# A COLOR PICTURE ENCRYPTION TECHNIQUE USING M. HENON'S DYNAMICAL SYSTEM AND DCT TRANSFORM

Irfan Khan
Assistant Professor, Department of Computer Science & Engineering
Shekhawati Institute of Engineering & Technology SIKAR RAJ

***Abstract:** The study of cryptography applications in chaotic system have been exponentially increasing in the recent years. Depending on the sensitivity to initial conditions, chaotic systems are characterized, similarity to continuous broad-band power spectrum and random behavior. The chaotic system is high sensitive to the initial condition and is a high complex nonlinear dynamic system. The chaotic sequence is unpredictable and extreme sensitivity to initial conditions. There are many applications to the chaotic system in several methods, image compression, encryption, modulation and digital communication system. In this paper, an algorithm based on Discrete Cosine Transform (DCT) has been introduced by using Henon map to get the scheme of chaos image encryption. The level of security is very high and this algorithm can improve small key space. Images are more convenient and effective way to represent the complex data. Today, such images are frequently moved from one corner to another corner of world using the Internet. And, as we all are known, that the Internet are always suffered from issues of security. As a result, images may become victim of content manipulation, unauthorized access, content destruction, privacy leakage, etc. To overcome all these issues, our system must have capability to encrypt the image before transmitting it over the Internet. In order to fix these issues, so many encryption approaches has been proposed by expert from all over the world. Most of these encryption approaches are worked either in spatial or frequency domain, but mostly only suitable with gray scale images. The main aim of this paper is to propose an image encryption approach that is done into spatial domain along with frequencies domain, but effective for color images as well as gray scale images. In encryption process of proposed work, the color images are first confused in frequency domain using the Discrete Cosine Transformation (DCT) and Arnold Cat Map. In second step, the confused image's frequencies are converted into spatial domain using the Inverse Discrete Cosine Transformation (IDCT), and defused the image's pixel using the Logistic Map followed by the Henon Map. At the end, we get the resulted encrypted image. At last, various tests have been done and its result has been analyzed to prove the strength and effectiveness of the proposed approach of encryption. The experimental result of proposed work has also been compared with the existing encryption techniques. The result of various test claim the effectiveness of the proposed work.*
***Keywords:** Encryption, Decryption, Diffusion, Confusion, Chaotic Map, Discrete Cosine Transformation, Key-Sensitivity, etc.*

## I. INTRODUCTION

Images carry the useful information that play important role incurrent information technology era. Images can be stored inthe storage devices or transmitted through the communicationchannel. However, store or transmit them in the plain formhave a lot of risks. The adversary can steal or tap the plain-images, sothat confidentiality of plain-images needs to be protected.Images encryption is the solution to this problem. The plainimages are encrypted so that it cannot be recognized byunauthorized party. In the literature, there exist severalwell-approved efficient algorithms for the textmessage encryption, such as: Data EncryptionStandard (DES), Advanced Encryption Standard(AES), International Data Encryption Algorithm(IDEA) and the Rivest-Shamir-Adlemancryptosystem (RSA). However those algorithms arenot well appreciated for image or video file encryptionapplications. Since the images differ from the textdata in many aspects such as high redundancy andcorrelation, the local structure and the characteristicsof amplitude frequency, the conventional encryptionmethods cannot be applicable to the images.

Many image encryption algorithms have been proposed. These image encryption techniques are worked in spatial domain or in frequencies domain or in both domain. An Image Encryption Algorithm Based on Henon Chaotic System in spatial domain has been proposed in [1]. A Block-based Image Encryption Algorithm in Frequency Domain using Chaotic Permutation has been proposed in [2]. A Robust Color Image Encryption Algorithm in Dual Domain using Chaotic Map has been proposed in [3].For a whole color image DWT based lossless chaotic encryption in frequency domain has been proposed in [4]. An Images encryption technique in spatial domain using Cubic Map, Henon Map, Quadratic Map, and Logistic Map has been proposed in [5]. An Image Encryption Using Hybrid Chaotic Map with Arnold' Cat Map, Logistic Map, and HenonMap has been proposed in [6]. An Image encryption algorithm based on Fractional Fourier Transform using Arnold's Map and Henon Map has been proposed in [7]. The image encryption techniques that worked in spatial domain are either confused the pixel location or diffused the pixel's value using various chaotic maps. The image encryption techniques that worked in frequencies are either confused the location of frequencies or diffused the frequency's value using various chaotic maps, or with suitable alteration or modification in chaotic maps. Image encryption performed in either domain has its own pros and cons. The advantages that available in one domain are generally not available in other. In the present study, we introduce a new image encryption

algorithm that performed encryption operation in frequency domain followed by the encryption in spatial domain. The proposed encryption algorithm is based on chaotic Logistic system along with the dynamical system of Michel Henon. According to the present method, our proposed algorithm first confuses the image pixel in frequency domain. Then, chaotic system runs in spatial domain for the generation of pseudo-random sequences, and then these pseudo-random sequences are used todiffuse the value of image pixels.

Our proposed algorithm includes the features of both as an encryption in spatial domain followed by an encryption infrequency domain. The analysis of experimental result revealed that how much our proposed image encryption technique is effective to resist any types of attacks.

## II. PRILIMENERY THEORIES

### A. Discrete Cosine Transformation
The two dimensional DCT of an $M$ by $N$ matrix is defined as follows [3]:

$$C(u,v)=\alpha_u\ \alpha_u\sum_{x=0}^{M-1}\ \sum_{y=0}^{N-1}\ I(x,y)\cos\frac{\Pi(2x+1)u}{2M}\cos\frac{\Pi(2y+1)v}{2N}$$

and the inverse DCT (or IDCT) is given by

$$I(x,y)=\alpha_u\ \alpha_u\sum_{x=0}^{M-1}\ \sum_{y=0}^{N-1}\ C(u,v)\ \cos\frac{\Pi(2x+1)u}{2M}\cos\frac{\Pi(2y+1)v}{2N}$$

Where

$$\alpha_u=\begin{cases}\frac{1}{\sqrt{M}} & ,u=0\\ \frac{1}{\sqrt{M}} & 1\le u\le M-1\end{cases}\quad;\quad \alpha_v=\begin{cases}\frac{1}{\sqrt{N}} & ,v=0\\ \frac{1}{\sqrt{N}} & 1\le v\le N-1\end{cases}$$

The values $C(u, v)$ are called the DCT coefficients of image $I$. The upper leftmost element is called DC coefficient and the rest are called AC coefficients. The DCT can be applied to transform the whole image or image blocks ($8 \times 8$ pixel).

### B. HenonMaP
Pseudo-random has been produced by using Henon map which is considered a prototypical twodimensional.The map relies on two parameters a and b that pick a point $(x_i,\ y_i)$. The Hénon map is a discrete-time dynamical system. It is one of the most studied examples of dynamical systems that exhibit behavior. This map is given by the equation below [7]

$$X_{n+1}=1-aX_n^2+Y_n$$
$$Y_{n+1}=bX_n$$

Usually, a is around1.4 and b is around 0.3 which makes Henon map gainchaotic behavior.

### C. Logistic Map
Logistic map show chaotic behavior that it is considered one the modest nonlinear chaotic discrete systems. It is one dimensional chaotic system that can be described as follows [3]:
$$X_{n+1}=\mu X_n(1-X_n)$$
whereμ isthe chaotic factor and n is the quantity of iterations, $\mu\epsilon[0,4]$, $x\epsilon[0,1]$ in which, the chaotic behavior is realized when $r\epsilon[3.54,4]$.

### D. Arnold Cat Map
Arnold Cat Map (ACM) is a two-dimensional chaotic map after discovered by Vladimir Arnold in 1960. ACM transform the coordinates $x$, $y$) in the image of size $N * N$ to the new coordinates ($x'$, $y'$). The equation of ACM [3] is

$$\begin{bmatrix}x_{i+1}\\y_{i+1}\end{bmatrix}=\begin{bmatrix}1 & K_b\\K_a & K_bK_a+1\end{bmatrix}\begin{bmatrix}x_i\\y_i\end{bmatrix}\mod(N)$$

where ($x_i$, $y_i$) is position of the pixel in the image, ($x_i$ +1, $y_i$ +1) is new pixel position after iteration $i$. Parameters $b$ and $c$ are any positive integer. Determinant of the matrix must be equal to 1 so that the transformation is area-preserving (remain in the same area of the image). ACM is iterated as $m$ times, and each iteration produces a random image. Values of $b$, $c$, and $m$ can be considered as the secret keys. The scramble image can be reconstructed into the original image using the same key ($b$, $c$, and $m$). The inverse equation of ACM [3] is

$$\begin{bmatrix}x_i\\y_i\end{bmatrix}=\begin{bmatrix}1 & K_b\\K_a & K_bK_a+1\end{bmatrix}\begin{bmatrix}x_{i+1}\\y_{i+1}\end{bmatrix}\mod(N)$$

## III. THE PROPOSED ALGORITHM
In proposed algorithm, the algorithm first takes a plain image and two keys Ka and Kb as an input. Then, it reads image pixel-by-pixel and each color component of every pixel are stored in respective matrix μRed, μGreen, and μBlue. At this stage, we have three matrices μRed, μGreen, and μBlue that have contain the value of red, green, and blue of plain image respectively. In the next step, IR, IG, and IB are divided into $8 \times 8$ blocks. Now, DCT is applied on each block of μRed, μGreen, and μBlue. As a result, we get μRed, μGreen, and μBluewith modified value that represent DCT coefficient. To add confusion, the algorithm scrambled each $8 \times 8$ block of every matrix μRed, μGreen, and μBlue using ACM transformation with keys Ka and Kb. Next, algorithm performed the reverse DCT operation on μRed, μGreen, and μBlue to get the image with confused frequency into spatial domain. Now in spatial domain the algorithm performed the diffusion operation twice with each element of matrices IR, IG, and IB. For the first step of diffusion operation, the algorithm produces a stream of keys using the Logistic Chaotic Map, and the XOR operation are performed between the key and each element of matrices IR, IG, and IB. For the second step of diffusion operation, the algorithm produces a stream of keys using the Henon Chaotic Map, and the XOR operation are performed between the key and each element of matrices IR, IG, and IB. The matrices IR, IG, and IB would now contained the twice diffused value of every color component of every pixel of the plain image. Finally, each color component matrices are combined to get the encrypted image.
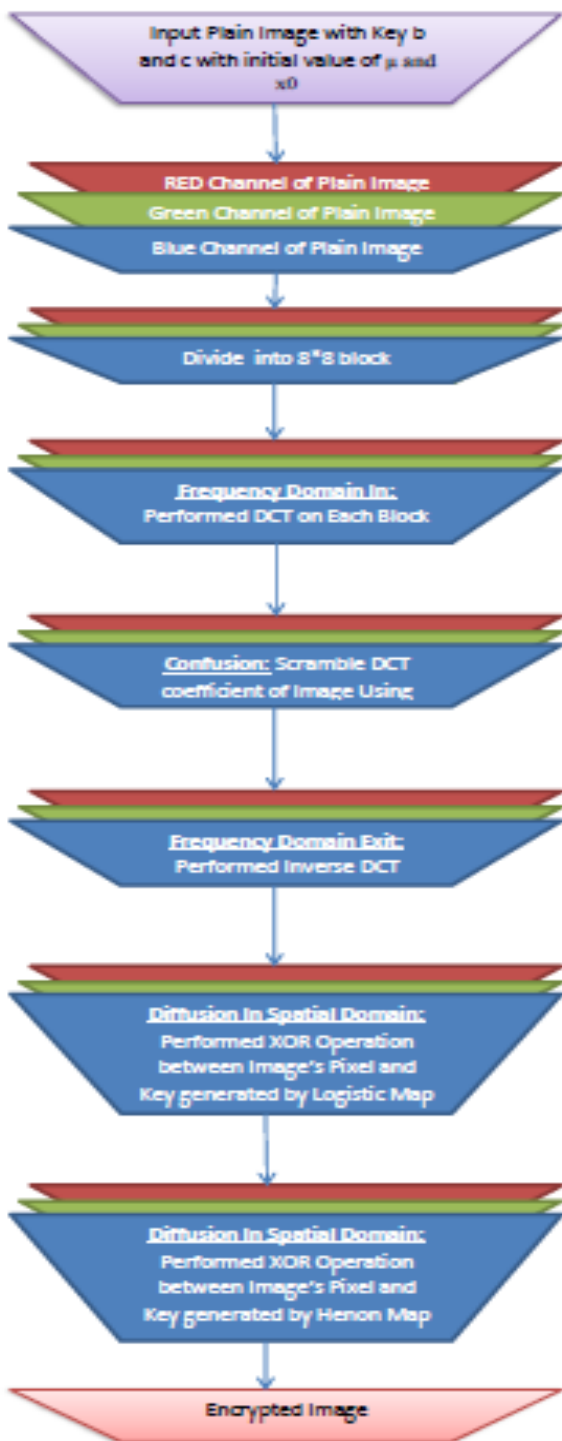
Figure 1- Flow of Encryption Process by Proposed Approach

## IV. EXPERIMENTAL RESULT AND ANALYSIS

For this study, the initial values and the parameters are adjusted as follows with a good accuracy:

$\mu = 3.9600$; $x_0 = 0.1234$; $K_a = 94$; $K_b = 50$;

In this study, we used three colorful images of Lena, Pepper, and Baboon for the demonstration of the efficiency of the proposed image encryption algorithm.When we applied our

proposed encryption and decryption algorithm with the mentioned initial value and keys, we get the result as shown in figure-2.
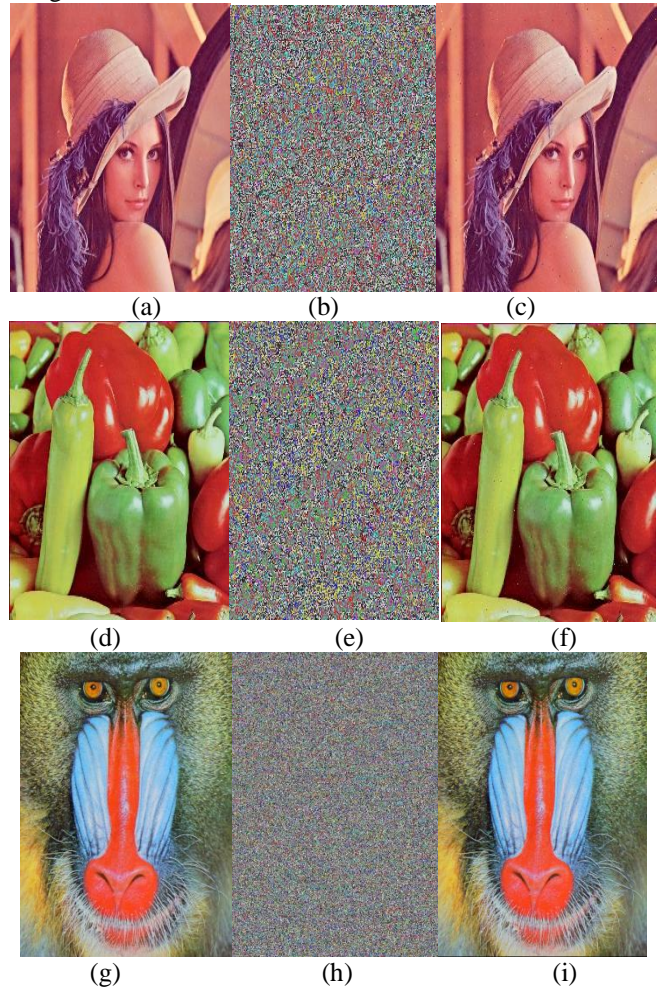


Figure 2- (a) Original image of Lena, (b) Encrypted image of Lena, (c) Decrypted image of Lena, (d) Original image of Peppers, (e) Encrypted image of Peppers, (f) Decrypted image of Peppers, (g) Original image of Baboon, (h) Encrypted image of Baboon, (i) Decrypted image of Baboon

To test and analyze the result MATLAB R2015a is used with a system of Intel CORE i3 processor and 4 GB of RAM.

### A. Histogram Analysis

The image histogram determines the distribution of each color intensity level of the individual pixels of an image. An ideal histogram for an encrypted image should be flat, implying the uniform distribution on the image range and the complete randomness. Infact, the flatness of a histogram could better preventthe leakage of the information by the statistical attacks. Figure-3shows the histograms of theoriginal Lena image and it's encrypted one.
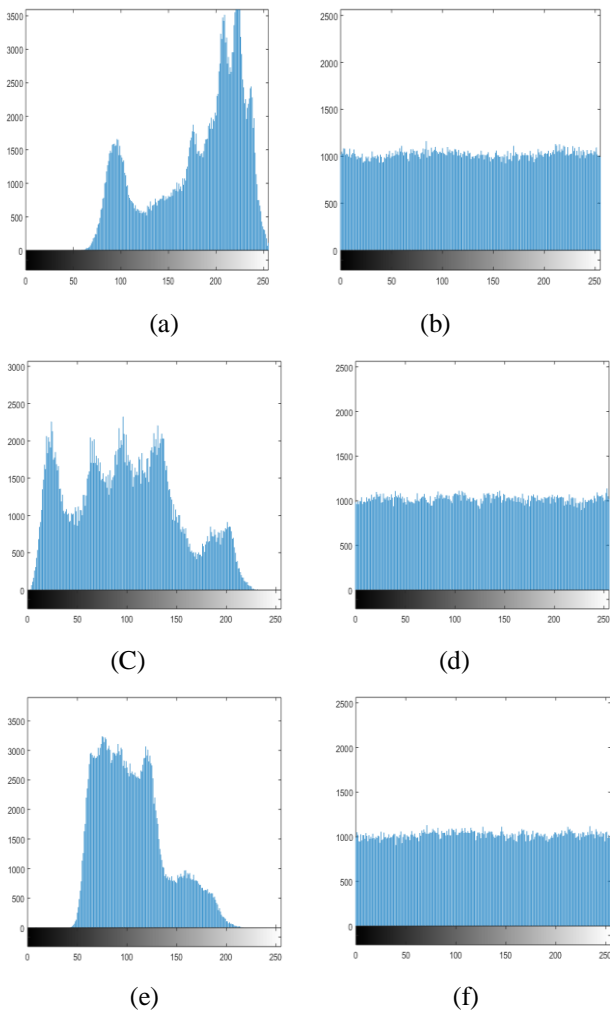
(a)


(b)


(C)


(d)


(e)


(f)

Figure 3 - (a) Histogram of Red color of plain image of Lena,
(b) Histogram of Red color of encrypted image of Lena, (c)
Histogram of Green color of plain image of Lena,
(d)Histogram of Green color of encrypted image of Lena, (e)
Histogram of Blue color of plain image of Lena, (f)
Histogram of Green color of encrypted image of Lena,

The histogram of the original image contains several peaks. However, the histogram of the ciphered image is uniform. Hence, it is proven that the histograms of the encrypted image do not give any clue to operate any statistical attack to recover the original one.

## B. Entropy Analysis

The information entropy measures the strength of the cryptosystem and gives the equally probable gray levels for a good image encryption algorithm by applying it to the encrypted image.

Table I gives the entropy values of three original images and their encrypted ones. According to the results, the information entropy is increased by the encryption system and the information entropies of the encrypted images are nearly 8. This proves that the proposed encryption algorithm is highly resistive to the information leakage.

TABLE I: Entropy values for the plain images and the corresponding decrypted image

| Entropy Value of Plain and Encrypted Image | | | | | | |
|---|---|---|---|---|---|---|
| | Plain Image | | | Encrypted Image | | |
| Images | R | G | B | R | G | B |
| Lena | 7.2531 | 7.594 | 6.9684 | 7.9989 | 7.9988 | 7.999 |
| Pepper | 7.3576 | 7.5929 | 7.129 | 7.9991 | 7.9989 | 7.9987 |
| Baboon | 7.7067 | 7.4744 | 7.7522 | 7.9991 | 7.9991 | 7.9993 |

TABLE II: Entropy values for the encrypted image in previous and proposed work

| Entropy Analysis of Previous Work and Proposed Algorithm | | | | | | |
|---|---|---|---|---|---|---|
| | Ref [3] | | | Proposed Work | | |
| Images | R | G | B | R | G | B |
| Lena | 7.9979 | 7.9987 | 7.998 | 7.9989 | 7.9988 | 7.999 |
| Pepper | 7.9985 | 7.999 | 7.9968 | 7.9991 | 7.9989 | 7.9987 |

## C. Correlation Coefficient:

In this section, the horizontal, vertical and diagonal correlation coefficients of the ciphered pixels have been calculated.Correlation between any two adjacent pixels of an image is a clue for attackers to gain the statistical information about the image. The value of correlation coefficient near to zero of an image has less meaningful statistical information of any two adjacent pixel.

TABLE III: Correlation coefficients of two adjacent pixels in the plain image and the cipher-image

| Correlation Coefficient of Plain and Encrypted Image | | | | | | | |
|---|---|---|---|---|---|---|---|
| Images | Direction | Plain Image | | | Encrypted Image | | |
| | | R | G | B | R | G | B |
| Lena | Vert. | 0.9894 | 0.9824 | 0.9578 | 0.0749 | 0.0727 | 0.063 |
| | Hor. | 0.9798 | 0.9690 | 0.9329 | -0.0356 | -0.0274 | -0.0124 |
| | Diag. | 0.9697 | 0.9555 | 0.9184 | 0.003 | 0.0016 | 0.0032 |
| Pepper | Vert. | 0.9750 | 0.9882 | 0.9752 | 0.0765 | 0.0734 | 0.0768 |
| | Hor. | 0.9719 | 0.9864 | 0.9748 | -0.0245 | -0.037 | -0.033 |
| | Diag. | 0.9524 | 0.9765 | 0.9549 | 1.02e-04 | -3.30e-04 | 0.0048 |
| Baboon | Vert. | 0.8597 | 0.7578 | 0.8777 | 0.0501 | 0.0468 | 0.0565 |
| | Hor. | 0.9228 | 0.8656 | 0.9072 | -0.0236 | -0.0181 | -0.0263 |
| | Diag. | 0.8543 | 0.7352 | 0.8399 | 0.0062 | 0.0039 | 0.0051 |

So, we take all pairs of two adjacent pixel first in horizontally and then vertically from plain image and encrypted image. In addition, we randomly take 2000 pairs of diagonally adjacent pixel from plain image and encrypted image. The table III shows the correlation coefficient of each plain image and correlation coefficient of respective encrypted image that used in this experiment.

TABLE IV: Correlation coefficients of two adjacent pixels in decrypted image in Previous and proposed work

| Comparative Analysis of Previous Work and Proposed Algorithm | | | | | | |
|---|---|---|---|---|---|---|
| Ddirection | Ref [4] | | | Proposed Algorithm | | |
| | Encrypted Image of Lena | | | Encrypted Image of Lena | | |
| | R | G | B | R | G | B |
| Vertical | 0.4807 | 0.4745 | 0.4553 | 0.0749 | 0.0727 | 0.063 |
| Horizontal | 0.4850 | 0.4925 | 0.4873 | -0.0356 | -0.0274 | -0.0124 |
| Diagonal | 0.4841 | 0.4791 | 0.4565 | 0.003 | 0.0016 | 0.0032 |

*D. PSNR Analysis:*

If the PSNR value of two images is equal or greater than 30, then human eyes can't differentiate between these two images. To analyze the quality of visibility of the decrypted image, we used the PSNR (Peak Signal-to-Noise Ratio) test with decrypted images and their respective plain images. The bigger PSNR value between plain image and its respective decrypted image confirm the less distortion in the original plain image. The table V has shown the PSNR value of images that we used in our experiments and it always above the standard. So, our proposed algorithm is enough capable to recover the decrypted image with enough visual quality.

TABLE V: The PSNR results between plain-image and corresponding decrypted image

| PSNR Analysis | |
|---|---|
| Decrypted Image | PSNR |
| Lena | 62.251 |
| Pepper | 65.626 |
| Baboon | 63.536 |

TABLE VI: The PSNR results of decrypted image by previous work and proposed work

| Comparative Study of PSNR Analysis | | |
|---|---|---|
| Decrypted Image | Ref [3] PSNR Value | PROPOSED PSNR Value |
| Lena | 34.2466 | 62.251 |
| Peppers | 34.6704 | 65.626 |

E. Key Sensitivity Analysis:

In this section, the horizontal, vertical and diagonal correlation coefficients of the ciphered pixels have been calculated.In our proposed algorithm the initial value of $\mu$ and $x_0$, and value of $K_a$ and $K_b$ are used as the key of algorithm. In this test, we have tried to decrypt an encrypted image of Lena, Peppers, and Baboon with same value of Ka, Kb, and same initial value of $x_0$ with a minor difference in initial value of $\mu$. As mentioned earlier, we have used following value of the key at the time of encryption of Lena image:

$\mu = 3.9600$;
$x0 = 0.1234$;
$K_a = 94$;
$K_b = 50$;

Now we have the same value of $x_0$, $K_a$, $K_b$, and make a minor difference of $\mu=3.9600$ to $\mu=3.9601$. In this case, the decrypted image of Lena, Peppers, and Baboon is shown in figure 4. (a),(b), and (c).
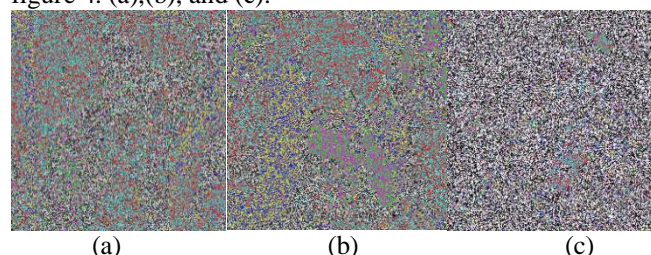


Figure 4 - (a) decrypted image of Lena with minor different key, (b) decrypted image of Peppers with minor different key, (c) decrypted image of Baboon with minor different key.

The result has shown that, the least possible change in the key produce an image that is a totally meaningless and even not to be a little bit of close to the original plain image. So, it is clarify that how much our proposed algorithm is sensitive about its key.

## V. CONCLUSION

In this paper has presented a block-based image encryption algorithm using a chaotic permutation. Experiment shows that the cipher-images that resulted from the algorithm are robust to common image processing operations. Such image processing are JPEG compression, image noising, and image resizing. The decrypted images can be still recognized well, although they are just like noised.

## REFERENCES

[1] C. Wei-bin, Z. Xin (2009): Image Encryption Algorithm Based on Henon Chaotic System, Proceeding of International Conference on Image Analysis and Signal Processing (IASP 2009).

[2] RinaldiMunir (2014) : A Block-based Image Encryption Algorithm in Frequency Domain using Chaotic Permutation, (IEEE 2014).

[3] Deepak Kumar Singh, KuldeepTomar: A Robust Color Image Encryption Algorithm in Dual Domain using Chaotic Map, 2ndInternational conference on Inventive Communication and Computational Technologies ( IEEE 2018)

[4] Xiangjun Wu, Zefan Wang (2015): A new DWT-based Lossless Chaotic Encryption Scheme for Color Images, 2015 International Conference on

Computer and Computational Sciences (ICCCS), (IEEE 2015).

[5] Kayhan CELİK, Erol KURT: A New Image Encryption Algorithm Based on Lorenz System, ECAI 2016 - International Conference – 8th Edition, (IEEE 2016).

[6] Mohamed A. Mokhtar, NayraM.Sadek, Amira G. Mohamed: Design of Image Encryption Algorithm Based on Different Chaotic Mapping, 2017, 34th NATIONAL RADIO SCIENCE CONFERENCE (IEEE 2017).

[7] Hikmat N. Abdullah, Hamsa A. Abdullah: Image Encryption Using Hybrid Chaotic Map, 2017 International Conference on Current Research in Computer Science and Information Technology (IEEE 2017).

[8] Matthews, R A J., On the Derivation of a Chaotic Encryption Algorithm, Cryptologia, 1989, 13(1), 29-42.

[9] Shannon, C., Communication Theory of Secrecy Systems, Bell System Technical Journal, 1949, 28(4), 656–715.

[10] Baptista, M.S., Cryptography with Chaos, Physics Letters A, 1998, 240, 50–54.

[11] "RC4 Encryption Algorithm. htm ",vocal Technologies, Ltd. 520 Lee Entrance, Suite 202 Amherst New York 14228Email: sales@vocal.com.

[12] Yen, J.C. and Guo, J.I., A New Chaotic Key Based Design for Image Encryption and Decryption, Proceedings of the IEEE International Symposium Circuits and Systems, 2000, 49-52 Vol.4.

[13] Rahma, A.S. and Yacob, B. Z, Real-Time Partial Encryption of Digital Video Using Symmetric Dynamic Dual Keys Algorithm (SDD), Eng.& Tech. Journal ,2012, 30(5).

[14] Rahma, A.S. and Ali, M. A., To Modify the Partial Audio Cryptography for Haar Wavelet Transform by Using AES Algorithm, Eng. & Tech. Journal, 2014, 32(1).

[15] Yen, J.C and J. I. Guo, A New Chaotic Image Encryption Algorithm, Proceedings of National Symposium on Telecommunications, 1998, 358-362.

[16] Yen, J. C. and J. I Guo., A New Chaotic Mirror-Like Image Encryption Algorithm and Its VLSI Architecture, Pattern Recognition and Image Analysis, 2000, 10(2), 236-247. [11] Yen, J. C. and J. I. Guo., Efficient Hierarchical Chaotic Image Encryption Algorithm and Its VLSI Realization, Proceedings of IEEE Vision, Image and Signal Processing, 2000, 147(2