# Optical Image Encryption and Data Hiding using Double Random Phase Encoding and Advanced Encryption Standard on Chaotic Baker Mapped Image

Deepak Thomas
Department of Electronics and Communication
Nehru Institute of Engineering and Technology,
Coimbatore, India

T. Prabu
Department of Electronics and Communication
Nehru Institute of Engineering and Technology,
Coimbatore, India

*Abstract*— **In every communication channel or methodology now a 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, Advanced Encryption Standard (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 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 is performed to check the effectiveness of the method**.

***Index Terms—Optical Image, DRPE, AES, Chaotic Baker Map***

## I. INTRODUCTION

The term Digital Image Processing (DIP) generally refers to the processing of a two-dimensional picture by a digital computer. In a broader context, it implies digital processing of any two-dimensional data. The image is converted to digital form using a scanner or digitizer and then process it. It is the 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.

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. Encryption is the process of transforming a piece of information using an algorithm 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.

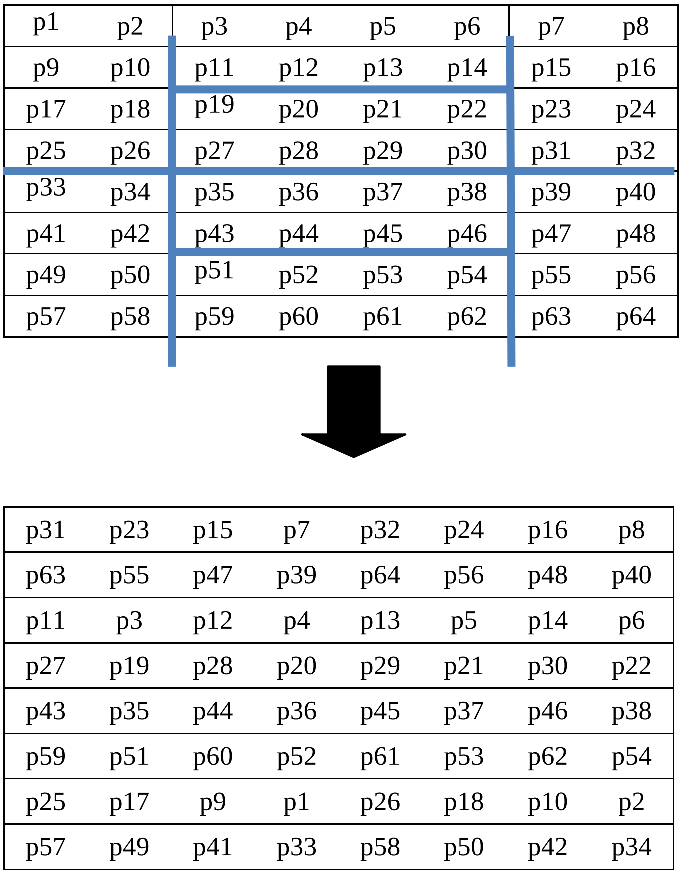
The optical encryption techniques play an important role in several fields like medical or biometric images for storage and transmission, video conferencing over optical fiber, military applications, online banking systems, governmental services, identity cards, satellite images etc. Care has to be taken while dealing with images. Problems occur with unauthorized use by hackers. Optical encryption provides a better and safe way for image communication. To retrieve the original optical information at the receiver side, the encryption method and keys are essentially required.

In this paper, first Chaotic Baker Map is applied to the input image. It is a unit square map. It is applied to image dividing the image to different parts. Then data hiding is carried out in the encoded image. After data hiding Advanced Encryption Standard is applied and then Double Random Phase Encoding is done. DRPE method uses two random phase masks, one is used in the input plane and the other in the Fourier plane. DRPE is used to encrypt the primary image into stationary white noise. To meet the high levels of security, DRPE with Chaoticmap pre-processing and AES is proposed in this paper.

The remaining sections of this paper are organized as follows. Section II gives an explanation of the chaotic Baker map and the data hiding technique used in the pre-processing step. Section III gives an explanation of the AES and then the section IV explains the DRPE method used. Section V discusses the proposed technique with required block diagrams. Section VI presents the simulation results. Finally, Section VII gives the conclusion.

## II. CHAOTIC BAKERMAP AND DATA HIDING

The baker's map is used in many deterministic dynamical systems, due to its action on the space of functions defined on the unit square. The baker's map defines an operator on the space of functions, which known as the transfer operator of the map. In the baker's map the Eigen functions and Eigen values of the transfer operator is easily determined.



| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 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 |

Fig.1. Chaotic Randomization of an 8X8 Matrix with a Secret Key S=[2,4,2]

The chaotic Baker map is a well-known tool of image encryption. It is a tool based on permutation which performs the randomization of a square matrix of dimensions $M$ x $M$ . It is done by changing the pixel positions based on a secret key. In this technique a pixel is assigned to another pixel position in a bijective way. The Baker map is denoted by

$$B(v1,v2,\ldots v_k) \qquad (1)$$

where the sequence of $k$ integers, is chosen such that each integer $v_i$ divides $M$ , and

$$M_i = v1+v2+\ldots+v_i \qquad (2)$$

The pixel at indices ($l$,$s$), is mapped to

$$B_{(n_1\ldots\ldots n_k)}(l,s)=$$

$$\left[\frac{M}{v_i}(l-M_i)+s \bmod \frac{M}{v_i}, \frac{v_i}{M}\left(s-s \bmod \frac{M}{v_i}\right)+M_i\right] \qquad (3)$$

where $M_i \le l < M_i + v_i$ and $0 \le s < M$

The square matrix $M$ x $M$ is divided into $k$ rectangles of width $v_i$ and number of elements $M$. Then the elements in each rectangle are rearranged to a row in the permuted rectangle. After that the rectangles are taken from right to left beginning with upper rectangles, and then lower ones. Then the scan begins from the bottom left corner towards upper elements which is done in each rectangle. Figure 1 shows chaotic randomization of an 8X8 matrix with a secret key S=[2,4,2].

Data hiding is done with the help of image pixels. The Least Significant Bit (LSB) of each pixel is changed to store the required message.Thus a byte of message is stored within eight pixels with ine bit of data in the LSB of each pixel. The length of the message is calculated and the first byte of data is the message length.This data hiding is done to the chaotic bakered image and the next stage of image encryption is carried out.

## III .AES ALGORITHM

Advanced Encryption Standard (AES) allows a data length of 128 bits. In AES there are four basic operation blocks which performs substitution of bytes, shifting rows, mixing columns and adding round key. The AES operates on array of bytes which is 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 each and a tenth round of three stages which is carried out for both encryption and decryption. The flow of the AES encryption algorithm is shown in Figure 2.

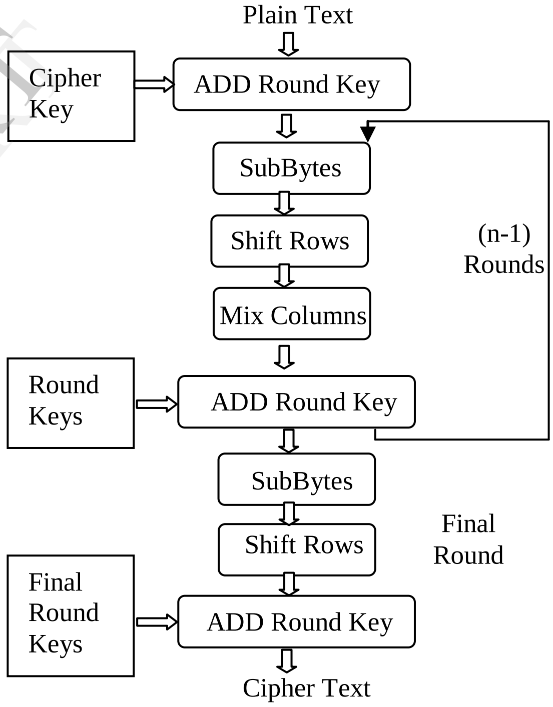


Fig. 2. Design flow of AES Encryption Algorithm

In the tenth round mixing of columns is not included. The first nine rounds of the decryption algorithm are governed by the four stages which includes, inverse shift rows, inverse substitute bytes, add round key and inverse mix columns. Again in the tenth round the inverse mix columns stage is not included. The AES decryption algorithm is explained in Figure 3.

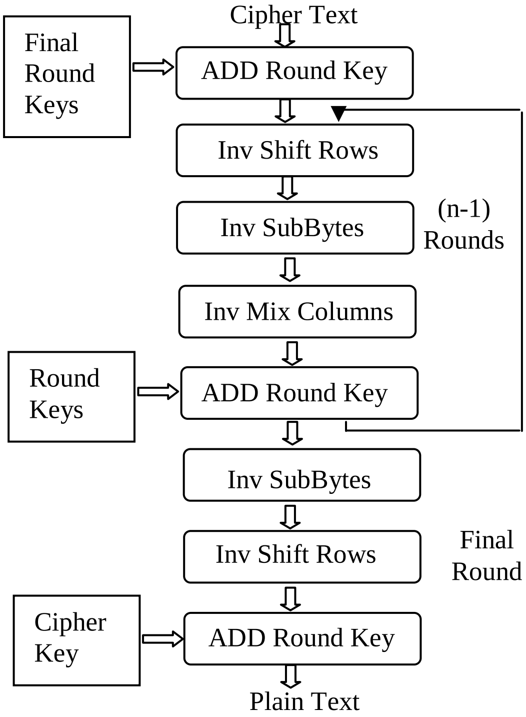
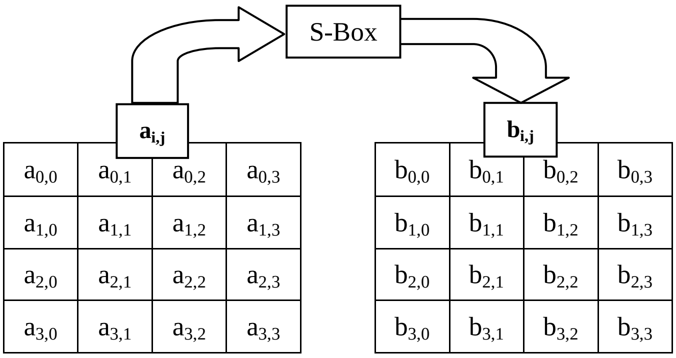


Fig.3. Design flow of AES Decryption Algorithm

The substitute bytes operation is a non linear byte substitution method using a substation table or S-box which is shown in Figure 4. Here each byte from the input state is replaced by another byte from S table. The substitution is invertible. Inverse substitute bytes is the reverse operation of the substitute bytes transformation. In the inverse substitute bytes operation the inverse S-box is applied to each byte of the state.

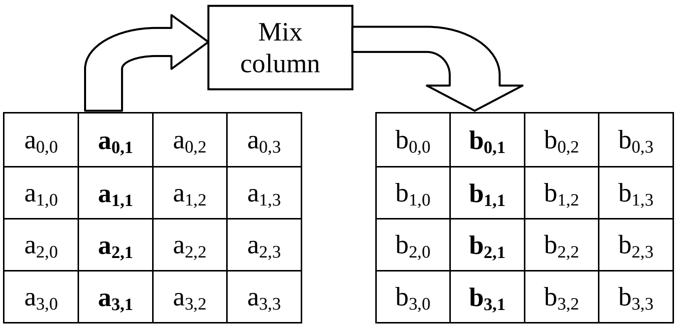


| | | | |
|---|---|---|---|
| $a_{0,0}$ | $a_{0,1}$ | $a_{0,2}$ | $a_{0,3}$ |
| $a_{1,0}$ | $a_{1,1}$ | $a_{1,2}$ | $a_{1,3}$ |
| $a_{2,0}$ | $a_{2,1}$ | $a_{2,2}$ | $a_{2,3}$ |
| $a_{3,0}$ | $a_{3,1}$ | $a_{3,2}$ | $a_{3,3}$ |

| | | | |
|---|---|---|---|
| $b_{0,0}$ | $b_{0,1}$ | $b_{0,2}$ | $b_{0,3}$ |
| $b_{1,0}$ | $b_{1,1}$ | $b_{1,2}$ | $b_{1,3}$ |
| $b_{2,0}$ | $b_{2,1}$ | $b_{2,2}$ | $b_{2,3}$ |
| $b_{3,0}$ | $b_{3,1}$ | $b_{3,2}$ | $b_{3,3}$ |

Fig.4. Substitute Bytes Operation

In the shift rows transformation, the first row of the state array remains unchanged and the bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the left respectively. Inverse shift rows is the inverse of the shift rows operation in which the first row of the state array remains unchanged. And the bytes in the second, third and forth rows are cyclically shifted by one, two and three bytes to the right, respectively. In the mix columns transformation, every column of the state array is considered as a polynomial and they are multiplied with a fixed polynomial. Figure 5 shows the resultant output state. And in the inverse mix columns transformation, every column of the state array is considered as a polynomial.



| | | | |
|---|---|---|---|
| $a_{0,0}$ | $\mathbf{a_{0,1}}$ | $a_{0,2}$ | $a_{0,3}$ |
| $a_{1,0}$ | $\mathbf{a_{1,1}}$ | $a_{1,2}$ | $a_{1,3}$ |
| $a_{2,0}$ | $\mathbf{a_{2,1}}$ | $a_{2,2}$ | $a_{2,3}$ |
| $a_{3,0}$ | $\mathbf{a_{3,1}}$ | $a_{3,2}$ | $a_{3,3}$ |

| | | | |
|---|---|---|---|
| $b_{0,0}$ | $\mathbf{b_{0,1}}$ | $b_{0,2}$ | $b_{0,3}$ |
| $b_{1,0}$ | $\mathbf{b_{1,1}}$ | $b_{1,2}$ | $b_{1,3}$ |
| $b_{2,0}$ | $\mathbf{b_{2,1}}$ | $b_{2,2}$ | $b_{2,3}$ |
| $b_{3,0}$ | $\mathbf{b_{3,1}}$ | $b_{3,2}$ | $b_{3,3}$ |

Fig.5. Mix Column Operation

## III. DRPE

Double Random Phase Encoding (DRPE) is used to encrypt an input image. The input image is rearranged by two random phase masks, one located at the input plane and the other one at the Fourier plane in a 4f optical system. The encryption and decryption keys used are conjugate to each other. So DRPE is regarded as a symmetrical key system. To reconstruct the input image at the receiver side, decryption keys or random phase masks are required to be sent through a secure channel. The decryption process uses the same Fourier Random Phase Mask (RPM) as in the encryption process.

In the DRPE method first consider a primary intensity image $f(x,y)$, where x and y denote the spatial domain coordinates. Also $\nu$ and $\eta$ denote the Fourier domain coordinates. $\psi(x,y)$ 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,

$$\psi_n(x,y) = \exp[2i\pi n(x,y)]$$

$$\psi_m(x,y) = \exp[2i\pi m(x,y)] \qquad (4)$$

$h(x,y) = m(x,y)$ is a phase function uniformly distributed in $[0,2\pi]$.The second RPM, $\psi_m(\nu,\eta)$,is the Fourier transform of the function $h(x,y)$,

$$FT\{h(x,y)\} = \hat{h}(\nu,\eta) = \psi_m(\nu,\eta) = \exp[2i\pi m(\nu,\eta)]$$

… (5)

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 a complex function with amplitude and phase. It is given by the following expression:

$$\psi(x,y) = \{f(x,y)\psi_n(x,y)\} * FT^{-1}\{\psi_m(\nu,\eta)\} \qquad (6)$$

where the symbol ( $*$ ) denotes convolution. The encrypted function has a noise-like appearance that does not reveal the content of the primary image. 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

$$FT^{-1}\left\{FT\left[\psi(x,y)\right]\psi_m^*(v,\eta)\right\}$$
$$= FT^{-1}\left\{FT\left[f(x,y)\psi_n(x,y)\right]\psi_m(v,\eta)\psi_m^*(v,\eta)\right\}$$
$$= f(x,y)\psi_n(x,y) \qquad (7)$$

If the encrypted data contains only either phase or amplitude, then the recording and storage is easier. The phase is often chosen to encode, convey, and retrieve information due to several reasons like higher efficiency, invisibility to the naked eye, and more security than the amplitude. The fully phase-encrypted image is given by the following equation:

$$\psi_p(x,y) = \left\{\exp\left[i\pi f(x,y)\right]\psi_n(x,y)\right\} * h(x,y)$$
$$= \left\{\exp\left[i\pi f(x,y)\right]\psi_n(x,y)\right\} * FT^{-1}\left\{\psi_m(v,\eta)\right\} \qquad (8)$$

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.

## V .PROPOSED METHOD WITH CHAOTIC BAKERMAP, DATA HIDING, AES AND DRPE

The proposed technique is based on adding a pre-processing chaotic Baker map layer  and AES algorithm before applying the DRPE. Figure 6 shows the encryption and data hiding used in the proposed system. Figure 7 shows the decryption processes of the proposed technique. This proposed technique has several advantages. With this method the cracking or hacking of the encrypted images becomes harder. If a hacker cracks the DRPE key, i.e., the second RPM, he still cannot obtain the target image as it is protected by the first auxiliary key of the Chaotic Baker Map and Advanced Encryption Standard. The proposed technique can also be used as a water-marketing technique. Some useful information can be hidden in the image prior to optical encryption. The decryption process is just the reverse operations at the encryption side.

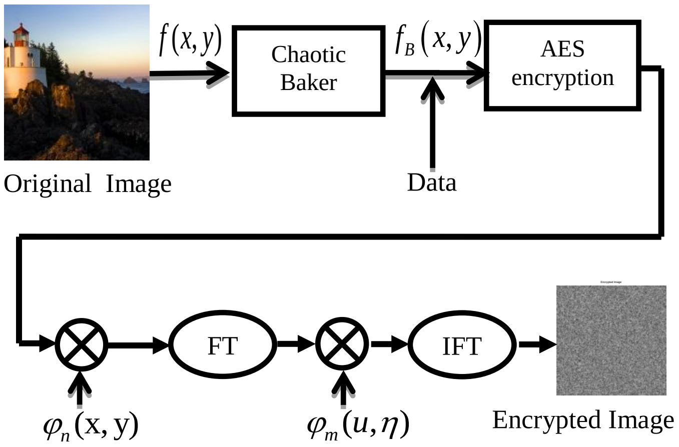


Fig.6. Block Diagram of Proposed Encryption Process

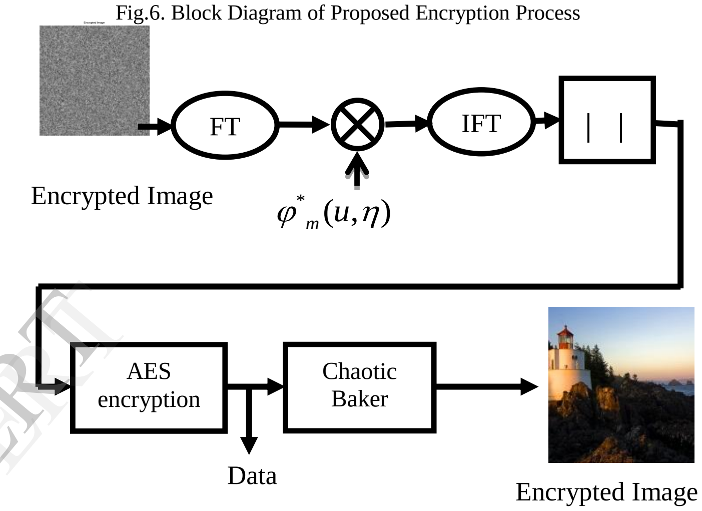


Fig. 7. Block Diagram of Proposed Decryption Process

## VI. Simulation Experiments

Several Matlab experiments are carried out to test the proposed technique and compare its performance with the performance of the DRPE and Chaotic Baker map encryption methods. The three images of the Girl, Lena, and Plane as shown in Figure 8 are used in the experiments. Figure 9 shows the encryption results of the Girl image with different algorithms.ie with DRPE, Chaotic Bakermap and with the proposed technique. The results are compared with the help of histogram analysis and then came to the conclusions.

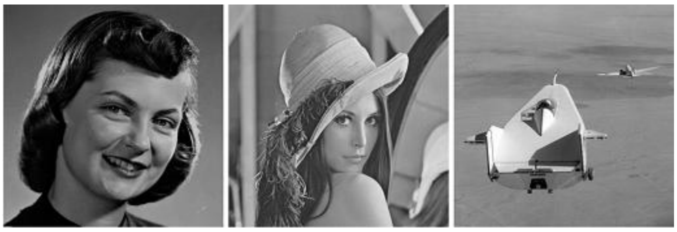


Fig. 8. Girl Lena and Plane images (a) Girl (b) Lena (c) Plane

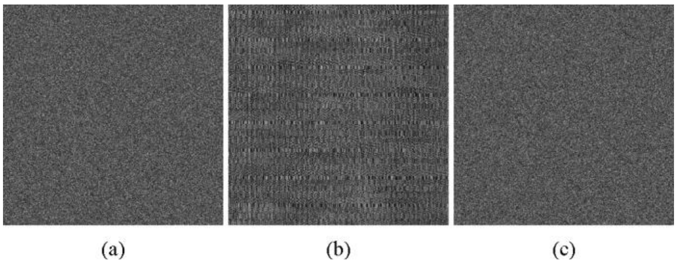


Fig.9. Encrypted Girl image with (a) DRPE, (b) chaotic Baker map, (c) the proposed technique

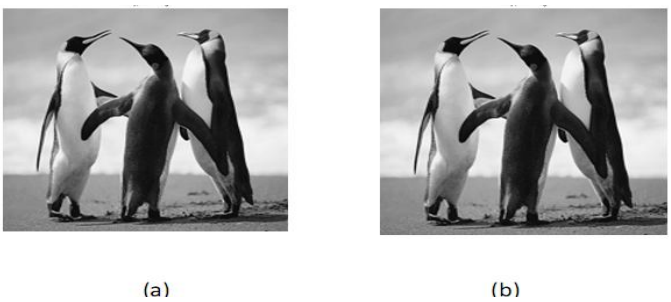


Fig. 10. Decrypted images for the DRPE and the proposed technique in the presenceof noise on the encrypted image with variance 0.01. (a) DRPE. (b) Proposed technique.

One of the important factors in examining the encrypted image is the visual inspection. But, depending on the visual inspection only is not enough in judging the data hiding process. So, other metrics are considered to evaluate the degree of encryption, quantitatively. So the results of histogram analysis is given in Figure 11. 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. 11 shows the histograms of the encrypted images in Fig. 9 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.

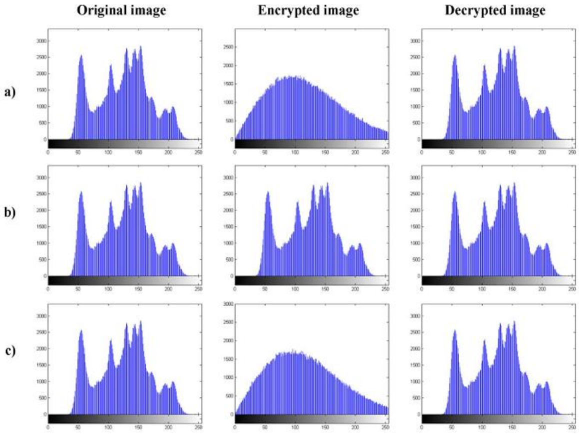


Fig. 11. The histograms of the images for (a) DRPE, b) chaotic Baker map encryption, and c) proposed technique.

## VII. CONCLUSION

Here, an encryption technique based on chaotic Baker map AES and the DRPE has been presented. Also data hiding is included along with the image encryption. The chaotic Baker map is used as a pre-processing layer to increase the security level. Then the AES algorithm and the DRPE are applied to that image and the reverse process is carried out at the decryption process. The implementation of the proposed technique is simple. This technique provides good permutation and diffusion mechanisms in a reasonable time. This gives large immunity to noise, which is a required property for communication applications.

## REFERENCES

[1] P. Refregier and B. Javidi, “Optical image encryption based on input plane and Fourier plane random encoding,” *Opt. Lett.*, vol. 20, pp. 767–769, 1995.

[2] B. Javidi, A. Sergent, G. Zhang, and L. Guibert, “Fault tolerance properties of a double phase encoding encryption technique,” *Opt. Eng.*, vol. 36, pp. 992–998, 1997.

[3] G. Unnikrishnan, J. Joseph, and K. Singh, “Optical encryption by double-random phase encoding in the fractional Fourier domain,” *Opt. Lett.*, vol. 25, pp. 887–889, 2000.

[4] S. Kishk and B. Javidi, “Information hiding technique with double phase encoding,” *Appl. Opt.*, vol. 41, pp. 5462–5470, 2002..

[5] N. Towghi, B. Javidi, and Z. Luo, “Fully phase encrypted image processor,” *J. Opt. Soc. Amer. A*, vol. 16, pp. 1915–1927, 1999.

[6] G. Unnikrishnan and K. Singh, “Optical encryption using quadratic phase systems,” *Opt. Commun.*, vol. 193, pp. 51–67, 2001.

[7] Y. Frauel,A. Castro, T. J. Naughton, and B. Javidi, “Resistance of the double random phase encryption against various attacks,” *Opt. Exp.*, vol. 15, pp. 10253–10265, 2007.

[8] J. W. Goodman, *Introduction to Fourier Optics*, 2nd ed. New York, NY, USA: McGraw-Hill, 1996.

[9] J. Fridrich, *Symmetric Ciphers Based on Two-Dimensional Chaotic Maps*. Singapore: World Scientific, 1998.

[10] Y. Honglei, W. Guang-shou, W. Ting, L. Diantao, Y. Jun, M. Weitao, F. Y. Shaolei, andM. Yuankao, “An image encryption algorithm based on two dimensional Baker map,” in *Proc. ICICTA*, 2009.

[11] I. F. Elashry, O. S. Farag Allah, A.M. Abbas, S. El-Rabaie, and F. E. A.El-Samie, “Homomorphic image encryption,” *J. Electron. Imag.*, vol.18, no. 3, pp. 033002-1–033002-14, 2009.

[12] B. Javidi, Ed., Optical and Digital Techniques for Information Security New York, Springer Verlag, 2005.

[13] O. Matoba, T. Nomura, E. Perez-Cabre, M. S. Millan, and B. Javidi,“Optical techniques for information security,” *Proc. IEEE*, vol. 97, no.6, pp. 1128–1148, Jun.2009.