IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

MULTISTORAGE DISTRIBUTED SYSTEM FOR IMAGE SECURITY USING DUAL MODE ENCRYPTION

[1]N.Prathipa, [2]V.Sathya

[1]PG Student, [2]Assistant Professor
[1] Computer Science and Engineering
[1] A.V.C College of Engineering , Mayiladuthurai, India

Abstract : In the recent world, security is a prime important issue and encryption is one of the best alternative ways to ensure security. Moreover, there are many image encryption schemes have been proposed each one of them has its own strength and weakness. Cryptography plays a significant role in transferring images securely. 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 a extreme complexity to the attacker/ hacker. At, the second stage the image are get encrypted with its binary values using Rubik's Cube encryption algorithm and Elliptic Curve Cryptographic (ECC) algorithm. The pixels with a random key generated will be encrypted by the followed algorithms. The input image of 2-D is transformed into a 1- D array by using binary sequence conversion where each pixels are followed with a rule based examination and divided. To make an efficiency of security over hackers the image gets stored in the distributed database on a random pixel storage manner for secured accessing over the server. The salient features of the proposed image encryption method are loss-less, good peak signal to noise ratio (PSNR), Symmetric key encryption, less cross correlation, very large number of secret keys, and key-dependent pixel value replacement with high security compared to the existing solutions.

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

I. INTRODUCTION

Network security is the process broad terms which cover the multitude of technologies, devices and processes. The configuration has designed to protect the integrity, confidentiality and accessibility over the computer networks. The layers across the network act as a security for the users and the organizations. There are many people who attempt to damage our Internet-connected computers, violate our privacy and make it impossible to the Internet services. The frequency variety of existing attacks which acts as the main function of attacking as well as the threat of new destructive future attacks, network security has become a central topic in the field of cyber security. Implementing network security measures allow computers, users and programs to perform their critical functions within a secure environment.

In cryptography is the process of changing the data from one form to the another using the algorithm or a mathematical function to make it in a unreadable form. In the image security systems two encryption algorithms are implemented for the image encryption systems they are rubik's cube and ECC algorithm. 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. RELATED WORK

In this section we mainly describe about the overview of the chaos and non chaos based image encryption technique. The existing is carried on the image encryption process and the proposed is carried on multistored distributed system using dual mode encryption.In [8] novel rubik's cube based scrambling in row and column directions is suggested for achieving high efficiency scrambling. In [2] the non chaos method is added to found out the BLP and the BLT technique with the efficiency of the PSNR values with the row level and column level permutation technique. The added implementation has enhanced the reached level of networks security where Zhi-liang Zhu [16] has proposed a chaotic based bit level permutation where the permutation of pixels has been added through it. The image compression using the gray scale image encryption technique has a wide spread in the image processing techniques [12] where the compression will change the pixel levels and added with the efficiency is loaded. But the user can add only the JPEG image to compress the pixels. The symmetric key encryption methodology added with the efficiency of the cyclic group transformation systems. [11] Has maintained a cyclic process which is proposed here with the efficiency of loading the methodology which is added. [2] A comparative analysis between the image encryption algorithms is made. The algorithm taken is AES, DES, genetic, XOR, ECC and affine transform algorithm. The comparison and the analysis result say that the ECC suits the best for the image encryption algorithm since the key sensitivity analysis is high. Researches have increased their attention towards multiple-image encryption because a high efficiency of secret information transmission is required for modern multimedia security technology. Many multiple-image algorithms have been presented. A multiple-image algorithm using the pixel exchange operation and vector decomposition system with an efficient security is placed. The main advantage over image encryption is the 3D chaotic map encryption technology [4] the chaotic map technique involved with the efficiency overloaded in it.

The existing methodology is based on two kinds of survey papers combine to form a high security image encryption scheme. A non chaos based encryption technique has been implemented to make a higher level security for the image transmitted over network. 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.

A novel Rubik's cube based pixel level scrambling and simple XOR based diffusion is proposed of this paper to safely transmit multimedia information (images) through an untrusted channel, such as social networks. The process adds the rubik's cube algorithm with Confusion and diffusion of pixel with the conventional of pixels. The implementation of this image accuracy system is to order the image security with the 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 with the ECC and Rubik's cube algorithm and stored in multi server environment. This perceivable information can be reduced by decreasing the correlation among the image elements using certain transformation techniques. The secret key of this approach is used to determine the seed. The seed plays a main role in building the transformation table, which is then used to generate the transformed image with different random number of block sizes. The transformation process refers to the operation of dividing and replacing an arrangement of the original image. The image can be decomposed into blocks; each one contains a specific number of pixels. The blocks are transformed into new locations. For better transformation the block size should be small, because fewer pixels keep their neighbors.

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 the image with any format which they are all get stored. The image comprises of many pixels where the pixel based encryption will be used for the phase 2. The image upload followed by the RGB color model system where the RGB pixel values are get separated. The conversion of a color image into a grayscale image is converting the RGB values (24 bit) into grayscale value (8 bit). The gray scale conversion is the one where the pixel can be converted as gray scale where the value of the pixel will be 0-255. The pixel variations can be identified with the histogram color variation and the values are taken as 0's and 1's. The grayscale image has represented by luminance using 8 bits value.

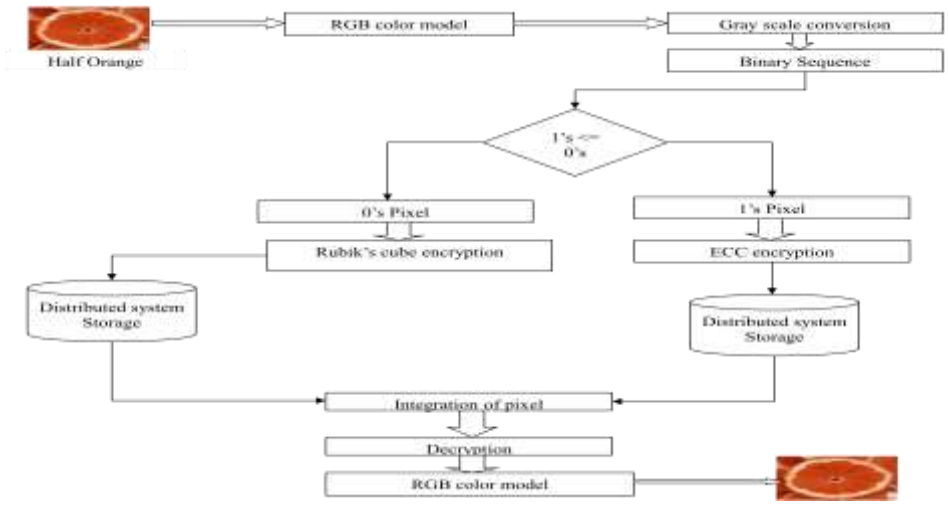


Figure 1 System Architecture of the Image Security Using ECC and Rubik's Cube Algorithm

(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.

Using this implementation the pixel is divided as two formats. Now this can be carried with further security systems called encryption which will be in a user not understandable format. Image encryption schemes have been increasingly studied to meet the demand for real-time secure image transmission over the Internet and through wireless networks. Encryption is the process of transforming the information for its security. With the huge growth of computer networks and the latest advances in digital technologies, a huge amount of digital data is being exchanged over various types of networks. It is often true that a large part of this information is either confidential or private. Dividing the image into a larger number of blocks made the performance even better. The results showed that the correlation was reduced even further and the entropy was increased as the number of blocks is increased. This method of encryption can be applied to any of the formats of images like jpg, tiff, ppm, pgm, png from the browser option. The advantages of this algorithm are that it is able to recover plain images completely and simplifies the computations. Experimental results demonstrate its practicality and high proficiency.

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. In the proposed system, the input image to the rubik's cube algorithm is the chaotic baker mapped image. The encryption algorithm includes the following steps.

Step 1: Generate randomly two vectors K_R and K_C of length M and N, respectively. Element $K_R(i)$ and $K_C(j)$ Each take a random value of the set A = {0, 1, 2, ... , 2α − 1}. Note that both KR and KC must not have constant values.

Step 2: Determine the number of iterations, $ITER_{max}$, and initialize the counter ITER at 0.

Step 3: Increment the counter by one: ITER = ITER + 1.s.

Step 4: For each row i of image I_o,

compute the sum of all elements in the row i, this sum is denoted by α(i),

compute modulo 2 of α(i), denoted by Mα(i),

row i is left, or right, circular-shifted by $K_R(i)$ positions (image pixels are moved $K_R(i)$ positions to the left or right direction, and the first pixel moves in last pixel.

Step 5: The Generated K_R and K_C will be used to encrypt the scrambled pixels on each Mα(i), each row and the 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 an approach to public key cryptography based on algebraic structure of elliptic curves over finite fields. ECC generates keys through the properties and underlying equations of the elliptic curve. In beginning, we take for granted that the distinguished points are at infinity, denoted ∞. (The coordinates are to be chosen from the fixed finite field of characteristic not equal to 2 or 3, and the curve equation should be somewhat more complicated.) This set together with the group of operation of elliptic curves is called as an Abelian group, with the points at infinity as identity element.

There is a rule called the chord-and-tangent rule, for adding two points on an elliptic curve E(Fp) to give a third elliptic curve point. In concert with this addition operation, the set points E (Fp) forms with O serving as the identity. This is the group which is utilised in the construction of elliptic curve cryptosystems. The addition formula is explained geometrically. Let P = (x1, y1) and Q = (x2, y2) be two discrete spots along 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 with the 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

$$LdB = 10 \log10 (P1/P0) \longrightarrow (4.2)$$

Now let

$$P1 = MAX^2 \text{ and} \longrightarrow (4.3)$$

$$P0 = MSE \longrightarrow (4.4)$$

We then have

$$PSNR = 10 \log10(MAX^2/MSE) \longrightarrow (4.5)$$

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

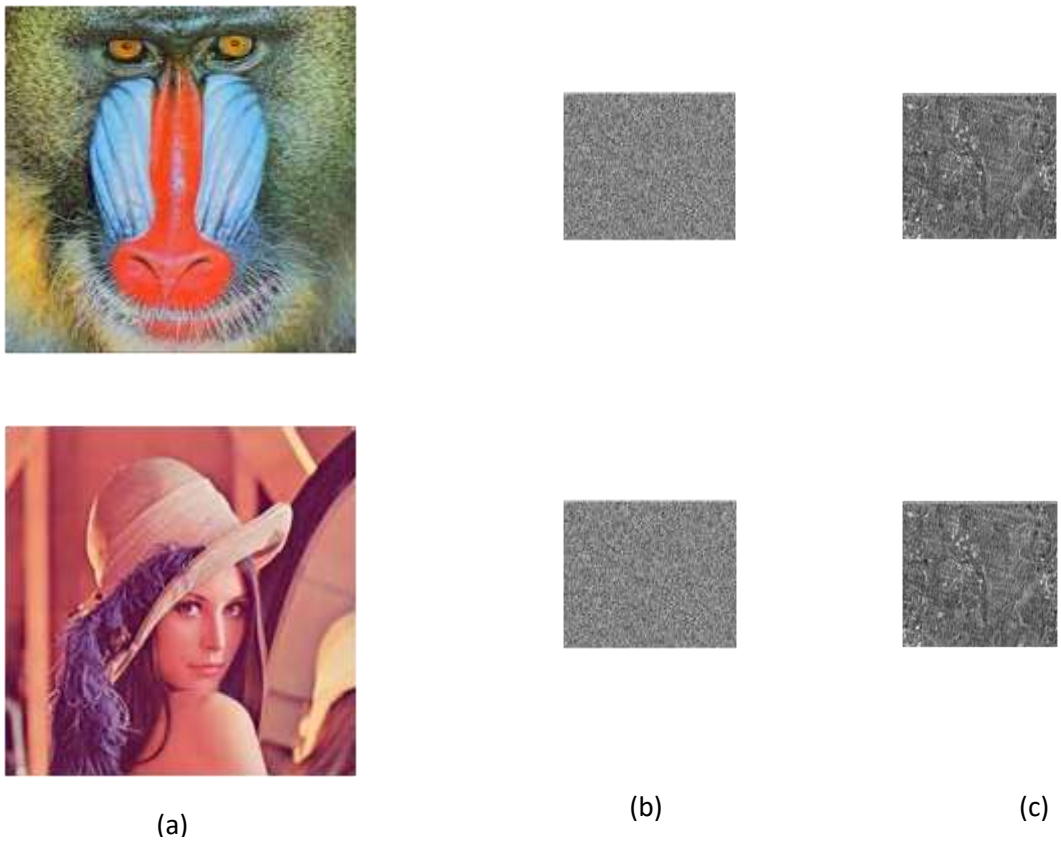
$$\sigma = \sqrt{\frac{\sum_{i=0}^{2^b}(x-x_i)}{2^b}} \longrightarrow (6.1)$$

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

$$Q_e = \sum_{i=1}^{2^b} |Hp - Hc| \longrightarrow (6.2)$$

The method has been applied on a database of 10 original images with size M*x*n. 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.



(a) (b) (c)

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 to ECC 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 key provides 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.

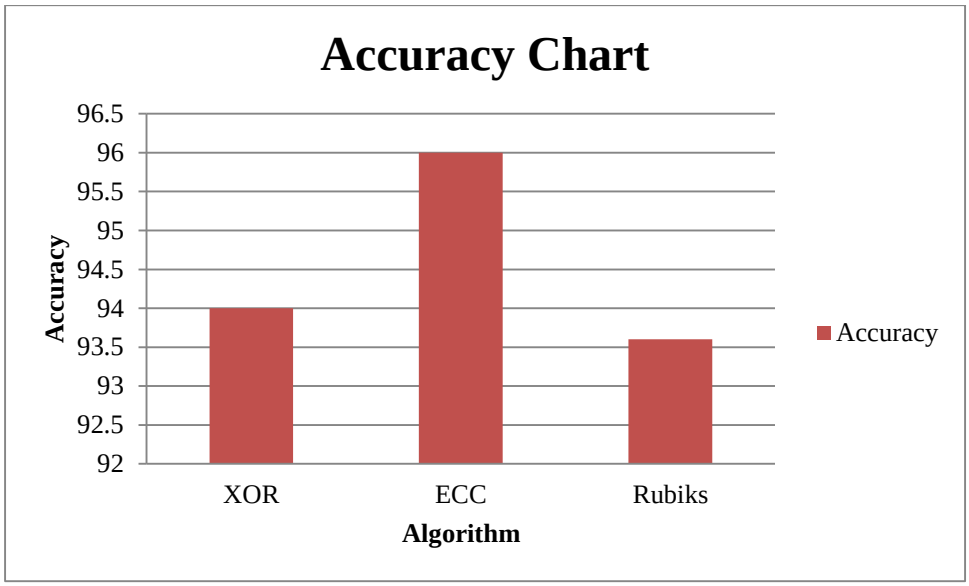


Figure 6.2 Comparison Chart for Accuracy of Three Algorithms in Level

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

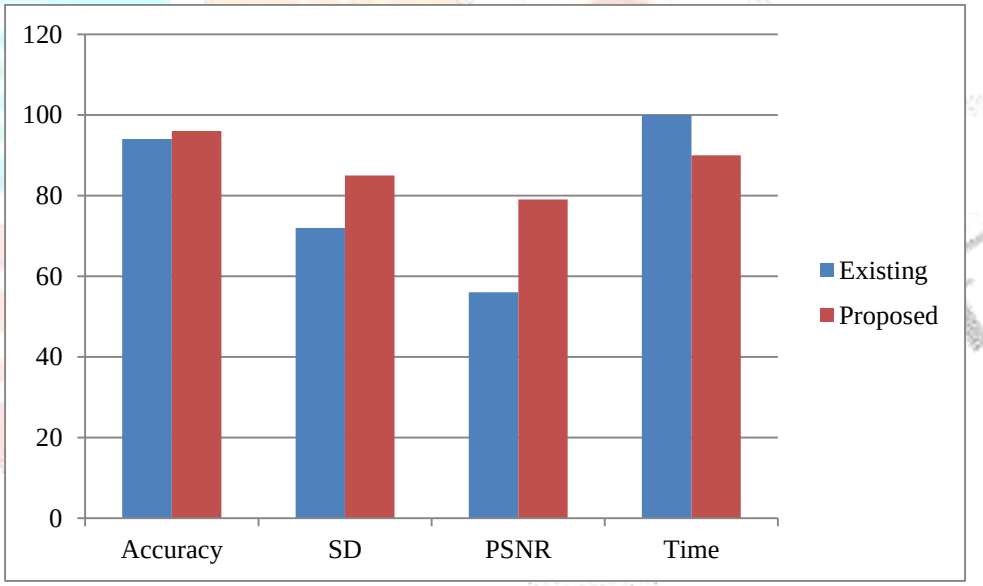


Figure 6.3 The Comparison Chart for the Existing and the Proposed System is Implemented and Analyzed

The above table gives comparison of standard Deviation, PSNR and Quality of Encryption for Plaintext and Cipher text. Entropy values are calculated for the plain image and the cipher images as stated by the formula. From the table it is noticed that the entropy of the cipher image is extremely close to the theoretical value of 8. Therefore, the information leakage in the proposed cipher is negligible and it is secure upon the entropy attack. Hence comparing with the existing system proposed system is well good in 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", PROCEDIA COMPUTER 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, , Pages 67-75.

[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 lossless compression 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.