CAREER POINT UNIVERSITY HAMIRPUR

CPUH-Research Journal: **2015***, 1(2),* 59-61
ISSN (Online): 2455-6076
http://www.cpuh.in/academics/academic_journals.php

Three Quadrant Method for Securing Image by Using Visual Cryptography

Chandan Sharma[1*], Vinod Sharma[2] and Ankush Sharma[2]

[1,2 & 3] *Career point University, School of computer science and Engineering, Bhoranj (Tikkar Kharwarian) MDR 35, Himachal Pradesh, India*

[*] *Correspondance E-mail: chandan786p@gmail.com*

ABSTRACT: Nowadays it becomes very necessary to protect digital media by some effective one of the method to secure digital media is visual cryptography. Naor and Shamir proposed first algorithm in the field of Visual Cryptography in 1994. So many methods have developed in the Visual Cryptography field. We have proposed new method for securing image here. Here we have use Eclipse. Image by using (2, 2) secret sharing scheme is best technique.

Key Words: Quadrant Method; digital media and visual cryptography.

INTRODUCTION: There are many aspects to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential aspect for secure communications is that of cryptography

Cryptography: The art of protecting information by transforming it (encrypting it) into an unreadable format, called cipher text. Only those who possess a secret key can decipher (or decrypt) the message into plaintext. Encrypted messages can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable.

Visual Cryptography: Visual Cryptography is a one of encryption technique by which information in images can be hided in such a way that it can be decrypted by the vision of human if the correct key image is used. It has two transparent images. One image has random pixels and the other image contains the secret information. We can retrieve the secret information from one of the images. Both transparent images and layers are required at the time of revealing the information. The easiest way to implement is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears

Sharing schemes (existing): In middle of 1979 this idea of secret sharing was proposed by Adi Shamir and G. Blakley. Asmuth and Bloom.Shamir In 1983 was proposed another method for secret sharing on the scheme which is based on Polynomial Interpolation; Asmuth-Bloom scheme is based on Chinese Remainder theorem. Whereas Blakley scheme is based on hyper plane geometry.

(2, 2) secret sharing: This scheme divides the secret information P into 2 shares
Let us assume that parts are, P1, P2 in such a way that Knowledge of any all 2 parts can show the secret information. Knowledge of 1 part will not reveal the secret information.

(2, n) secret sharing: This scheme divides the secret information P into n number of parts
Let us suppose that these parts are, P1, P2……Pn
in such a way that Knowledge of any 2 parts can show the secret information. Knowledge of 1 part will not show the secret information.

(k, n) secret sharing[11]:This scheme divides the secret information Pinto n number of shares
Let us suppose that these parts are, P 1, P2……Pn
in such a way that-

Knowledge of k or more shares among Pi (i n) can reveal the secret information.
Knowledge of less than k shares reveals no information about the secret share.
This technique is called (k, n) secret sharing [10].
(n, n) Secret sharing [12]

This scheme divides the secret information P into n number of shares

Let us suppose that these parts are, P 1, P2……Pn
in such a way that Knowledge of n shares can reveal the secret information.

Knowledge of n-1 shares will not reveal the secret information.

Proposed Work: Quadrant Based (2, 2) Secret Sharing Visual Cryptography Scheme
In this proposed technique we use (2, 2) secret sharing method for encryption and decryption. In this technique we divide the original Image in to 2 quadrants
Encryption:

This technique has the following steps:-

Step 1: Take the first quadrant of the original image i.e. Q1 and encrypt the 1st quadrant with (2, 2) cryptography technique. When we apply (2, 2) secret sharing technique we get share1 and share2 of the 1st quadrant.

Step 2: Take the second quadrant of the original image i.e. Q2 and encrypt this 2nd quadrant with (2, 2) secret sharing technique. When we apply (2, 2) visual cryptography technique we get share3 and share4 of the 2nd quadrant.

We get the original image in the encrypted form after applying these steps. If we divide the original image in 2 quadrants then we get the 4 number of shares.

Generally if an image is divided into AN number quadrants then after apply (2, 2) visual cryptography technique we get 2AN number of shares

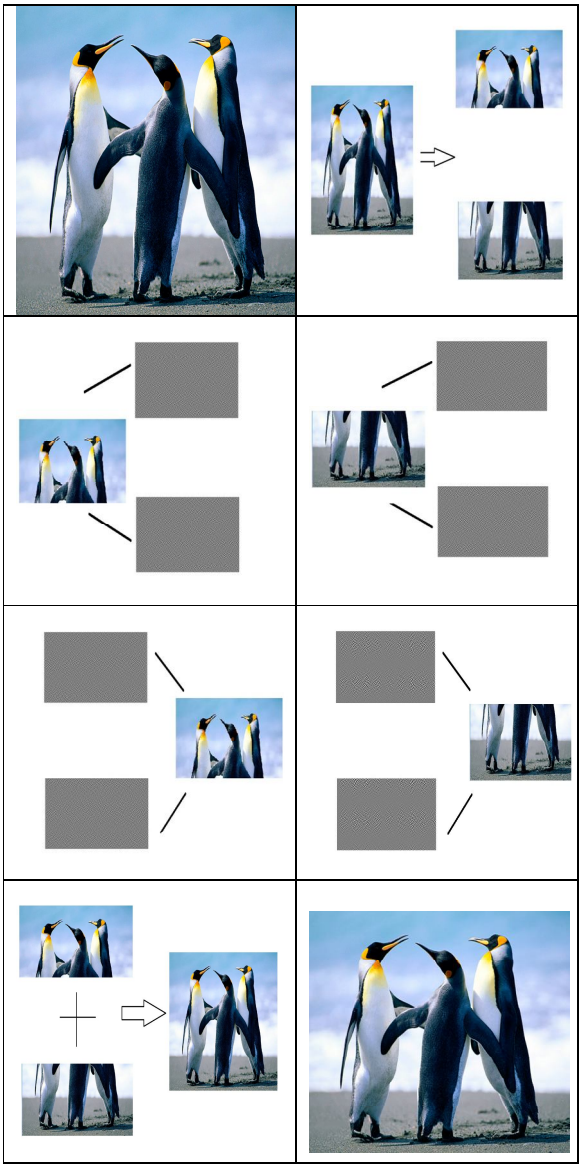
Mathematically it can be represented as:-
By using "Quadrant Based (2,2) Secret Sharing Visual Cryptography Scheme"
If we divide Original image in AN quadrants.
Number of shares = 2AN.

Decryption: In this process of decryption we retrieve the original image by stacking the shares of the relevant quarter. After applying encryption we got 4 shares and original image is retrieve only by superimposing the share that are related to that quarter.
We have shares as follow share1, share2, share3, share4.

Step1: We take share 1 and share 2 By stacking share 1 and share2 we get the 1st quadrant of the original image.

Step2: We superimpose share 3 and share 4 , after superimposing these shares we get the 2nd quadrant of original image.

Purposed technique pictorial overview:-



CONCLUSION: By using the proposed method we can encrypt the image with high level of security even by using simple (2, 2) secret sharing scheme. The proposed method is faster than other schemes because it follow simple (2, 2) secret sharing scheme which generate only two share for encryption and required only these two shares for decryption. All shares are required to regenerate the original image, missing of any share will not result in the reveling the original image. We can also increase the security just by increasing the number quadrants of image. Our future work will be to code a program in which division, encrypt and decryption are performed in a single program. We further study the impact of image size in the following technique. We will also implement the following method for the audio encryption.

REFERENCES:

1. Sumedha Kaushik & Ankur Singhal 2012. Network Security Using Cryptographic Techniques, 2(12), IJARCSSE.
2. Shamir 1979. How to share a secret, Communications of the Association for Computing Machinery, 22(11) 612-613.
3. Sonali Patil1, Sandip Sathe and Pravin Mehetre 2013. Secure and Verifiable (2, 2) Secret Sharing Scheme for Binary Images" IJCSI International Journal of Computer Science Issues, 10(1).
4. Suman Chandrasekhar, Akash H.P, Adarsh. K, Mrs. Smitha Sasi 2013. A Secure Encryption Technique based on Advanced Hill Cipher For a Public Key Cryptosystem, 11(2), IOSR-JCE.
5. Yogesh Kumar, Rajiv Munjal and Harsh Sharma 2011. Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures, 11(3), IJCSMS.
6. Pratap Chnadra Mandal 2012. Superiority of Blowfish Algorithm, 2(9), IJARCSSE.
7. M. Naor and A. Shamir 1995. Visual cryptography, Advances in Cryptology-Eurocrypt 94, pp. 1–12.
8. Bibhas Chandra Dhara 2011. k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence, IJCA, 25(11).
9. Shyamalendu Kandar & Bibhas Chandra Dhara 2011. k-n Secret Sharing Visual Cryptography Scheme on Color Image using Random Sequence, IJCA, 25(11).
10. Abhishek Kr Mishra, Ashutosh Gupta & Ashish Kumar 2012 (n, n) Visual Cryptography based on Alignment of Shares, IJCA 60(18).