2nd Science Engineering and Technology (SET) Conference 2019

IMAGE ENCRYPTION USING RUBIK'S CUBE BASED ALGORITHM

- Mohit Joshi – Nirajan Karki – Kushal Ghimire – Moses Thapa Magar

Advanced College of Engineering and Management

ABSTRACT

The image encryption is widely used to secure transmission of data in an open internet works which encodes secret image with the help of encryption algorithm based on Rubik's cube principle in such a way that unauthorized users can't access it. In Rubik's cube principle the original image is scrambled using the principle of Rubik's cube then, XOR operator is applied to rows and columns of the scrambled image using two secret keys.

This project overcomes most of the drawbacks from the other algorithms and the encrypted image having good values in terms of standard testing techniques and has high key sensibility. This project is modified existing algorithm which performs pixel transformation using Rubik's cube algorithm, which makes it almost impossible for hackers to retrieve information..

INTRODUCTION

Cryptography is the science of information security which has become a very critical aspect of modern computing systems towards secured data transmission and storage. The exchange of digital data in cryptography results in different algorithms that can be classified into two cryptographic mechanisms: symmetric key in which same key is used for encryption and decryption and asymmetric key in which different keys are used for encryption and decryption. Images are broadly used in numerous processes. As a result, the safety of image data from unauthorized access is crucial at the hands of user.

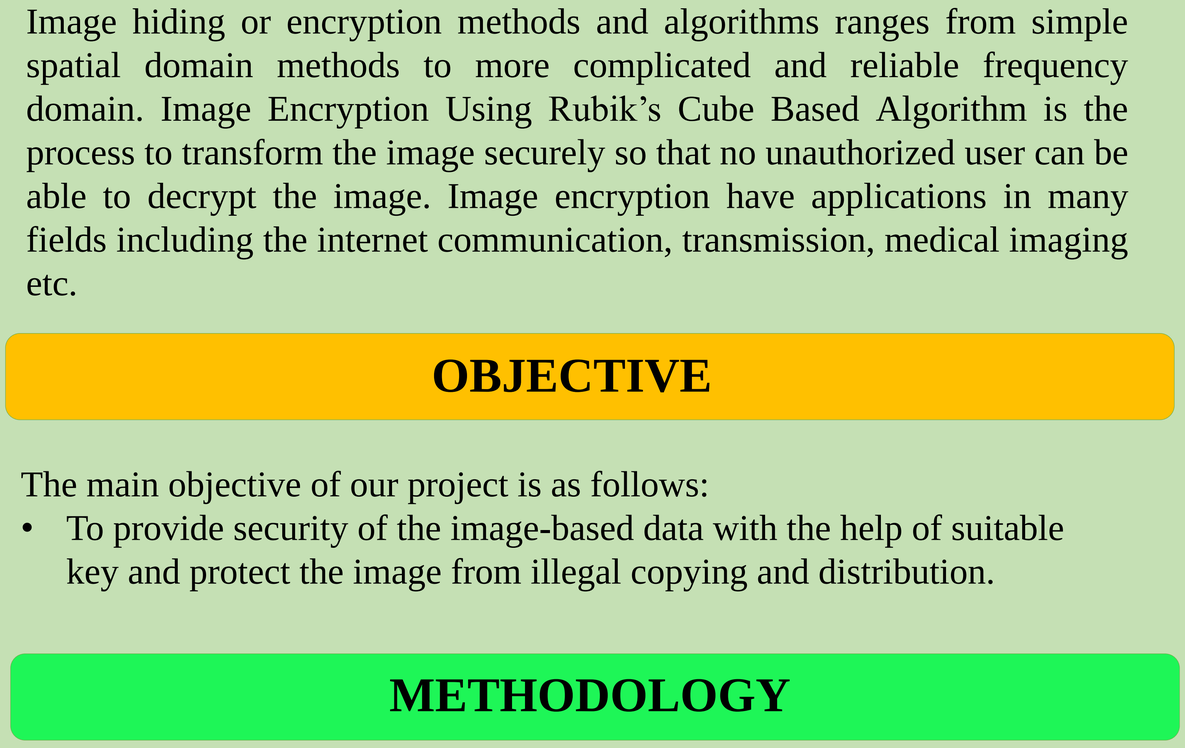
Image encryption plays a significant role in the field of information hiding. Image hiding or encryption methods and algorithms ranges from simple spatial domain methods to more complicated and reliable frequency domain. Image Encryption Using Rubik's Cube Based Algorithm is the process to transform the image securely so that no unauthorized user can be able to decrypt the image. Image encryption have applications in many fields including the internet communication, transmission, medical imaging etc.

OBJECTIVE

The main objective of our project is as follows:

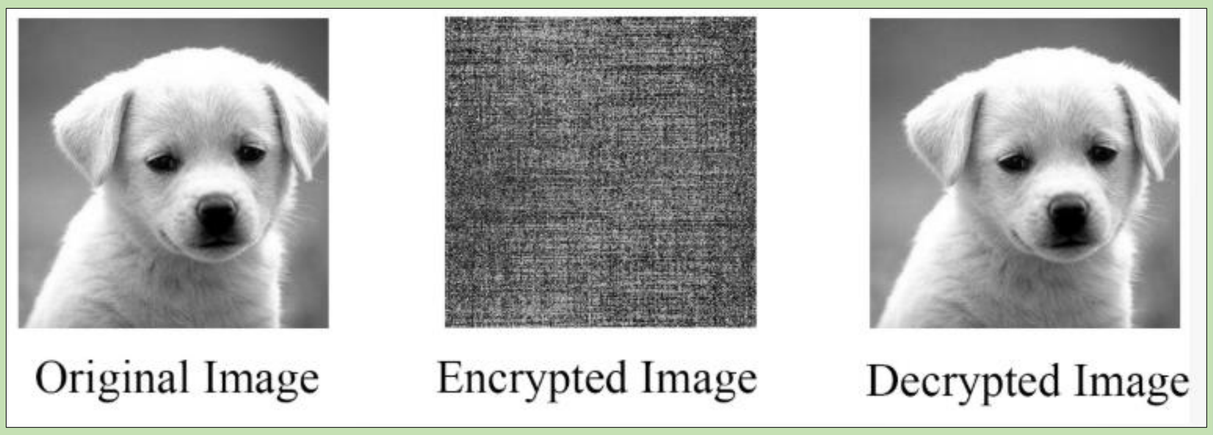
- To provide security of the image-based data with the help of suitable key and protect the image from illegal copying and distribution.

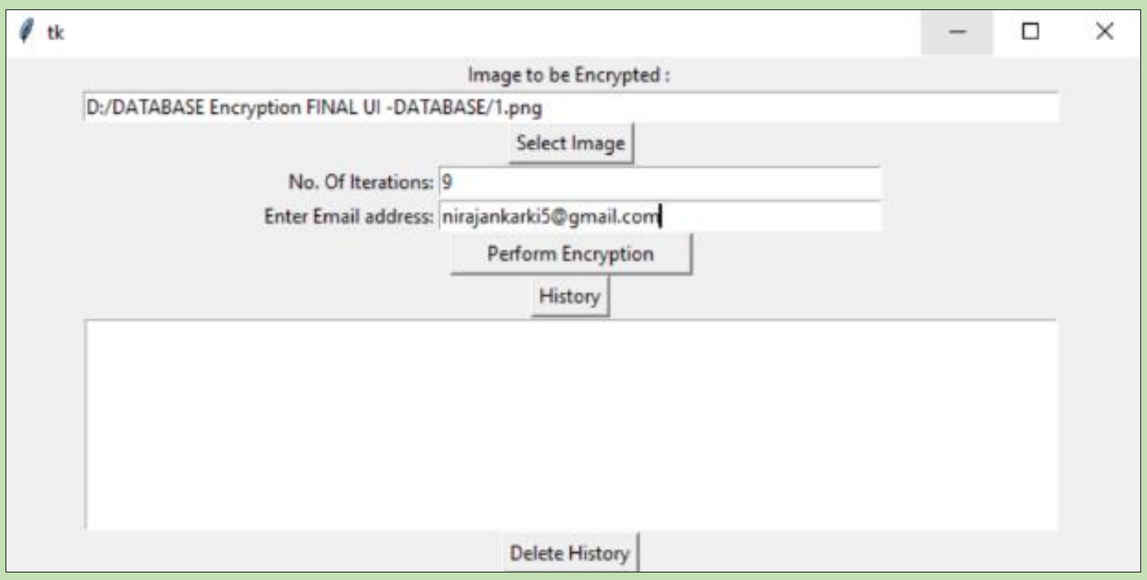
METHODOLOGY



RESULT

We have design and implement a system which provide highly secure data storage for different governmental and non- governmental sector. To implement this system, we have used encryption algorithm based on Rubik's cube principle that encrypted the image and generate the key for future decryption and send the generated key into respected email id of an individual's organization. After the completion, the obtained output is shown as shown in figure below:





CONCLUSION

This algorithm is based on the principle of Rubik's cube to permute image pixels. To confuse the relationship between original and encrypted images, the XOR operator is applied to odd rows and columns of image using a key. The same key is flipped and applied to even rows and columns of image. Experimental tests have been carried out with detailed numerical analysis which demonstrates the robustness of the proposed algorithm against several types of attacks such as statistical and differential attacks (visual testing). Moreover, performance assessment tests demonstrate that the proposed image encryption algorithm is highly secure.

REFERENCES

1. C. K. Huang, H. H. Nien, S. K. Changchien, and H. W. Shieh, "Image encryption with chaotic random codes by grey relational grade and Taguchi method," Optics Communications, vol. 280, no. 2, pp. 300–310, 2004.

2. G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps," Chaos, Solitons and Fractals, vol. 21, no. 3, pp. 749–761, 2014.

3. Y. Wang, K. W. Wong, X. Liao, and G. Chen, "A new chaos-based fast image encryption algorithm," Applied Soft Computing Journal, vol. 11, no. 1, pp. 514–522, 2011.

4. "An Improved Secure Image Encryption Algorithm Based on Rubik's Cube Principle and Digital Chaotic Cipher", Adrian-Viorel Diaconu and Khaled Loukhaoukha, Mathematical Problems in Engineering, Volume 2013, Article ID 848392.