International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-11 Issue-3, February 2022

Advanced Image Encryption & Decryption using Rubik's Cube Technology

Renusree Varma Mudduluri, Akhila Golla, Sushanth Raghava, Tammana Jyothi Sai

Abstract: ***The world changing at a fast pace and more than ever there's this need to secure data and preserve one's privacy. Advanced algorithms and technologies that can be used for secure transmission of texts, images and videos are being tried and tested. We have used the Rubik's Cube Technology for secure encryption and decryption of colored images.***

Keywords: ***Rubik's Cube Algorithm, Encryption, Decryption, Coloured Images, Secure, Advanced***

I. INTRODUCTION

In recent years, technology has moved leaps but it has also come with its downsides. One of them is illegal copying of digital intellectual property. Several works have been done to curb this issue. Some of the main ones are done by using encryption. This project focuses on using encryption for protecting digital images. Encryption is a process of transforming data into an unreadable format using certain algorithms to make sure that the data is available to only legitimate users i.e. only authorized parties can access the data. The main objective is encryption of mainly digital images. There are already well-known encryption methods such as symmetric-key algorithms, asymmetric-key algorithms and also algorithms based on Elliptic-curve-cryptography in place for data encryption but these are not the most suitable for image encryption. This is mostly applicable in real-time communication or in cases where fast encryption is needed. The proposed encryption schemes in recent years can be mainly classified into categories pixels position permutation, value transformation, and chaotic systems. Image encryption has been studied extensively. Some permutation-based encryption schemes have already been found to be insecure against certain attacks such as chosen-plaintext and cipher-text only. It is due to high data redundancy in such schemes and as secret permutations could be redeemed by plaintext and ciphertext comparison, It is quite understandable [1].

Manuscript received on December 22, 2022.
Revised Manuscript received on January 12, 2022.
Manuscript published on February 28, 2022.
* Correspondence Author
Renusree Varma Mudduluri, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore (Tamil Nadu), India.
Akhila Golla, Department of Computer Science Engineering, Vellore Institute of Technology, Vellore (Tamil Nadu), India.
Sushanth Raghava, Department of Electronics and Communication Engineering, Vellore Institute of Technology, Vellore (Tamil Nadu), India.
Tammana Jyothi Sai, Department of Computer Science Engineering, Vellore Institute of Technology, Vellore (Tamil Nadu), India.

Also, chaotic system are well-defined on real numbers Although, chaos-based algorithms are used more often in image encryption in general, they have a high computational cost. whereas the cryptosystems are well-defined on a finite set of integers. We are going to consider the Rubik's cube principle for image encryption. We are going to implement this algorithm which has been specified and extensively studied in the papers mentioned below [2].

II. OBJECTIVE

We have developed a code for more secure and fast encryption of images using a unique image encryption algorithm based on Rubik's cube principle**.** Pixels of the image are shuffled in a way similar to that of a Rubik's cube in a random manner using two randomly generated vectors. Then the same vectors are used for performing bitwise operation row-wise and column-wise. XOR operation is performed on odd columns and rows of image with a key to decrease association between encrypted and original images. Same key is flipped and XOR operation is performed on even columns and rows of image [3].

Finally, algorithm which we used to develop the encryption system (Rubik's cube principle) can achieve good encryption standards and perfect hiding ability but also can resist statistical, exhaustive and differential attacks [4].

Various research, performance assessment tests and experimental tests done on similar type of image encryption algorithm shows it is apt for transmission applications and Internet encryption because of its fast encryption/decryption speeds it also demonstrates robustness of the proposed algorithm against numerous attacks [5].

III. INNOVATION COMPONENT

In this project we are implementing image encryption algorithm in python based on Rubik's cube principle described in the following research paper. " Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. Journal of Electrical and Computer Engineering, 2012, 7"

The encryption algorithm described is capable of fast encryption and decryption and is found to be highly secure based on the assessment tests carried out in the above paper. Hence, it proves to be apt for transmission applications and Internet encryption [6].

Paper from which we are implementing the encryption method describes the usage of the algorithm only in case of black and white images. We extend this encryption method to work with colour (RGB) images [7].

IV. WORK DONE AND IMPLEMENTATION

Methodology adapted: Rubik's cube algorithm

Encryption Algorithm

Let I0=pixels values matrix of a α-bit grayscale image (M×N). Steps involved in encryption are:

1. Create two vectors KR and KC with random values of length M and N, where the values in the vectors should be >0 and <2α-(KR and KC should not have constant values)
2. Set the iteration value, ITERmax, and initialize the counter ITER at 0.
3. Increment the counter by one: ITER=ITER+1.
4. For each row i of image Io,
   a. calculate sum of all elements in the row, this sum is denoted by $\alpha(i)=Nj=1Io(i,j),i=1,2,\ldots,M$

   b. compute modulo 2 of $\alpha(i)$, denoted by $M\alpha(i)$,

   c. row is left or right, circular- shifted by K R(i) positions to right or left direction and first pixel

$$I_1(i,2j-1) = I_{ENC}(i,2j-1) \oplus K_R(j),$$
$$I_1(i,2j) = I_{ENC}(i,2j) \oplus \text{rot } 180\,(K_R(j)),$$

   If Mα(i)=0→right circular shift
   else→left circular shift.

$$I_{SCR}(2i-1,j) = I_1(2i-1,j) \oplus K_C(j),$$
$$I_{SCR}(2i,j) = I_1(2i,j) \oplus \text{rot } 180\,(K_C(j)).$$

5. For each column j of image Io,

   a. compute sum of elements in the column j, sum is represented as

$$\beta_{SCR}(j) = \sum_{i=1}^{M} I_{SCR}(i,j), \quad j = 1,2,\ldots,N,$$

$\beta(j)$, $\beta(j)=Mi=1Io(i,j),j=1,2,\ldots,N$.

   b. compute modulo 2 of $\beta(j)$, denoted by $M\beta(j)$.

   c. column j is down, or up, circular- shifted by $KC(i)$ positions:

$$\text{if } M_{\beta_{SCR}(j)} = 0 \longrightarrow \text{up circular shift}$$
$$\text{if } M_{\alpha_{SCR}(j)} = 0 \longrightarrow \text{right circular shift}_{\text{left}}$$
$$\text{else} \longrightarrow \text{left circular shift.} \qquad 2,\ldots,M,$$

   Steps 4 and 5 above will generate a scrambled image denoted by ISCR.

6. Using vector KC, the bitwise XOR operation is performed on each row of scrambled image using:

$I1(2i-1,j)=ISCR(2i-1,j)\oplus KC(j)$,
$I1(2i,j)=ISCR(2i,j)\oplus rot180(KC(j))$

where $\oplus$ and rot180(KC) are bitwise XOR operator and flipping of vector KC from left to right, respectively.

7. Using vector KR, XOR operation is performed on each column of image$I1$ using:

$IENC(i,2j-1)=I1(i,2j-1)\oplus KR(j)$
$IENC(i,2j)=I1(i,2j)\oplus rot180(KR(j))$

where rot180(KR) is the left to right flip of vector KR.

8. If ITER=ITERmax, encrypted image IENC is created and encryption process is done; otherwise, the algorithm branches to step 3.

KR, KC & ITERmax are the secret keys.

Decryption Algorithm:

Decrypted image, Io, is obtained from the encrypted image, IENC, and the secret keys, KR, KC, and ITERmax as follows in the following.

1. Initialize ITER=0.

2. Increment the counter by one: ITER=ITER+1.

3. Bitwise XOR operation is performed on KR vector and each column of the encrypted image IENC as follows:

4. Then, using the KC vector, the bitwise XOR operator is applied to each row of image $I1$:

   1. For each column j of scrambled image ISCR,
      a. calculate sum of elements in that column j, denoted as βSCR(j):
      b. compute modulo 2 of βSCR(j), denoted by $M\beta$SCR(j),
      c. column j is up or down, circular shifted by $KC(i)$ positions:

   2. For each row i of scrambled image$I$SCR,

      d. calculate sum of elements in row i, this sum is denoted by αSCR(i):
      e. compute modulo 2 of αSCR(j), denoted by $M\alpha$SCR(j),
      f. row i is then left, or right, circular-shifted by $K(i)$ according to the following:

3. If ITER=ITERmax, then image IENC is decrypted otherwise,
   algorithm branches back to step 2.

V. IMPLEMENTATION

Encryption: To encrypt the image we need to save the images in a folder named "input". Code takes image input using PIL library and converts it into RGB matrices and starts the encryption process using the Rubik's cube algorithm.

The encrypted images are then saved in another folder. After the encryption the the values of Kr, Kc and Iterations(ITER_MAX) saved in a file named “keys”.

Decryption: This code takes Kr, Kc, Iterations (ITER_MAX) values along with the encrypted image and start the decryption process.

Dataset used:

This project is an encryption algorithm so any kind of image can be taken as input for the encryption which produces a highly encrypted, secure image(output). For evaluating the results we take standard black and white images such as Lena, Black, Baboon and Checkerboard [8].

Our project implements image encryption algorithm based on Rubik's cube principle described in the following research paper. “Loukhaoukha, K., Chouinard, J. Y. & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering*, *2012*, 7”

The paper from which we are implementing the encryption method describes the usage of the algorithm in case of black and white images. We extend this encryption method to work with colour(RGB) images [9].

Tools used:

Hardware and software requirements:

- Python2, Numpy and Image libraries.
- Processor - 2.5 GHz
- RAM - 1GB

VI. SCREENSHOT AND DEMO

Sample Image that we used:

Fig. 1 This is the original image which we encrypt.

Fig. 2 Encrypted Image

Fig. 3 Kr, Kc values

Fig. 4 Decrypted Image

VII. RESULTS AND DISCUSSION

To obtain the encrypted image the pixels of the original image are shuffled in a way similar to that of a Rubik’s cube in a random manner using two randomly generated vectors. Then the same vectors are used for performing bitwise operation row-wise and column-wise. XOR operation is performed on odd columns and rows of image with a key to decrease association between encrypted and original images. Same key is flipped and XOR operation is performed on even columns and rows of image [10].

Safe image cryptography should be able to resist varied attacks like cipher-text-only attack, plain text, applied math analysis and brute-force attacks. In our main reference paper, extensive security analysis on projected algorithm is performed and also safety assessment has been performed on key area and applied math analysis. Apart from this various testings were done in the algorithm to check its performance on the level of encryption gained. One of such testing is Visual testing which is done by calculating and comparing the number of pixels change rate (NCPR) and unified average changing intensity (UACI) values.

UACI values illustrate that all pixel gray-scale values of encrypted image are different from that of original images, which makes it difficult to discriminate original and encrypted image pixels. High NPCR percentage values specify that the position of pixels have been changed randomly. So for a good image encryption algorithm, NPCR values must be high and UACI values must be around 33%. Values obtained from testing gave appropriate values which are satisfactory for the algorithm. From the testing results shown in the paper, the proposed algorithm was not only found to attain good encryption standards and perfect hiding ability but also can resist statistical, exhaustive and differential attacks.

VIII. CONCLUSION

A unique picture encryption technique is proposed in this research. This approach is based on the Rubik's cube to develop image pixels. The proposed approach is stabilly illustrated with precise quantitative analysis against various forms of assaults such as analytical and parametric attacks. The experiments also show that the proposed encryption technique is suits for real-time Internet protection and assessments as it is highly secured.

REFERENCES

1. Loukhaoukha, K., Chouinard, J. Y., & Berdai, A. (2012). A secure image encryption algorithm based on Rubik's cube principle. *Journal of Electrical and Computer Engineering*, *2012*, 7**.**
2. Ionescu, V. M., & Diaconu, A. V. (2015, June). Rubik's cube principle based image encryption algorithm implementation on mobile devices. In *2015 the 7th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)* (pp. P -31). IEEE.
3. Loukhaoukha, K., Nabti, M., & Zebbiche, K. (2013, May). An efficient image encryption algorithm based on blocks permutation and Rubik's cube principle for iris images. In *2013 8th International Workshop on Systems, Signal Processing and their Applications (WoSSPA)* (pp. 267-272). IEEE.
4. Gomathi, T., & Shivakumar, B. L. (2015). Multistage Image Encryption using Rubik's Cube for Secured Image Transmission. *International Journal of Advanced Research in Computer Science*, *6*(6).
5. Helmy, M., El-Rabaie, E. S. M., Eldokany, I. M., & El-Samie, F. E. A. (2017). 3-D Image Encryption Based on Rubik's Cube and RC6 Algorithm. *3D Research*, *8*(4), 38.
6. Abitha, K. A., & Bharathan, P. K. (2016). Secure Communication Based on Rubik's Cube Algorithm and Chaotic Baker Map. ProcediaTechnology,24,782,7
7. R.Vindhya & M.Brindha (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
8. Joffin Joy & Litty Koshy(2019). RubiCrypt: Image Scrambling Encryption System Based on Rubik's Cube Configuration.IEEE
9. M. J. Aqel, Z. AlQadi, A. A. Abdullah(2018).RGB Color Image EncryptionDecryption Using Image Segmentation and Matrix Multiplication.International Journal of Engineering and Technology, Vol. 7, No. 3.13, pp. 104-107, 2018
10. Majed O. Al-Dwairi, Amjad Y. Hendi & Ziad A. AlQadi(2019). An Efficient and Highly Secure Technique to Encrypt and Decrypt Color Images. Engineering, Technology & Applied Science Research Vol. 9, No. 3, 2019, 4165-4168

AUTHORS PROFILE

Mudduluri RenuSree Varma, pursued his Bachelor of Technology in electronics and communication engineering from Vellore Institute of Technology, Vellore. She is currently working as Incident Response Analyst at Eli Lilly.

Golla Akhila, pursued his Bachelor of Technology in computer science engineering from Vellore Institute of Technology, Vellore. She is currently working as Software Engineer at Bank of America continuum India Pvt. Ltd

Sushanth Raghava, pursued his Bachelor of Technology in electronics and communication engineering from Vellore Institute of Technology, Vellore. He is currently working as Associate ColdFusion Developer at Schlumberger.

Tammana Jyothi Sai, pursued his Bachelor of Technology in computer science engineering from Vellore Institute of Technology, Vellore. He is currently working as BI Engineering Specialist at WABTEC Corporation.