International Journal of Computing Science and Information Technology, 2018
ISSN: 2278-9669, April 2018 (http://ijcsit.org)

A Keyless Approach to Image Encryption and Decryption by applying Transformations

Vasantha Kumari N

Assistant Professor, Department of Computer Application,
Presidency College, Bangalore, India
Email: vasantha.kn@gmail.com

Abstract

Key oriented technologies limits to maintain the records of the key and high computational cost. Improvisation in key less approach to encrypt an image in Lossless color images is proposed in this paper. Two methods to implement an image is followed to encrypt an image .First, Image Splitting and second, multiple shares. The aim of the paper is to increase security by pixel value distribution through the entire image and improve the storage capability using SST technique. In this approach, originality and quality of the image is maintained.

Keywords: Transformation, Encryption, RGB image.

1. Introduction

Most commonly existing issue in distributed Networks is security during data transfer. There are so many types of encryption techniques to protect data from unauthorized access. In many areas, images are used for encryption. For example, it is must to protect military database, online video conferencing, etc. Nowadays, traditional Cryptosystem have been designed to protect textual data. In current era of networks, images are protected by Keyless image encryption.

A digital image defined as two dimensional array of pixels. Each pixel has intensity value and location address ie row and column. Each pixel consists of colors. Pixels are like small compact particle in pictorial image, henc

e arranged in rows and columns and store in different manner. **Bitmap** is mapping from some domain to bits that is values which are 1 or zero.

Upon reception, the cipher text can be transformed back into original plain text by using a decryption algorithm. However, images are different from text although the traditional cryptosystem, such as RSA and DES. Cryptosystem may be used to encrypt image directly, it has some limits:

1.Image is always greater than text. Hence forth, traditional cryptosystem need much time to directly encrypt the image data.

2. Decrypted text must be equal to that of original text. A Decrypted image containing small distortion is usually acceptable. However images are different from text although the traditional cryptosystem such as RSA and DES may be used. Cryptosystem can be used but has few disadvantages:

a. Image should always be greater than that of text which takes more time for traditional cryptosystem to directly encrypt the image data.

b. Decrypted text must be equal to original text

A digital image is a numeric representation of a two dimensional image where as an Image is a two-dimensional function f(x,y), where x and y are the spatial (plane) coordinates, and the amplitude of f at any pair of coordinates (x,y) is called the intensity of the image at that level.

	R	G	B
R	RR	RG	RB

G	GR	GG	GB
B	BR	BG	BB

Fig 1 Structure of Digital image

2. Related Work

2.1. Splitting of an image

Image is divided into number of shares. In the paper[1] Saeed Alharhi and Pradeep K Atrey introduced the idea of dividing a secret image into two shares. The individual share should not reveal any information about original image. In this encryption is based on SDS algorithm which defines Sieving, Division, and Shuffling. In Seiving technique generates split images are randomly divided. Shuffling shuffles and finally combines all the shares. Division divides the images randomly.

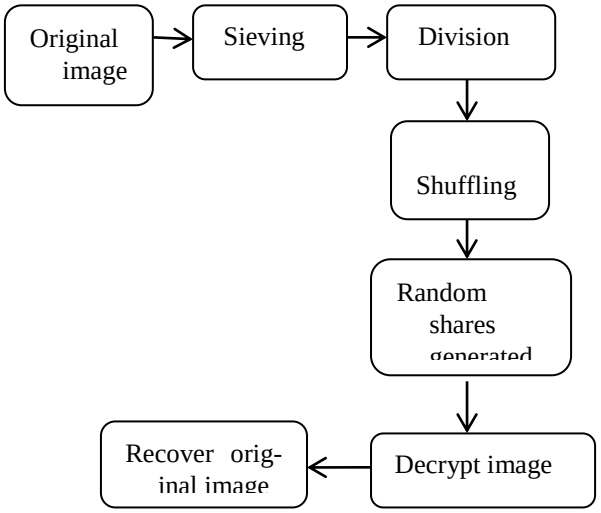


Fig 2. SDS Technique

2.2. Division

After getting the filtered individual R,G and B components, the next step involves dividing the R,G and B components into z parts/ shares each.

R_(RB,RC,RD,……..,RZ)
G_(GB,GC,GD,……..,GZ)
B_(BB,BC,BD,……..,BZ)

While dividing it is ensured that each element in RB-Z,GB-Z and BB-Z is assigned values randomly.The shares generated should regenerate R and G/B components.

2.3 Shuffling

Last step is shuffle operation. This involves interchange the elements in individual shares. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated.

3. Problem Definition

Existing system has some of the limitations:

When the size of the image increases so as the problem increases. Key records has to be maintained as well as computation involved in encryption.

The encryption algorithm is very poor in security because of using cryptanalysis. The new encrypted image not only shuffles the pixel positions of the original image but also changes the color values of the original image.

The motivation behind this research is growing the need for harder to break encryption and decryption algorithms as the computer and network technologies to develop. By proposing SST Keyless image encryption and decryption algorithm, it helps to reduce the relationship among encryption time complexity.

4. Solution Approach

4.1 SST System

The objective of this paper is to improve the security level of the encrypted images using transformation algorithm. In this technique, Sieving, Shuffling and Transformation is applied for image security. This technique involves three steps. First step, Secret image is split into Primary (R,G,B) colors, In Second step, RGB bits are shuffled within itself. In third step, using transformation to transform the original image format into unreadable formatted image. Finally these shuffled pixels reversed to get original image.

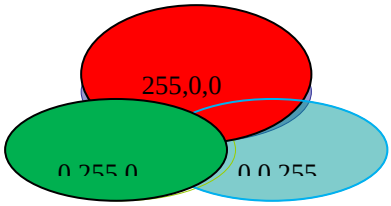


Fig.3 RGB bits

4.2 Flow of Data

- Input is an secret image where sieving is applied to get the RGB value and height X weight of an original image.
- The shuffling process is divided into two phases that is vertical and horizontal shuffling. Vertical shuffling technique used to shuffle pixel

Swapped into vertical manner and tiled on vertical side and this image go to horizontal shuffling (phase 2).In horizontal shuffling technique, used to shuffle pixel bits swapped into horizontal manner and image tiled Horizontal side.

- Then shuffling process to send encrypted image

Transformation process.

- Display encrypted image.

In the reverse process of sieving, shuffling and Transformation to get a original image and reversible image encryption will be done.

4.3 Algorithm

Step 1: START

Step 2: Input image

Step 3: Image is sieved into R,G and B colors and get height and weight of an image.

Step 4: Image is shuffled with the bits itself.

In phase 1, Horizontal shuffling

In pahse 2, Vertical Shuffling

Step 5: Transformation process

Step 6: Encrypted image

Step 7: STOP

4.4 SST Approach

The proposed technique is implemented with SST algorithm and involves three steps that is sieving, shuffling and Transformation. In step one, sieving the image into primary (R,G,B) colors. In step two, bits in the image is shuffled into RGB combination each within itself. In step three Transformation is used for pixel in the form of vertical, horizontal and diagonal direction. Finally these shuffled pixels reversed to retrieve the original image.

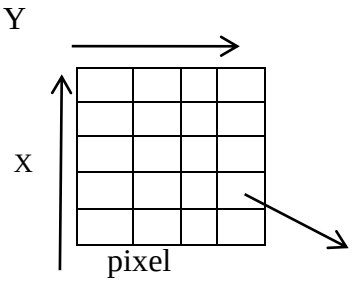
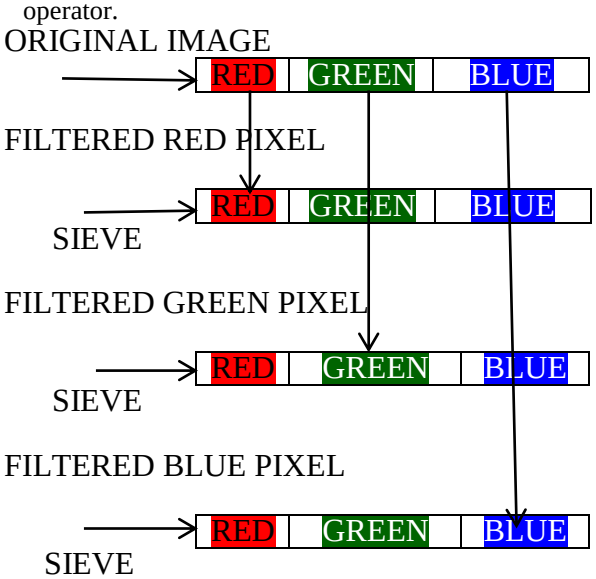


Fig 4. Pixels in a image

4.4.1 Sieving

Sieving involves filtering the combined RGB components into individual R,G and B components. The Granularity of the sieve depends on the range of values That R/G/B component may take individually. To make The process computationally inexpensive, sieving uses XOR operator.



4.4.2 Shuffling

We perform the shuffle operation of sieving image. This involves shuffling the elements in the individual shares i.e, RA-Z, GA-Z and BA-Z. The sequence in which the elements within the shares are shuffled depends on the value of one of the other shares generated from same primary color. In other words, RB decides how RA is shuffled, RC decides how RB is shuffled,…..RZ decides RZ-1 is shuffled and RA decides how Rz is shuffled. The shuffling operation uses the comparison operator on the LSB of the determining element to decide the shuffle sequence.

Phase 1: Vertical shuffling

In this phase the pixels copied into the position after the adjacent pixel in vertical manner.

Phase 2: Horizontal Shuffling

In this phase the pixels copied into the position after the adjacent pixel in horizontal manner

Transformation:

As per Bourke (1998), the BMP bitmaps are defined as a regular rectangular of cells called pixels.

BMP Files:

Header of the file stores general information about the BMP file. Information header contains the detailed contents about the bitmap image. Paletting stores the information of the colors being used for indexed color bitmaps.

JPEG Files:

The Joint Photographic Experts Group (JPEG) is one of the most popular formats of web Graphics. There are 24 colors supported by this format which stores all the color information in an RGB image and then compresses the size of the file to the saves the memory, or it saves the only the color information that is very important for the image. JPEG does not support transparency as like of GIF files.

Fig: 5 Original image

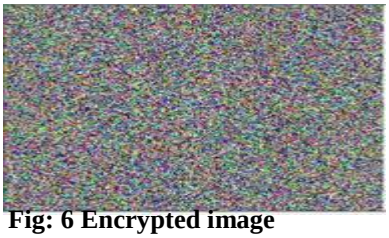


Fig: 6 Encrypted image

5. Experimental Results:

To implement the scheme on java platform, it was run over a range of photographs including dull/bright, dark/light and white..etc. The JPG with the name flower.jpg is used to demonstrate the result. It is a 250 X 190 pixel image. For processing the image, RGB of each pixel should be identified and get function of each pixel. After processing each pixel, RGB is separated to get different shades. After which Shuffling is applied and after applying horizontal and vertical shuffling of image bits, transformation techniques are applied. In Transformation technique, original image is encrypted into different types of unreadable pixel image which can be securely transmitted t the receiver. The main objective of this paper is to provide security and avoid thefts and to get the originality of the image without loss of any pixel by using reversible encryption techniques.

6. Conclusion

In this paper , improvisation to the keyless approach to lossless RGB image encryption is proposed. It is a emerging technique for multimedia image security. In the previous technique using key management, which has limita-

tions to security. The purpose is to increase image security and normalize the CPU utilization time.

7. References

1."A Keyless approach to image encryption" Siddharth Malik, Anjali Sardana(2011).

2. An improved scheme for secret image sharing Adi Shamir in 1979.

3. A Hyper-chaos Based Image Encryption Algorithm Chen zaiping, Li haifen, Dong enzeng, Du yang in 2010.

4. AlokaSinha and Kehar Singh, "A technique for image encryption using digital signature", Optics communications(2003).

5.
5.M. Lakshmi, S. Kavitha, keyless user defined optimal security encryptionISSN:2319-7242 Volume 2 Issue 6 June, 2013 Page No. 1788-1793 .

6. Chin-Chen Chang, Min-Shian Hwang, Tung-Shou Chen, "A new encryption algorithm for image cryptosystems", The Journal of Systems and Software 58 (2001), pp. 83-91.

7.Analysis on an Image Encryption Algorithm Shubo Liu1,2, Jing Sun1, Zhengquan Xu2, Jin Liu2.

8. S. Manjunath, N.G. Kurahatti, "Lossless image compression and encryption using SCAN", ...