International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

New Keyless Approach of Image Encryption

Prof. Chandra Mohan
, Dept.of CSE,
Christu Jyothi
Institute of Technology
and Science, Janagon, TS,INDIA

Abstract:

Some limitations of key oriented techniques ,to maintain the key records and increase the high computational cost ,to overcome the limitation of image size and key records, brute force attacks .This paper proposes an improved keyless approach for image encryption in lossless RGB images .There are two different approaches being followed an image encryption ,first approach is image splitting and second approach is the multiple shares .The objective of this work is to increase the security level by randomly distributing the pixel bit over the entire image .It can also improve the storage capacity by SST technique. In this keyless approach the reversible encryption will be done to maintain the originality of image without any loss of quality.

1. Introduction:

A security issues play a crucial role and must be aware about the attacks while transferring data over the distributed networks, and also safe guard to the user information. In this process previous work has been done and discovered different techniques, and algorithms to prevent and protect the data .In these models encryption and decryption of the confidential data took place while transferring the data through channels. According to previous work we have analyzed the different research articles and studied the papers. In current scenario we discovered for protection of user data that is images are protected by encryption that is a key less approach**.**

1.1 Digital Image and Bitmap

A digital image which consists of 0‘s and 1‘s is composed of pixels (short for picture elements). Each and every pixels are going to be represents the colors.(or gray level for black or white photos) by a single point in the image, so we can represent pixel is similar to a tiny dot of a particular color. Through measure the color of an image next to a large numbers of points, we can create a digital estimate of image from which a copy of the unique can be reconstructed. Pixels are a little like small compact particle in a predictable pictorial image, but arranged in a regular model of rows and columns and store information in a different way., that means a digital image is a array of pixels is called as **bitmap.**

International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

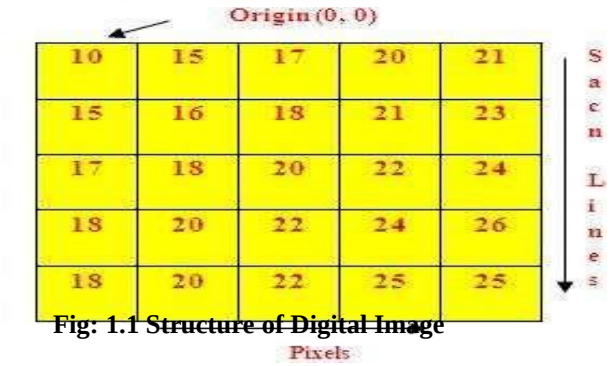


Fig: 1.1 Structure of Digital Image

Digital image processing is use of computer algorithm to perform image processing on digital images. Since a digital processing filed has many reward over the analog image processing. It allow a much wider range of algorithm to be useful to the input data and can avoid problems such as the increase of noise and signal alteration during processing. Because images are defined over two dimensions (perhaps more) digital image processing may be modeled in the form of multidimensional systems.

2. REALATED WORK

2.1 Image splitting:

In this technique image splitting is performed in which an image divided into at pixel level that is two or more shares. Saeed Alharthi and Pradeep K. Atrey in 1979 are credited for introducing the idea of dividing a secret data into 2 random shares. The individual shares should not convey any information about the original image, but a proper arrangement of these shares will help regenerate the ori ginal image.

To implement this technique does not need any key management and no computation in description but the main limitation of this approach pattern will be identified

2.2. Multiple Shares

A new method which performs, "without key we can approach to image encryption" to splitting an image into multiple shares proposed. In this encryption is based on SDS algorithm. SDS means Sieving(divide combined particls), Division, and Shuffling(interchange of their places). In the first step sieving technique generates the secret image is split into Red, Green, Blue colors. In the second steps Division technique generates the split images are randomly divided. In the last steps shuffling technique shuffled each shares and finally combined all shares.

International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

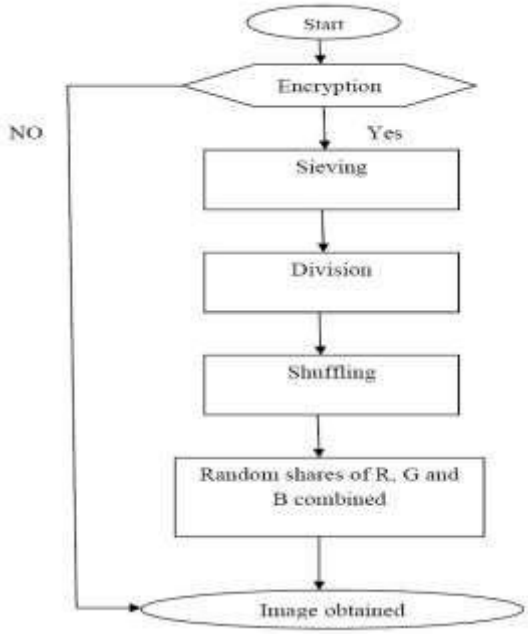


FIG: 2 SDS FLOWCHART

2.2.1 Sieving

Sieving is the process of filtering the group RGB components into individual R, G and B components .To makes the process computationally inexpensive and sieving uses the XOR operator.

2.2.2 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, we can get the entire domain for randomized selection; in case x = 7, then individual elements should be randomly assigned a value varying from 0- 255. The shares so generated should be such that (RA, RB, RC, ---------- RZ) should regenerate R and similarly for G/B components.

2.2.3 Shuffling

We can perform the last step that is shuffle operation. This involves interchange the elements in the 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 identification in existed system

In the, existing system used algorithm, in this algorithm the following are the some of the limitations:

It will creates a problem when increasing the image size and we should maintain the key records as well as computation involved in encryption as also weak security functions issue.

The algorithm is very long so that data has to be wait for long time. The encryption algorithm is very poor in security, because of by using cryptanalysis they can break the cryptosystem

.

The new encrypted arithmetic not only shuffles the pixel positions of the original-image, but also changes the color values of the original-image.

Image encryptions have applications in worldwide communication that is multimedia systems, medical and military imaging systems and organizations and industry. Each type of multimedia data has its own uniqueness such as high correlation among pixels and high ambiguity. Thus, different techniques should be used to protect confidential image data from unauthorized access .The motivation behind this research is the growing need for harder-to-break encryption and decryption algorithms as the computer and network technologies to develop. We consider that by proposing SST keyless image encryption and decryption algorithm, it will helps to reduce the relationship among image encryption time complexity.

4. SOLUTION APPROACH

4.1 SST System

The objective of this research paper is to improve the security level of the encrypted images using the proposed transformation algorithm. In this proposed technique using a Sieving, shuffling, transforming algorithm for image security .In this research using a (vertical and horizontal shuffling) to shuffle the image pixel bit and then we need to apply transformation techniques to covert image into un understandable image format. This algorithm will be used as a preencryption transform that means before encryption to confuse the relationship between the original images and the generated image. Correlation, Shuffling, Transformations have been used to measure the security level of the images.

Furthermore, the focus of this research was concerning a bit mapped (bmp) images as well as JPEG (Joint picture expert group) using the SST algorithm.

The proposed technique is implemented with the SST algorithm and involves three steps. Sieving, Shuffling and Transformation .In step one (Sieving) the secret image is split into Primary(R, G, and B) colors. Then (Shuffling) the shuffled all bit of RGB combination each within itself. Then (Transformation) using transformed techniques to transform the original file format into cipher formatted image. Transformation based system have many properties to achieve high security level, such as sensitivity to change initial conditions and parameters, periodicity (a system that tends in probability to a limiting form that is independent of the initial conditions), random behavior and un neutral periodic orbits with long periods. It has very high spreading and mystification properties that are desirable for encryption and decryption. Finally these shuffled pixels reversed get original image.

International Journal of Research in Science advanced Technology and management studies (IJRSTMS)

ISSN: 2459-425X • Website: www.ijrstms.com

5. SYSTEM ARCHITECTURE

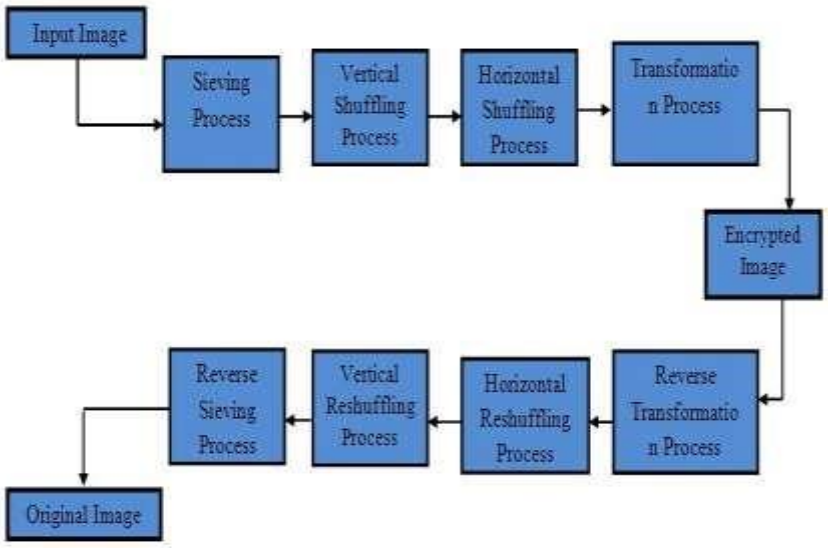


FIG: 3 SYSTEM ARCHITECTURE

In this SST (Sieving, shuffling and transformation) techniques firstly input an original color RGB image. In this image apply the sieving operation to identify the RGB color image in different shades. Then shuffling operation will be done, in this shuffling process we can approach two ways that is vertical and horizontal shuffling. In this vertical process, shuffled the swap the neighbor pixel bits of image are processed in vertical manner. These images pass into next horizontal shuffling, this process, shuffled the swap neighbor pixel bit of vertical image again processed in horizontal manner and at last this image goes to the next stage that is transformation process. In this process to identify shuffled image as working bitmap image and to bitmap file header to use. Inside the Image DES algorithms are through encrypted image and these transformation processes to 54 bit header byte to remove the shuffle horizontal image and then this encrypted image send into the receiver side. In this receiver side just reveres approach to apply that is decrypting. In this reverse transformation process, to add the original file header byte in encrypted image and then pass into horizontal reshuffling process will be done. In this process reshuffled the horizontal neighbor pixel bits arrange and then go to the next stage, in vertical reshuffling process, to neighbor vertical neighbor pixel bits arrange and reverse sieving process to get different RGB image.

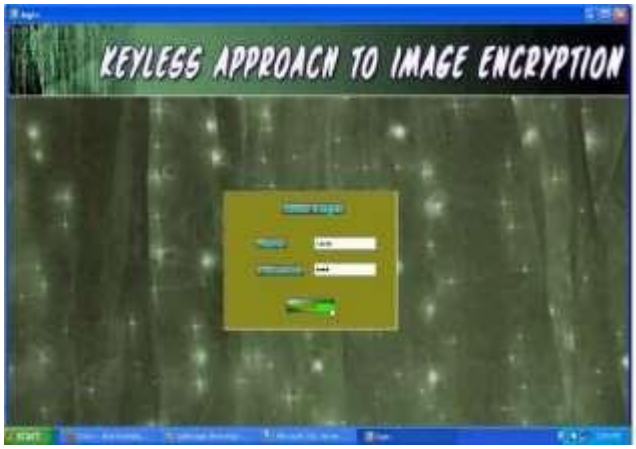
6. EXPERMENTAL RESULTS

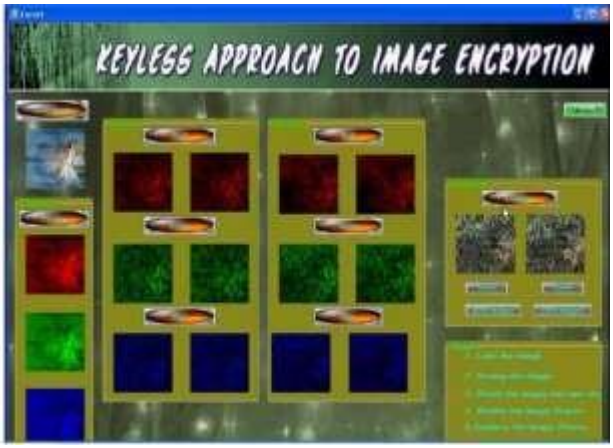
To validate our algorithm we implemented a modified (2,2) threshold VCS. This scheme was identified to validate the results as this could have it's real world application to authenticate a user. A photograph of a user could be clicked and divided into two shares. One of the shares would be caught by the authenticating agency and the other would be held by the user who is being authenticated. The process of creating two random shares has been represented in Figure 1.

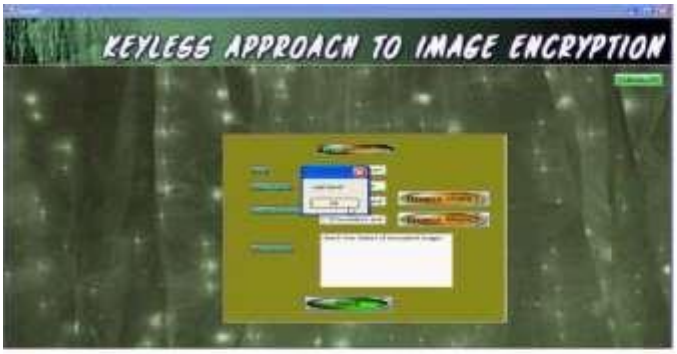
We implemented the scheme on the java platform using eclips IDE. The scheme was run over a wide range of photographs including bright/dull, colored/black and white etc. A jpg(joint photographic experts group) image titled

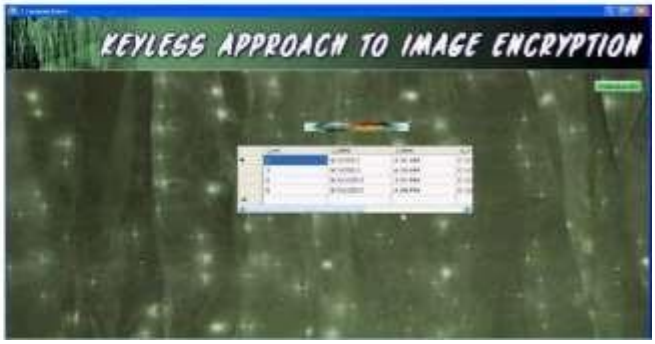
Leena.jpg is used to demonstrate the results (Figure 1). It is a 300 X 168 pixel image with an image depth of 24 bits (8 bits each for R/G/B).

6.1 SCREEN SHOTS









7. CONCLUSION

In this paper a new enhanced encryption method is introduced using visual cryptographic scheme which is a hybrid of the traditional VCS and the standard image encryption schemes. A secret image is split into multiple random images and with minimum computation the original secret image can be retrieved back. The proposed algorithm has the following eminence

(a) The original secret image can be retrieved as it is

(b) There is no pixel expansion and hence storage requirement per random share is same as original image

(c)No need to bother about key management because no secret keys involved as encryption is carried out based on the distribution of values amongst various shares

(d) The scheme is robust to withstand brute force attacks.

The scheme is suitable for authentication based application or where trust cannot be reposed in any one participant for decision making and a collective acceptance is required to proceed. A typical scenario for this could be thought of as a secret code which has to be fed in to commence a nuclear strike; the said code could be converted into an image and split into random shares, held with the collective decision making body. To retrieve the secret code random share of all the participants would be required.

8. REFERENCES

[1] A Keyless approach to image encryption" Siddharth Malik, Anjali Sardana, IEEE (2012).

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

[3] An improved scheme for secret image sharing Saeed Alharthi and Pradeep K. Atrey, 2010 IEEE. [4] Image Cryptography: The Genetic Algorithm Approach, Sandeep Bhowmik, Sriyankar Acharyya, 2011 IEEE.

[5] "A Hash based Approach for Secure Keyless Steganography in Lossless RGB Images", Ankit Chaudhary, J.

Vasavada, J.L. Raheja, Sandeep Kumar, Manmohan Sharma3 The 22nd International Conference on Computer Graphics and Vision and image processing Russia, Moscow, October 01, 2012

[6] An Improved Pixel Sieve Method for Visual Cryptography, Vaibhav Choudhary, Pravin Kumar, Kishore Kumar, D.S. Singh, International Journal of Computer Applications (0975 – 8887) Volume 12– No.9, January 2011.

[7] A New Cryptology Approach for Image Encryption, Nidhi Sethi and Deepika Sharma, 2012 2nd IEEE.

[8] A New Encryption Method For Secure Embedding In Image Watermarking, MohammadReza Keyvanpour, Famoosh Merrikh-Bayat, 2010 IEEE.

[9] Image Encryption Algorithm Based on Henon Chaotic System Chen Wei-bin1, Zhang Xin 2009 IEEE.

[10] Keyless user defined optimal security encryption M. Lakshmi, S. Kavitha volume 2 issue 6 2013 International Journal of Engineering and Computer Science.

[11] Analysis on an Image Encryption Algorithm, Shubo Liu1,, Jing Sun, Zhengquan Xu, Jin Liu, 2008 IEEE.

Image Encryption Using Different Techniques: A Review komal D patel, Sonal Belani, International Journal of Emerging Technology and Advanced [12]

Engineering, Nov 2011.