ISSN 2348-375X

Unique Journal of Engineering and Advanced Sciences

Available online: www.ujconline.net

Research Article

OPTICAL IMAGE ENCRYPTION AND DATA HIDING USING DRPE AND AES ON CHAOTIC BAKEREDE IMAGE

Narmatha P[1*], Sabarmathi D[2], Anbukaruppusamy S[2], Manikandaprabu N[3]

[1]PG Scholar, Shree Venkateshwara Hi-tech Engineering College, TN, India
[2]Associate professor, Department of ECE, Shree Venkateshwara Hi-tech Engineering College,TN, India
[3]Assistant Professor, Department of ECE, Nandha Engineering College, Erode, TN, India

Received: 24-01-2014; Revised: 23-02-2014; Accepted: 22-03-2014

*Corresponding Author: **Narmatha P**
PG Scholar, Shree Venkateshwara Hi-tech Engineering College, TN, India pnarmathaece@gmail.com

ABSTRACT

In every communication channel or methodology now days, there is a necessity of secure transmission from sender to the authentic receiver. In this paper a new technique for optical image encryption based on chaotic Baker map, AES and Double Random Phase Encoding (DRPE) is presented. This technique is implemented in three layers to enhance the security level of the classical DRPE. At first layer a pre-processing layer, which is performed with the chaotic Baker map on the original image. Then AES algorithm is used to encrypt the image for the security and confidentiality of the image. A message is also stored in the pixels of the image. After AES encryption the classical DRPE is done. DRPE is done using two random phase masks, one in the input plane and the other in the fourier plane, to encrypt the primary image in to stationary white noise. MATLAB simulation experiments show that the proposed technique enhances the security level of the DRPE, and at the same time has a better immunity to noise .Histogram analysis ,maximum deviation analysis, and irregular deviation analysis are performed to check the effectiveness of the method.

Keywords: DRPE, AES, Chaotic Baker Map.

INTRODUCTION

Image Processing is a technique to enhance raw images received from cameras/sensors placed on satellites, space probes and aircrafts or pictures taken in normal day-to-day life for various applications. During the last four to five decades several techniques have been developed in the field of Image Processing. Most of the techniques developed are for enhancing the images obtained from unmanned spacecrafts, space probes and military flights. Image Processing systems are becoming popular due to easy availability of powerful personnel computers, large size memory devices, graphics software's etc[1,2].

Digital computers are used to process the image. The image will be converted to digital form using a scanner digitizer) and then process it. It is defined as the subjecting numerical representations of objects to a series of operations in order to obtain a desired result. It starts with one image and produces a modified version of the same. It is therefore a process that takes an image into another. The term digital image processing generally refers to processing of a two-dimensional picture by a digital computer[3]. In a broader context, it implies digital processing of any two-dimensional data. A digital image is an array of real numbers represented by a finite number of bits. The principle advantage of Digital Image Processing methods is its versatility, repeatability and the preservation of original data precision[4].

Encryption (sometimes called as encipherment) is the process of transforming a piece of information (known as the plaintext) using an algorithm (known as the cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key. The output is known as the cipher text. The reverse process of transforming cipher text to plaintext is known as decryption (sometimes called as decipherment).

Over the years extensive studies have been carried out to apply coherent optics methods in real-time communications and image transmission. This is especially true when a large amount of information needs to be processed, e.g., in high-resolution imaging. The recent progress in data-processing networks and communication systems has considerably increased the capacity of information exchange. However, the transmitted data can be intercepted by unauthorized people. This explains why considerable effort is being devoted at the current time to data encryption and secure transmission. In addition, only a small part of the overall information is really useful for many applications. Consequently, applications can tolerate information compression that requires important processing when the transmission bit rate is taken into account. To enable efficient and secure information exchange, it is often necessary to reduce the amount of transmitted information. In this context, much work has been undertaken using the principle of coherent optics filtering for selecting relevant information and encrypting it. Compression and encryption operations are often carried out separately, although they are strongly related and can influence each other. Optical processing methodologies, based on filtering are described that are applicable to transmission &/or data storage. The global economic infrastructure is becoming increasingly dependent on information technology, with computer and communication technology being essential and vital components of government facilities, power plant systems, medical infrastructures, financial centers, and military installations, to name a few. Finding effective ways to protect information systems, networks, and sensitive data within the critical information infrastructure is challenging even with the most advanced technology and trained professionals. The increasing number of information-security-related incidents, organized crimes, and phishing scams means that securing information is becoming a major issue in the current information-based economy[5].

To secure information, many research directions have been suggested in the past decade. Some security systems rely on the secrecy of the protocol for the algorithm encoding the information or on cryptography (software approaches), and some rely on aspects of the architecture (hardware approaches). In fact, electronic devices consume power, take time to compute, and emit electromagnetic radiation highly correlated with the decoding processing. In this tutorial we focus on the software approach. We distinguish two kinds of software solution. First, there are solutions based on cipher techniques, like the symmetric Data Encryption Standard (DES) or asymmetric Rivest–Shamir–Adleman (RSA) .As these techniques rely on factorials of large numbers, they are easily correlated to hardware aspects. The second type of solution consists in encoding the input image into two chosen noise functions by using the 4fsetup, i.e., convolution between the input image multiplied by the first noise function and the impulse response of the second function noise[6].

DRPE

Without any prior information about the spectral modification or the target image at the receiver, the image decoding cannot be done. The main idea of this approach, depends on inserting two encoding keys (random phase) in a setup called "4f". The Setup is an optical system consisting of two cascaded lenses separated by two focal lengths, with each of the input and output image planes one focal length outside the lens system from different directions (i.e., the total length is four focal lengths, hence "4f").

The decryption process uses the same Fourier Random Phase Mask (RPM) as in the encryption process. The DRPE, when applied in an optical processor, requires the complex conjugate Fourier phase key to decrypt the image. The DRPE consists mainly of three stages:

1. The first key, i.e., the RPM1, is multiplied by the target image to be encrypted. The resulting image should be displayed in the input plane of the "4f" setup and lighted with a parallel coherent light resulting from a Laser generator. This procedure introduces the first modification to the spectrum of the target image.
2. The second key, i.e., RPM2, is directly inserted into the image spectrum in the Fourier plane. The multiplication of the RPM2 by the spectrum obtained in the first stage can introduce the second modification into the spectrum of the target image.
3. A second optical Fourier transform is carried out using a second lens to obtain the encoded image in the original 2-D space of images.

To explain the DRPE in detail, we consider a primary intensity image $f(x,y)$ with positive values, where x and y denote the spatial domain coordinates. Also, v and η denote the Fourier domain coordinates. Let $\psi(x,y)$ denote the encrypted image, and $n(x,y)$ and $m(x,y)$, denote two independent white sequences uniformly distributed in $[0,2\pi]$. To encode $f(x,y)$ into a white stationary sequence, two RPMs are used, $\psi_n(x,y)=\exp[2i\pi n(x,y)]$ and $\psi_m(x,y)=\exp[2i\pi m(x,y)]$. $h(x,y)=m(x,y)$ is a phase function uniformly distributed in $[0,2\pi]$. The second RPM, $\psi_m(v,\eta)$, is the Fourier transform of the function $h(x,y)$, $FT\{h(x,y)\}=\hat{h}(v,\eta)=$

$$\psi_m(v,\eta)=\exp[2i\pi m(v,\eta)] \qquad (1)$$

The encryption process consists of multiplying the primary image by the first RPM $\psi_n(x,y)$. The result is then convolved with the function $h(x,y)$. The encrypted function is complex, with amplitude and phase, and is given by the following expression:

$$\psi(x,y)=\{f(x,y)\psi_n(x,y)\}*FT^{-1}\{\psi_m(v,\eta)\} \qquad (2)$$

where the symbol ($*$) denotes convolution. The encrypted function in (2) has a noise-like appearance that does not reveal the content of the primary image. Regarding the amplitude-coded primary image $f(x,y)$, (2) is a linear operation.

In the decryption process, $\psi(x,y)$ is Fourier transformed, multiplied by the complex conjugate of the second RPM $\psi_m(v,\eta)$ that acts as a key, and then inverse Fourier transformed. As a result, the output is

$$FT^{-1}\{FT[\psi(x,y)]\psi_m^*(v,\eta)\}=$$

$$FT^{-1}\{FT[f(x,y)\psi_n(x,y)]\psi_m(v,\eta)\psi_m^*(v,\eta)\} \qquad (3)$$

whose absolute value turns out the decrypted image $f(x,y)$ .The whole encryption–decryption method can be implemented either digitally or optically. In the encryption process, the $4f$-processor has the first RPM stuck to the primary image in the input plane and the second RPM in its Fourier plane. In the output plane, the encrypted function is recorded, in amplitude and phase, using holographic techniques. In the decryption process, the $4f$-processor has the encrypted function in the input plane and the key that is the complex conjugate of the second RPM, in its Fourier plane. In the output plane, the decrypted image is recovered using an intensity-sensitive device such as a CCD camera[7].

Optical information can be hidden either in the complex-amplitude form or in the phase-only form or in the amplitude-only form. If the encrypted data $\psi(x,y)$ are complex (amplitude and phase) functions, such as those described in the method originally proposed by Refregier and Javidi[1], then there are some practical constraints to encode them. However, if the encrypted data can be either phase or amplitude only, then the recording and storage is easier[8].

The phase is often chosen to encode, convey, and retrieve information for many reasons such as higher efficiency, invisibility to the naked eye, and more security than the amplitude. Towghiet al. modified the linear encoding technique of the DRPE by introducing a nonlinear (full-phase) encoding, for which a phase-only version of the primary image is encoded[2]. Thus, the fully phase-encrypted image is given by the following equation:

$$\psi_p(x,y)=\left\{\exp\left[i\pi f(x,y)\right]\psi_n(x,y)\right\}*h(x,y)=$$

$$\left\{\exp\left[i\pi f(x,y)\right]\psi_n(x,y)\right\}*FT^{-1}\left\{\psi_m(v,\eta)\right\} \qquad (4)$$

And it can be generated either optically or electronically in a way similar to that described in (2). The same optical setup is used for decryption, but in this case, the complex conjugate of both RPMs referred to as keys, are necessary for decryption.

$$\psi_n^*(x,y)=\exp\left[-2i\pi n(x,y)\right] \text{ and}$$

$$\psi_m^*(v,\eta)=\exp\left[-2i\pi m(v,\eta)\right], \qquad (5)$$

The Fourier phase key $\psi_m^*(v,\eta)$ is placed in the Fourier plane, whereas the phase key $\psi_n^*(x,y)$ is placed at the output plane of the optical processor. The phase-only version of the primary image $\exp\left[i\pi f(x,y)\right]$ is recovered in the spatial domain. The primary image $f(x,y)$ can be visualized as an intensity distribution by extracting the phase of $\exp\left[i\pi f(x,y)\right]$ and dividing it by π.

Double random phase encoding (DRPE), which is used to encrypt a plain image by means of random phase modulations on spatial domain and Fourier domains respectively, is a typical technique for applying optical information processing methods to information security. DRPE is a combination of data ciphering and pattern matching; that is, the degree of restoration of the plain image reproduced in the decrypted image depends on the degree of similarity between two key images used in the encryption and decryption process. Therefore, the key image used in DRPE is allowed to include some redundancy between encryption and decryption. Biometrics information, which is difficult to be used as a cipher key on conventional cryptographic technology because of variety of acquired data, can be used as a cipher key by employing DRPE. As an application of this method, we proposed a smart card authentication system, which is a combination of fingerprint verification and conventional personal identification number (PIN) verification systems. In this system, a PIN is encoded to a bit pattern image, encrypted by a fingerprint image, and recorded as a hologram on a smart card. In addition, we proposed a file encryption system in which fingerprints are used as a key; in this system, a file is encrypted using a common-key cryptosystem and the common key is encrypted by DRPE using a fingerprint as a cipher key. However, it has recently been reported that DRPE is vulnerable to certain types of attacks such as the chosen cipher text attack, chosen plaintext attack, and known plaintext attack (KPA).

AES ALGORITHM

AES comes in three favors, namely AES - 128, AES -192, and AES-256, with the number in each case representing the size (in bits) of the key used. All the modes are done in 10, 12 or 14 round depends on the size of the block and the key length chosen. AES merely allows a 128 bit data length that can be divided into four basic operation blocks. These blocks operate on array of bytes and organized as a 4*4 matrix that is called the state. The algorithm begins with an Add round key stage followed by nine rounds of four stages and a tenth round of three stages which applies for both encryption and decryption algorithm.

These rounds are governed by the following four stages:

- Substitute Bytes
- Shift rows
- Mix columns
- Add round key

  The tenth round Mix columns stage is not included. The first nine rounds of the decryption algorithm are governed by the following four stages:
- Inverse Shift rows
- Inverse Substitute Bytes
- Add round key
- Inverse Mix columns

Again the tenth round Inverse Mix columns stage is not included. The Overall flow of the encryption and decryption algorithm of the AES algorithm is show in Figure 1. Substitute Bytes: Is a non linear byte substitution, using a substation table (S-box) each byte from the input state is replaced by another byte. The substitution is invertible and is constructed by the composition of two transformations as described below [2] [8]. The substitute bytes operation is as shown in Figure 3.

1. The state bytes are constructed by multiplicative inverse in the finite field GF (2^8) that is used in the AES. This field is derived using the following irreducible polynomial of degree 8:

$$m(x)=x^8+\mathrm{x}^4+\mathrm{x}^3+\mathrm{x}+1$$

2. Affine transformation is applied on the result of above statement. The fixed matrix and the fixed vector over GF (2) in the affine transformation are shown in the Figure 2.

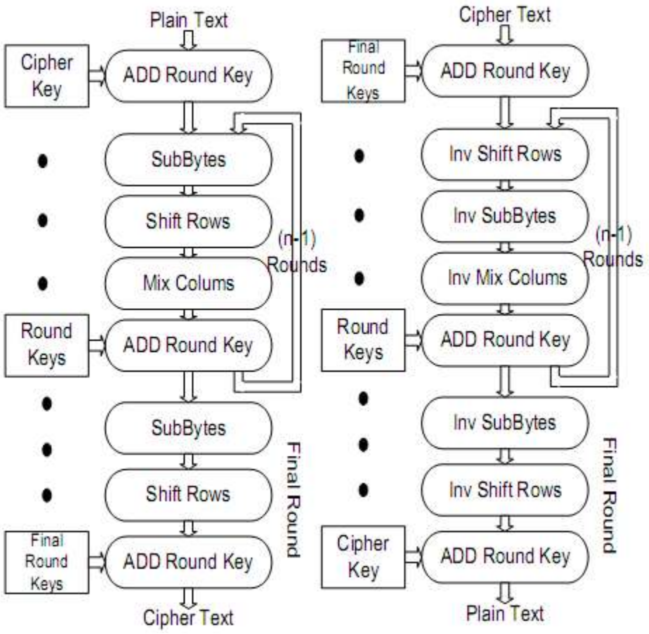


Figure 1: Design flow of AES Algorithm (a) Encryption Process (b) Decryption Process

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} * \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{bmatrix} + \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{bmatrix}$$

Figure 2: Affine transformation of Substitute Bytes

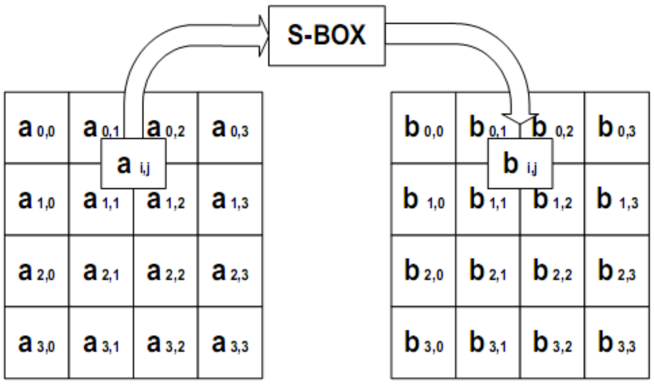


Figure 3: Substitute Bytes Operation

Inverse Substitute Bytes: Is the reverse operation of the Substitute Bytes transformation, in which the inverse S-box is applied to each byte of the State. This is obtained by applying the inverse of the affine transformation followed by taking the multiplicative inverse in GF (2^8). Shift rows: In the Shift Rows transformation, the first row of the state array remains unchanged. The bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the left, respectively as shown in Figure 4. Inverse Shift rows: Is the inverse of the shift rows, the first row of the state array remains unchanged. The bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the right, respectively.

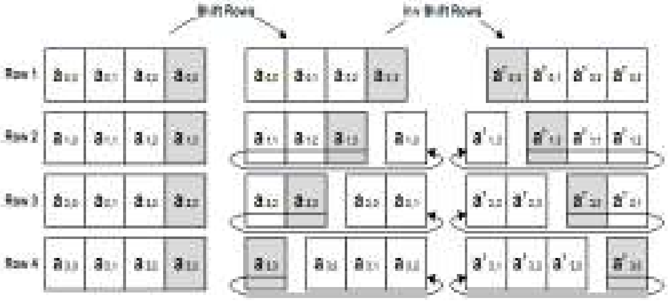


Figure 4: Shift Rows Operation

Mix columns: In the Mix Columns transformation, every column of the state array is considered as polynomial over GF (2^8). After multiplying x^4+1 with a fixed polynomial a(x) [2], the operation of MixColumn is as shown in Figure 5.

$$a(x) = 03*x^3 + 01*x^2 + 01*x + 02$$

The result is the corresponding column of the output state is as shown in Figure 5. As it can be noticed this operation requires multiplication by „two“ and „three“ that is relatively simple shift operation in hardware.

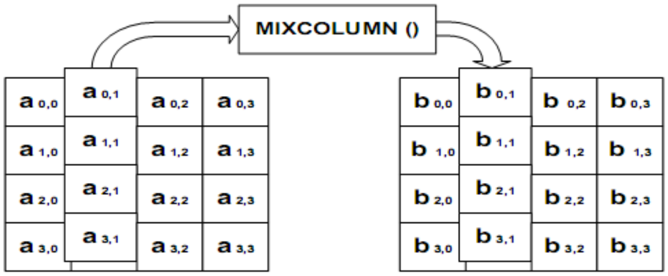


Figure 5: MixColumn Operation

Inverse Mix columns: In the Inverse Mix Columns transformation, every column of the state array is considered a polynomial over GF (2^8). After multiplying modulo x^4+1 with a fixed polynomial b(x),

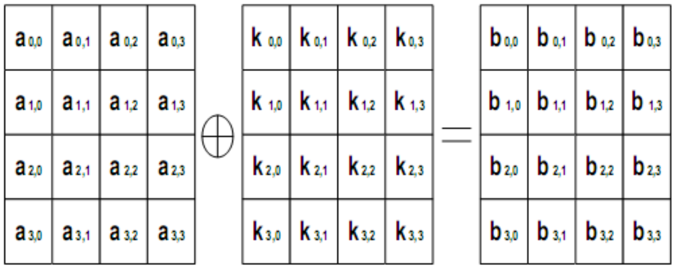
$$b(x)=0B*x^3 + 0D*x^2 + 09*x + 0E$$

The result is the corresponding column of the output state. As it not so straightforward hardware implementation as Mix column, so if we compare both, InvMixCol requires more logic resources for implementation.

Addroundkey: The AddRoundKey operation is as shown in Figure 6, which is a simple XOR operation between the State and the Round Key. The Round Key is derived from the Cipher key by means of key schedule process. The State and Round Key are of the same size and to obtain the next State an XOR operation is done per element:

b (i, j) = a (i, j) $\oplus$ k (i, j)

Where a is the current State, b the next State and k the round Key



$$\begin{bmatrix} a_{0,0} & a_{0,1} & a_{0,2} & a_{0,3} \\ a_{1,0} & a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,0} & a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,0} & a_{3,1} & a_{3,2} & a_{3,3} \end{bmatrix} \oplus \begin{bmatrix} k_{0,0} & k_{0,1} & k_{0,2} & k_{0,3} \\ k_{1,0} & k_{1,1} & k_{1,2} & k_{1,3} \\ k_{2,0} & k_{2,1} & k_{2,2} & k_{2,3} \\ k_{3,0} & k_{3,1} & k_{3,2} & k_{3,3} \end{bmatrix} = \begin{bmatrix} b_{0,0} & b_{0,1} & b_{0,2} & b_{0,3} \\ b_{1,0} & b_{1,1} & b_{1,2} & b_{1,3} \\ b_{2,0} & b_{2,1} & b_{2,2} & b_{2,3} \\ b_{3,0} & b_{3,1} & b_{3,2} & b_{3,3} \end{bmatrix}$$

Figure 6: Add Round Key Operation

There are three steps, in each Key schedule round [6]. Keyrotate: The function Keyrotate takes a four-byte word and rotates one byte to the left.

Keysubytes: The Keysubytes operation takes four-byte input word by substituting each byte in the input to another byte according to the S-Box.

KeyRcon: The first byte of a word is XORed with the round constant. Each value of the Rcon table is a member of the Rinjdael finite field. Add round key is same for the both encryption and decryption[9].

CHAOTIC BAKERMAP

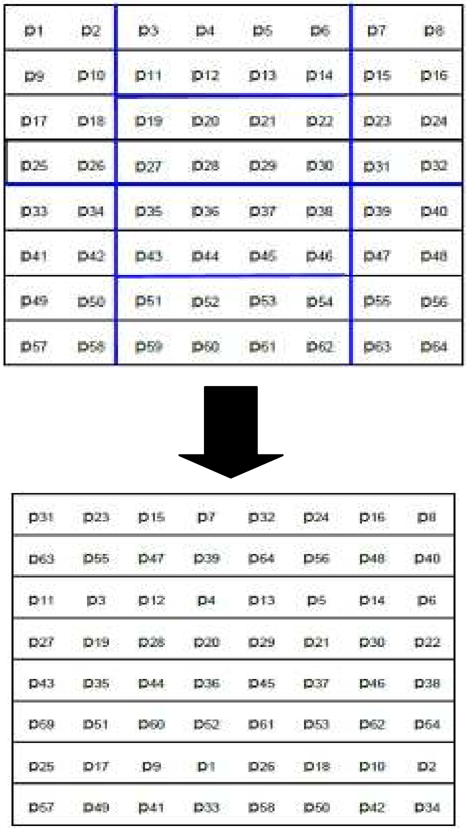
Chaos has been widely used in cryptography in recent years However, some actual digital chaos systems face the problem of degradation dynamics .The two-dimensional chaotic maps can 'stretch-and-fold' images by use of the natural features of images. Small changes in keys for a plain image can diffuse to everywhere in an encrypted image. At the same time, the analysis of keys is very difficult because there are too many combinations of encryption. Typical chaotic maps used for image encryption include the cat map, the baker map, the standard map the tent map etc. Fridrich proposes a class of invertible encryption systems based on the baker map. It uses a two-dimensional chaotic map to permute the position of pixels. The permutations induced by the baker map behave as typical random permutations. The encryption has good diffusion properties with respect to the plain image and the keys. However, the baker map does not have a simple formula and the keys are limited by the size of the image[10].

Baker Map Based Image Encryption presents the detailed implementation of the chaos based image encryption algorithm that we implemented. The procedure that we present here was implemented and tested and is based on the work of Mao. In turn, their work is based on the general framework provided by Fridrich. In dynamical systems theory, the baker's map is a chaotic map from the unit square into itself. It is named after a kneading operation that bakers apply to dough: the dough is cut in half, and the two halves are stacked on one another, and compressed[11].

The baker's map can be understood as the bilateral shift operator of a bi-infinite two-state lattice model. The baker's map is topologically conjugate to the horseshoe. In physics, a chain of coupled baker's maps can be used to model deterministic diffusion. The Poincare recurrence time of the baker's map is short compared to Hamiltonian maps. Many deterministic dynamical systems, the baker's map is studied by its action on the space of functions defined on the unit square. The baker's map defines an operator on the space of functions, known as the transfer operator of the map. The baker's map is an exactly solvable model of deterministic chaos, in that the Eigen functions and Eigen values of the transfer operator can be explicitly determined[12].

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 M x M by changing the pixel positions based on a secret key [12]. It assigns a pixel to another pixel position in a bijective manner. The disretized Baker map is denoted by B(v1,v2,… v_k) , where the sequence of k integers, is chosen such that each integer v_i divides M , and M_i=v1+v2+…+v_i . The pixel at indices (l,s) , $M_i < M_i + v_i$ with and 0<s<M is mapped to

$$B_{(n_1......n_k)}(l,s) = \left[\frac{M}{v_i}(l - M_i) + s \bmod \frac{M}{v_i}, \frac{v_i}{M}(s - s \bmod \frac{M}{v_i}) + M_i \right]$$



p1	p2	p3	p4	p5	p6	p7	p8
p9	p10	p11	p12	p13	p14	p15	p16
p17	p18	p19	p20	p21	p22	p23	p24
p25	p26	p27	p28	p29	p30	p31	p32
p33	p34	p35	p36	p37	p38	p39	p40
p41	p42	p43	p44	p45	p46	p47	p48
p49	p50	p51	p52	p53	p54	p55	p56
p57	p58	p59	p60	p61	p62	p63	p64

p31	p23	p15	p7	p32	p24	p16	p8
p63	p55	p47	p39	p64	p56	p48	p40
p11	p3	p12	p4	p13	p5	p14	p6
p27	p19	p28	p20	p29	p21	p30	p22
p43	p35	p44	p36	p45	p37	p46	p38
p59	p51	p60	p52	p61	p53	p62	p54
p25	p17	p9	p1	p26	p18	p10	p2
p57	p49	p41	p33	p58	p50	p42	p34

Figure 7: Chaotic Randomization of an 8X8 Matrix with a Secret Key S=[2,4,2]

This formula is implemented in the following steps:

- The square matrix MxM is divided into k rectangles of width v_i and number of elements M.
- The elements in each rectangle are rearranged to a row in the permuted rectangle. Rectangles are taken from right to left beginning with upper rectangles, and then lower ones.

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

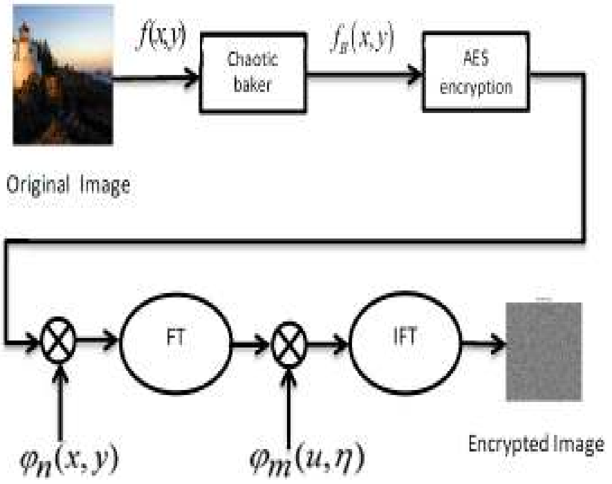


Figure 8: Block Diagram of Proposed Encryption Process

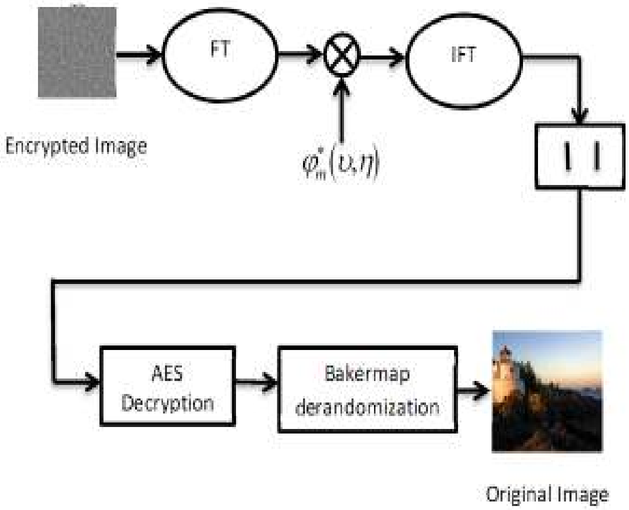


Figure 9: Block Diagram of Proposed Decryption Process

Double Random Phase Encoding (DRPE) was proposed by Refregier and Javidi in 1995 to encrypt an input image. The input image is disarranged by two random phase masks, located at input and Fourier planes in a 4f optical system. Since encryption and decryption keys are conjugate to each other, DRPE can be regarded as a symmetrical key system. To reconstruct the input image, decryption keys (random phase masks) are required to be sent through a secure channel[13]. Sending large phase masks is a major shortcoming of DRPE method. Real and imaginary parts of the encoded image are embedded into a large enough normalized host image after being modulated with sine and cosine function. The modulation process reduces visual degradation and enhances its transparency.The DRPE presented by Refregier and Javidi is based on the modification of the spectral distribution of the image. Without any prior information about this spectral modification or the target image at the receiver, the image decoding cannot be done.

SIMULATION EXPERIMENTS

Several Matlab experiments have been carried out to test the proposed technique and compare its performance with those of the DRPE and chaotic Baker map encryption. The three images of the Girl, Lena, and Plane shown in Fig. 10 have been used in the experiments. Visual results for the Girl image only are shown in the paper, and the other results are tabulated.

Figure 10 Girl Lena and Plane images (a) Girl (b) Lena (c) Plane

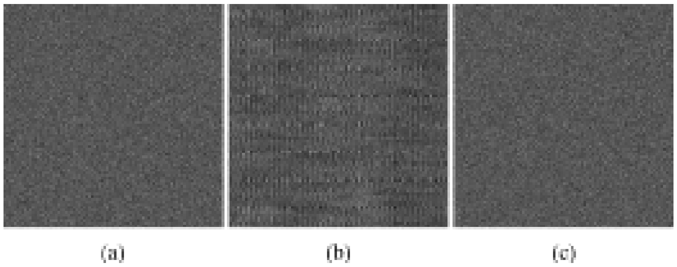


Figure 11: Encrypted Girl image with (a) DRPE, (b) chaotic Baker map, (c) the proposed technique

Histogram analysis of the decrypted and the original images has also been performed to validate the proposed method. For image encryption algorithms, the histogram of the encrypted image should be totally different from the histogram of the original image. Fig. 13 shows the histograms of the encrypted images in Fig. 11 and their decrypted versions. It is clear from this figure that the histograms of the original and decrypted images are identical. It is also clear that the histograms of the encrypted images are different from that of the original image for the DRPE and the proposed technique.

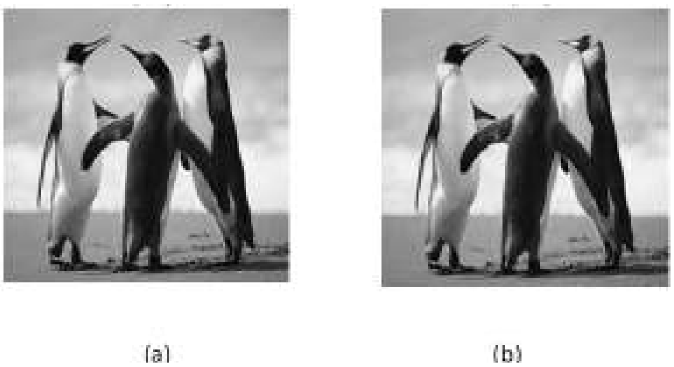


Figure 12: Decrypted images for the DRPE and the proposed technique in the presenceof noise on the encrypted image with variance 0.01. (a) DRPE. (b) Proposed technique.

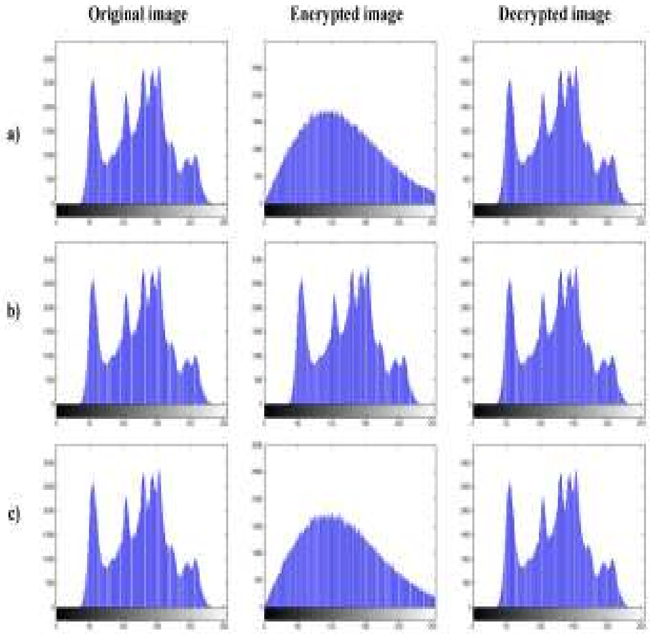


Figure 13 The histograms of the images for (a) DRPE, b) chaotic Baker map encryption, and c) proposed technique.

CONCLUSION

Here, an encryption technique based on chaotic Baker map AES and the DRPE has been presented. The chaotic Baker map is used as a pre-processing layer to increase the security level. The implementation of the proposed technique is simple, and achieves good permutation and diffusion mechanisms in a reasonable time with large immunity to noise, which is a required property for communication applications.

REFERENCES

1. Refregier P and Javidi B, Optical image encryption based on input plane and Fourier plane random encoding, Opt. Lett., 1995; 20: 767–769.
2. Javidi B, Sergent A, Zhang G, and Guibert L, Fault tolerance properties of a double phase encoding encryption technique, Opt. Eng., 1997; 36: 992–998.
3. Unnikrishnan G, Joseph J, and Singh K, Optical encryption by double-random phase encoding in the fractional Fourier domain, Opt. Lett., 2000; 25: 887–889.
4. Kishk S and Javidi B, Information hiding technique with double phase encoding, Appl. Opt., 2002; 41: 5462–5470.
5. Towghi N, Javidi B, and. Luo Z, Fully phase encrypted image processor, J. Opt. Soc. Amer. A, 1999; 16: 1915–1927.
6. Unnikrishnan G and Singh K, Optical encryption using quadratic phase systems, Opt. Commun., 2001; 193: 51–67.
7. Frauel Y, Castro A, Naughton TJ, and. Javidi B, Resistance of the double random phase encryption against various attacks, Opt. Exp., 2007; 15: 10253–10265.
8. Goodman JW, Introduction to Fourier Optics, 2nd ed. New York, NY, USA: McGraw-Hill, 1996.
9. Fridrich J., Symmetric Ciphers Based on Two-Dimensional Chaotic Maps. Singapore: World Scientific, 1998.
10. Honglei Y, Guang-shou W, Ting W, Diantao L, Jun Y, Weitao M, Shaolei FY, and. Yuankao M, An image encryption algorithm based on two dimensional Baker map, in Proc. ICICTA, 2009.
11. Elashry IF, Farag Allah OS, Abbas AM, El-Rabaie S, and El-Samie FEA, Homomorphic image encryption, J. Electron. Imag., 2009; 18(3): 033002-1–033002-14.
12. Javidi B, Optical and Digital Techniques for Information Security New York, Springer Verlag, 2005.
13. Matoba O, Nomura T, Perez-Cabre E, Millan MS, and Javidi B, Optical techniques for information security, Proc. IEEE, 2009; 97(6): 1128–1148.

Source of support: Nil, Conflict of interest: None Declared