Image Encryption and Decryption using Rubik's Cube Algorithm

Name : Kulvir Singh
Register Number : 19BCE2074

Abstract :

In today's world, almost 80% of our lives have been digitized and in the near future everyone and everything will be connected to a digital system of the internet and its subsidiaries. This paves the way for a huge security concern in the form of privacy of information and data. To evade such privacy concerns various countermeasures need to be incorporated. Image encryption and decryption is just an example of one such countermeasure. In recent times several algorithms have been put forth based on chaotic systems for encryption and decryption, however they offer very limited security. In this project a new encryption technique is discussed which will use the Rubik's Cube Algorithm. The algorithm will be applied on coloured images and the pixel values of red, blue and green will be in action. The pixel values will be used in the algorithm to provide encryption by scrambling them using the XOR operation. The decryption of the image will be the reverse of the encryption process with the help of the keys produced in the previous phase.
On successful completion of the project, one will be able to perform full encryption and decryption. The user can input any image coloured or black-white into the algorithm. The program will then encrypt the image and scramble the pixel value using the mentioned algorithm and produce two security private keys and the encrypted image. The encrypted image can be decrypted by providing the keys and the encrypted image into the program and the final result would be the retrieval of the original input image.

Keywords :

Rubik's Cube, XOR, chaotic systems, noise utilization, pixel scrambling, asymmetric encryption, symmetric encryption

Introduction :

Since the dawn of the computer age, security has been a primary goal of man. The advancements in the field of security have been duly noted and has been seen in the form of various security mechanisms and algorithms being developed. Cryptography has always played a major role and the combination of numbers and operations has proved to be an amazing tool to encapsulate user data. There are various cryptographic paradigms that involve ciphers based on mathematical tools. Since it all comes down to playing with numbers, the same tools have been used by researchers to provide encryption of images by manipulating pixel values. The pixel values of images are just numbers which can be scrambled, jumbled to make a new sequence and in turn a new distorted image. This project has a particular interest in providing image security using image processing techniques mixed with a security algorithm.

There are various techniques, methods and schemes revolving around image encryption and decryption. Waness et al. [8] has presented three particular methods of image encryption that are - symmetric, asymmetric and chaotic systems. Out of the three symmetric systems are rarely used, hence a deep study of chaotic system techniques and asymmetric algorithms have been made before selecting the choice of algorithm to be used in this project. Some valuable and resourceful information on chaotic systems is given below. [4][5]
One of the chaotic system techniques dealt with use of a generalized logistic map for real time image processing [5]. Shah et al. [5] presents a scheme that makes use of encryption with an efficient permutation based technique based on a modular logistic map to bring down the size of the chaotic value vector, required to permute a real-time image. The chaotic key sequence used in this technique changes the pixel values of a grayscale image. This optimises the chaotic key generation but is only extended on a grayscale image. Another chaotic system based encryption deals with double spiral scans and chaotic maps [4]. Tang et al. [4] presents the Double Spiral Scans which take a random scan of the image matrix and jumble those particular locations it scans twice. This results in randomization of the image and hence makes it distorted and encrypted. However if the entire image is based on the same pixel value then there will be no encryption despite the double scans.

Another technique is by using basic image processing concepts [7][9][10]. They make use of XOR operations along with image matrix arithmetic operations. Ahmad et al. [9] makes use of XOR and the formation of the orthogonal matrix and skew tent map using image pixels for providing a secure cipher image. Astuti et al. [10] deals with steganography and gives a vivid description on steganography. It also uses bit plane slicing along with XOR operation to work on the image and provide security. Another technique discussed is really interesting as it revolves around using destructive techniques on images to provide for security [7]. Mivule et al. [7] presents a scheme that will add noise to the image matrix and perform certain arithmetic operations on the pixels to change the original image. This technique however would not be beneficial for the retrieval process as the computation would be very difficult.

Another approach to encryption is one which is advanced and allows cloud features to come into play. Fu et al. [2] deals with the outsourcing of computation to a third party which provides

image processing resources and thereby giving security. It deals with the application of an extended code base which helps other applications to function at the same computational complexity level without having to spend more on the computation of the image encryption algorithm. Another extension to this uses traditional image processing techniques combined with a homomorphic secret key to work on floating point numbers and provide an encrypted image [3].

Also, multiple images can be encrypted at once using ghost imaging. This deals with a multiple image encryption technique in which a group of plain images are encrypted. Each plain image is encrypted into an intensity vector by using the computational ghost vectoring scheme. Then all the vectors are superimposed on each other to result in a single ciphertext image [6].

Finally after a thorough examination and survey of all possible techniques, a new algorithm became the inspiration for this project's encryption and decryption mechanism. It deals with the Rubik's Cube algorithm [1]. This is a novel algorithm which can encrypt an image without any chaotic means and uses the asymmetric encryption-decryption ideology combined with XOR operations and certain arithmetic operations. The algorithm suggested only applies to gray scale images but with the help from multiple image encryption techniques as seen above my project aims to extend it to coloured images. The coloured images can be divided into three separate planes of red, blue and green pixel values. These pixel values will form three different image matrices which will be encrypted separately and then superimposed together to get the final single encrypted image as the output. For decryption, the reverse of the encryption process will be followed which means dividing the encrypted image into red, blue and green pixel matrices, performing decryption and then superimposing to get the original image back.

Literature Survey :

- **Efficient image encryption scheme based on generalized logistic map for real time image processing**
  The paper discusses an efficient encryption algorithm which has been tested with real-time images. The scheme makes use of encryption with an efficient permutation based technique based on a modular logistic map to bring down the size of the chaotic value vector, required to permute a real-time image. The chaotic key sequence used in this technique changes the pixel values of a grayscale image. This optimises the chaotic key generation but is only extended on a grayscale image.

- **Image Encryption with Double Spiral Scans and Chaotic Maps**
  This paper discusses a chaotic map based encryption technique which uses two scans of the image matrix. The Double Spiral Scans take a random scan of the image matrix and jumble those particular locations it scans. This results in randomization of the image and hence makes it distorted and encrypted. This process is repeated twice hence the name double spiral scan. However if the entire image is based on the same pixel value then there will be no encryption despite the double scans.

- **Fully Homomorphic Image Processing**
  This paper deals with the outsourcing of computation to a third party which provides image processing resources and thereby giving security. It deals with the application of an extended code base which helps other applications to function at the same computational complexity level without having to spend more on the computation of the image encryption algorithm. This paper also shows the fully homomorphic image processing techniques and its drawbacks.

- **An efficient secret key homomorphic encryption used in image processing service**
  This paper has explained the homomorphic encryption technique for images. This technique uses traditional image processing techniques combined with a homomorphic secret key to work on floating point numbers and provide an encrypted image. The technique is quite advanced and complex and can be hosted to provide security on cloud platforms. The paper explains the use of coloured images and the manipulation of the colour pixel values.

- **A secure image encryption algorithm based on Rubik's cube principle**
  This paper explains the drawbacks of traditional encryption techniques for image processing. It uses the Rubik’s cube algorithm and implements image processing methods to get an encrypted image. The paper only deals with a single grayscale image matrix and hence cannot be extended to coloured images.

- **Multiple-image encryption based on computational ghost imaging.**
  This paper deals with a multiple image encryption technique in which a group of plain images are encrypted. Each plain image is encrypted into an intensity vector by using the computational ghost vectoring scheme. Then all the vectors are superimposed on each other to result in a single ciphertext image. A similar model work was described and gives a great insight on how to work with multiple images.

- **Utilizing Noise Addition for Data Privacy, an Overview**
  This paper gives a very unique idea of encrypting an image by spoiling the image. This scheme will add noise to the image matrix and perform certain arithmetic operations on the pixels to change the original image. This technique however would not be beneficial for the retrieval process as the computation would be very difficult.

- **A Survey on the Image Encryption Methods.**
  This paper deals with various image encryption techniques. It gives a comparative analysis of all the various systems of encryption including symmetric, asymmetric and chaotic based. The paper provides an overview and a good distinctive study of all these techniques.

- **A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation**
  This paper deals with the image encryption based on the XOR operation and other image arithmetic operations. The paper explains the use of XOR and the formation of the orthogonal matrix and skew tent map using image pixels for providing a secure cipher image.

- **Simple and secure image steganography using LSB and triple XOR operation on MSB**
  This paper deals with steganography and gives a vivid description on steganography. It also uses bit plane slicing along with XOR operation to work on the image and provide security.

Problem Statement :

Any image when provided as an input to the project should result in the generation of a new image which is distorted, unrecognisable and has minimal resemblance to the input image. Also, a file containing keys should be generated. When the distorted image is input in the project with the set of keys, the original image should be generated.

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.

[2] Fu, W., Lin, R., & Inge, D. (2018). Fully Homomorphic Image Processing. arXiv preprint arXiv:1810.03249.

[3] Yang, P., Gui, X., An, J., & Tian, F. (2017). An efficient secret key homomorphic encryption used in image processing service. Security and Communication Networks, 2017.

[4] Tang, Z., Yang, Y., Xu, S., Yu, C., & Zhang, X. (2019). Image encryption with double spiral scans and chaotic maps. Security and Communication Networks, 2019.

[5] Shah, A. A., Parah, S. A., Rashid, M., & Elhoseny, M. (2020). Efficient image encryption scheme based on generalized logistic map for real time image processing. Journal of Real-Time Image Processing, 17(6), 2139-2151.

[6] Wu, J., Xie, Z., Liu, Z., Liu, W., Zhang, Y., & Liu, S. (2016). Multiple-image encryption based on computational ghost imaging. Optics Communications, 359, 38-43.

[7] Mivule, K. (2013). Utilizing noise addition for data privacy, an overview. arXiv preprint arXiv:1309.3958.

[8] Abd El Waness, A. K., & Eldib, M. M. (2020). A Survey on the Image Encryption Methods. Journal of Computer Science and Information Systems, 11(2 June 2020).

[9] Ahmad, J., Khan, M. A., Ahmed, F., & Khan, J. S. (2018). A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation. Neural Computing and Applications, 30(12), 3847-3857.

[10] Astuti, Y. P., Rachmawanto, E. H., & Sari, C. A. (2018, March). Simple and secure image steganography using LSB and triple XOR operation on MSB. In 2018 International Conference on Information and Communications Technology (ICOIACT) (pp. 191-195). IEEE.