2012 International Conference on Image and Information Processing (ICIIP 2012)
IPCSIT vol. 46 (2012) © (2012) IACSIT Press, Singapore

A High Fidelity OFDM Image Communication System with Chaotic Maps

Hossam M. Kasem [+], Mohamed E.Nasr and Amr H. Hussein

Faculty of Engineering, Tanta University, Tanta, Egypt

Abstract. Image transmission has evolved as an important research branch in multimedia broadcasting communication systems in the last few decades. This paper is devoted to the transmission of encrypted images over Orthogonal Frequency Division Multiplexing (OFDM) systems. Encryption is carried out with both Baker and logistic maps, while a chaotic Baker map interleaving approach is used to increase the immunity to noise and fading over the communication channel. Linear equalization is utilized in this paper as a tool to enhance the communication system performance. Simulation results show that image transmission over wireless channels using the proposed chaotic encryption and interleaving techniques is much more immune to noise and fading. .

Keywords: chaotic maps, OFDM, image encryption, equalization.

1. Introduction

Due to Internet growth, multimedia content such as image, video, and audio signals can be easily transmitted from a contentprovider to a consumer. This gives a huge impact for development of entertainment industry,multimedia, and E-commerce, which rely on the Internet. Thus, to prevent multimedia content from an unauthorized user, security plays a significant role for content protection. In the past few years, encryption has become a major tool for securing multimedia content. Since 1990s, an increasing attention has been devoted to theusage of chaotic functions to implement the encryption process. Many researchers have noticed that there exists a tightrelationship between chaos and cryptography. Many properties of chaotic systems have their correspondingcounterparts in traditional cryptosystems. A comparison between chaos and cryptography properties can be found in[1]. Two general ways to design digital chaotic ciphers are using chaotic systems to generate a pseudo-random key stream, which is used to mask the plaintext, and the use of the plaintext and/or the secret key(s) asthe initial conditions and/or control parameters, iterating/counter iterating chaotic systems multiple times to obtain the cipher text. The first way corresponds to stream ciphers and the second to block ciphers. In our study, we combine both ways to get a more secure encryption. From the analysis, the chaotic-based encryption schemes consist of two main operations; the key stream generation and the encryption operation. The advantages of a chaotic-based image encryption are the easiness of implementation,the faster encryption speed and the strength against attacks [2]. Many image encryption schemes based on chaotic maps have been proposed [3-5]. However, most of them use 1-D chaotic maps, which has security weaknesses [6].

Recently, Elbakay et al. have presented a 2-D chaotic Baker map encryption algorithm with a study for the efficiency of this algorithm for image encryption [7]. The results in [7] have shown that the chaotic Baker map has achieved a great success in the image communication over OFDM and MC-CDMA systems. This success was attributed to the permutation nature of the Baker map. In this paper, a modified approach for image encryption is adopted. This approach is based on the utilization of the 2-D Baker map and an XOR

[+] Corresponding author. Tel.: +2 01224058659.
*E-mail address:*Eng_kasem@yahoo.com.

process with a logistic map to change the nature of encryption from just a permutation process to a permutation and masking process in order to enhance the security. A comparison study between the proposed approach, Baker map, and logistic map encryption is presented.

The proposed approach is used for efficient image communication over a fading channel with OFDM. The effect of channel equalization is investigated in this paper. The rest ofthis paper is organized as follows. Section 2 surveys the Baker Map. Section 3discusses the logistic map.Section 4 gives the proposed OFDM model. Section 5gives the simulation results. Finally section 6 gives the conclusion.

2. Chaotic Backer Map

The Baker map is a chaotic map, which converts a unit square into itself using a 2-D map. Its operation is cut in half, and the two halves are stacked on one another. The Baker map, B, can be described with the following formulas:

$$B(x, y) = (2x, y/2) \text{ where } 0 \le x \le 1/2 \quad (1)$$

$$B(x, y) = (2x-1, y/2+1/2) \text{ where } 1/2 \le x \le 1 \quad (2)$$

Indeed, this simple case of dividing the square into two rectangles of the same size is not used in randomization. There are two versions of the chaotic Baker map, in which a transfer operator U called the secret key is used. It is used for the division of the Baker map. The secret key is a vector, which has k elements such that the square is divided into k vertical rectangles as shown in Fig (1-a). A discretized version of this map is shown in Fig (1-b).

2.1. Generalized Baker Map

The Baker map can be generalized as follows:

1, An N×N square matrix is divided into k vertical rectangles of height N and with width ni (value of each element in U where n1+n2+….nk = N).

2, These vertical rectangles should be stretched horizontally by the value of rectangle height.

3, Then, rectangles are stacked to have the left one in the bottom and the right one on the top.

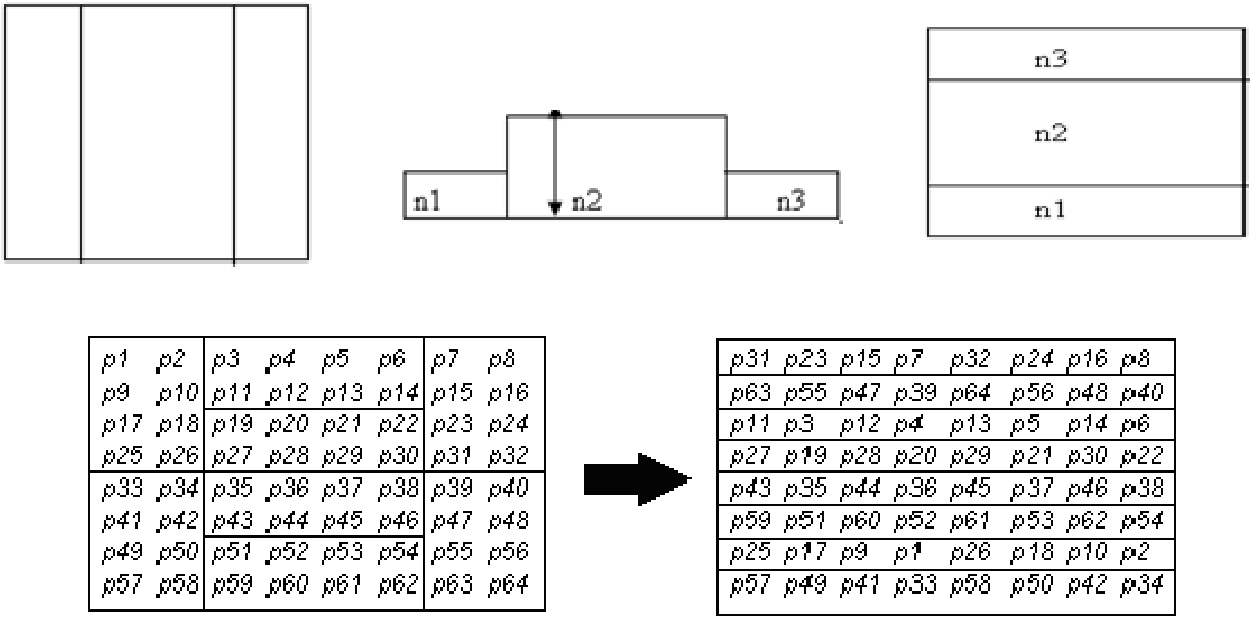


Fig. 1: The Baker map for an 8×8 pixel image using a key of (2, 4, 2).

(a) Generalized Baker map. (b) The discretized Baker map.

3. Logistic Maps

Pareek et al. proposed an image encryption scheme based on two chaotic logistic maps [8].To make the cipher more secure against any attack, seven different types of operations have been used to encrypt the pixels and the secret key is modified after each encryption of the image. A secret key of 80-bits and two chaotic logistic maps have been employed. The initial conditions for both logistic maps have been derived using the external secret key by providing differentweights to its bits. In this algorithm, the first logistic map is used to generate numbers ranging from 1 to 24, which may be repeated. The initial condition of the second logistic map is modified from the numbers generated by the first logistic map. By modifying the initial conditions of the second logistic map in this way, its dynamics get further randomized. The procedure of this image encryption scheme is implemented as follows [8].**Step 1:**The image encryption process uses a key of 80-bits long.

$$K = k_1 k_2 \ldots\ldots k_{20} \qquad \text{(in hexadecimal)} \tag{3}$$

ki's are the alphanumeric characters (0-9 and A-F) and each group of two alphanumeric characters represents a session key. Alternatively, the secret key can be represented in ASCII mode as:

$$K = K_1 K_2 \ldots . K_{10} \qquad \text{(in ASCII)} \tag{4}$$

each Ki represents one 8 bit block of the secret key i.e. session key.

Step 2: Two chaotic logistic maps are employed in this encryption process as follows [8]:

$$X_{n+1} = 3.9999 X_n (1 - X_n) \tag{5}$$

$$Y_{n+1} = 3.9999 Y_n (1 - Y_n) \tag{6}$$

Step 3: In order to calculate the initial condition X0, we chose three blocks of session key i.e. K4,K5, and K6 and convert them into a binary string as:

$$B = K_{41} K_{42} \ldots K_{48} K_{51} K_{52} \ldots K_{58} K_{61} K_{62} \ldots K_{68} \tag{7}$$

Kij's are the binary digits (0 or 1) of the ith block of the session key. Next, a real number X01 is computed using the binary representation as:

$$X_{01} = (K_{41} \times 2^0 + K_{42} \times 2^1 + \ldots + K_{48} \times 2^7 + K_{51} \times 2^8 + K_{52} \times 2^9 + \ldots + K_{58} \times 2^{15} + K_{61} \times 2^{16} + K_{62} \times 2^{17} + \ldots + K_{68} \times 2^{23}) / 2^{24}. \tag{8}$$

Furthermore, we compute another real number X02 as follows:

$$X_{02} = \sum_{i=13}^{18} (k_i)_{10} \; / 96 \tag{9}$$

ki's are parts of the secret key in hexadecimal mode as explained in step.1. Computation of the initial condition X0 for the logistic map using X01 and X02 is carried out as:

$$X_0 = (X_{01} + X_{02}) \bmod 1 \tag{10}$$

Step 4: By iterating the first logistic map using the initial conditions obtained in Step 3, a sequence of 24 real numbers f1, f2… f24 is generated. The values, which fall in the interval [0.1, 0.9], are considered. The real number sequence is converted into an integer sequence using the following formula:

$$P_k = \text{int} (23 \times (f_k - 0.1) / 0.8 + 1) \tag{11}$$

where k=1,2,…,24.

Step 5: To calculate the initial condition Y_0 for the second logistic map, three blocks of session key i.e. $K_1 K_2 K_3$, are selected and converted into a binary string as:

$$B_2 = K_{11} K_{12} \ldots K_{18} K_{21} K_{22} \ldots K_{28} K_{31} K_{32} \ldots K_{38} \tag{12}$$

K_{ij}'s are the binary digits (0 or 1) of the i^{th} block of the session key. We then convert B_2 from binary form into decimal form as in step 3, then compute a real number Y_{01} as follows:

$$Y_{01} = (B_2)_{10} / 2^{24} \tag{13}$$

Furthermore, we compute another real number Y_{02} as follows:

$$Y_{02} = (\sum_{k=1}^{24} B_{2}[p_k] * 2^{k-1}) / 2^{24} \quad (14)$$

B2 [Pk] denotes the value of p_k^{th} bit in the binary string B2 i.e.it is either 0 or 1. Now we compute the initial condition Y0 for the second logistic map using Y01 and Y02 as:

$$Y_0 = (Y_{01} + Y_{02}) \bmod 1 \quad (15)$$

Step6: Each pixel of the image is encrypted using an XOR operation with the second logistic map.

$$C_i = I_i \oplus Y \quad (16)$$

Step 7: After encryption of the image file, we modify the session keys K1 to K9 as follows:

$$(K_i)_{10} = ((K_i)_{10} + (K_{10})_{10}) \bmod 256. \qquad (1 < i < 9) \quad (17)$$

4. The Proposed OFDM Model

The proposed modifications are based on incorporating an encryption stage at the transmitter and a frequency-domain equalization stage at the receiver. Fig.2 illustrates these modifications for OFDM system.

The proposed OFDM system model for image transmission consists mainly of 4 stages; Baker map encryption, an image data formatting stage, a logistic map encryption stage on the binary image data, an OFDM modulation stage which contains an IFFT process and insertion of Cyclic Prefix (CP) .The block diagram of the proposed system model is shown in Fig. 2

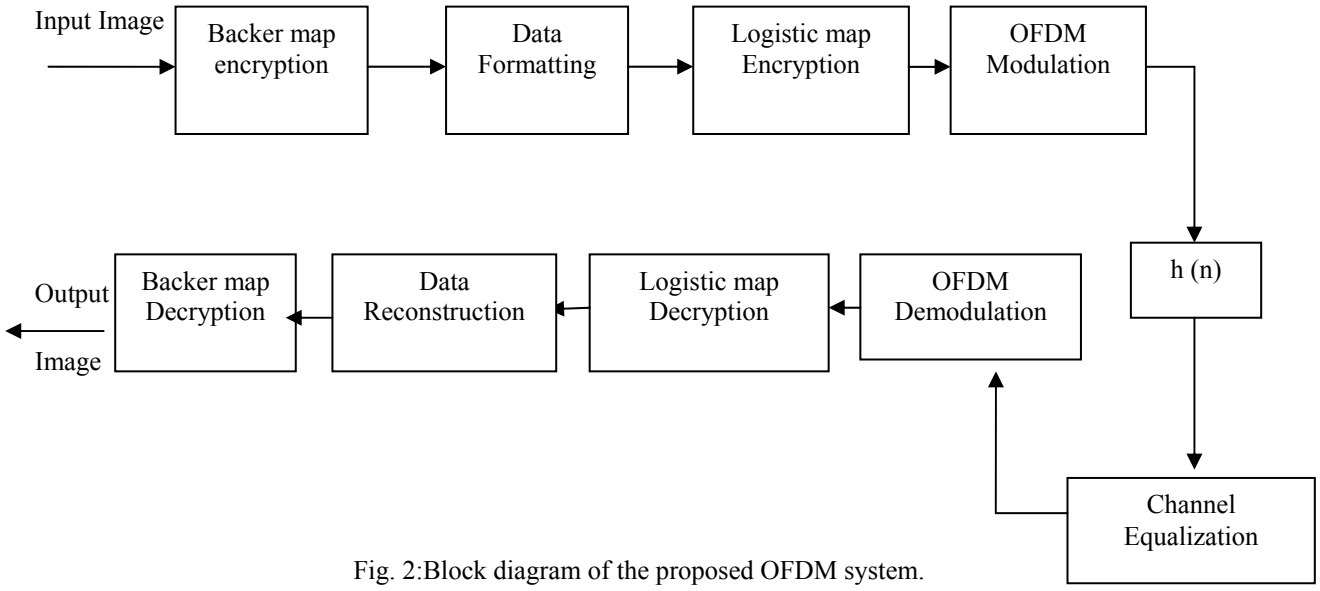


Fig. 2:Block diagram of the proposed OFDM system.

Image transmission over the proposed model follows the following steps:

1. The image is transformed into a square M×M matrix.
2. Chaotic Baker map encryption is applied to this square matrix.
3. This matrix is reshaped into a matrix of binary bits on a pixel-by-pixel basis.
4. Logistic maps encryption is applied to this square matrix.
5. An OFDM modulation step is performed on the binary data.
6. At the receiver, the equalization is performed with a frequency-domain equalizer.
7. An OFDM demodulation process is performed.
8. Logistic map decryption is performed.
9. Data are transformed from a binary stream to a square matrix.
10. Chaotic Baker map decryption is applied to this square matrix.

5. Simulation Results

The Peak Signal to Noise Ratio (PSNR) is used to measure the quality of the reconstructed images at the receiver. It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of this signal. Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. The PSNR is defined as follows:

$$PSNR = 10\log_{10}\left(\frac{(255)^2}{MSE}\right) \tag{18}$$

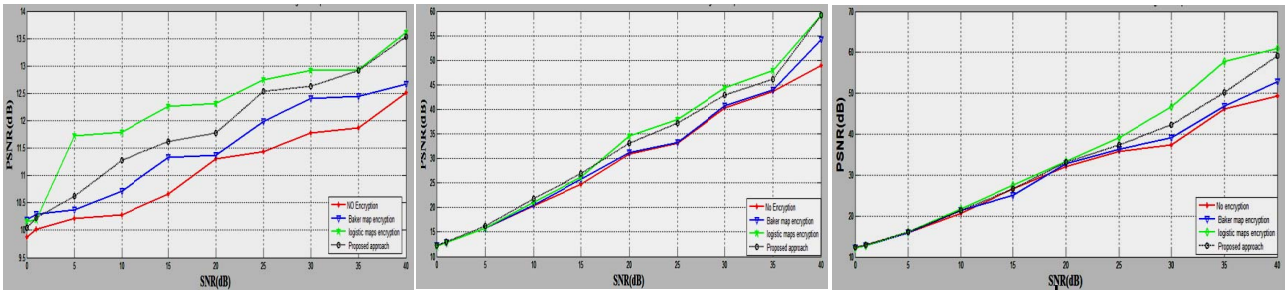
where 255 is the maximum possible pixel value of the image. MSE is the Mean Square Error. For an N ×N monochrome image, it is defined as:

$$MSE = \frac{\sum[f(i,j) - \hat{f}(i,j)]^2}{N^2} \tag{19}$$

where $f(i,j)$ is the source image, and $\hat{f}(i,j)$ is the received image.

To evaluate the performance and efficiency of the proposed encryption scheme, the Cameraman image of size 256×256 is used. Several simulation experiments have been carried out in this section to test the performance of the proposed scheme. The simulation environment is based on the OFDM system, in which each user transmits BPSK information symbols. The wireless channel model used in the simulation is the SUI-3 channel which is one of six channel models adopted by the IEEE 802.16a standard for evaluating the performance of broadband wireless systems in the 2–11 GHz band. It has three Rayleigh fading taps at delays of 0, 0.5 and 1 μs, with relative powers of 0 dB, -5 dB, and -10 dB, respectively. The fading is modelled as quasi-static (unchanging during a block). The simulation parameters are modulation type is BPSK , image size is 256×256 , cyclic prefix is 20 samples,Transmitter IFFT size is M= 256 symbols, Fading channel isSUI-3 channel ,Equalization is ZF and LMMSE and Channel estimation is Perfect

For the encryption purpose, the variation of PSNR of the received image with the channel Signal to Noise Ratio (SNR) has been studied and the results are shown in Fig. (3) .



(a) (b) (c)

Fig. 3: PSNR versus SNR for the received Cameraman image. (a) Without equalization, (b) with ZF equalization and (c) with LMMSE equalization.

6. Conclusion

This paper presented an efficient image communication scheme with OFDM. This scheme adopts both logistic and Baker maps for image encryption. A comparison study has been held between this proposed approach and traditional logistic maps approach. The channel communication impairments have been studied. Simulation results have proved that the proposed approach can achieve a tradeoff between fidelity and security of communicated images..

7. References

[1] G. Alvarez and S. Li," *Some Basic Cryptographic Requirements for Chaos-based Cryptosystems*". Int. J.Bifurcation and Chaos, Vol.16, 2006.

[2] J.Fridrich, , "*Symmetric ciphers based on two-dimensional chaotic maps*" Internat. J. Bifurcat. Chaos, 8 (6), 1988, pp. 1259-1284.

[3] M.S. Baptista, "*Cryptography with chaos*," Phys. Lett. A 240, 1998, pp.50-53.

[4] L.Kocarev, and G.Jakimoski, "*Logistic Map as a Block Encryption Algorithm*" Phys. Lett. A 289, 2001, pp.199-206.

[5] N.K. Pareek, VinodPatidar, and K.K. Sud, "*Cryptography using multiple one-dimensional chaotic maps*" Commun. Nonlinear Sci.Numer. Simul. 10, 2005, pp. 715-723.

[6] T. Xiang, K. W. Wong, and X. Liao, "*A novel symmetrical cryptosystem based on discretized two-dimensional chaoticmap*," Phys. Lett. A 364, pp. 252-258, 2007.

[7] E. M. El-Bakary, O. Zahran, S. A. El-Dolil , and F. E. Abd El-Sami, ” *Chaotic Maps: A tool to Enhance te performance of OFDM system*”, International Journal of Communication Networks and Information Security (IJCNIS), Vol. 1, No. 2, August 2009, pp54-59.

[8] N. K. Pareek, VinodPatidar, and K.K. Sud, " *Image encryption using chaotic logistic map*" Image and Vision Computing, v24. 926-934.