JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

MULTISTORAGE DISTRIBUTED SYSTEM FOR IMAGE SECURITY USING DUAL MODE ENCRYPTION

[1]M.Angel Shalini, [2]Rajan. R
[1] Assistant Professor, [2] Scholar,
[1,2]Department of Computer Applications(PG),
[1,2]Hindusthan College of Arts & Science, Coimbatore.

Abstract : In today's world, security is a top priority, and encryption is one of the best alternatives for ensuring security. Furthermore, many image encryption schemes have been proposed, each with its own set of strengths and weaknesses. Cryptography is important in securely transferring images. So, that cryptographic method with higher level of transformation with the image pixels. With a development of image processing technologies the image first get placed with pixels to make an extreme complexity to the attacker/ hacker. The image is then encrypted with its binary values using the Rubik's Cube encryption algorithm and the Elliptic Curve Cryptographic (ECC) algorithm in the second stage. The pixels with a random key generated will be encrypted by the followed algorithms. The input 2-D image is converted into a 1-D array using binary sequence conversion, with each pixel examined and divided using a rule-based examination. To improve security against hackers, the image is stored in a distributed database in a random pixel storage manner for secure server access. In comparison to existing solutions, the proposed image encryption method has lossless, good peak signal to noise ratio (PSNR), symmetric key encryption, less cross correlation, a very large number of secret keys, and key-dependent pixel value replacement with high security.

Index Terms - Image Encryption, Image Decryption, Security, Rubik's cube Algorithm, Elliptic Curve Cryptography, XOR Algorithm**.**

I. INTRODUCTION

Network security is a broad term that encompasses a wide range of technologies, devices, and processes. The configuration was created to safeguard the integrity, confidentiality, and accessibility of computer networks. The network layers provide security for both users and organisations. Many people try to harm our Internet-connected computers, violate our privacy, and prevent us from using Internet services. Because of the frequency and variety of existing attacks, as well as the threat of new destructive future attacks, network security has emerged as a critical topic in the field of cyber security. Network security measures enable computers, users, and programmes to perform critical functions in a se

In cryptography, the process of converting data from one form to another uses an algorithm or a mathematical function to render it unreadable. Rubik's cube and the ECC algorithm are two image encryption algorithms that are implemented in image security systems. The ECC based public key cryptography system makes the efficiency of the image encryption system. It is used for both encryption and the decryption methodology using the JAVA window form system. The security can be enhanced at a high level where the multiple complex techniques have been added to predict the image before encryption and after decryption. Image encryption tries to convert the image into a non understandable form. This process adds to secure the image from the hacker side and the attacker side. As the pixel gets stored in the distributed server so that the pixel can't be misused by any number of users. The public key is utilized for the encryption and the decryption process.

II. II. RELATED WORK

This section primarily describes an overview of chaos and non-chaos-based image encryption techniques. The existing method is used for image encryption, whereas the proposed method is used for multistored distributed systems with dual mode encryption. [8] proposes a novel rubik's cube-based scrambling in row and column directions for high efficiency scrambling. The non chaos method is used in [2] to determine the BLP and BLT techniques with the efficiency of the PSNR values using the row level and column level permutation techniques. The added implementation has improved the level of network security where Zhi-liang Zhu [16] proposed a chaotic based bit level permutation with pixel permutation added through it. Image compression using the grey scale image encryption technique is widely used in image

processing techniques [12], where the compression changes the pixel levels and is combined with efficiency. However, the user can only add the JPEG image to compress the pixels. The efficiency of cyclic group transformation systems combined with symmetric key encryption methodology. [11] Has maintained a cyclic process, which is proposed here, with the added efficiency of loading methodology. [2] A comparison of image encryption algorithms is performed. The algorithms used are AES, DES, genetic, XOR, ECC, and affine transform. According to the comparison and analysis results, ECC is the best choice for the image encryption algorithm because the key sensitivity analysis is high. Researchers have shifted their focus to multiple-image encryption because modern multimedia security technology requires a high efficiency of secret information transmission. There have been numerous multiple-image algorithms presented. A multiple-image algorithm with efficient security is placed, which employs the pixel exchange operation and vector decomposition system. The main advantage of 3D chaotic map encryption technology [4] over image encryption is the chaotic map technique involved with the efficiency overload in it.

The current methodology is based on two types of survey papers that work together to form a high security image encryption scheme. To increase the security of images transmitted over networks, a non-chaos-based encryption technique has been implemented.. A cyclic group progression is enhanced where the pixel based security are employed. A permutation based techniques is proposed with an iterative process where the confusion and the diffusion phase produced. This makes the higher security compared to the normal chaos based encryption techniques. An XOR algorithm based image encryption is implemented in the existing approaches. The image before encryption is added with the Confusion and diffusion of pixels with the cyclic group properties. The image retrieval will be more difficult when this process are get implemented.

This paper proposes a novel Rubik's cube-based pixel level scrambling and simple XOR-based diffusion to safely transmit multimedia information (images) over an untrusted channel, such as social networks. The process combines the Rubik's cube algorithm with pixel confusion and diffusion with conventional pixels. The purpose of implementing this image accuracy system is to order image security with good enhancement.The rest of the chapter is followed by the proposed work in chapter 3describe the proposed the image encryption algorithm based on rubik's cube and ECC algorithm. Result and discussion are discussed in section 4. Finally, we conclude in section 5.

III. PROPOSED WORK

Here it is proposed a multi storage system with distributed system is enhanced for the higher level of security system. The RGB color model system is used to found out whether the original image has been retrieved without any distortions. The pixel can be divided as black 0 and white pixel 1 as binary numbers conversion. The pixel will be divided and encrypted using the ECC and Rubik's cube algorithms before being stored on multiple servers. This perceptible information can be reduced by lowering the correlation between image elements through the use of specific transformation techniques. The seed is determined using the approach's secret key. The seed is crucial in the construction of the transformation table, which is then used to generate the transformed image with a random number of block sizes. The operation of dividing and replacing an arrangement of the original image is referred to as the transformation process. The image can be divided into blocks, each of which contains a set number of pixels. The blocks have been repurposed as new locations. The block size should be kept small for better transformation.

In this case, the correlation will be decreased and thus it becomes difficult to predict the value of any given pixel from the values of its neighbors. At the receiver side, the original image can be obtained by the inverse transformation of the blocks. The distributed servers will be added for high security of pixel storage system.

The image acquisition technique uploads images in any format, which are all saved. The image contains many pixels, and pixel-based encryption will be used in phase 2. The image upload is followed by the RGB colour model system, which separates the RGB pixel values. The process of converting a colour image to a grayscale image involves converting the RGB values (24 bit) into grayscale values (8 bit). The grey scale conversion is one in which the pixel can be converted to grey scale with a value of 0-255. The histogram colour variation identifies the pixel variations, and the values are taken as 0's and 1's. Grayscale images are represented by 8 bit value

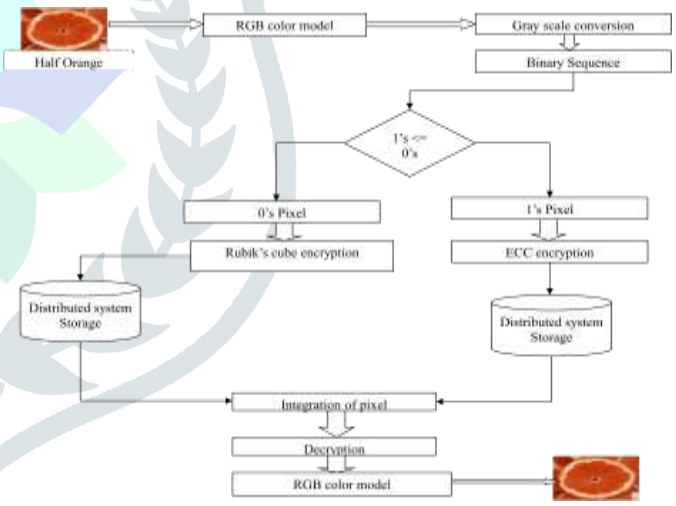


Figure 1 System Architecture of the Image Security Using ECC and Rubik's Cube Algorithm

(i) Pixel Division With Encryption

Here the pixel division are get carried out by the implemented system where the pixels are get divided with the binary values 0's and 1's. Usually the pixel value makes from 0-255 when it comes to black and white where the grey combinations will be added in the system. The divisions are combined with the two levels of rules taken place:

- The pixel values greater than equal to one are taken as the 1's pixel (i.e) given p is the pixel if (p>=1) taken as 1's value pixel. For an example p=156 then the pixel comes under 1's value.
- The pixel values lesser than 0 comes as 0's pixel (i.e) (p<=0)

then 0's value.

The pixel is divided into two formats using this implementation. This can now be carried out with additional security systems known as encryption, which will be in a user-incomprehensible format. Image encryption schemes are increasingly being researched in order to meet the demand for real-time secure image transmission over the Internet and wireless networks. Encryption is the process of transforming data to ensure its security. A massive amount of digital data is being exchanged over various types of networks as computer networks continue to expand and digital technologies advance. It is frequently true that much of this information is either confidential or private. Dividing the image into more blocks improved performance even more. The results showed that as the number of blocks increased, the correlation decreased and the entropy increased. From the browser, this encryption method can be applied to any image format such as jpg, tiff, ppm, pgm, or png. The advantages of this algorithm are that it can completely recover plain images and simplifies computations. The results of the experiments show that it is both practical and proficient.

Here two style of encryption is enhanced for high level of security.

- Rubik's cube Algorithm.
- ECC (Elliptic Curve Cryptography) Algorithm.

Rubik's Cube Encryption Algorithm

A Rubik's Cube algorithm is an operation on the puzzle which reorients its pieces in a certain way. An efficient image encryption using Rubik's cube algorithm for secure transmission of images is to achieve high efficiency.

Rubik's Cube Key Generation System

At first the rubik's cube key generation added where with the random numbers the key can be generated. Consider a gray scale image , yxI 0 of size M X N .Here each yx),(co-ordinates represent the pixel values of the image. The chaotic baker mapped image is used as the input image to the rubik's cube algorithm in the proposed system. **The encryption algorithm includes the steps listed below**.

Step 1: Generate two vectors KR and KC of lengths M and N at random. KR(i) and KC(j) each take a random value from the set A = 0, 1, 2,..., 2 1. It should be noted that KR and KC cannot have constant values.

Step 2: Determine the maximum number of iterations, ITERmax, and set the counter ITER to 0.
Step 3: Add one to the counter: ITER = ITER + 1.s.

Step 4: Compute the sum of all elements in each row I of image Io; this sum is denoted by (i),compute modulo 2 of I denoted by M(i), row I is left or right, circular-shifted by KR(i) positions (image pixels are moved by KR(i) positions to the left or right direction, and the first pixel moves into the last pixel).

Step 5: Use the Generated KR and KC to encrypt the scrambled pixels on each M(i), row, and column**.**

First, M x M image matrix is divided into k rectangles. Each rectangle should have a width of i v and contains M elements. x Select each rectangle, and arrange the elements are to a row in the permuted rectangle. Rectangles are selected from right to left. And then select upper rectangles, and then select lower rectangles. x Each rectangle is scanned from bottom left corner towards upper elements.

Elliptic Curve Cryptography Encryption Algorithm

Elliptic curve cryptography (ECC) is a public key cryptography approach that is based on the algebraic structure of elliptic curves over finite fields. The elliptic curve's properties and underlying equations are used by ECC to generate keys. At first, we assume that the distinguished points are at infinity, denoted by. (The coordinates must be chosen from a fixed finite field with a characteristic that is not equal to 2 or 3, and the curve equation must be slightly more complicated.) This set, along with the group of elliptic curve operations, is known as an Abelian group, with the points at infinity serving as the identity element..

The chord-and-tangent rule is used to add two points on an elliptic curve E(Fp) to get a third elliptic curve point. The set points E (Fp) form in conjunction with this addition operation, with O serving as the identity. This is the group that is used in the development of elliptic curve cryptosystems. Geometrically, the addition formula is explained. Let P = (x1, y1) and Q = (x2, y2) represent two discrete points on an elliptic curve E.

ECC Key Generation System

Input: An integer k>0 and a point P.

Output: Q=k*P.

Step 1: Set $k=(k_{l-1}\ldots k_1 k_0)_2$

Step 2: Set $P_1=P$, $P_2=2P$

Step 3: for I from l-2 down to 0 do

Step 4: If $k_i=1$ then

$P_1=P_1+P_2$, $P_2=2P$

Else

$P_2=P_2+P_1$, $P_1=2P_1$

Step5: RETURN (Q=P1).

Rubik's Cube and ECC Decryption Algorithm

The conversion of encrypted data into its original form is called Decryption. In the decryption process a key will be generated withthe encryption system which will be the private key. The generated key will be placed randomly where the original image can be combined from the distributed storage when the original user get accessed. Here the image can be stored with the 2 levels of encryption further decryption can be processed with two level of decryption. The Rubik's cube and the ECC algorithm key combined and decrypt the image. Now the scrambled image with multiple

pixels with 0's and 1's are obtained.The pixel with 0's and 1's will be turned with the 0-255 pixels wits its original pixel value. The pixel value gets combined and the binary value changed with the Gray scale conversion technique and the original image will be retained with the same PSNR values. Here the RGB values identified at before and after are getting matched to identify the original image retrieval. The original image are get compared with the related results obtained discussed in result and discussion session. Express the PSNR in decibels.

From Step 1, we have the decibed value LdB as

LdB = 10 log10 (P1/P0) ⟶ (4.2)

Now let

P1 = MAX^2 and ⟶ (4.3)

P0 = MSE ⟶ (4.4)

We then have

PSNR = 10 log10(MAX^2/MSE) ⟶ (4.5)

From the obtained PSNR values before the image could be taken and after the image taken will be identified for the retrieval of the original.

IV. Result and discussion

In this section result of color image encryption using ECC and Rubik's cube is presented. The result includes image during binary conversion and image during the process of quantization is presented. It likewise includes the decrypted result. Usually, Encryption Process is evaluated by the following procedure:

1. Standard Deviation
2. Quality of Encryption.

1. Standard Deviation

Let b be the number of bits used in the pixel of the image Plaintext / Ciphertext indicating 2b levels, xi be the individual value of occurrence of the ith pixel Plaintext / Ciphertext, m× n be the image size and x be the mean ,then x =(xi)/m × n 2 b−1 i=0 . Standard Deviation (σ) of occurrence of the Plaintext and occurrence of the Ciphertext can be calculated as

$$\sigma = \sqrt{\frac{\sum_{i=0}^{2b}(x - x_i)}{2b}}$$

2. Quality of Encryption (QE)

Let Hp be the Plaintext histogram, Hc be the Ciphertext histogram and b is the number of bits used in the pixel of the image.Quality of Encryption (QE) can be calculated as

$$Q_e = \sum_{i=1}^{2b} |H_P - H_c|$$

The method has been applied on a database of 10 original images with size Mxn. Figure 6.1 shows a sample of Color images and encrypted pixel images in both algorithm encrypted. The quality of the encryption determines the encrypted level of the two algorithms and the Standard deviation executes the original image obtained.

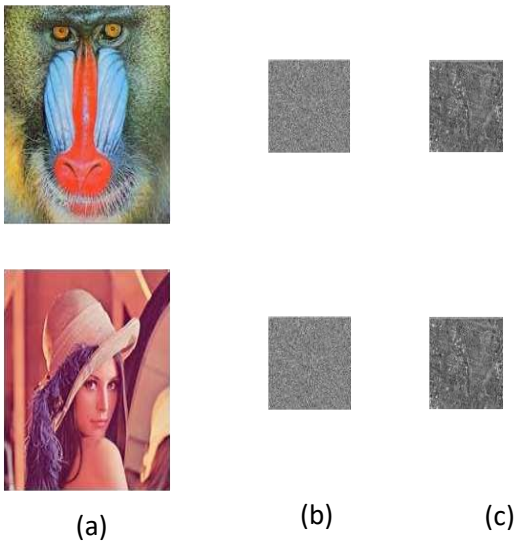


Figure 6.1 (a) shows the original lena and baboon image (b) shows the encrypted pixel image using rubik's cube algorithm and (c)shows the encrypted pixel image using ECC encryption algorithm

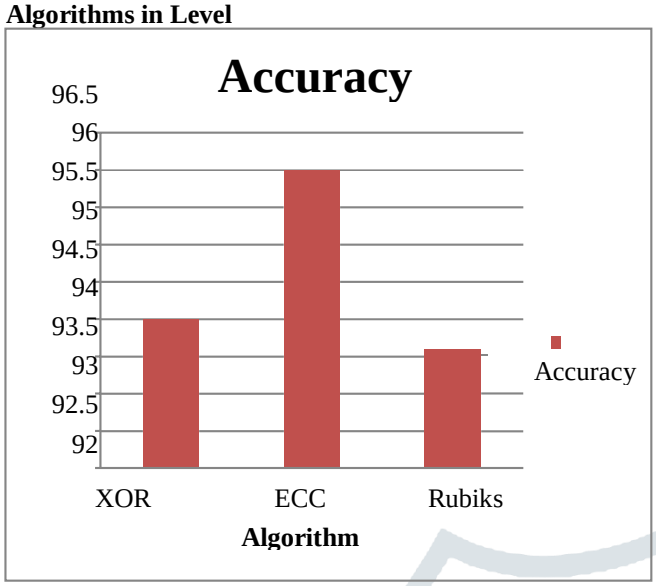
This is how the image encryption takes place using the ECC and rubiks cube the respective solutions. Now another thing related toECC and rubiks cube is related to the degree of protection. Hence in case of ECC, it acts on the DLP in which it is very hard for the hacker/third person to take out the key which turns over the beginning point of cipher pair (kG) and the generator point G. Even a small keyprovides a high level of security compared with rubik's cube algorithm and the existing solutions.

Table 1 Represents the Comparison for the Existing and the Proposed Solution

Algorithms	PSNR		Standard Deviation	Encryption Quality
	BEFORE	AFTER		
XOR algorithm	0.125	0.198	122.57	94
Hybrid ECC and Rubiks Cube	0.125	0.137	135.69	96

The above encryption is carried out for an image, where each pixel of an image has four components alpha, red, green, blue. Each component has 8 bits. The red component of the first pixel of an image is encrypted by additive encryption algorithm using the key (Ki) to form red ciphertext. Similarly the next pseudorandom number is taken to encrypt green and blue component using additive modulo repeat the same next pixel.

Figure 6.2 Comparison Chart for Accuracy of Three Algorithms in Level



The accuracy is computed by the time taken with a standard deviation, PSNR, Quality of encryption and the entropy value

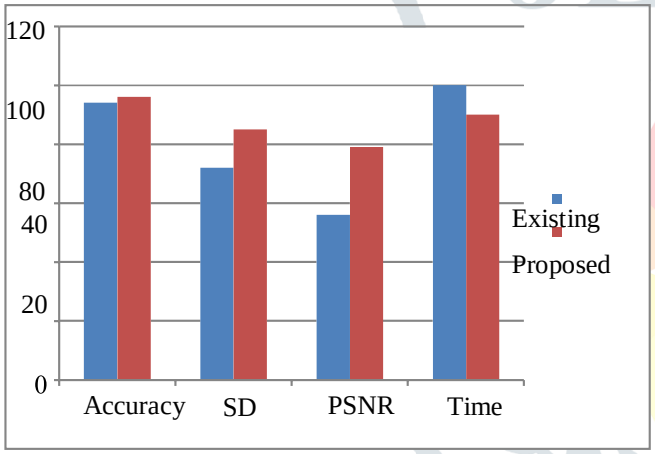


Figure 6.3 The Comparison Chart for the Existing and the Proposed System is Implemented and Analyzed

The table above compares standard deviation, PSNR, and encryption quality for plaintext and cypher text. According to the formula, entropy values are calculated for the plain image and the cypher images. According to the table, the entropy of the cypher image is extremely close to the theoretical value of 8. As a result, the proposed cypher has negligible information leakage and is secure against the entropy attack. As a result, when compared to the existing system, the proposed system is far superior in terms of accuracy and time.

V. CONCLUSION

This report introduces the concept of an image encryption using elliptic curve cryptography and rubik's cube . The outcome establishes that the ECC and rubiks cube fulfill the total requirement to not even encrypt image, but also supplies a high degree of protection. In this proposed hybrid encryption scheme, the images are protected at two levels:

At the first level using ECC and at the second level using Rubik's cube system. It also upholds the tone and the vividness of the picture. It concludes that ECC can further practice for the transferring multimedia providing high protection with less memory use. From the implemented system a safe and secured image sharing system is achieved. Here an Rubik's cube and ECC algorithm is implemented such that the encryption and the decryption PSNR value gets high compared with the existing system. The PSNR rate will be matched and now the RGB values are matched after the image retained. So,that shows the accuracy of the ECC and the Rubik's cube algorithm.

The future enhancement system will be added with other algorithm to make a good accuracy. Image encryption with less time complexity will be added with the system. Multiple point failures at retrieval stage should be overcome when the further proceedings are made. Steganography can also be added for further hiding of multiple images.

REFERENCES

[1] ABDELLATIF JARJAR (2019). "A NEW CRYPTOSYSTEM OF COLOR IMAGE USING A DYNAMIC-CHAOS HILL CIPHER ALGORITHM", SECOND INTERNATIONAL CONFERENCE ON INTELLIGENT COMPUTING IN DATA SCIENCES VOLUME 148, PAGES 399-408.

[2] Avinash Ray , Anjali Potnis , Prashant Dwivey , Shahbaz Soofi , Uday Bhade,(October 2017) "Comparative Study of AES, RSA,Genetic, Affine Transform with XOR Operation, And Watermarking for Image Encryption" International conference on Recent Innovations is Signal Processing and Embedded Systems, pp: 27-29.

[3] BatuhanArpac (September 2019). "A new algorithm for the colored image encryption via the modified Chua's circuit", Engineering Science and Technology, an International Journal 12.

[4] Deepak Kumar Singh, Dr. Kuldeep Tomar, (2018)"A Robust Color Image Encryption Algorithm in Dual Domain using Chaotic Map",International Conference on Inventive Communication and Computational Technologies, pp: 931-935.

[5] G.A.SATHISH KUMARA, K.BHOOPATHY BAGANB, V.VIVEKANANDA (2011). "A NOVEL ALGORITHM FOR IMAGE ENCRYPTION BY INTEGRATED PIXEL SCRAMBLING PLUS DIFFUSION [IISPD] UTILIZING DUO CHAOS MAPPING APPLICABILITY IN WIRELESS SYSTEMS", PROCEDIACOMPUTER SCIENCE, VOLUME 3, PAGES 378-387.

[6] M.I.Fath Allah, (March 2020). "Chaos based 3D color image encryption", Ain Shams Engineering Journal Volume 11, Issue 1, , Pages67-75.

[7] Mustapha Benssalah ,Yasser Rhaskali , Mohamed Salah Azzaz, (2018). "Medical Image Encryption Based on Elliptic Curve Cryptography and Chaos Theory", International Conference on Smart Communications in Network Technologies.

[8] R.Vidhyaa, M.Brindhaa(2020). " A chaos based image encryption algorithm using Rubik's cube and prime factorization process(CIERPF)", Journal of King Saud University - Computer and Information Sciences.

[9] Ramkrishna Das , Sarbajit Manna , Saurabh Dutta(2017). "Cumulative image encryption approach based on user defined operation, character repositioning, text key and image key encryption technique and secret sharing scheme", IEEE International Conference on Power,Control, Signals and Instrumentation Engineering (ICPCSI), 2017.

[10] Shyamalendu Kandar, Dhaibat Chaudhuri, Apurbaa Bhattacharjee, Bibhas Chandra Dhara (2019). "Image encryption using sequence generated by cyclic group", Journal of Information Security and Applications", pp: 117-129.

[11] Sowmya S and Dr. S. V. Sathyanarayana, (2014)"Symmetric Key Image Encryption Scheme with Key Sequences Derived from Random Sequence of Cyclic Elliptic Curve Points over GF(p)", pp:1345-1350.

[12] Tatsuya Chuman, Warit Sirichotedumrong and Hitoshi Kiya,(2018) "Encryption-then-Compression Systems using Grayscale-based Image Encryption for JPEG Images", IEEE Transactions on Information Forensics and Security, pp;1-11.

[13] Valeriu Manuel Ionescu , Adrian-Viorel Diaconu, (2015). " Rubik's cube principle based image encryption algorithm implementation on mobile devices", International Conference on Electronics, Computers and Artificial Intelligence.

[14] Wenying Wen , Yushu Zhang , Yuming Fang , Zhijun Fang (2016). A novel selective image encryption method based on saliency detection", Visual Communications and Image Processing (VCIP).

[15] Ziya Arnavut , Meral Arnavut , Basar Koc , Hüseyin Koçak (2016). "Investigation of row and column permutations for losslesscompression of images".

[16] Zhi-liang Zhu , Wei Zhang , Kwok-wo Wong , Hai Yu(2011) , "A chaos-based symmetric image encryption scheme using a bit-level permutation", Information Sciences, pp: 1171–1186.