ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

RGB Image Encryption and Decryption Using Two Stage Random Matrix Affine Cipher Associated With Discrete Wavelet Transformation

Ravi Kiran K
Assistant Professor,
Department of CSE,
JNTUK, Kakinada, India.

G.Venkata Siva
Assistant Professor,
Department of CSE,
JNTUK, Kakinada, India.

Kalumsaraswathi
M.Tech Student,
Department of CSE,
JNTUK, Kakinada, India.

Saderla Siva Nageswara Rao
M.Tech Student,
Department of CSE,
JNTUK, Kakinada, India.

Abstract:

To increase confidentiality of image,we propose an RGB image encryption and decryption using two stage random matrix affine cipher associated with discrete wavelet transformation. In our proposed approach, color image encryption associated with DWT is immune to the known-plaintext attack and chosen-ciphertext attack, etc. This proposed approach is suitable for secure transmission of large size images that ensure the total number of possible keys (key space of the whole cryptosystem) for attackers to decrypt correct (or wrong) images depending upon the correct (or wrong) arrangement of parameters is very large.

INTRODUCTION TO IMAGEPROCESSING:

1. Image:

An image is a picture that has been created or copied and stored in electronic form. An image can be described in terms of vector graphics or raster graphics. An image stored in raster form is sometimes called a bitmap. In **image processing**, the input is an image (a video frame or photograph) and the output is that same image or certain characters associated with that image. The process involves a signal dispensation. The images are two dimensional signals where set signal processing methods are applied to the image.

Fig.1 RGB Image

1.1 Different Types of Image Models in Using Image Processing:

Color Image Models:

Visible light is composed of relatively narrow band of frequencies in the electromagnetic energy spectrum - approximately between 400 and 700 nm. A green object, for example, reflects light with wavelength primarily in the 500 to 570 nm range, while absorbing most of the energy at other wavelengths. A white object reflects light that is relatively balanced in all visible wavelengths.

Blue (B)	= 435.8 nm
Green (G)	= 546.1 nm
Red (R)= 700.0 nm	

The primary colors can be added to produce the secondary colors magenta (red + blue), cyan (green + blue), and yellow (red + green), Color television reception is based on this three color system with the additive nature of light. There exists several useful color models: RGB, CMY, YUV, YIQ, and HSI - just to mention a few.

RGB colormodel:

The colors of the RGB model can be described as a triple (R, G, B), so that R, G, B . The RGB color space can be considered as a three-dimensional unit cube, in which each axis represents one of the primary colors, Colors are points inside the cube defined by its coordinates. The primary colors thus are red=(1,0,0), green=(0,1,0), and blue=(0,0,1). The secondary colors of RGB are cyan=(0,1,1), magenta=(1,0,1) and yellow=(1,1,0).

Advantages of Image Processing:

1. In many businesses, image processing applications are particularly crucial.
2. In rapidly growing technologies today, such as computer science and engineering, image processing is necessary in core research.
3. In image processing technique are mostly used in Military services,Scientific Experiments ,Medical Imaging and Online education and training .
4. For security of images we can use this process.

Disadvantages of Image Processing:

1. It's very costly depending on the system used, the number of detectors purchased.
2. Time consuming
3. Lack of qualified professional Easy to manipulate. Compact storage.

Applications of Image Processing:

1. **Intelligent Transportation Systems** – This technique can be used in Automatic number plate recognition and Traffic sign recognition.
2. **Remote Sensing** – For this application, sensors capture the pictures of the earth's surface in remote sensing satellites or multi – spectral scanner which is mounted on an aircraft. These pictures are processed by transmitting it to the Earth station.
3. **Defense surveillance** – Aerial surveillance methods are used to continuously keep an eye on the land and oceans. This application is also used to locate the types and formation of naval vessels of the ocean surface. The important duty is to divide the various objects present in the water body part of the image.

1.1 Organization of The Paper:

InSection2,we explained the proposed approach of TSRMA C and DWT. Aftera quick overview of TSRMAC and DWT ingeneral, We then presented in Section3, Demon stature of procedure.. Our Section 4 discussed about security analysis and robustness of the approach. In Section 5, we have drawn conclusion of this approach.

2. Two stager and ommatrix affine cipher and discrete wavelet transformation Affine Cipher:

The **affine cipher** is a type of Monoalphabetic substitution cipher, wherein each letter in an alphabet is mapped to its numeric equivalent, encrypted using a simple mathematical function, and converted back to a letter. After taking RMAC on an RGB image of size n x m. The Encryption is pixels of an RGB image is given matrix form in which even numbered rows and columns are shifted by parameters α and γ, and multiplied by parameters χ and λ, and Odd numbered rows and columns are shifted by parameters β and δ, and multiplied by parameters η and σ, respectively. Here selected even number of rows is shifted and odd number of rows will be zero in particular image of even number of pixels will be changed. To apply matrix affine cipher on an RGB image, we have 1st direction.

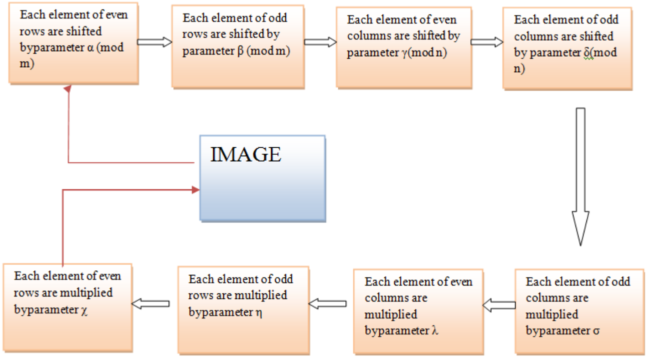

Each element of even rows are shifted byparameter α (mod m)
Each element of odd rows are shifted by parameter β (mod m)
Each element of even columns are shifted by parameter γ(mod n)
Each element of odd columns are shifted by parameter δ(mod n)
IMAGE
Each element of even rows are multiplied byparameter χ
Each element of odd rows are multiplied byparameter η
Each element of even columns are multiplied byparameter λ
Each element of odd columns are multiplied byparameter σ

Fig 2. Structure of random matrix affine cipher parameters.

For the process of RMAC parameters in RGB image size n X m are following equation,

$$X'_{EvenRow,k} = \chi X_{EvenRow,j+\alpha \bmod(m)}$$

$$X'_{OddRow,l} = \eta X_{OddRow,j+\beta(\mathrm{mod} m)}$$

$$X'_{P,Evencolumn} = \lambda X_{i+\gamma(\mathrm{mod} n),evencolum}$$

$$X'_{P,oddcolumn} = \sigma X_{i+\delta(\mathrm{mod} n),oddcolum}$$

For the process of IRMAC parameters in RGB image size n X m are following equation,

$$X_{Evenrow,j} = \mu X'_{Evenrow,k+m-\alpha(\mathrm{mod} m)}$$

$$X_{oddrow,j} = \kappa X'_{Evenrow,l+m-\beta(\mathrm{mod}\ m)}$$

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

$$X_{i,Evencolumn} = \nu X'_{p+n-\gamma\ (\mathrm{mod}\ n),\ EvenColoum\ n}$$

$$X_{i,oddcolumn} = \nu X'_{q+n-\delta\ (\mathrm{mod}\ n),\ OddColoumn}$$

In DWT has the RGB image are passed through a low filter(L) and high-pass filter (H) of images and then decomposed into four filters(i.e. LL,LH,HL,HH.)each of them is a quarter size of the original image.

DWT of an RGB image of f(x,y) size NxM is defined as

$$W_{\psi}(j_0,n,m)=\frac{1}{\sqrt{MN}}\sum_{X=0}^{N=1}\sum_{Y=0}^{M-1}(x,y)_{\varphi_{j0,n,m}}(x,y)$$

$$W_{\psi}^{i}(j,n,m)=\frac{1}{\sqrt{MN}}\sum_{X=0}^{N=1}\sum_{Y=0}^{M-1}f(x,y)_{\psi_{j0,n,m}^{i}}(x,y)$$

for j>j0

IDWT of an RGB image of f(x, y) size NxM is defined as

$$f(x,y)=\frac{1}{\sqrt{MN}}\sum_{n}\sum_{m}w_{\varphi_{j0,N,M}}(x,y)+\frac{1}{\sqrt{MN}}\sum_{i=H,V,D}\sum_{j=j0}\sum_{n}\sum_{m}W^{i}_{\psi_{j,n,m}}(x,y)$$

where jₒ, is an arbitrary starting scale. Here index 'i' identifies the directional wavelets that assumes the values H, V, and D and Equations are define the scaled and translated basis functions, respectively.Normally, we let j_0=0and select N_1,N_2 to be a power of 2 (N_1 =N_2 =2^J) , so that the summations are performed over j = 0,1….J-1 and k1=k2=0,1,2……2^{j-1} . The Discrete Wavelet Transform (DWT) is obtained by filtering the signal through a series of digital filters at different scales. The scaling operation is done by changing the resolution of signal by process of sub sampling.

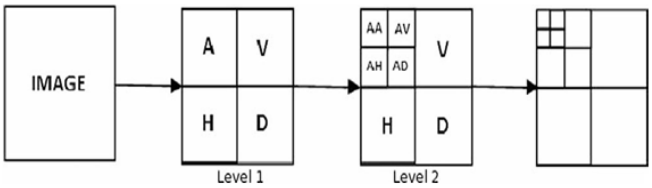


Fig. 3The Structure Of Wavelet Decomposition At Different Levels.

Wavelet analysis is computed by filter bank. There is two type of filter

1) High pass filter:

high frequency information is kept, low frequency information is lost.

2) Low pass filter:

law frequency information is kept, high frequency information is lost.

3) Demonstration of the procedure:

The procedure is applied on a JPEG RGB image of size 256x256x3 pixels as shown in Fig.3.1

Encrypted RGBimage with the following keys and the RMAC parameters are:

Alpha R=1, betaR=2, gamaR= 3, deltaR=4, chiR=5, sigmaR=8,

Alpha G=9, betaG=10, gamaG=11, deltaG=12, chiG=13, sigmaG=16,

Alpha B=17, betaB=18, gamaB=19, deltaB=20, chiB=21, sigmaB=24 with 'db4' wavelet.

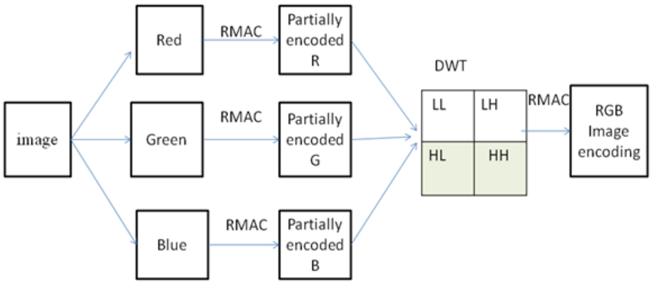


Fig.3.1.Encryption process for anRgb image

Hence here correctly decrypted RGB image with exact keys and correct arrangement of RMAC parameters. Alpha R=1, beta R=2, gama R= 3, delta R=4, chi R=5, sigma R=8,

Alpha G=9, beta G=10, gama G=11, delta G=12, chi G=13, sigma G=16,

Alpha B=17, beta B=18, gama B=19, delta B=20, chi B=21, sigma B=24.

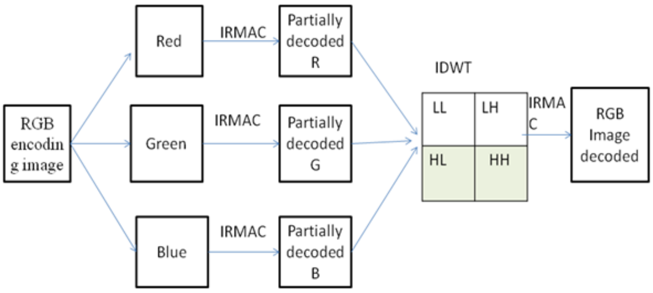


Fig.3.2.Decryption process for an Rgb image

4. Security analysis:

The proposed system has been investigated using digital simulation carrying out on Mat lab platform to verify the performance, security and robustness of a proposed algorithm.

Performance and security:

Comparing restoration results requires a measure of image quality. Two commonly used measures are

1 .**Mean-Squared Error and**

2. Peak Signal-to-Noise Ratio

1. MSE is One problem with mean-squared error is that it depends strongly on the image intensity scaling. A mean-squared error of 100.0 for an 8-bit image (with pixel values in the range 0-255) looks dreadful, but a MSE of 100.0 for a 10-bit image (pixel values in [0, 1023]) is barely noticeable.

Following the equation measured in Mean Square Error

$$\text{MSE}=\frac{1}{M*N}\sum_{i=1}^{M}\sum_{j=1}^{N}[I_i(i,j)-I_0(i,j)]^2$$

Where $I_i(i,j)$ and $I_0(i,j)$ are respectively input and output images at pixel position (i, j). M*N denotes the total number of pixel of the image.

2. PSNR is measured in decibels (dB). The PSNR measure is also not ideal, but is in common use. Its main failing is that the signal strength is estimated rather than the actual signal strength for the image. PSNR is a good measure for comparing restoration results for the same image, but between-image comparisons of PSNR are meaningless.

$$\text{PSNR}=10\log_{10}\left[\frac{R^2}{MSE}\right]$$

Where R is the maximum fluctuation in the input data type. The higher of MSE or Lower of PSNR values indicates the color information of image.

3. Histogram analysis

An **image histogram** is a type of histogram that acts as a graphical representation of the tonal distribution in a digital image. It plots the number of pixels for each tonal value. The histogram plots the number of pixels in the image (vertical axis) with a particular brightness value (horizontal axis). Histogram analysis of RGB image of size 256x256x3 pixels.

3.2.Histogram Analysis in Rgb encrypted image

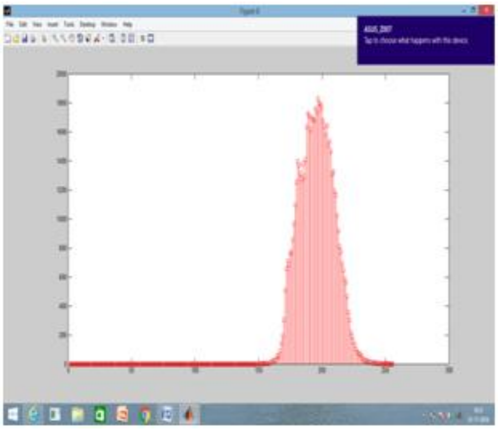


Fig.3.2.1. Red colorhistogram in encrypted rgbcolor image

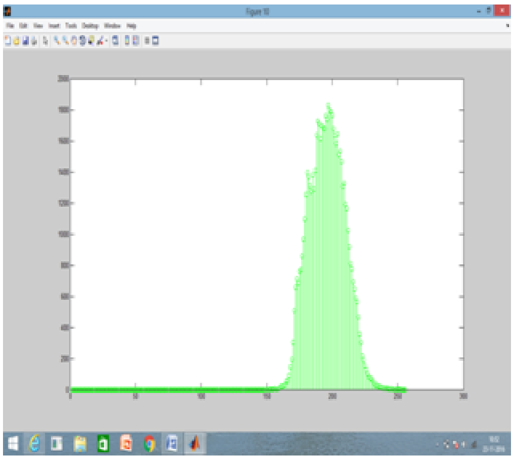


Fig.3.2.2. Green colorhistogram in encrypted rgbcolor image

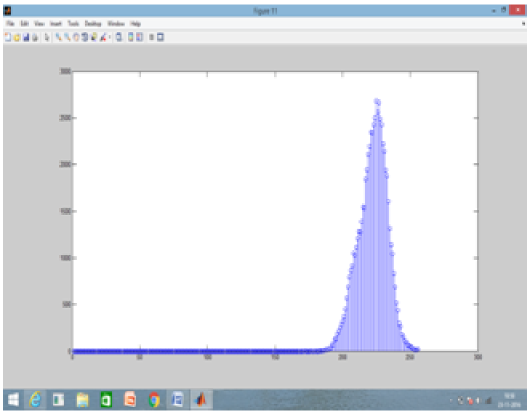


Fig.3.2.3.Blue colorhistogram in encrypted rgbcolor image

The x axis of the histogram shows the range of pixel values. Since its an 8 bppimage , that means it has 256 levels of gray or shades of gray in it. Thats why the range of x axis starts from 0 and end at 255 with a gap of 50. Whereas on the y axis , is the count of these intensities.

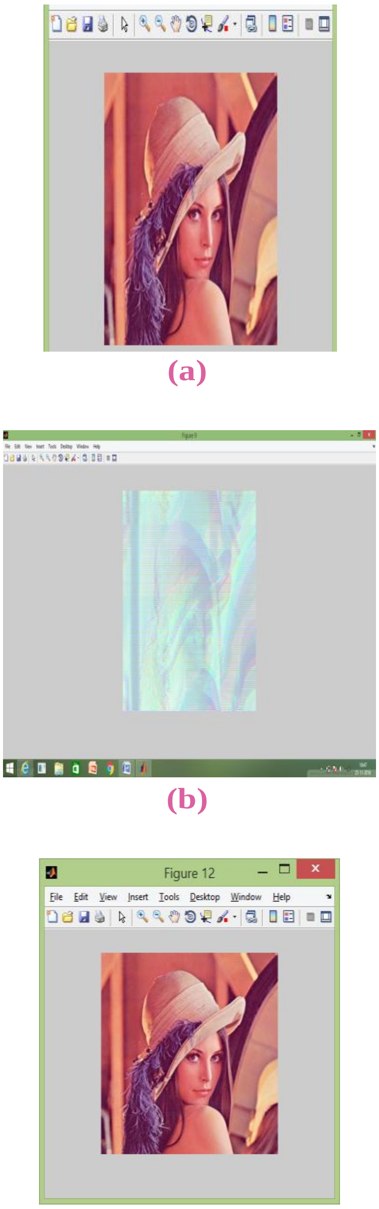
Robustness Text:

The robustness of the proposed algorithm has been confirmed against the chosen and known plaintext attacks. Image encryption should be robust against all types of cryptanalytic. In known plaintext attack a cryptanalyst has an access to a plaintext and the corresponding ciphertext and try to derive a correlation between these two or by applying the same key try to decrypt ciphertext for the encrypted plaintext.

5.Result and Analysis

Encrypted and decrypted rgb image of output

RGB image encryption scheme such as known-plaintext attack and chosen-ciphertext attack. In knownplaintext attack a cryptanalyst has an access to a plaintext and the corresponding ciphertext and try to derive a correlation between these two or by applying the same key try to decrypt ciphertext for the encrypted plaintext.



(a)

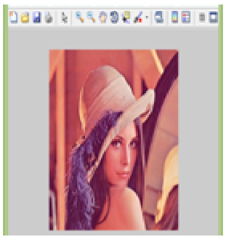
(b)

(c)

Fig.5.1 Plain Image 256x256 pixels

Fig. b) Color image Correctly encrypted with RMAC parameters and key 256x256 pixels. Fig.5.1 c)Correctly decrypted image with correct keys and correct. In this fig.5.2.is Correctly encrypted image in 256x256 pixels with applying for the RMAC parameters and key. Here using shifting and multiplying parameters then applying to each pixel of particular color image.

Fig.5.1 Plain Image 256x256 pixels



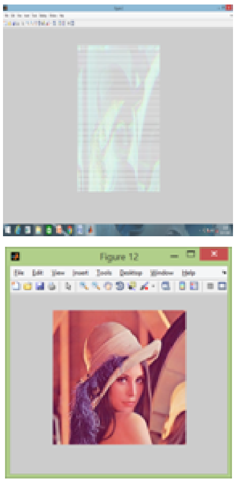


Fig.6.1.4 Incorrectly decrypted image

In this Fig6.1.4.has Incorrect decrypted image with pixel size is 256x256x3 wrong arrangement of parameters and keys. Here shifted parameters and pixels may be changed to encrypted image.

6.CONCLUSION:

In this thesis we have proposed RGB image encryption and decryptionusing two stage random matrix affine cipher (RMAC) associated with discrete wavelet transformation. For large size of images the possible to range of key size is excessive so it is computationally infeasible to correctly decrypt the original image by intruders. In this method, decryption process is more unmanageable, especially in the case when there is no further information about the correct keys and the possible correct arrangement of RMAC parameters. Security Analysis is comparison between our approach and other approach shows that our correctly encrypted and decrypted image has very low information in Mean Square Error (MSE), when compared to PSNL signals ratio (Peak Signal Noise Ratio). So, This approach can be used for transmission of RGB image data efficiently and securely through unsecured channels.

5.1 Future Scope:

In future, In a generalized scheme we may want to provide Flexibility, Spatial selectivity, Self sufficiency and compliance that may be added to provide a better state of confidentiality of information. Also a generalised image encryption scheme should provide Robustness against known-plaintext attack and chosen cipher text attack, the same is tend to achieve in our future and the future work for such scheme is in the process. So as to provide ruggedness, for instance If attacker knows about all the possible exact keys, but not aware about correct arrangement of RMAC parameters, intruder cannot decrypt the image correctly.

References:

[1] Antonini M, Bar laud M, Mathieu P, Daubechies I. Image coding using wavelet transform. IEEETransImageProcess1992;1:205–20.

[2] Andreas Savakis and Richard Carbone14623, Discrete Wavelet Transform Core for Image Processing Applications.

[3] Muhammad RafiqAbuturab,Color image security system using double random-structured phase encoding in gyrator transform domain.

[4] Abuturab MR. Noise-free recovery of color information using a joint-extended gyrator transformcorrelator.

[5] Chen L, Zhao D. Optical image encryption with Hartley transforms.

[6] Liu S, Mi Q, Zhu B, Optical image encryption with multistage and multichannel fractional Fourier-domain filtering.

[7] Anand Joshi1, ManeeshaKumari, Encryption of RGB image using involuntary matrix associated with Arnold transformation.

[8] Akhilesh Prasad, Manish Kumar, Devdeep Roy Choudhury Colour image encoding using fractional Fourier transformation associated with wavelet transformation.

[9] Abuturab MR. Color image security system based on discrete Hartley transform in gyrator transform domain. Opt Lasers Eng 2013;51:317–24.

[10] Zhang Y, Zheng CH, Tanno N. Optical encryption based on iterative fractional Fourier transform. Opt Commun 2002;202:277–85.

[11] Joonku Hahn, Hwi Kim, and Byoungho Lee, Optical implementation of iterative fractional Fourier transform algorithm.

[12] Z. Liu, J. Dai, X. Sun, and S. Liu, “Color image encryption by using the rotation of color vector in Hartley transform domains,” Opt. Laser Eng. 48, 800–805 (2010).

[13] H.M. Ozaktas, Z. Zalevsky, M.A. Kutay, The Fractional Fourier Transform with Applications in Optics and Signal Processing, Wiley, New York, 2001.

[14] Chen L, Zhao D. Image encryption with fractional wavelet packet method, Optik; 119:286-91, 2008.