EasyChair Preprint

№ 7341

RGB Image Encryption and Decryption Using Discrete Wavelet Transformation

Lova Kumari Mudiduddi, Priyadarshini Cholla,
Supriya Jalamanchi and Saraswathi Kalum

January 18, 2022

RGB Image Encryption and Decryption Using Discrete Wavelet Transformation

M Lovakumari[1], Dept of CSE,University college of Engineering Kakinada,JNTUK,lovakumari584@gmail.com
Ch Priyadarshini[2], Dept of CSE,University college of Engineering Kakinada,JNTUK, ch.priyadarshini84@gmail.com
J Supriya[3],Dept of CSE, Ashoka womens Engineering college karnool, supriyajalamanchi76@gmail.com
kalum Saraswathi[4], Dept of CSE,University college of Engineering Kakinada,JNTUK, saraswathi.kalum@gmail.com

Abstract. Because digital RGB colour photographs are the furthermost extensively used information type on the internet, nearby is a demand for safe digital images, which is a high-priority activity. RGB picture encryption and decryption exhausting a two-stage random matrix affine cypher connected to discrete wavelet transformation to boost image confidentiality. The colour image encryption coupled with discrete wavelet transform in our anticipated technique is subject to known-plaintext and chosen cipher- textbook attacks, among other things. This suggested method is appropriate for secure conduction of enormous images, as it ensures that the overall amount of probable keys (key space of the entire cryptosystem) for assailants to decrypt proper (or incorrect) imageries based on the right (or incorrect) parameter organization is precise vast.

Keywords: image encryption, Discrete wavelet transformation, image decryption, Discrete Wavelet Transformation

1 Introduction

The major goal of this research is to create a high level of safety for image transmission over an open network. The encryption method used here is centered on the Two Stage Random Matrix Affine Cipher (TSRMAC), which is combined through the Discrete Wavelet Transformation (DWT) to provide safe image data transmission. The protection of photographs has become a top priority in the modern era. Several options for sending photographs around the world are available thanks to network and communication technology. Images are widely employed in a variety of fields, including defence, engineering, scientific investigations, medical imaging, publicizing, art exhibitions, and online teaching and training. The ultimate dispute of securing images for privacy, reliability, validation, and non-repudiation is a key distress with the aggregate usage of digital systems for sending and storage images. Several methods for securely encrypting and decrypting image data have been proposed. Authors like as [1–4] suggested image encryption and decryption consuming fractional Fourier transformation; [5–10] proposed image encoding and decoding above gyrator transform domain collective by further procedures; [11,12] proposed image encryption expending Hartley transform; [13–15] proposed image

coding using wavelet transform; [16–19] suggested optical transforms for encrypting and decrypt Recent investigations on the security of colour images, however, have demonstrated that they are vulnerable to assaults like as the known-plaintext attack, chosen-ciphertext attack, among others [22,23]. Image data is not the only type of data that can be attacked; text data, signals, and other types of data can also be targeted. The colour picture encryption we propose utilising RMAC and DWT is insusceptible to known-plaintext also chosen-ciphertext attacks, among other things.

1.1 Image

An image is a portrait that had remained generated, replicated, and hoarded in digital procedure. Vector graphics then raster graphics are two categories of graphics that could be used to describe an image. A bitmap is a raster image that is stored in a raster format. An image (a photograph or video frame) is the input, and the output was the equivalent image or specified characteristics connected thru an image. A signal exemption is part of the process. The images were two-dimensional signals that have been subjected to a set of signal processing procedures.

Fig. 1. RGB Image

2. Image Models of Various Types in Image Processing

2.1. Models of Color Image

On the electromagnetic energy spectrum, noticeable light is undistributed of a very narrow group of frequencies among 400 and 700 nm. As a prototype, a green objective reproduces light by wavelengths mostly in the 500 to 570 nm range although captivating the majority of energy on other wavelengths. A white object reproduces light with a fairly even distribution of perceptible wavelengths.

Green (G) = 545.3 nm
Blue (B) = 434.9 nm
Red (R) = 701.2 nm

The tributary colours magenta (red + blue), cyan (green + blue), and yellow (red + green) can be made by mixing the basic colours. Color box response is centered on these 3color schemes by the preservative fauna of sunlight. Nearby are numerous colour models that are useful: To name a few, there's RGB, YUV, CMY, YIQ, and HSI.

2.1 RGB color model

The RGB mockup's colours could be designated equally per a triple (R, G, B), meaning R, G, B. Colors are points classified the cube definite by their organizes, and the RGB colour interplanetary can be thought of as a 3D entity dice with respectively axis representing one for main colours. As a result, the primary colours are red=(1,0,0), green=(0,1,0), and blue=(0,1,0) (0,0,1). Cyan=(0,1,1), magenta=(1,0,1), and yellow=(0,1,1) are RGB's secondary colours (1,1,0).

3. Image Processing's Benefits

• Image processing applications are extremely important in many organisations.
• Image processing is required in essential research in today's fast evolving technologies, such as computer science and engineering.
• Scientific experiments, Military services, medicinal imaging, and online education and training are all examples of image processing techniques.
• We can utilise this approach to secure photos.

4. Image Processing Disadvantages

• It is extremely expensive, reliant on a system employed and the amount of indicators obtained.
• It takes a long time
• A scarcity of qualified personnel It's simple to run. Storage that is little.

Please attach a readme with your final files, indicating whichever of our titles is/are your first title(s) and whichever is/are our family title(s). For Spanish and Chinese names, this is very significant. In the author index, the authors are listed alphabetically by surname..

5. Image Processing Applications

- Intelligent Transportation Systems (ITS)– ITS is commonly utilised in involuntary amount plate identification and traffic signal recognition.
- Remote Sensing — In this submission, sensors in a remote sensing satellite broadcasting or a multi-spectral scanner positioned on an aeroplane collect photos of the globe's superficial. These imageries are then analysed by sending them to the planet station.

- Defense surveillance - Airborne surveillance is employed to maintain a constant eye on the terrestrial and oceans.
- This tool can too be used to discover the categories and formations of ocean surface naval vessels. The most crucial task is to divide the many things found in the image's water section.

6. Two stage then ommatrix affine cipher and discrete wavelet transformation Monoalphabetic substitution cipher

Monoalphabetic substitution cipher could be a style of the affine cipher, respectively epistle of a alphabet is recorded to its numeric equivalent, encrypted with a elementary measured formula, and formerly distorted hindmost to a message. Afterward applying RMAC to an RGB image with dimensions of n x m. Smooth totaled columns and rows are removed by constraints, also reproduced by constraints and, although odd totaled columns and are rows lifted by constraints and, and grew by constraints and, correspondingly. In this case, an even amount of rows is lifted and an peculiar quantity of rows is set to nothing, resulting in a new image with an level amount of pixels. The first direction is used to apply matrix affine cypher to an RGB image.

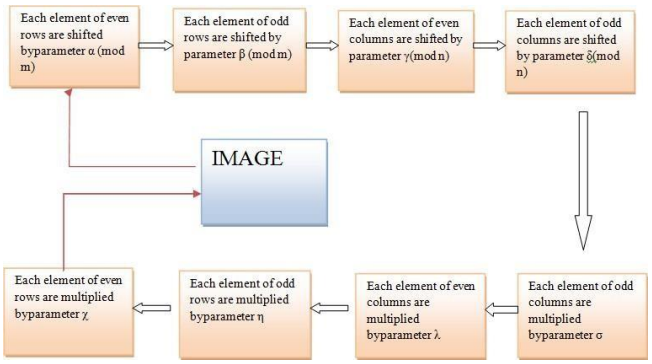

Fig 2. Parameters for affine cyphers with random matrix structure.

The following equation is used to calculate RMAC parameters in RGB images with a dimension of n X m,

$$X_{EvenRow,k} = \chi X_{EvenRow,\, j+\alpha \bmod(m)} \quad (1)$$

$$X_{OddRow,l} = \eta X_{OddRow,\, j+\beta \,(\mathrm{mod} m)} \quad (2)$$

$$X_{i,Evencolumn} = \lambda X_{i+\gamma \,(\mathrm{mod} n),evencolum} \quad (3)$$

$$X_{i,oddcolumn} = \sigma X_{i+\delta \,(\mathrm{mod} n),oddcolum} \quad (4)$$

The following equation is used to calculate IRMAC parameters in RGB images with a dimension of n X m,

$$X_{Evenrow,j} = \mu X_{Evenrow,k+m-\alpha\,(mod m)} \quad (5)$$

$$X_{OddRow,l} = \eta X_{OddRow,j+\beta\,(mod m)} \quad (6)$$

$$X_{i,Evencolumn} = \nu X_{p+n-\gamma\,(mod n),evencolum} \quad (7)$$

$$X_{i,oddcolumn} = \nu X_{p+n-\delta\,(mod n)_i,oddcolum} \quad (8)$$

The RGB picture in DWT is processed through a high-pass filter (H) and a low-pass filter (L) before being broken into 4 filters (i.e. LH, LL, HH, HL,.) Individually one is a fourth of the imaginative image's size.

The DWT for a RGB image of size NxM with f(x,y) is definite as

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

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

The IDWT for a RGB image of size NxM with f(x, y) is demarcated as

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

Wherever jo is a arbitrary scale to begin with. The directional wavelets with the standards V, H, and D are identified by the index "i." The scaled then translated center functions are defined via equations. Usually, we contract j_0=0and select N_1, N_2 to be a power of 2 (N_1 =N_2 =2^J) , so that précises are done above j = 0,1,...J-1 and k1=k2=0,1,2.....2j-1 Filtering a signal done a succession of digital filters at diverse sizes yields the DWT. Scaling might accomplished via adjusting a signal's tenacity concluded the subsampling process.

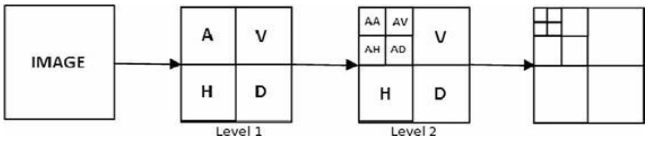

Fig. 3 Wavelet Decomposition Structure at Different Levels.

The filter bank does wavelet analysis. Filters are divided into two categories.

6.1 High pass filter:

High-frequency data was saved, but low-frequency data is vanished.**6.2 Low pass filter:**Info with a low frequency is maintained, while information with a high frequency is lost.**The process will be demonstrated:**

The technique is performed on a 256x256x3 pixel JPEG RGB image as publicized in Fig. 3.1 Encrypted RGBimage per the subsequent keys and RMAC constraints:

betaR=2, Alpha R=1, gamaR=3, deltaR=4, chiR=5, sigmaR=8,
betaB=18, Alpha B=17, gamaB=19, chiB=21, deltaB=20, sigmaB=24,
betaG=10, Alpha G=9, gamaG=11, chiG=13,deltaG=12, sigmaG=16,
betaB=18, Alpha B=17, deltaB=20, gamaB=19.

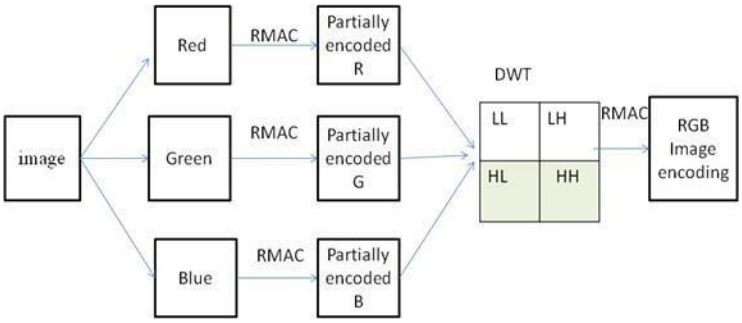

Fig.4. The process of encrypting an RGB image

As a result, we have a properly decrypted RGB image with precise keys and RMAC settings. beta R=2, Alpha R=1, delta R=4, gama R=3, sigma R=8,chi R=5, beta G=10, Alpha G=9, delta G=12, gama G=11, sigma G=16, chi G=13, beta B=18, Alpha B=17, delta B=20, gama B=19, beta B=18, Alpha B=17, delta B=20, gama B=19, sigma B=24, chi B=21.

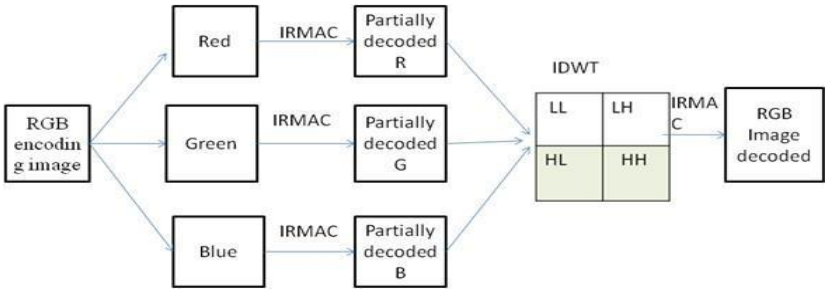

Fig.5. An RGB image's decryption procedure

6.3 Security analysis:

To authorize the presentation, security, also resilience of a given method, the suggested system was inspected utilising digital simulation on the Matlab platform.

6.5 Security and performance

A measure of image quality is required to differentiate restoration results. The

following are two regularly used measures:

6.5.1 Mean-Squared Error and

6.5.2 Peak Signal-to-Noise Ratio

Error-in-Squares (MSE) One dispute through mean squared error is which it is constantly dependent on image concentration scaling. An MSE of 100.0 aimed at an 8bit image (pixel standards in the range 0255) appears to be terrible, while an MSE of 100.0 for a 10bit image (pixel standards in the range [0, 1023]) is scarcely perceptible.

In order to calculate the Mean Square Error, use the equation below.

$$MSE=\frac{1}{M*N}\sum[I_{i}(i,j)-I_{0}(i,j)]^{2}$$

Where $I_{i}(i,)$ then $I_{0}(i,j)$ are the pixel positions of the input and output images, correspondingly (i, j). The total quantity of pixels in an image is denoted by M*N.

The PSNR is expressed in decibel (dB). The PSNR metric is moreover not optimal, nevertheless it is widely used. Its primary flaw is that signal intensity is guessed somewhat than the image's definite signal strength. PSNR may be a useful metric for associating reinstatement consequences for similar images, however PSNR comparisons between images are nonsensical.

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

Where R is the computer file type's maximum fluctuation. The colour information of a picture is indicated by the greater or lower PSNR values.

6.5.3 Analyzing histograms

An image histogram has a category of histogram which works as a graphical illustration of a digital image's tonal distribution. It displays the quantity of pixels associated with respectively tonal significance. The histogram shows the quantity of pixels in a picture (vertical axis) corresponding to a specific illumination significance (horizontal axis). Review of the histogram of a 256x256x3 pixel RGB image.

6.5.3. RGB Encrypted Image Histogram Analysis

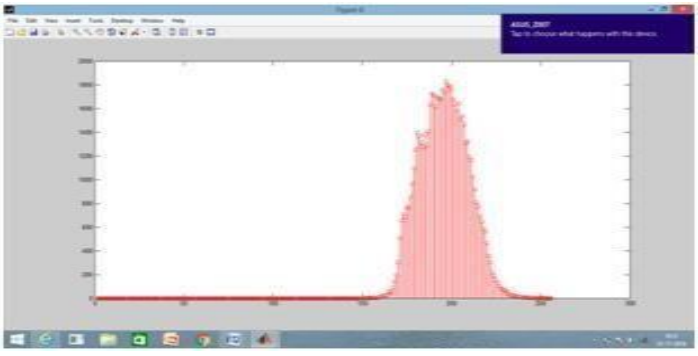

Fig.7. Red color histogram in encrypted RGB color image

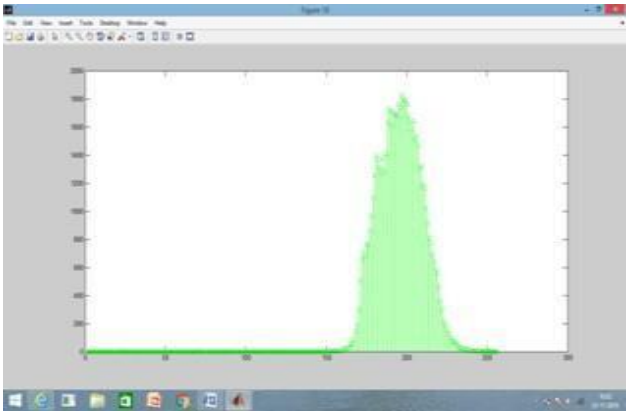

Fig.8. Red color histogram in encrypted RGB color image

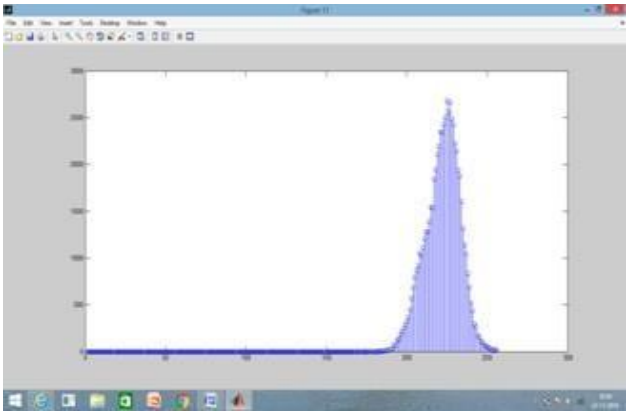

Fig.9. The blue color histogram in encrypted RGB color image

The histogram's x-axis displays the range of pixel standards. In the case of an 8 bpp image, this incomes that it contains 256 levels of grey or obscuration of grey. As a result, the x-axis range began at 0 and ended on 255, through a 50-point gap. Because the consequence of these concentrations may be seen on the y-axis.

6.5.4 Text on Robustness

The predicted algorithm's stability has been proven against selected and known-plaintext assaults. All sorts of cryptanalytic should be resistant to image encryption. A cryptanalyst with access to the interaction between these two can use the identical key to decrypt ciphertext on behalf of the encrypted plaintext into a known-plaintext occurrence.

6.5.5 Analysis and Result

RGB image of output that has been encrypted and decoded

The known-plaintext occurrence and the chosen-cipher text occurrence were two RGB picture encryption schemes. In a known-plaintext occurrence, a cryptanalyst had admittance toward plaintext also the matching cypher text and attempts to originate a correspondence among the two, or decrypts cypher text for the encrypted plaintext using the same key.

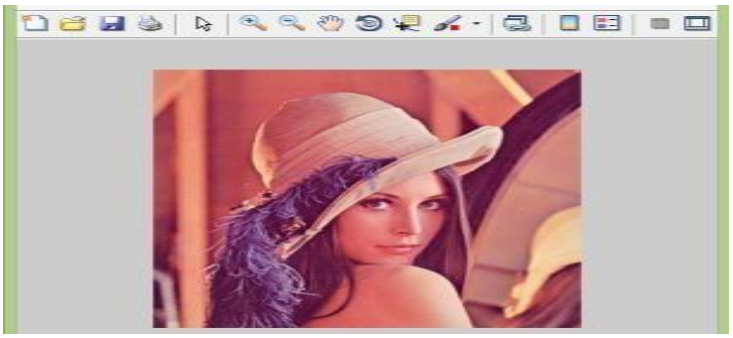

Fig.10. Color image

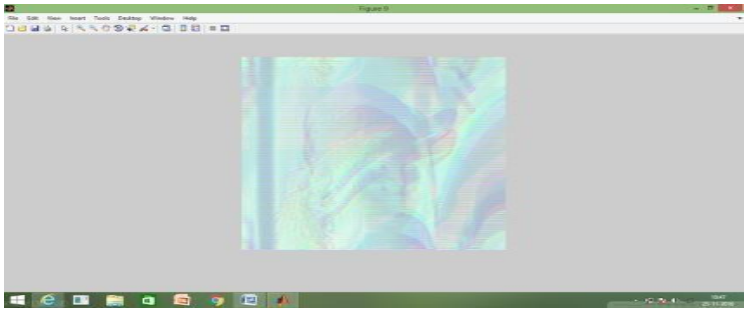

Fig.10. Image in colour RMAC parameters and a key of 256x256 pixels were used to properly encrypt the data. Figure 5.1 c) With the necessary keys and decryption, the image was correctly decoded. Figure 5.2 shows a successfully encrypted image into a 256x256 pixels by an RMAC limits then key applied. Exhausting fluctuating with the multiplying parameters, separately pixel of the given colour image is then applied.

Fig.11 256x256 pixels plain image

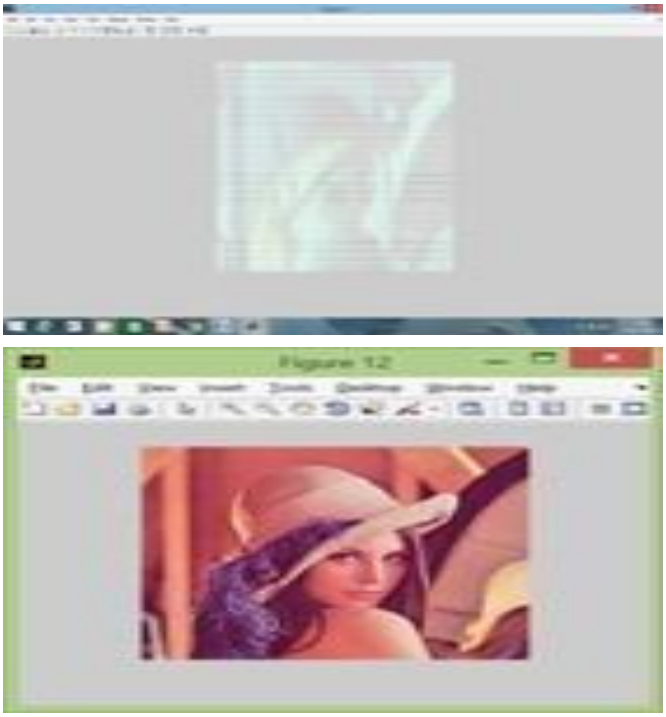

Fig.12. incorrectly decrypted image

In this Fig.12. Has an Incorrectly decoded image with pixel size of 256x256x3 and incorrect parameter and key structure. To the encrypted image, shifting settings and pixels can be modified here.

7. CONCLUSION

In this paper, we present a two-staged random matrix affine cypher (RMAC) through discrete wavelet modification for RGB picture encryption and decryption. The allowable range of key sizes for huge photos is excessive, making it computationally impossible for intruders to properly decrypt an original image. The decryption procedure is further insurmountable in this manner, especially when such no additional knowledge nearly a correct keys or the likely precise RMAC parameter preparation. When comparing our technique to other approaches, security analysis demonstrates our appropriately encrypted then decrypted image has actual low info into Mean Square Error (MSE) once related to PSNL signals ratio (Peak Signal Noise Ratio). As a result, this method could be recycled to send RGB picture statistics over insecure channels proficiently and steadily.

8. Future Prospects

In the future, we might famine to add Tractability, Self-sufficiency, Spatial selectivity, and conformance to a generalised scheme to create a improved formal of information privacy. A comprehensive image encryption technique could also be robust beside known-plaintext and chosen cypher text attacks; this is something we want to complete in the forthcoming and prospect work on like a organization is already underway. For example, if an attacker recognizes all of the conceivable precise keys however are unaware of the proper RMAC parameter procedure, the intruder will be unable to decrypt the picture successfully.

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 ore for Image Processing Applications.

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

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

[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 the 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.
[15] Hahn J,KimH,LeeB.Opticalimplementationo fiterative fractional Fourier transform algorithm.OptExpress2006;14:11103–12.
[16] Hennelly B,SheridanJT. Optical image encryption by random shifting infractionalFourierdomains.OptLett2003;28:269–71.
[17] Liu Z,LiuS.RandomfractionalFouriertransform.OptLett2007;32:2088–90.