18]. The close relationship between chaos and cryptography makes a chaos-based cryptographic algorithm a natural candidate for secure communication and cryptography [1]. Chaotic maps and cryptographic algorithms (or, more generally, maps defined on finite sets) have similar properties, such as sensitivity to changes in the initial conditions and parameters, pseudorandom behavior, and unstable periodic orbits with long periods. In a cryptographic algorithm, repeated encryption rounds lead to the desired diffusion and confusion properties of the algorithm. Iterations of a chaotic map spread the initial region over the entire phase space. The parameters of the chaotic map may represent the key to the encryption algorithm.

An important difference between chaos and cryptography is that encryption transformations are defined on finite sets, whereas chaos has meaning only for real numbers. Moreover, at present, the notion of cryptographic security and the performance of cryptographic algorithms have no counterpart in chaos theory [20]. In summary, we note that chaos-based encryption techniques are considered promising candidates for practical applications because these techniques provide an effective combination of speed, high



FIGURE 3: Test image 1 (Lena.PGM) when  $x(1) = 0.12345$ ,  $\alpha = 4$ ,  $\text{key1} = 1234567890223344$ , and  $\text{key2} = 0987654321001122$ ,  $\text{Thr} = 30$ ,  $\text{PSNR} = 28.1240$ .

security, complexity, reasonable computational overhead and computational power [1]. Chaotic maps have attracted the attention of cryptographers as a result of the following fundamental properties.

- (i) Chaotic maps are deterministic, meaning that their behavior is predetermined by mathematical equations.
- (ii) Chaotic maps are unpredictable and nonlinear because they are sensitive to initial conditions. Even a very slight change in the starting point can lead to a significantly different outcome.
- (iii) Chaotic maps appear to be random and disorderly but, in fact, they are not; beneath the random behavior is an order and pattern.

Chaotic phenomena are analogous to stochastic processes in that they appear in nonlinear dynamical systems; such processes are nonperiodic and nonconvergent and are extremely sensitive to initial conditions [20].

In cryptography, we focus on dynamic *discrete-time* system. A dynamic system is chaotic if all trajectories are bounded and nearby trajectories diverge exponentially at every point of the phase space. A chaotic system is given by an iterated function (chaotic map)  $f$  of a state space  $X$ . The

iterated function transforms the current stage of the system into the next one, that is,

$$x_{n+1} = f(x_n), \quad (1)$$

where  $x_n \in X$  denotes the system state at the discrete time. In chaos-based cryptography, the state space is typically a finite binary space

$$X = P = C = \{0, 1\}^n, \quad n = 1, 2, \dots, \quad (2)$$

where  $P = \text{Plaintext}$  and  $C = \text{Ciphertext}$ .

The initial condition is a vector  $x_0 \in X$ , and it is assigned to an internal state variable before the first iteration. The vector  $c \in K = \{0, 1\}^n$  contains the parameters of the dynamic system. The parameters are kept constant through all cycles (iterations) [21].

In this work, we are concerned with image encoding with the generation and use of 1D-chaotic maps. A one-dimensional dynamical system is a couple  $(I, \phi)$ , where  $I$  is real interval and  $\phi$  is a transformation from  $I$  to  $I$ . Chaotic maps are nonlinear maps presenting the property of sensitivity to initial conditions.



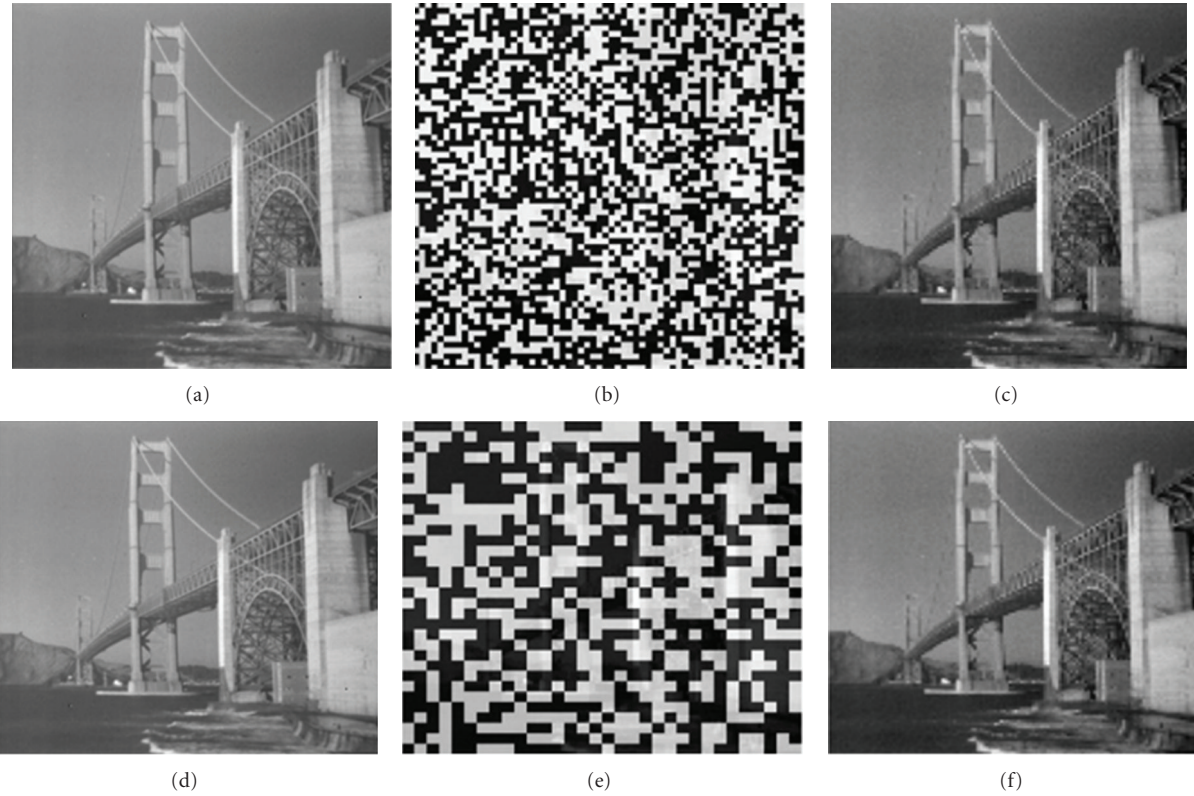


FIGURE 4: Results of application of chaotic algorithm to SF.GIF. (a) and (d) original image. (b) and (e) Image resulting from encryption with L1 or L2, respectively, using only one external encryption key in the larger size. (c) and (f) Reconstructed image in each case.

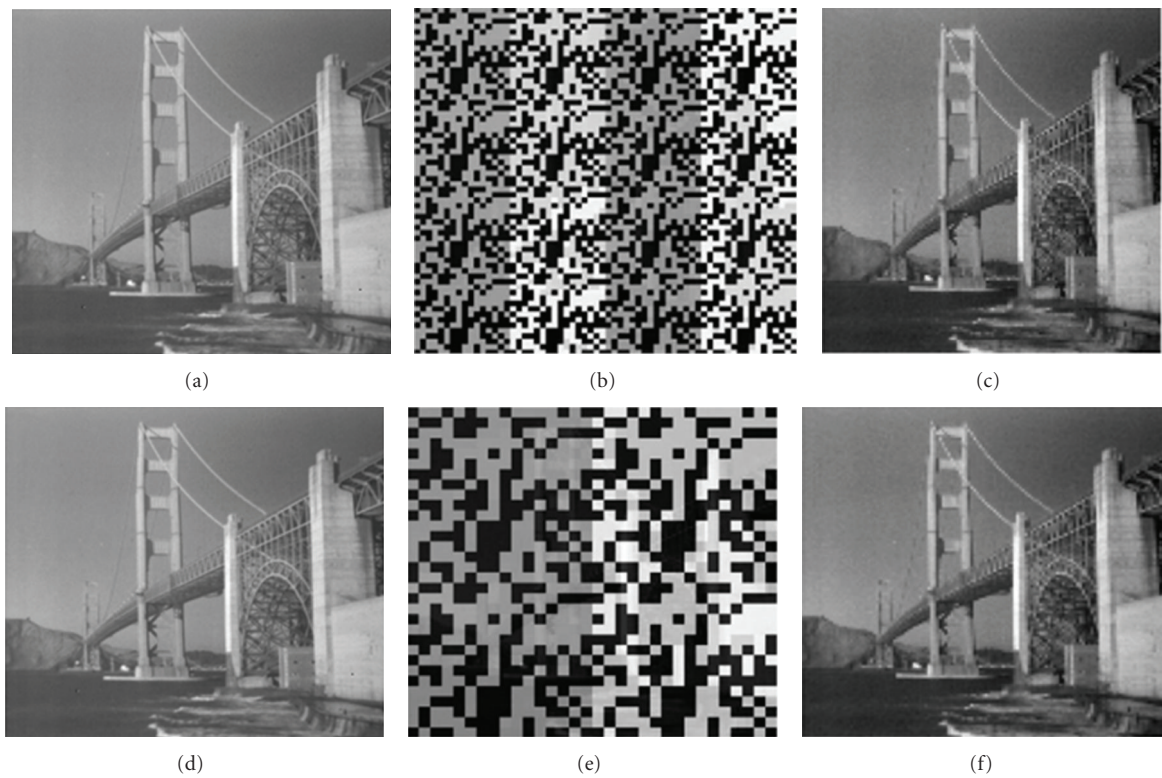


FIGURE 5: Results of application of chaotic algorithm to SF.GIF. (a) and (d) original image. (b) Image resulting from encryption with L1 or L2, respectively, using two external encryption keys in the larger size. (c) and (f) Reconstructed image in each case.

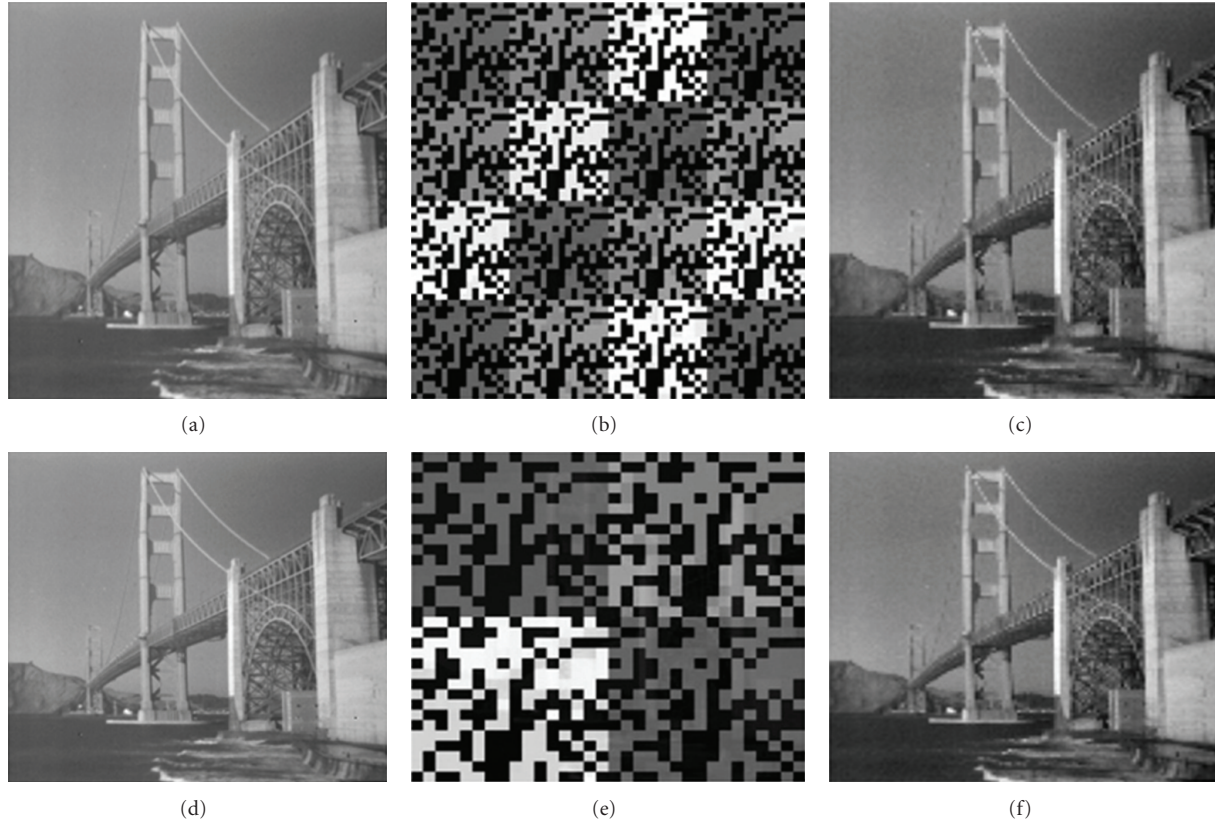


FIGURE 6: Results of application of chaotic algorithm to SF.GIF. (a) and (d) original image. (b) image resulting from encryption with L1 or L2, respectively, using three external encryption keys in the larger size. (c) and (f) reconstructed image in each case.

The nonlinear transformation used here is defined as an iterative scalar map [22]

$$\begin{aligned} x_{n+1} &= F(x_n, \alpha), \\ x_{n=0} &= x_0, \end{aligned} \quad (3)$$

where  $\alpha$  is a set of real parameters. The use of (3) for image encoding means that the image is seen as a dynamical system; the main difference is that images are presented by integer values, while they are mapped into real values under system in (3).

One of the most known chaotic maps is the logistic map. It is defined by the following equation:





$$\begin{aligned} x_{n+1} &= \alpha x_n(1 - x_n), \\ x_{n=0} &= x_0. \end{aligned} \quad (4)$$

The use of chaos for image encoding yields to three types of keys; these keys may be used together or separately, in order to enhance the privacy. They are the external or (control) parameter  $\alpha$ , the initial state  $x_0$ , and the number of iterations [21]. The number of iterations is fixed during all the cycles and equal to the size of the important part of the image, which should be encrypted. In this paper, one two or three external encryption keys are used, then three types of approaches are performed as following: first using one external encryption key: in this type, the chaotic

map will generate a threshold vector of two values: 0 and 1. The pixels of the image vector that are corresponding to the zeros of the threshold vector will be encrypted by one external encryption key and the other pixels will be normalized in such a way to hide the details of the image vector. Second, using two external encryption keys: in order to increase the security, the second type uses two external encryption keys such that the chaotic map will also generate a threshold vector of two values: 0 and 1, and the pixels of the image vector that are corresponding to the zeros of the threshold vector will be encrypted by the first key, and other pixels that are corresponding to the ones will be encrypted by the second key. Third, using three external encryption keys: in order to increase the security further, the third type uses three external encryption keys. In this case the chaotic map will generate a threshold vector of three different values: 0, 0.5, and 1. The pixels of the image vector that are corresponding to the zeros will be encrypted using the first key; the pixels that are corresponding to 0.5 values will be encrypted by the second key, and finally the pixels that are corresponding to the ones will be encrypted by the third key. The encryption process is done for one-level decomposition and two-level decomposition; also it is repeated for two different sizes of external keys. The previous schemes will be applied for chaotic maps given in (4). The decryption process is the reverse operation to each process in the encryption procedure as shown in Figure 1(b).



TABLE 1: Test images.

#	Images	Names
1		SF.GIF
2		ROAR512.JPG
3		GREEN ROSE.JPG
4		GOLDRUSH.JPG

## 5. Experimental Results

In this work, a 2D grayscale image is divided into subbands and subsampled using a discrete wavelet transform. The test images and their sizes can be shown in Table 1. Each coefficient represents a spatial area of approximately  $2 \times 2$  pixels from the original image. The total number of components remaining after the vertical and horizontal decompositions is four. These components are referred to as subbands. As shown in Figure 3, the most important component of these subbands is the LL component because it is much more similar to the original image; LL is called the *approximate image*. To provide security for this component, the second step is to encrypt this component using a chaos-based image-encryption algorithm, as described above. The algorithm described previously will be implemented for one 2D-gray scale image and one 2D-color image, each of them has size

of  $(128 \times 128)$  pixels. The test images and their sizes can be shown in Table 1.

The correlation coefficients between the original image and the encrypted image for all the three cases of encryption which are explained previously, are illustrated in Tables 2 and 3. The results obtained for one-level and two-level decomposition. Note that the initial state for which the encrypted images is computed is  $x_0 = 0.65440$  and the number of iterations is fixed during all cycles equal to the size of the important part of the image, which should be encrypted. The chaotic map parameters are the initial values which are also used to select the external encryption keys (see Section 4). In this paper, the parameters are set as follows: the parameter  $\alpha = 4$ , one, two, or three external encryption keys. Here, our aim is to compare the output images for different values of parameters (we have considered six cases). They are: small keys sizes (key1 = 4567, key2 = 3336, and key3 = 5892) and large keys sizes (key1 = 4567332, key2 = 3336877, and key3 = 5892117). These results are obtained by applying chaotic partial encryption to the image after the wavelet transform operation is performed. Table 2 shows the results for the two grayscale images, while Table 3 shows the results for the two color images for small key size and large key size. Figures 4, 5, and 6 show the results for SF.GIF grayscale image in one, two, and three external encryption keys, respectively.

A good encryption procedure should be robust against all kinds of cryptanalytic, statistical, and brute-force attacks. In this section, we discuss the security analysis of our method.

From the results, we can confirm that our cipher is excellent, and this is clear from the below analysis to the results of our experiments.

For a secure image cryptosystem, the encryption key plays a very important role against the brute force attack; so for high security, the key space should be large enough to make the brute force attack infeasible but may decrease encryption/decryption speed. In this algorithm, we used a key space of 94 bit combination, then we increased the key space up to 97 bit combination and compared the results (Tables 2 and 3). Out of this comparison, we found that the correlation between the cipher image and the original image decreased when we increased the key space size. Moreover using more than one external encryption keys which is a perfect way to conclude that increasing the number of keys means increasing the security because this makes the intruder suffers when trying to attack the cipher image and find the secret keys. In addition to the external encryption keys, we should mention that our algorithm depends also on the parameters of logistic map, which is sensitive to the initial condition that can be connected with confusion and diffusion property in good cipher.

We have performed statistical analysis by calculating the histograms and correlations of cipher and reconstructed image with the original one. The correlation between the original image and the cipher image is nearly equal to zero expressing the original image and cipher image being almost independence. The correlation between the original image and the reconstructed image is nearly equal to one that means a perfect reconstruction at the receiver and

TABLE 2: Results of encryption of different amount for grayscale SE:GIF and ROAR512.JPG images using small and large keys sizes.

Image	Key size	Amount %	One key		Two keys		Three keys	
			Cipher-image correlation	Reconstructed-image correlation	Cipher-image correlation	Reconstructed-image correlation	Cipher-image correlation	Reconstructed image correlation
1	Small	L1 = 25	0.07462337	0.99999286	0.03005224	0.99999287	0.00513192	0.99999287
		L2 = 6.25	0.14151426	0.99999784	0.13672353	0.99999784	0.0433832	0.99999784
1	Large	L1 = 25	0.01197778	0.99999286	0.00645548	0.99999287	0.00495562	0.99999287
		L2 = 6.25	0.07438078	0.99999784	0.02457648	0.99999784	0.00654208	0.99999784
2	Small	L1 = 25	0.13040771	0.99999835	0.05808717	0.99999836	0.04030919	0.99999836
		L2 = 6.25	0.24379369	0.99999949	0.15640678	0.99999949	0.07057224	0.99999949
2	Large	L1 = 25	0.01142504	0.99999835	0.00668093	0.99999836	0.00121170	0.99999836
		L2 = 6.25	0.10455903	0.99999491	0.07915913	0.99999492	0.02147876	0.99999492



TABLE 3: Results of encryption of different amount for color GREEN ROSE.JPG and GOLDRUSH.JPG images using different keys.

Image	Key size	Amount %	One key		Two keys		Three keys	
			Cipher-image correlation	Reconstructed-image correlation	Cipher-image correlation	Reconstructed-image correlation	Cipher-image correlation	Reconstructed-image correlation
3	Small	L1 = 25	0.06636301	0.99999996	0.04991651	0.99999897	0.04777646	0.99999897
		L2 = 6.25	0.13200788	0.99999998	0.08473995	0.99999967	0.07023566	0.99999967
3	Large	L1 = 25	0.02938994	0.99999996	0.00519053	0.99999897	0.00418059	0.99999897
		L2 = 6.25	0.03215505	0.99999998	0.02981104	0.99999967	0.01996734	0.99999967
4	Small	L1 = 25	0.03293707	0.99999995	0.02655446	0.99999833	0.00998768	0.99999833
		L2 = 6.25	0.06094592	0.99999998	0.03180833	0.99999470	0.01329204	0.99999947
4	Large	L1 = 25	0.00525827	0.99999995	0.00494368	0.99999833	0.00218012	0.99999833
		L2 = 6.25	0.02447215	0.99999998	0.01329412	0.99999470	0.00979585	0.99999470

the encryption algorithm works in a very good manner to protect the image. Out of the results of our experiments, one can see that as the amount of the encrypted part is decreased (from  $L1 = 25\%$  to  $L2 = 6.25\%$ ), the execution time is decreased too (about 0.218 sec for one external encryption key, 0.453 sec for two external encryption keys, and 0.5 sec for three external encryption keys), which indicates a high speed in performing encryption and decryption process and in getting the results, but also we should mention that decreasing the amount of encrypted part makes the correlation between the cipher image and the original image increase. All the proposed algorithms were programmed in MATLAB version 7.0. Performance was measured on a 2.0 GHz. Pentium IV with 1 GB of RAM running Windows XP Professional.

## 6. Conclusion

In this paper, we have proposed a method for the selective encryption of an image combined with a compression method. The technique used here results in a significant reduction in encryption and decryption time. This method consists of three steps; in each step, we used selected properties that served the goal of this paper, which were to obtain an effective cipher and high-quality image compression to achieve both security against unauthorized access during data transmission through an unsecured channel and high compression to allow for a low transmission rate. For the encryption, we used an efficient algorithm based on a chaotic map to encrypt the low subband of the image; this algorithm has very good diffusion and confusion properties, and we obtained a very good cipher of the subband, as evidenced by the low correlation between the original image and the coded image. For the compression, we used the wavelet transformation, and the results were highly satisfactory; this method allowed us to achieve a perfect reconstruction with a good PSNR. The basic idea of this work is to show the influence of using multiple keys in increasing security by increasing the number of external encryption keys in each time such that the important part of the image is encrypted with one, two, or three external encryption keys; the encryption is done by a new 1D chaotic map. We show from the results that the correlation coefficients between the original image and the encrypted image are decreased when the number of external encryption keys is increased, and this increases the security. Also, we show how the correlation coefficient changed exponentially when using different values of the control parameter in each time. In future work, we can use more than 128 bits for the external keys to increase overall security, and we can use another method for compression.

## References

- [1] H. Hossam El-din, H. M. Kalash, and O. S. Farag Allah, "An efficient chaos-based feedback stream cipher (ECBFSC) for image encryption and decryption," *Informatica*, vol. 31, no. 1, pp. 121–129, 2007.
- [2] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps," *International Journal of Bifurcation and Chaos in Applied Sciences and Engineering*, vol. 8, no. 6, pp. 1259–1284, 1998.
- [3] R. Pfarrhofer and A. Uh, "Selective image encryption using JBIG," in *Proceedings of the Communications and Multimedia Security (CMS '05)*, pp. 98–107, September 2005.
- [4] T. Kunkelmann, "Applying encryption to video communication," in *Proceedings of the Multimedia and Security Workshop at (ACM Multimedia '98)*, pp. 41–47, England, UK, September 1998.
- [5] L. Qiao and K. Nahrstedt, "Comparison of mpeg encryption algorithms," *Computers and Graphics*, vol. 22, no. 4, pp. 437–448, 1998.
- [6] B. Bhargava, C. Shi, and S. Y. Wang, "MPEG video encryption algorithms," *Multimedia Tools and Applications*, vol. 24, no. 1, pp. 57–79, 2004.
- [7] J. But, "Limitations of existing MPEG-1 ciphers for streaming video," Tech. Rep. CAIA 040429A, Swinburne University, Melbourne, Australia, April 2004.
- [8] A. Pommer and A. Uhl, "Selective encryption of wavelet-packet encoded image data: efficiency and security," *Multimedia Systems*, vol. 9, no. 3, pp. 279–287, 2003.
- [9] H. Cheng and X. Li, "Partial encryption of compressed images and videos," *IEEE Transactions on Signal Processing*, vol. 48, no. 8, pp. 2439–2451, 2000.
- [10] X. Li, J. Knipe, and H. Cheng, "Image compression and encryption using tree structures," *Pattern Recognition Letters*, vol. 18, no. 11–13, pp. 1253–1259, 1997.
- [11] S. Roche, J.-L. Dugelay, and R. Molva, "Multi-resolution access control algorithm based on fractal coding," in *Proceedings of the IEEE International Conference on Image processing (ICIP'96)*, pp. 235–238, IEEE Signal Processing Society, Lausanne, Switzerland, September 1996.
- [12] T. S. Chen, C. C. Chang, and M. S. Hwang, "A virtual image cryptosystem based upon vector quantization," *IEEE Transactions on Image Processing*, vol. 7, no. 10, pp. 1485–1488, 1998.
- [13] J. Scharinger, "Fast encryption of image data using chaotic Kolmogorov flows," *Journal of Electronic Imaging*, vol. 7, no. 2, pp. 318–325, 1998.
- [14] Y. Mao and G. Chen, "Chaos based image encryption," in *Handbook of Computational Geometry for Pattern Recognition, Computer Vision, Neural Computing and Robotics*, E. B. Corrochano, Ed., Springer, Heidelberg, Germany, 2004.
- [15] M. S. Azzaz, C. Tanougast, S. Adoudi, A. Bouridane, and A. Dandache, "An FPGA implementation of a feed-back chaotic synchronization for secure communications," in *Proceedings of the 7th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP '10)*, pp. 239–243, July 2010.
- [16] M. S. Azzaz, C. Tanougast, S. Sadoudi, A. Dandache, and F. Monteiro, "Real-time image encryption based chaotic synchronized embedded cryptosystems," in *Proceedings of the 8th IEEE International NEWCAS Conference (NEWCAS '10)*, pp. 61–64, June 2010.
- [17] S. Sadoudi, C. Tanougast, M. S. Azzaz, A. Dandache, and A. Bouridane, "Embedded genesisio-tesi chaotic generator for ciphering communications," in *Proceedings of the 7th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP '10)*, pp. 234–238, July 2010.
- [18] A. Cohen and J. Kovacevic, "Wavelets: the mathematical background," *Proceedings of the IEEE*, vol. 84, no. 4, pp. 514–522, 1996.
- [19] G. Lekutai, *Adaptive self-tuning neuro wavelet network controllers*, Ph.D. thesis, Electrical Engineering Department, Virginia

Polytechnic Institute and State University Blackburg, Virginia, Va, USA, March 1997.

- [20] C.-H. Hsu, *A study of chaotic image encryption algorithm*, M.S. thesis, Electrical Engineering Department, Chung Yuan Christian University, 2004.
- [21] F. Belkhouche and U. Qidwai, "Binary image encoding using 1D-chaotic maps," in *Proceedings of the IEEE Region 5 Annual Technical Conference*, pp. 39–42, New Orleans, La, USA, April 2003.
- [22] R. M. May, "Simple mathematical models with very complicated dynamics," *Nature*, vol. 261, no. 5560, pp. 459–467, 1976.





**Hindawi**

Submit your manuscripts at  
<http://www.hindawi.com>

