Multilevel Image Encryption and Decryption Using Pixel Value Rotation

Spoorthi B.S
th Semester,ISE Department MIT, Mysore

Nikitha Ballur
th Semester,ISE Department MIT, Mysore

Nischitha P2
th Semester,ISE Department MIT, Mysore

Ajay Kumar B R
Assistant Professor, ISE Department MIT, Mysore

Abstract- The field of encryption is becoming very important in the present era in which information security is of at most concern. Security is an important issue in communication and storage of images, and encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Although we may use the traditional cryptosystems to encrypt images directly, it is not a good idea for two reasons. One is that the image size is almost always much greater than that of text. Therefore, the traditional cryptosystems need much time to directly encrypt the image data. The other problem is that the decrypted text must be equal to the original text.

Keywords: Image encryption and decryption, block shifting, pixel value rotation.

I. INTRODUCTION

Encryption is the process of transforming the information to insure 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. As a result, different security techniques have been used to provide the required protection. The security of digital images has become more and more important due to the rapid evolution of the Internet in the digital world today. The security of digital images has attracted more attention recently, and many different image encryption methods have been proposed to enhance the security of these images. Image encryption techniques try to convert an image to another one that is hard to understand. On the other hand, image decryption retrieves the original image from the encrypted one. There are various image encryption systems encrypt and decrypt data, and there is no single encryption algorithm satisfies the different image.

In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text . This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm, that usually requires a secret decryption key that adversaries do not have access. For technical reasons, an encryption scheme usually needs a key-generation algorithm to randomly produce keys. There are two basic types of encryption schemes: Symmetric-key and public-key encryption. In symmetric-key schemes, the encryption and decryption keys are the same. Thus communicating parties must agree on a secret key before they wish to communicate. In public-key schemes, the encryption key is published for anyone to use and encrypt messages. However, only the receiving party has access to the decryption key and is capable of reading the encrypted messages.

II.PROPOSED METHODOLOGY

Encryption

The objective Double Encryption technique is to tackle the security issues while storing images and transmitting images. In the first phase, Biometric of the user is used as security key. Biometric value is used for creating image “blocks shifting” and number of pixel value rotations. In the 2nd phase BLOCK SHIFTING algorithm implemented. Here, the image is divided into 8 blocks and are shuffled.

In the 3rd phase, PIXEL VALUE BASED ROTATION algorithm is used. Here, value of each pixel of every block is rotated, based on the sum of integer values of key entered by the user.

Decryption

To obtain back the original image, double Decryption is applied. It is the reverse process of Encryption. If the Biometric is matched, then PIXEL VALUE BASED ROTATION algorithm is applied. And second phase of

Decryption uses BLOCK SHIFTING process will be performed.

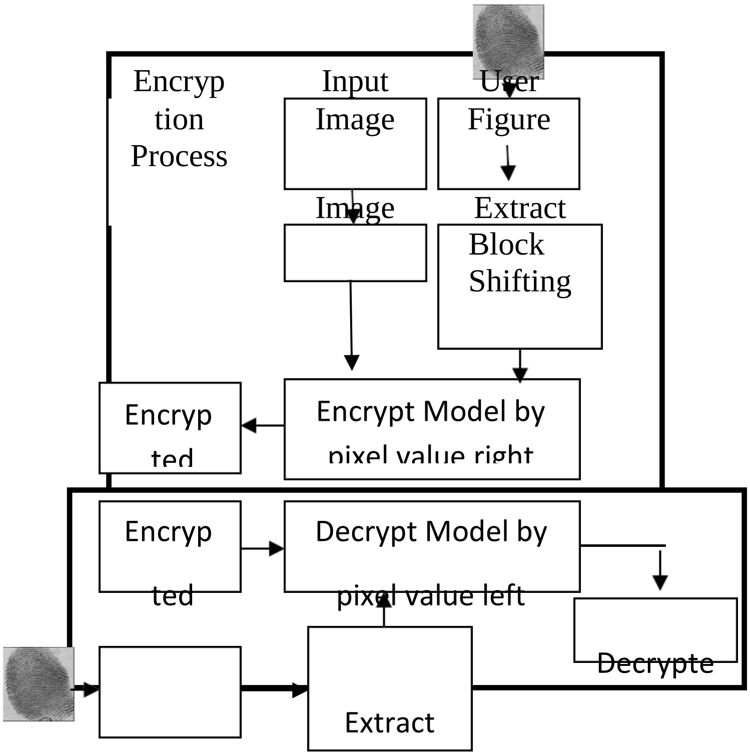
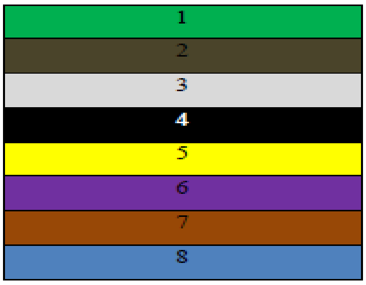


Figure: Block diagram of the proposed system

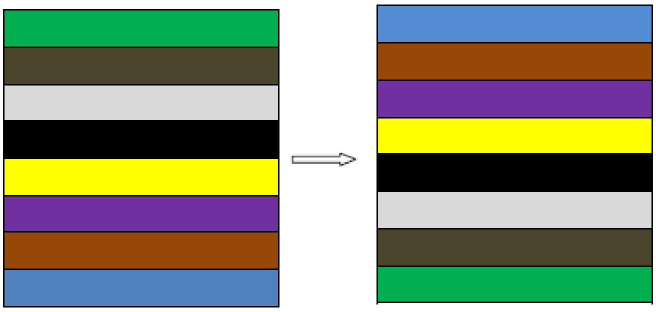
1. Dividing into blocks

The image is divided into 8 blocks.



2. Block Shifting

The divided blocks are shuffled using "BLOCK SHIFTING" algorithm. This is the second phase of Decryption.

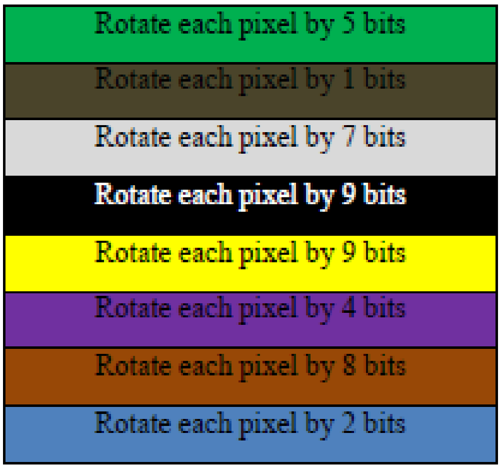


1) 3. Encrypt each block

This is the second phase of Encryption. "PIXEL VALUE BASED ROTATION"

algorithm is applied. By assigning each bit of sum to each block, each pixel value of every block is left rotate

Example:


Rotate each pixel by 5 bits
Rotate each pixel by 1 bits
Rotate each pixel by 7 bits
Rotate each pixel by 9 bits
Rotate each pixel by 9 bits
Rotate each pixel by 4 bits
Rotate each pixel by 8 bits
Rotate each pixel by 2 bits

I. SOFTWARE DEVELOPMENTPLATFORM

The focus in this paper is on the use of an image file as a carrier, and hence, the taxonomy of current steganography techniques for image files has been presented. Digital image stored in computer system are composed of finite number of elements in the form of array, each pixel has three color components: Red, Green and Blue (RGB). The three primary colors (red, green, blue) and their combination in visible light spectrum.

A. Color image

24 bit color image is best define by RGB color model in which each color appears in its primary spectral components of red, green and blue .This model is based on Cartesian coordinate system.

B. Least significant bit(LSB)

In LSB message bits are embed in least significant bit of cover image. LSB steganography can be classified by two methods LSB replacement and LSB matching.

C. Partition patterns

There are three basic partition patterns that include

1. B type partition patterns
2. Z type partition patterns
3. X type partition patterns.

D. Scanning patterns

There are four types of scanning patterns

1. Continuous Raster C
2. Continuous Diagonal D
3. Continuous Orthogonal O
4. Spiral

II. RESULT ANALYSIS

In this Paper we proposes a image hiding process by LSB substitution method. Read the RGB color image into our required size, a new image encryption algorithm is proposed that consider the input image of size m*n and works by shuffling the values of the RGB pixels. Large number of security approaches have been used in this regard like applying encryption and decryption.

III.CONCLUSION

The project “Multi Level Image Encryption and Decryption Approach based on Block shifting and Pixel Value Rotation using Biometric“ provides a very good enhanced encryption algorithm for image encryption. Where the algorithm uses a key value to divide and rotate

the pixels which is Bio-metric feature based value. This value is more secure than the user key. It consumes less CPU compare to RSA algorithm.

REFERENCES

[1] Manju Kumari, Shailender Gupta, Pranshul Sardana, ”A Survey of Image Encryption Algorithms”, 3DR Review First Online: 13 November 2017.

[2] Suchita Tayde, Asst Prof. Seema Silender, “ File Encryption, Decryption Using AES Algorithm in Android phone“,2015.

[3] Savithri G, K.L.Sudha, “Android Application for Secret Image transmission and Reception Using Chaotic Steganography“,2014 .

[4] Ankit Gupta, Namita Tiwari, Meenu Chawla, Madhu Shandilya, “An Image Encryption using Block based Transformation and Bit Rotation Technique “, 2014

[5] Honnaraju B, Manoj Kumar M, Shiva Sumanth Reddy, “Image Encryption by using Pixel Value Rotation",2012.