International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878, Volume-8 Issue-3, September 2019

Highly Secured Method for Image Encryption Based Mathematical Model and Bit Plane

Inaam.R.Al-Saiq, Hind Rustum Mohammed, Rewayda Abo-Alsabeh

Abstract:The important area of network communication research is the protection of clandestine image data from prohibited access. Therefore, we develop a highly guaranteed model for image encoding as we use a new mathematical model. This helps anyone to encrypt and decrypt gray image more securely and skillfully. Image encryption technique plays a vital role in image processing. Lot of image encryption technique has been developed so far. The technique such as segment the image into four parts, exchange first part of matrix instead of fourth part ,as well as exchange second part instead of third part, after that we exchange the main diagonal of fist part with fourth part ,as well as, the main diagonal of second part exchange with third part. After that, we will use mathematical function to hide the image. The decrypted gray image has two distinct steps. First, using invertible mathematical model to obtain gray image with noise. Second, using Bit Plane in order elicit the actual image back.

Keywords: Elementary Functions; Segmentation; Image Encryption; Bit-Plane Decomposition.

I. INTRODUCTION

In the present study, image is reconstructed and extracted in a process of convolution that is signal based on a function of continuous interpolation. The sampling procedure is performed on pixel dots of the taken away image. Later, the consequence of the sampling is stockpiled inside a matrix which has enrolment data construct as a control point for interpolation procedure [1].

The sent images of commercial, military and medical applications may contain important and confidential information. Before transmission, it is necessary to encrypt the image datum so as to maintain the safety of the information. In recent years, a numeral of various image encryption systems has been proposed to ensure the confidentiality of information transmission [2].

Formerly, the chaos theory had big attentiveness for many papers and researchers. It had been used vastly in the fields of coding, safeness of data.

Manuscript published on 30 September 2019
* Correspondence Author
Inaam.R.Al-Saiq*, Department of Mathematical Sciences, University of Kufa, Iraq
Hind Rustum Mohammed, Department of Computer Sciences, University of Kufa, Iraq
Rewayda Abo-Alsabeh, Department of Mathematical Sciences, University of Kufa, Iraq

It guarantees connecting assistance from its great properties like cyclicity, incompetence to portend, and sensibility to the seed and parameters where some conditions have been met like diffusion and confusion in the sensitiveness of coding.

Such a chaotic system characterizes properties and has excellent of diffusion and confusion; it has been used vastly to design various cryptographic planner [3].

Digital images appear in idiom of pixels can be demonstrated in terms of bits. Given an X-bit per pixel image, slitting the image at distinct planes (bit-planes) takes a fundamental part in image processing [4]

We achieve the prospect of crest and zero point to get better the concealing ability in every non- imbrication chunks in thecove

[5] Cryptosystem Image is classified into two main parts: the first is used for encryption and the second is used for decoding. There are many scientific methods used to find the private and the public key in encryption [6].

Evaluation algorithms can best be defined in terms of finite sequences of operations $F = (F_0, \dots, F_n)$; both evaluations of the 'built-in' functions and the arithmetic operation to determine the sequences [7]An image technique has shown an exciting technique based on bit image analysis. Excellent coding performance is a technique that initially analyzes the image into different binary bits when we use a particular decomposition method like traditional diode analysis, gray decomposition, and p-code decomposition [8, 9, 10].

Encrypting methods work by manipulating and analyzing image data into binary files in their binary repositories by an XOR operation of one-by-one image encryption. The order of every bit planes is then reversed. Then, all the plane bits are combined. When applying the scrambling algorithm, the output encrypted image can be obtained. This method increases the security. The image is considered efficient in terms of storage and transport applications [11].

The arrangement of the paper is as follows: Section 2 presents the characteristics of the mathematical model and the level of the bit. The method is proposed in Section 3. Section 4 is the results. Finally, the conclusions in Section 5.

II. Mathematical Model and bit plane

A. Mathematical Model.

Fractional Calculus has been attracted researchers and particularist in the past years. It is the reason in the amelioration of assorted applications. Since the nineties of the last century fractional calculus is being rediscovered and related in an expanding number of fields, like some areas of Physics, Control Engineering, and Signal Processing [12]. The Exponential function is defined as follows:

If $a > 0$ and $a \neq 1$, then a function of the form $g(x) = a^x$ is described as an exponential function $y = f(x)$.

The element x is called the indicator and the a is any number called the base. The group of all real numbers $(-\infty, \infty)$ is the domain of an exponential function. Below are some of the paramount properties of the exponential function g with base a:

- The range of g is the set of positive real numbers, that is, $(0, \infty)$.
- The y- protract of g is $(0, 1)$.The graph of f has no x-intercept.
- In the interval $(-\infty, \infty)$ the function g is increasing for $a > 1$ and decreasing on the interval $(-\infty, \infty)$ for $0 < a < 1$.
- The function f is one-to-one.

When the base is selected to be $a = e$ where e = 2.718281828459…, the function $g(x) = e^x$ is called the natural exponential function. Since $a = e > 1$ and $a = 1/e < 1$.

Since an exponential function $y = a^x$ is one–to-one, then it has an inverse function. We get the inverse by reciprocating the variables x and y to obtain $x = a^y$. This formula defines y as a function of x. Now, we will define the logarithmic function with base > 0 , $a \neq 1$, as $y = \log_a x$ if and only if $x = a^y$. For $a > 0$ there is no real number y for which a^ycan either be 0 or negative. It then follows from $x = a^y$ that $x > 0$. In other words, the group $(0, \infty)$ is the domain of a logarithmic function $y = \log_a x$. The important properties of the logarithmic function $g(x) = \log_a x$ are:

- Set of $(0, \infty)$ is the domain of g.
- Set of $(-\infty, \infty)$ is the range of g.
- x-oppose of f is $(1, 0)$. Graph of f has no y-oppose.
- Function g is increasing on the interval $(0, \infty)$ for $a > 1$ and decreasing on the interval $(0, \infty)$ for $0 < a < 1$.
- The function f is one-to-one.

A logarithm is called natural logarithm when the base $= e$. Furthermore, it is customary to write the natural logarithm $log_e x$ as $\ln x$. For base $a = e$ becomes $y = \ln x$ if and only if $x = e^y$ and $ln\, 1 = 0$ since $e^0 = 1$, $ln\, e = 1$ since $e^1 = e, x = e^{\ln x}$ and $y = ln\, e^y$ [13].

B. Bit-Plane Slicing:

Dividing a digital image to its bit-planes is beneficial to analyze the genealogical magnitude that played by each bit. It specifies the sufficiency number of bits that used for quantizing every pixel. It is important for image compressing.

In an image, if the density of each pixel has been composed of 8 bits, the range of image is 0 to 255 gray values. The image is decomposed into 8 bit planes in bit-plane slicing. The leaflet of the Least Significant Bit (LSB) of the pixel is the first plane and the eighth plane has the Most Significant Bit (MSB) value for all the pixels of the image [14].

At levels of 8-bits bytes, all the lowest arrangement bits are composed in plane 0 and plane 7 composes all the high arrangement bits.

Bit plane slicing is applied to cut off the image at distinct bit planes. It is constituted at higher and lower arrangement bits. MSB has the important addendum to the total image; it plays a part in the plurality of the data of an image. LSB plays a part only less specifics of an image. Bit plane plays a great role in compression and image processing [15].

In idiom of extraction bit–plane for an eight-bit image, it has been shown that the image of binary for 7-bit plane is gained by transferring the datum image with a thresholding gray-grade conversion action that charts every grades between 0 and 127 to one grade (e.g. 0) and charts every grade from 129 to 253 to latest (e.g. 255) [16].

Both the encoding and decoding parts were found in Matlab and the results were analyzed. Encoding begins with grayscale images, because a total of 24-bit planes for each image are made by dividing out R, G and B color components and generating 8 bit planes for every component of color [17]. Therefore, it is quite convenient to deal with grayscale as it has only 8 bit planes.

III. The Proposed Method

A. Encryption

Steganography is section of knowledge hiding which is established to be beneficial in finding the settling to network safety. The aim of steganography is to send confidential data by entrenching it into some unhurt overlay objects like digital images or any other medium such as audio, video, etc. [18].

In this part, we insert narrative image encryption steps, first we squander the original image. The value of a pixel represented by single sample stands for what is called grayscale digital image. This suggests that it only includes intensive information. Such images are sometimes called as black-and white images that are essentially and exclusively composed of some shades of gray that vary from black at ‘O’ intensity at the one end to ‘1’ intensity at the other; the former is the weakest while the latter is the strongest [19].

Image Database can use various sizes such as 256×256 pixels and 512×512 pixels. Several image encryption steps have been advanced to safeguard images .One method is based on converting grayscale image as a square matrix (i.e. the size of row and column are the same). We divide the matrix into four equal submatrices and do an interchanging between them.

To illustrate this; let M be a matrix of size $N \times N$ and contains four submatrices A, B, C, and D of size $\frac{N}{2} \times \frac{N}{2}$. We exchange submatrix A with submatrix D and submatrix B with submatrix C.

$$M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}, \qquad M' = \begin{bmatrix} D & C \\ B & A \end{bmatrix}$$

In the other side, we exchange the main diagonal of each submatrix in M'.

We replace the main diagonal of submatrix D with the main diagonal submatrix of A and the main diagonal submatrix of C with the main diagonal submatrix of B.

$$M'' = \begin{bmatrix} D = \begin{bmatrix} a_{11} & \cdot & \cdot \\ \cdot & \ddots & \cdot \\ \cdot & \cdot & a_{\frac{N}{2}\times\frac{N}{2}} \end{bmatrix} & C = \begin{bmatrix} b_{11} & \cdot & \cdot \\ \cdot & \ddots & \cdot \\ \cdot & \cdot & b_{\frac{N}{2}\times\frac{N}{2}} \end{bmatrix} \\ B = \begin{bmatrix} c_{11} & \cdot & \cdot \\ \cdot & \ddots & \cdot \\ \cdot & \cdot & c_{\frac{N}{2}\times\frac{N}{2}} \end{bmatrix} & A = \begin{bmatrix} d_{11} & \cdot & \cdot \\ \cdot & \ddots & \cdot \\ \cdot & \cdot & d_{\frac{N}{2}\times\frac{N}{2}} \end{bmatrix} \end{bmatrix}$$

Then we use the mathematical model by multiplying each pixel by the exponential function. Finally, we use different process in the spatial domain to obtain image encryption skillful.

B. Decryption

Image decryption is carried out in the adverse order of encryption. The decoding process is done in two steps. First, we use the mathematical model by multiplying each pixel by the natural logarithm. Then the image is divided into four equal parts. These parts are exchanged as follows: The first part is replaced with the fourth part and the second part is replaced with the third part. As well as, for the resulting matrix, we replace the main diagonal of sub matrices as follows: We replace the main diagonal of first part with the main diagonal of fourth part and replace the main diagonal of the second part with the main diagonal of the third part. Finally, we obtain gray image but not clear. So we use bit-plane.

Second, bit plane is applied to show the important datum of an image. It is constituted of 8 bit planes. When the image includes interference, the connotation of bit plane slicing is to locate or consider datum in the code of bit plane. As a result, the alteration of MSB bit is achieved; it creators increased deformation than LSB bits. It is simple to encode minimum considerable bits and it is fundamental to maintain the generality big bits [20].

Bit plane are fundamentally of considerable stratums anywhere; every stratum displays the special field of bit planes. Standard of safety as well counts on the digit of bit planes have been applied to degrade the image. Bit planes are obtained much darker image when the image is of higher order [20]

Bit plane slicing is best comprehended. The procedure of dividing an image into two or more parts of the ingredient duple planes is named as "bit plane slicing". However, pixels constitute digital number of bits. In an 8-bit image, density of every pixel is performed by 8-bit. The 8-bit image contains eight 1-bit plane region from bit plane "0" (LSB) to bit-plane "7" (MSB). So, plane"0" decompose each lowest order bits of each pixel in the image whilst plane "7" decompose each higher order bits. Bit plane slicing is useful for image compressing. Complication of every bit-plane format addition monotonically from MSB to LSB [21].

Finally, it has been found out the first image and the final established image evidence must be conformable to the person eye.

C. Algorithms

In cryptography method, the original image is considered to generate the key image. The latter is the input of the encrypt algorithm and the output of this algorithm is the input of the decryption algorithm [21].

Algorithm 1: Encryption

Input: Original grayscale image of size N×N.

Output: Encryption of image of the same size.

Step 1: Convert the original image into the matrix M of size N×N

Step 2: Divide M into four equal submatrices of sizes $\frac{N}{2}\times\frac{N}{2}$.

Step 3: Replace between the submatrices.

Step 4: Replace between the main diagonal of submatrices.

Step 5: Multiply each pixel by the exponential function to obtain the encrypted image.

Algorithm 2: Decryption

Input: The encrypted image of size N×N.

Output: Original image of size N×N.

Step 1: Convert the encrypted image into the matrix of size N×N.

Step 2: Divide the matrix into four equal submatrices of sizes $\frac{N}{2}\times\frac{N}{2}$.

Step 3: Replace between the submatrices.

Step 4: Replace between the main diagonal of submatrices.

Step 5: Multiply each pixel by the natural logarithm function.

Step 6: Bit–plane slicing is carried out when using bitwise and every pixel in the image take out the original image.

V. Results of Experiment

The method has been applied on a database of 50 original images with size N×N. Figure 1 shows a sample of grayscale images. In Figure 2, (a) is the original image, (b) is the proposed cryptosystem where the technologic method is used, (c) shows the result of applying the exponential function. The encryption process is performed in (d) and the decryption process is applied in (e). We used the inverse technical method and the inverse of mathematical model, so the natural logarithm function has been used, but it's not clear. Finally, the original image (decrypted) is obtained by using bit-plane.

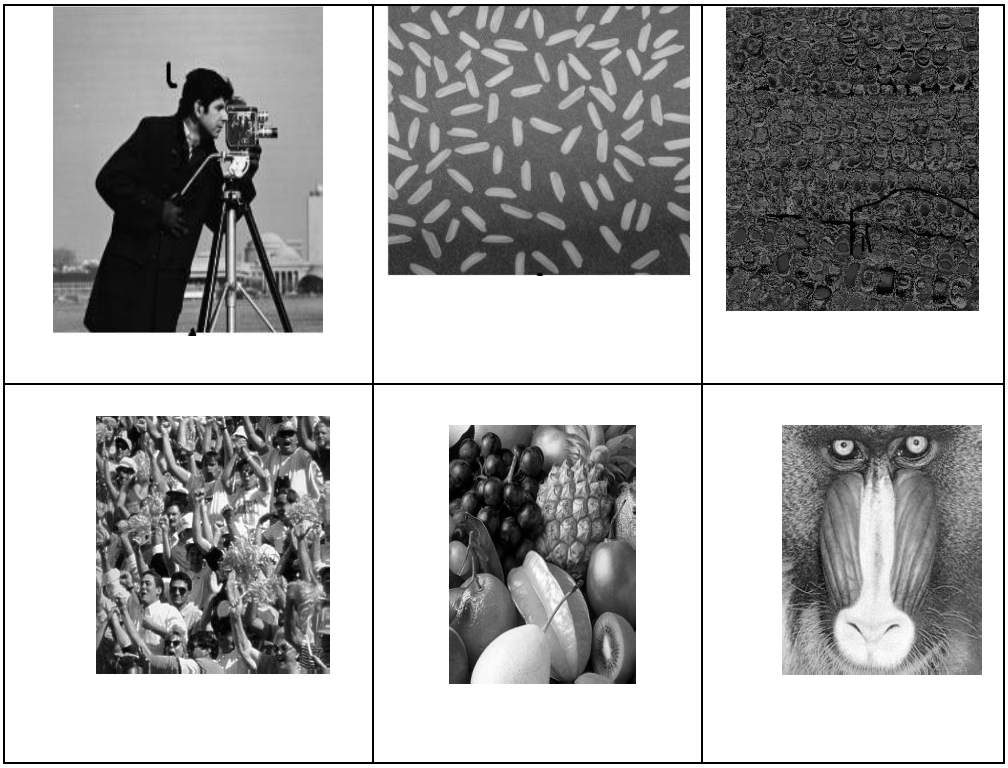
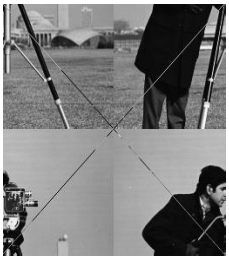


Figure 1: Sample of original grayscale images.

(a) Source Image

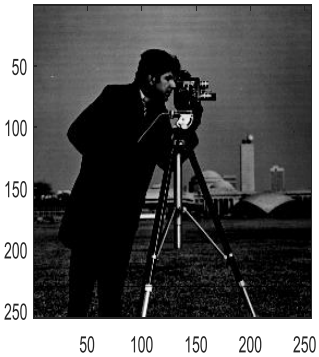


(b) Replace the matrix and Main diagonal

(c)Using exponential function

(d) The encrypted image

(e) Using the natural logarithm function



(f) Using bit-plane

Retrieval Number: B3798078219/19©BEIESP
DOI:10.35940/ijrte.B3798.098319
Journal Website: www.ijrte.org

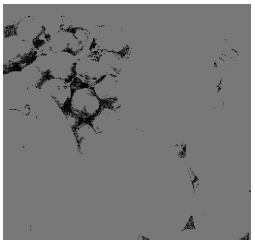
Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

(a) Source image

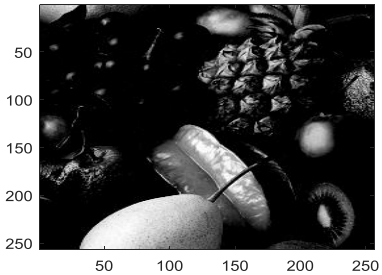
(b) Replace the matrix and The main diagonal

(c)Using exponential function

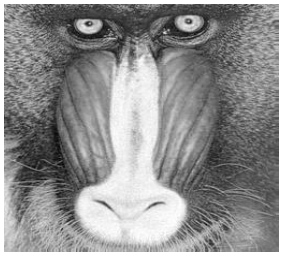
(d) The encrypted image



(e) Using the natural logarithm function



(f) Using bit-plane



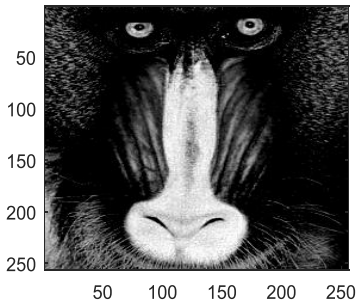
(a) Source image

(b) Replace the matrix and the main diagonal

(c) Using exponential function

(d) The encrypted image

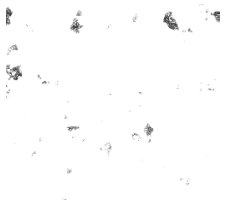
(e) Using the natural logarithm function



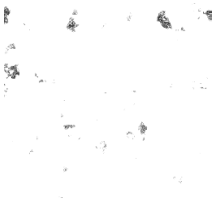
(f) Using bit-plane

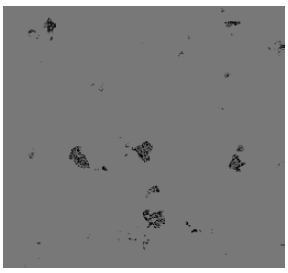
(a) Source image

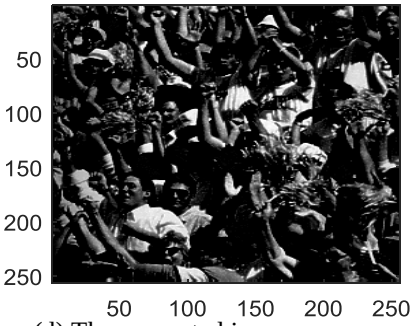
(b) Replace the matrix and the main diagonal



(c) Using exponential function







(d) The encrypted image

(e) Using the natural logarithm function

(f) Using bit-plane

Figure 2: The steps of encrypted image and decrypted image

VI. CONCLUSION

We suggested a new method for image encryption algorithm. In this method the encryption is carried out only on images of gray scale. By the following steps, first, the image is transformed to a matrix of size N×N and then divided into four submatrices, each one of size N/2×N/2. Second, we replaced between the submatrices. As well as, we replaced between the main diagonal of the new submatrices. Later, the mathematical tool is used by multiplying each pixel by the exponential function. Finally, encrypted images have been obtained. The experimental results showed that the encrypted images have been unknowable visually and totally distinct from the original images.

Image decryption is carried out in the reversed order of encryption. In the decryption process, we divided the matrix of size N×N into four submatrices of size N/2×N/2 and replaced between them. Also, we exchanged between the main diagonal of the submatrices. Then, the inverse of mathematical model is performed by multiplying each pixel by the natural logarithm function. We obtained the decrypted image but it is not clear. So, we used the bit plane. Finally, the original image is obtained.

REFERENCES

1. Arman Adel Abdullah, Rodiah, Emy Haryatmi, Lung Cancer Nodule Extraction and 3D Modeling using Bit-Plane Slice and Outlining, International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181,Vol.5 Issue 09, September-2016.
2. Sukalyan Som, Sayani Sen, A Non-adaptive Partial Encryption of Grayscale Images Based on Chaos, First International Conference on Computational Intelligence: Modelling , Techniques and Applications(CIMTA-2013), Procedia Technology 10 (2013) 663-617, Published by Elsevier Ltd. 2013.
3. Ekhlas Abbas Al-Bahrani, Riyam N. J Kadhum, A New Cipher Based on Feistel Structure and Chaotic Maps ,Baghdad Science Journal ,Vol.16(1)Supplement 2019.
4. Deepa Raj and Seema Gupta, Segmentation and Reassembly of Images using Biplane Slicing in Adaptive Lossless Dictionary based Compression, International Journal of Computer Applications (0975-8887), National Seminar on Future Trends & Innovations in Computer Engineering (NSFTICE' 2015).

5. Rashid Abbasi , Bin Luo, Gohar Rehman, A new multilevel reversible bit-planes data hiding technique based on histogram shifting of efficient compressed domain, Springer, Vietnam Journal of Computer Science(2018) 5:185-196.
6. Shahad Adil Taher, Hind Rustum Mohammed, Combination Mathematical, Distance Measure Approach for Some Image Processing Application, Journal of theoretical and Applied Information Technology, 30th April. Vol. 96. No. 8, 2018.
7. Shawki A. M. Abbas, A Note on the Perturbation of arithmetic expressions, Baghdad Science Journal ,Vol.13(1) 2016.
8. Zhou Yicong, Cao Weijia, Philip Chen C.L., " Image encryption using binary bit plane", Science Direct, Signal Processing, 197-207, www.elsevier -com/locate/sigpro, 2014,
9. Y-Zhou, K. Panetta, S. Agaian, C. L. P. Chen," Image encryption using p-Fibonacci transform and decomposition, " Opt. Commun .285(5), 594- 608, 2012.
10. Madhuchhanda Dasgupta and J.K.Mandal, Bit-plane Oriented Image Encryption Through Prime-Nonprime based Positional Substitution (BPIEPNPS), International Journal of Computer Sciences and Engineering, Volume-4, Special Issue-6, Aug. 2016.
11. R. Pravallikal, Lossless Encryption Using Bitplane and Edgemap Crypt Algorithms, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06, June -2017.
12. Mohammed G.S.AL-Safi, An Efficient Numerical Method for Solving Volterra-Fredholm Integro-Differential Equation of Fractional Order by Using Shifted Jacobi-Spectral Collocation Method, Baghdad Science Journal, Vol.15(3) 2018.
13. Dennis G.zill and Warren S.Wright, "Calculus Early Transcendental", United States of America, Fourth Edition, 2011.
14. R. Aarthi and Mrs. S.Kavitha , "IMAGE ENCRYPTION USING BINARY BIT PLANE AND ROTATION METHOD FOR AN IMAGE SECURITY", International Journal of Engineering Development and Research(www.ijedr.org), Volume 5, Issue 2, ISSN: 2321-9939, 2017.
15. [15] R.Vijayaraghavan, S. Sathya and N. R. Raajan, Security for an Image using Bit-Slice Rotation Method-image Encryption, Indian Journal of Science and Technology, Vol 7(4S), 1-7, April 2014.
16. SHRIKANT S.KHAIRE and DR. SANJAY L. NALBALWAR,"Review: Steganography-Bitplane Complexity Segmentation (BPCS) Technique ", International Journal of Engineering Science and Technology, Vol. 2(9), 2010, 4860-4868.
17. N S T Sai and R C Patil, IMAGE RETRIEVAL USING BIT-PLANE PIXEL DISTRIBUTION, International Journal of Computer Science & Information Technology (IJCSIT), Vol 3, No 3, June 2011. V. Namias, The fractional order Fourier transform and its application in quantum Mechanics, Journal of the Institute of Mathematics and its Applications 25 (1980) 241-265.
18. S. Sathya, Image Encryption using bit-slice rotation method–for an image security, International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)Vol.3, Special Issue2 , March 2016.
19. Rafael C. Gonzalez, Richard E. Woods: Digital Image Processing, Third Edition, Pearson Education, June 20, 2012 .pp. 117-119.
20. R. Pravallika, LOSSLESS ENCRYPTION USING BITPLANE AND EDGEMAP CRYPT ALGORITHMS, International Research Journal of Engineering and Technology (IRJET), Volume: 04 Issue: 06, June-2017.

الملخص

من اهم مجالات البحث العلمي في اتصال الشبكات هو حماية البيانات السرية للصور من اي وصول محظور. لذا عمدت الدراسة الراهنة الى تطوير نموذج مضمون ضمانا عاليا لتشفير مثل هذه الصور بأستخدام نموذج رياضي/ رياضياتي جديد. الغرض من هذه الدراسة هو ابداء المساعدة لاي شخص في تشفير او فك تشفير الصور الرمادية بأمان. ولتشفير الصورة الرمادية خطوتان اولاهما استخدام النموذج الرياضي القابل للقلب من اجل الحصول على صورة رمادية مع بعض من الوضوح والثانية بأستخدام (Bit Plane) لاستعادة الصورة الفعلية.

AUTHORS PROFILE

Inaam R.Al-Saiq 2000 I got a M.Sc from the University Mustansiriya ,I served as Amina College Council for 2001 I participated in the first National Congress of Mathematics / Mustansiriya University Science On 26-25 / 9 for the year (2001) I participated in a conference Faculty of Sciences / University of Mustansiriya On 23-24 / 10 for the year (2001) I served as a responsible unit calculator / Faculty of Science / University of Kufa for the year 2002 I got the title of teacher in 2008 I served as a responsible unit of Statistics Faculty of Computer Science and Mathematics, I got Assistant Prof at 6/2017. I served as graduate and responsible member of the Scientific Committee for the year (2015)r (2008) Teaching Interests: 1- Calculus 2- Linear Al-gebra 3- Ordinary Differential Equation 4-Numerical Analysis using Matlab 5-computer(Windows, C++ language and Matlab) 6-theory of Matrices.

II-M.Sc from University of Babylon 2000, Computer Lab manager, College of Education for woman, University of Kufa. 1993-1997, Computer Center head, College of Education for woman, University of Kufa.1997-1999. Asst. in Dept. of Mathematics 2000-2001, College of Education for woman, University of Kufa, Central Computer unit director 2002, College of Education for woman, University of Kufa, Computer Department Head 2003-2005, College of Education for woman, University of Kufa, Asst. in Department of Computer Science 2009, Faculty of Mathematics & Computer Science, University of Kufa Asst. Dean for Scientific Affairs/ Faculty of Computer Science &Mathematics /2010-2013, Computer Department Head / Faculty of Computer Science &Mathematics / University of Kufa 28-2-2013 to 29-12-2016,