International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Color Image Encryption and Decryption by Using Chaotic Baker Map Bit Interleaver

[1]SAFA AHMED ABED ALABASS, [2]MORTADA ABDULRAHEEM HAYDER, [3]ZAID SALAH ABDUlSATTAR, [4]OLA HAMZA RASOOL, [5]MARWAH ADIL HASAN

[1]Assistant Lecturer, Dep. of Communication Engineering , Al-Hussain University College, Karbala, Iraq.*
[2] Laboratory of computer management, University of Karbala, Karbala, Iraq.
[3,4] Scientific Affairs, University of Karbala, Karbala, Iraq.
[5] B.Sc student, Al-Hussain University College, Karbala, Iraq.

Abstract- *With the progress in communication technology, the necessity of information security has become a global issue. Due to advancement in multimedia application, security becomes an important issue of communication and storage of data. This paper studies the encryption approach for color images. The proposed approach in the paper is based on the chaotic Baker map. The improvement encryption of image by applying the chaotic baker map on bit, which achieves high encryption efficiency. Simulation and statistical analysis show that this approach works well. Here MATLAB is used to design and implement the algorithm.*

Key Words: Chaotic Baker Map, Chaotic Baker Map pixel interleaver, Chaotic Baker Map bit interleaver.

INTRODUCTION

With the special and reliable security in the transmission and storage of images is needed in several applications like pay TV, biometric images or medical for transmission or storage, confidential video conferencing over optical fiber, military applications, police identification procedures, online banking systems, governmental services, identity (ID) cards, etc.

Generally speaking, there are two major approaches that are used to protect digital image. One is information hiding such as digital watermarking of image/video. The other is image encryption, which includes conventional encryption schemes and others such as the chaotic encryption [1]. Traditional image encryption technique regards the plaintext as original data stream, due to some intrinsic features of images, such as bulk size data and high correlation among pixels, traditional encryption algorithms such as DES, IDEA and RSA are not suitable for practical image encryption [2]. With the development of nonlinear dynamics and chaos theory, some common features, such as sensitivity to variables and parameters, between chaos and cryptography was revealed and exploited [3]. It has drawn increasing efforts to use chaotic systems for enhancing the security of communications.

In recent years, a number of digital chaotic cryptographic schemes have been proposed [1-8]. In [2], 3D cat map was employed to shuffle the positions of Image pixels, and another chaotic map was used to confuse the relationship between the cipher-image and the plain-image. In this way, the resistance to statistical and differential attacks is significantly increased. In [4], a baker map was used to speed up image encryption while retaining its high degree of security. A chaotic key-based algorithm for image encryption was developed [5]. According to a binary sequence generated from a chaotic map, the pixel of image was XOR-ed or XNOR-ed to the predetermined keys. A method that can provide more than one level of decryption and can solve the trade-off between the encryption speed and the security level for JPEG2000 image was proposed [6]. The permutation of pixels, the substitution of gray level values, and the diffusion of the discretized chaotic map can encrypt an image effectively [7, 8]. In [9], a systematic procedure to create chaos cipher was proposed; the author claimed that their ciphers are resistant to known attacks. This paper proposes an improved chaotic Baker map based on reference [7, 8] in order to encrypt bulk size images. The cipher key can be any integer rather than those divides pixel number in a row/column in a square image. This improvement can achieve high encryption efficiency. We also proposed to use different keys on bit of image, so that there is a large cipher key space, which makes the encrypted image more resistive to exhaustive search.

The rest of the paper is organized as follows: Section 2 introduces the chaotic Baker map. Simulation and valuation of proposed modification in Section 3. Result and discussion in Section 5.

2. Chaotic Baker Map

The chaotic Baker map is well-known to the image processing community as a tool of encryption. It is a permutation- based tool, which performs the randomization of a square matrix of dimensions N x N by changing the pixel positions based on a secret key [10]. It assigns a pixel to another pixel position in a bijective manner. The discretized Baker map is an efficient tool to randomize the items in a square matrix. . Let $B(n_1, \ldots, n_k)$,

denote the discretized map, where the vector, $[n_1, \ldots n_k]$, represents the secret key, S_{key}. Defining N as the number of data items in one row, the secret key is chosen such that each integer n_i divides N, and $n_1+\ldots,+n_k = N$.

Let $Ni = n_1+\ldots,+n_{i-1}$. The data item at the indices (r, s), is moved to the indices [70]:

$$B(r,s) = \left[\frac{N}{n_i}(r - N_i) + s \bmod \left(\frac{N}{n_i}\right), \frac{n_i}{N}\left(s - s \bmod \left(\frac{N}{n_i}\right)\right) + N_i\right]$$

Where $N_i \le r < N_{i+ni}$, $0 \le S < N$, and $N_1 = 0$.

In steps, the chaotic permutation is performed as follows:

A square matrix of N×N is divided into N rectangles of width n_i and number of elements N.

The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from left to right beginning with upper rectangles, then the lower ones.

Inside each rectangle, the scan begins from the bottom left corner towards upper elements.

Fig. (1) shows an example of the chaotic interleaver of an 8 × 8 square matrix (i.e., N = 8). The secret key, $S_{key} = [n_1, n_2, n_3] = [2, 4, 2]$.

B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8
B_9	b_{10}	B_{11}	B_{12}	B_{13}	B_{14}	B_{15}	b_{16}
B_{17}	B_{18}	B_{19}	B_{20}	B_{21}	B_{22}	B_{23}	B_{24}
B_{25}	B_{26}	B_{27}	B_{28}	B_{29}	B_{30}	B_{31}	B_{32}
B_{33}	B_{34}	B_{35}	B_{36}	B_{37}	B_{38}	B_{39}	B_{40}
B_{41}	B_{42}	B_{43}	B_{44}	B_{45}	B_{46}	B_{47}	B_{48}
B_{49}	B_{50}	B_{51}	B_{52}	B_{53}	B_{54}	B_{55}	B_{56}
B_{57}	B_{58}	B_{59}	B_{60}	B_{61}	B_{62}	B_{63}	B_{64}

(A) The 8×8 matrix divided

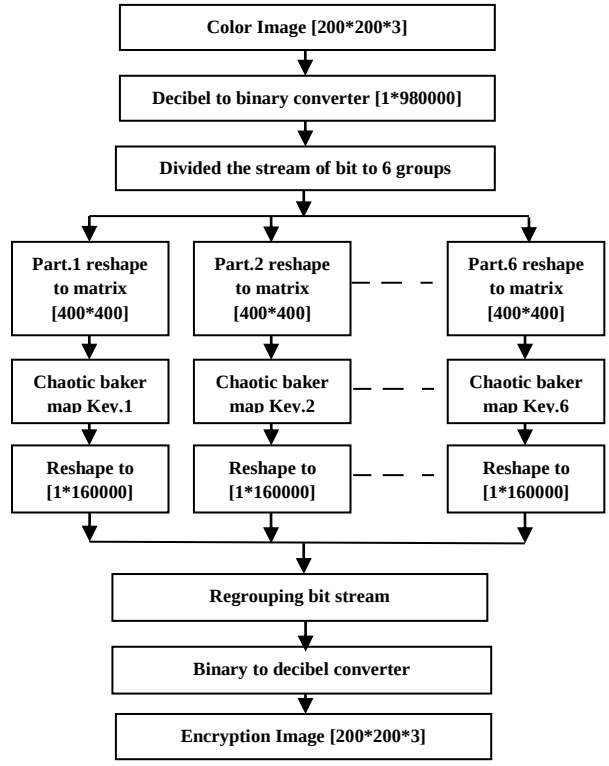
B_{31}	B_{23}	B_{15}	B_7	B_{32}	B_{24}	B_{16}	B_8
B_{63}	B_{55}	B_{47}	B_{39}	B_{64}	B_{56}	B_{48}	B_{40}
B_{11}	B_3	B_{12}	B_4	B_{13}	B_5	B_{14}	B_6
B_{27}	B_{19}	B_{28}	B_{20}	B_{29}	B_{21}	B_{30}	B_{22}
B_{43}	B_{35}	B_{44}	B_{36}	B_{45}	B_{37}	B_{46}	B_{38}
B_{59}	B_{51}	B_{60}	B_{52}	B_{61}	B_{53}	B_{62}	B_{54}
B_{25}	B_{17}	B_9	B_1	B_{26}	B_{18}	B_{10}	B_2
B_{57}	B_{49}	B_{41}	B_{33}	B_{58}	B_{50}	B_{42}	B_{34}

(B) chaotic interleaving of the matrix.

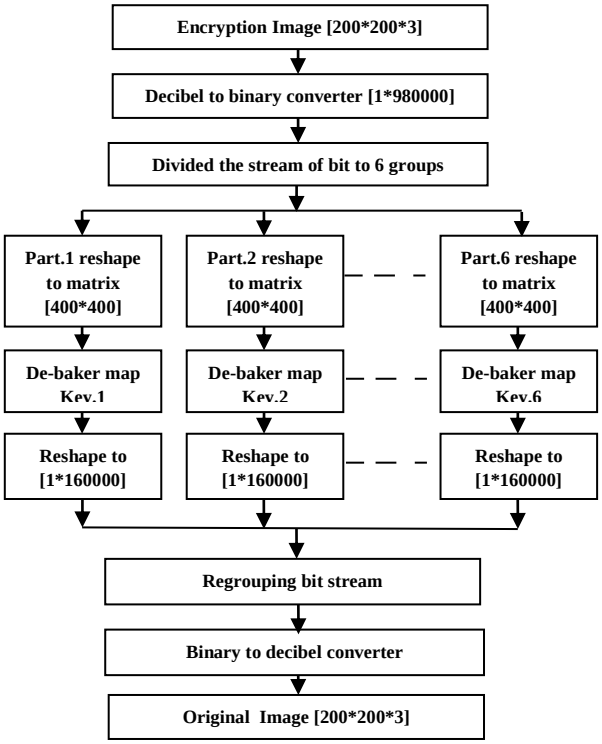
Fig.(1) Chaotic interleaving of an 8×8 matrix.

3. Proposed Modification

In this section, operations nearly returned the same operations in the previous section, but the processing on the bits, we will increase the size of the matrix to which they apply in chaotic Interleaver, that represent each pixel from an image will converted to 8-bit for read color, 8-bit for green color and 8-bit for blue color (24-bit for each pixel in color image). The key of Chaotic will increase in the encryption and decryption. This leading to more permutation in the original image hence these yields to more security, s show in flowchart (2).



(A) Encryption Image



(B) Decryption Image

Flowchart.(2) Chaotic Baker Map Bit interleaving.

4. Results and Discussion

The simulation and Evaluation of encryption and decryption color image by chaotic baker map bit interleaver. It is performed and the performance of color image in the terms of Histogram. Fig. (3) shows Encryption and Decryption color image and histogram performance by chaotic baker map pixel interleaver.

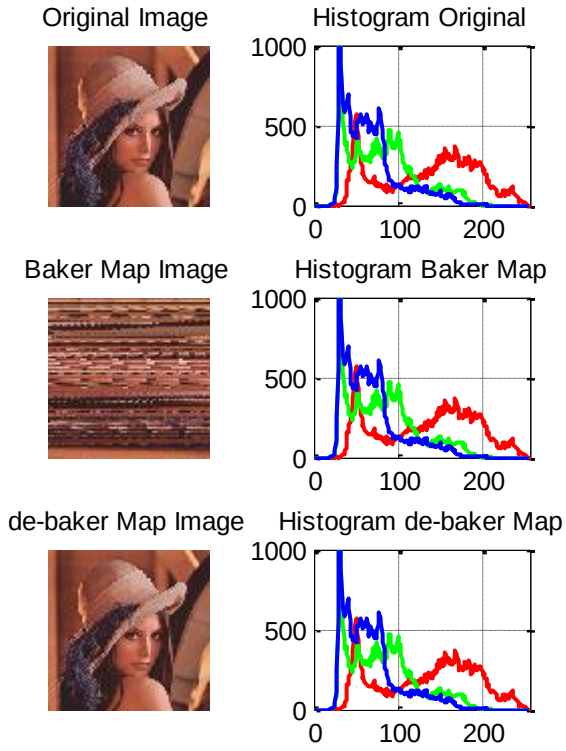
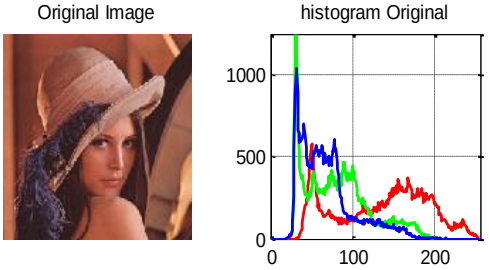


Fig.(3)Encryption and Decryption Color Image By Chaotic Baker Map Pixel Interleaver and Histogram

Fig. (4) Shows Encryption and Decryption color image and histogram performance by chaotic baker map bit interleaver.



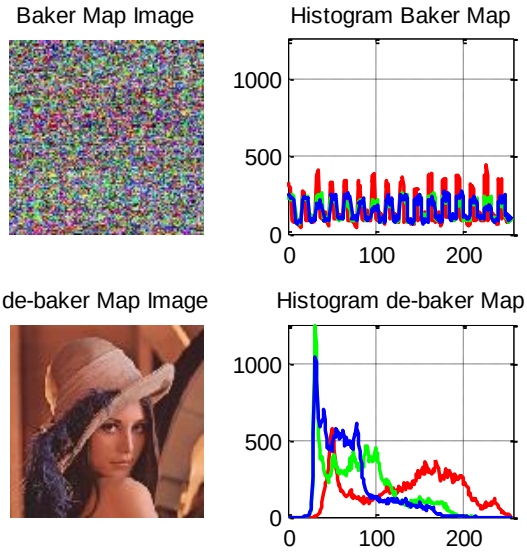


Fig.(4)Encryption and Decryption Color Image By Chaotic Baker Map Bit Interleaver and Histogram

Histogram analysis of three channels (red, green, and blue) of the original image and encrypted images in chaotic baker map in pixel and bit interleaver. The results also indicate that image incryption in pixel shows the worst performance of histogram compared with image incryption in bit. It is observed that the histograms of the encrypted image in pixel are the similar histogram of original image that mean the encryption image in pixel interleaver is not change the level values of pixel just change position, although the histogram of the encryption image was highly non-uniform, where observed that the histograms of the encrypted image in bit are significantly uniform and different from that of the original image that mean the encryption image in bit interleaver is change the level values and position of pixel. One can see that the histogram encryption image in bit interleaver has much better statistic character, that means the resulting substitution cipher can create a random looking image with uniform histogram, so the image can be will hidden.

REFERENCES

[1] L. Zhang, X. Liao and X. Wang, "An image encryption approach based on chaotic maps", Chaos, Solitons & Fractals, 24(3), 759-765, 2005.

[2] G. Chen, Y. Mao and C. Chui, "A symmetric encryption scheme based on 3D chaotic cat map", Chaos, Solitons & Fractals, 21: 749-761, 2004.

[3] L. Kocarev, G. Jakimoski, T. Stojanovski and U. Parlitz, "From chaotic maps to encryption schemes", Proc. IEEE Int. Sym. on Circuits and Systems, IV: 514-517, Monterey, California, June 1998.

[4] Y. Mao, G. Chen and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker

maps", International Journal of Bifurcation and Chaos, 14(10): 3613-3624, 2004.

[5] J. C. Yen and J. I Guo, "A new key-based design for image encryption and decryption", Proceedings of the IEEE Circuits and Systems, 4, 49-52, 2000.

[6] 0. Watanabe, A. Nakazaki and H. Kiya, "A scalable encryption method allowing backward compatibility with JPEG2000 images," IEEE International Symposium on Circuits and Systems, 6324 -6327, 23-26 May 2005.

[7] J. Fridrich, "Symmetric ciphers based on two-dimensional chaotic maps", Int. J. Bifurcation and Chaos, 8(6): 1259-1284, 1998.

[8] J. Fridrich, "Secure Image Ciphering Based on Chaos", Final Report for AFRL, Rome NY, March 1997.

[9] G. Jakimoski and L. Kocarev, "Chaos and cryptography: Block encryption ciphers based on chaotic maps", IEEE Trans. on Circuits and. Systems, 48(2): 163-169, 2001.

[10] Mohsen A. M. M. et al, "An Efficient Chaotic Interleaver for Image Transmission over IEEE 802.15.4 Zigbee Network", Journal of telecommunication and information technology 2/2011.

BIOGRAPHIES

Safa Ahmed Al-Waely. Date of the birth is 18/1/1988. Academic Qualification: Bachelor's Degree, Communication Engineering, Al-Hussain University College, Karbala, Iraq (2010). Master's Degree, Electrical Engineering, Department Communication Engineering, University of technology, Baghdad, Iraq (2015). Working Experience: 2015-until the present: Assistant lecturer, Al-Hussain University College, Karbala, Iraq.

Mortada Abdulraheem Hayder. Date of the birth is 11/1/1986. Academic Qualification: Bachelor's Degree, Computer Techniques Engineering, Al-Rafdeen University College, Baghdad, Iraq (2011). Working Experience: 2012-until the present: Laboratory computer management, University of Karbala, Karbala, Iraq.

Zaid Salah Abdulsattar. Date of the birth is 23/8/1985. Academic Qualification: Bachelor's Degree, Software Engineering, Al-Mansour University College, Baghdad, Iraq (2011). Working Experience: 2012-until the present: Scientific Affairs, University of Karbala, Karbala, Iraq.

Ola Hamzah Rasool. Date of the birth is 11/3/1987. Academic Qualification: Bachelor's Degree, Dep. of Computer Science, University of Babylon, Babylon, Iraq (2009). Working Experience: 2012-until the present: Scientific Affairs, University of Karbala, Karbala, Iraq.

Marwah Adil Hasan. Date of the birth is 20/10/1994. Academic Qualification: Bachelor's student, last year, Computer Engineering, Al-Hussain University College, Karbala, Iraq.(2017).