**Available Online at www.ijcsmc.com**

**International Journal of Computer Science and Mobile Computing**

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

***IJCSMC, Vol. 3, Issue. 6, June 2014, pg.438 – 443***

**RESEARCH ARTICLE**

# A Key Division Scheme to Improve Visual Cryptography on Half Tone Images

**Aruna Tomar**
Student, Electronic & Communication Engineering Department
DCR University of Science & Technology, Murthal (HR), India
aruna_tomar07@yahoo.com

**Sunita Malik**
Asstt. Prof., Electronic & Communication Engineering Department
DCR University of Science & Technology, Murthal (HR), India
sntmlk76@gmail.com

***Abstract*— Visual Cryptography is a special encryption technique to hide information in images in such a way that will not be retrieved by human visual system. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into n number of parts let n. k-n secret sharing scheme is a special type of Visual Cryptographic technique where at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information. In our paper we have proposed a new k-n secret sharing scheme for black and white image where encryption (Division) of the image is done using Random Number generator.**

***Keywords*— Encryption, ANN, DWT, Lossy, Lossless**

## I. Introduction

Any web based computer system is susceptible to attacks from system hackers who could attempt to overwhelm a compute0r system to gain information for illegal use. They could also attempt to crash a system for the aim of sabotaging a Company's business operations. There are a number of system attacks that have been established to sabotage computer systems.

### A) Authentication

Authentication is the process of establishing whether someone or something is who or what it is declared to be. In most internet network systems authentication is generally done through the use of login usernames and passwords. The user of the system is assumed to know the password in order to get authenticated. Every user is initially registered on the system by a system administrator using an assigned or self-declared password. On each subsequent use, the user must know and use the previously declared password. The main weakness of these kinds of systems is that the passwords can be guessed, stolen, accidentally revealed, or forgotten by the user.

System hackers use password guessing as a simple method of attacking a computer system, be it on a network or offline.

Password guessing requires the hacker to have known usernames and suitable password guesses, by persistently trying the guessed passwords into the system, the attacker could finally break in, and this is mainly due to poor passwords being chosen by users. The best way to protect a system from this form of unwanted intrusion is to prevent users from having an infinite number of login attempts with wrong passwords; the user should be locked out of the system after a specific number of failed login attempts. [2] Another form of password theft can be achieved by a hacker illicitly tapping into a system terminal on a network and logging the passwords entered. A way of countering this form of attack is by encrypting the data traffic on the network. [3] For this reason, Internet business and many other transactions require a more stringent authentication process. The use of digital certificates issued and verified by a Certificate Authority (CA) as part of a public key infrastructure is considered likely to become the standard way to perform authentication on the Internet.

### B) Encrypted Communication

The communication process over the internet is intrinsically insecure, due to the fact that data being transferred over the internet medium can be susceptible to attacks and eavesdropping from different points of the transmission route. There is a essential need that online system's which deal with confidential and sensitive data, such as an online voting system, have to provide a means in which data communication between the client to the server is encrypted, thereby making the data being transmitted unusable to a would be system attacker. There are a number of cryptographic algorithms which can be used to encrypt data; algorithms like RSA, DES, and Blowfish can all be used at some point of an online system to make to it secure. These algorithms are going to be discussed, but the main encryption processing techniques which are behind these algorithms are the Symmetric key cryptography and the Asymmetric key cryptography.

### C) Symmetric Key Cryptography

This form of encryption is also known as the secret key cryptography. Symmetric key cryptography makes use of the same private key while performing an encrypted communication between two users. The same secret key is used for the encryption and decryption of data being transmitted between the two or more users. This form of cryptography makes use of stream ciphers and block ciphers for encrypting plain text. A stream cipher is an encryption method that is used to encrypt plain text or digits one character at a time while block ciphers encrypts blocks of data. Symmetric Key cryptography example is the Data Encryption Standard (DES) algorithm.

### D) Block Ciphers

A block cipher is an encryption method which encrypts large blocks of text; the block cipher regards the input stream for encryption as blocks of fixed sized bytes which can be up to 128 bits long. The block cipher can encrypt a 128 bit plaintext and generate a 128 bit cipher text as the output result. The block cipher also has a reverse mechanism, which is in form of a decryption function that converts the 128 bit cipher text and decrypts it back to the 128 bit plaintext. In order for a block cipher to encrypt data, the function would need a secret key which comes as a string of bits normally 128 to 256 bits long.

### E) Asymmetric Key Cryptography

This form of encryption makes use of one public key which is available to all users and a private key which is known only by the message recipient. The public key can be exchanged between users who can use it to encrypt data being transmitted to another user, the private key which should be kept secret, is used to decrypt the encrypted data to produce the original unencrypted data. This form of key cryptography is used by the Rivest, Shamir, and Adleman (RSA) encryption algorithm.

### F) Digital Certificates

A digital certificate is security identification medium used in juxtaposition with Asymmetric cryptography. Digital certificates can be provided by the certification authority (CA). The true owner of the public key is determined and the owner is verified to determine if the owner of the public key is who he/she claims to be. The certificate can hold the digital signature of the CA which the CA signs using their private key. The CA's public key is also included to verify that the certificate is valid. Through the use of a digital certificate the user of an online system can be sure of whom they may be dealing with on the internet. The process of verifying the certificate is done by the user's browser software.

## II. RELATED WORK

Alfre Jo De Santk et.al [1] has proposed visual cryptography schemes in which two pixels combine in XI arbitrary way and analyze the pixel expansion and the contrast of *(2,* n)-threshold visual cryptography schemes. In this scheme, any pair of n shares can visually reconstruct the secret image, but any single share has information on the secret image. Author considered all the possible ways to perform pixel sharing and expension under contrast analysis**.** Chin-Chen Chang et.al [2] has presented a visual cryptography scheme for color image hiding. By means of little additional computations, it goes through a color index table to hide and recover a secret image. A secret color image hides itself in two arbitrary color images, which can be constructed and then are kept by two participants, separately. This paper proves that only one of the two camouflage color images cannot reveal the secret image. Thus, the hidden information is recurred. In sharing and recovering a secret image, very small memory space and simple computations are required, and that indeed deserves today's common mobile communication platform. Chin-Chen Chang et.al [3] has proposed colored visual cryptography schemes based on modified visual cryptography. By means of a few additional computations, users can hide a colored secret image into some shares. However, the size of the shares and the implementation complexity in these schemes depend on the number of colors appearing in the secret image. Author defined a work on secret color image generation using visual cryptography. The size of the shares is fixed; it does not vary when the number of colors appearing in the secret image differs. Since the newly proposed scheme has the advantage of low computation and avoids the drawbacks mentioned in the previous approach, it is indeed suitable for today's requirement of low power. Stelvio Cimato et.al [4] has defined an effective Visual cryptography scheme that allow the encoding of a secret image into *n* shares which are distributed to the participants, such that only qualified subsets of participants can "visually" recover the secret image. In colored threshold visual cryptography schemes the secret image is composed of pixels taken from a given set of c colors. This paper shows the c-color (k, n)-threshold visual cryptography schemes and provides a characterization of contrast-optimal schemes. Constructive proof of optimality, with respect to the pixel expansion, of c-color *(n, n)* -threshold visual cryptography schemes. Author has defined a construction method for c-color *(n,* n)-threshold schemes. Indeed, once we have fixed an arbitrary value for p (p, n), and finally gives the values for all other multiplicities of the scheme. Zhi Zhori and Gonzalo et.al [5] has proposed the method of Visual cryptography that encodes a secret image SI into n shares of random patterns. If the shares are xeroxed onto transparencies. Method can visually decode the secret image by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. Such a scheme is mathematically secure; however, it produces random patterns which have no visual meaning, raising the suspicion of data encryption. In this paper, to achieve a higher level of security, the propose halftone visual cryptography. Where all shares are halftones of grey level images carrying significant visual information. The proposed methods utilize blue-noise dithering principles to construct halftone shares having visually pleasing attributes. The pleasing visual quality is obtained on the key complementary pair, share 1 and 2. Further studies are required to improve the visual quality of the other shares. Wei-Qi Yan, Duo Jin [6] has proposed the applications of Visual Cryptography on print and scan images. Visual cryptography is not much in use in spite of possessing several advantages. One of the reasons for this is the difficulty of use in practice. The shares of visual cryptography are printed on transparencies which need to be superimposed. However, it is not very easy to do precise superposition due to the fine resolution as well as printing noise. The proposed method employs the Walsh transform to embed marks in both of the shares so as to find the alignment position of these shares. Experimental results show that our technique can be useful in print and scan applications. In this paper, we have tried to solve the practical problem associated with the use of visual cryptography. Therefore propose the use of the Walsh transform to embed alignment marks in the transform domain. These marks are used as guides to precisely align the shares automatically. The experimental results point to the viability of the use of VC for print and scan applications. Future work will focus on the applications of visual cryptography on the 2D bar code. Chih-Ming Hu and Wen-Guey Tzeng [7] has proposed the method to detect the Cheating Prevention in Visual Cryptography. In this paper, we studied the cheating problem in VC and extended VC. The method considered the attacks of malicious adversaries who may deviate from the scheme in any way. Presented three cheating methods and applied them on attacking existent VC or extended VC schemes, improved one cheat-preventing scheme. They proposed a generic method that converts a VCS to another VCS that has the property of cheating prevention. The overhead of the conversion is near optimal in both contrast digression and pixel expansion. The transformation incurs minimum overhead on contrast and pixel expansion. It only added two sub pixels for each pixel in the image and the contrast is reduced only slightly. Zhi Zhou, et.al [8] has proposed Halftone Visual Cryptography scheme. Visual cryptography encodes a secret binary image (SI) into shares of random binary patterns. If the shares are xeroxed onto transparencies, the secret image can be visually decoded by superimposing a qualified subset of transparencies, but no secret information can be obtained from the superposition of a forbidden subset. The binary patterns of the shares, however, have no visual meaning and hinder the objectives of visual cryptography. Extended visual cryptography was proposed recently to construct meaningful binary images as shares using hyper graph colorings, but the visual quality is poor. In this paper, a novel technique named halftone visual cryptography is proposed to achieve visual cryptography via half toning. Based on the blue-noise dithering principles, the proposed method utilizes the void and cluster algorithm to encode a secret binary image into halftone shares (images) carrying significant visual information. The simulation shows that the visual quality of the obtained halftone shares is observably better than that attained by any available visual cryptography method known to date. The new method can be broadly used in a number of visual secret sharing applications which require high-quality visual images, such as watermarking, electronic cash, etc. Geum-Dal Park et.al [9] has proposed a scheme on Copyright Protection Scheme with Visual Cryptography. This paper proposes a new efficient and secure copyright protection scheme using visual cryptography technique. The proposed scheme uses simple codebook to generate a watermark image. The proposed scheme does not need to expand the watermark image. The proposed scheme uses simple codebook to generate a watermarked image. The scheme does not need to expand the watermark image. By using some experiments, we showed that the proposed method not only can verify the ownership of the copyright, but also is robust to resistant the variety of attacks. Debasish Jena1 et.al [10] has proposed a Novel Visual Cryptography Scheme. The proposed method of Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm which is a modified version of Data hiding in halftone images using conjugate error Diffusion technique (DHCED). In proposed scheme generates the shares using basic visual cryptography model and then embed them into a cover image using a DHCOD technique, so that the shares will be more secure and meaningful.

## III. PROPOSED APPROACH

Visual cryptography is a cryptographic technique which allows visual information (Image, text, etc) to be encrypted in such a way that the decryption can be performed by the human visual system without the aid of Computers. [1] Image is a multimedia component sensed by human. The smallest element of a digital image is pixel. In a 32 bit digital image each pixel consists of 32 bits, which is divided into four parts, namely Alpha, Red, Green and Blue; each with 8 bits. Alpha part represents degree of transparency. If all bits of Alpha part are '0', then the image is fully transparent.

In this paper we have proposed an algorithm to divide a digital image into n number of shares where minimum k numbers of shares are sufficient to reconstruct the image. If k numbers of shares are taken then the remaining shares are (n−k). In an image if certain position of a pixel is 1, then in (n−k) +1 number of shares in that position of that pixel there will be 1. In the remaining shares in that position of the pixel there will be 0. A random number generator is used to identify those (n−k) +1 number of shares.

### Algorithm

```
Algorithm(Img)
/*Img is the image on which the visual cryptography will be applied*/
{
    1. Divide the Image in N sub Images or blocks.
    2. Obtain K Bit values from N block data to define the data
       sequence
    3. Now K Bit Data will represent the Information Bits
    4. Now split the information in two sub blocks of size k/2
    5. If (Pixel=White)
       {
    6. Set the new random sequence for the pixel
       }
       Else
       {
    7. Set Other Bit sequence for Pixel
       }
    8. Reconstruct the pixel at gray level analysis and under the
       contrast specification for reconstruction of image.
    9. Return Image;
}
```

In the case of visual cryptography, decryption is done by human visual system. It is already discussed that human visual system acts as an OR function. In the case of decryption, for computer generated program; OR function can be used.

Here the numbers of shares are taken as input from user. As the shares are created from the image taken as input in encryption algorithm, each share must be of equal height and width as the source image. Then bitwise OR operation is performed among pixels of the shares, and final pixel values are stored in an array. The decryption algorithm is as follows.

Algorithm

```
Algorithm(Img)
/*Img is the encrypted image taken as input for the decryption process*/
{
    1.  For i=1 to Size(Image)
        {
    2.  Px=GetPixel(Image(i))
        [Read the pixel from Image]
    3.  Divide the Pixel in N sub blocks called Px1,Px2….PxN
    4.  Process Each Pixel Sub-Block under binary value analysis
    5.  If (Px>Threshold)
        {
    6.  Set Px=Black
        }
        Else
        {
    7.  Set Px=White
        }
    8.  If (Count(black)>Count(White))
        {
    9.  Generate the subimage to black
        }
        Else
        {
    10. Generate the subimage to White
        }
    11. Reconstruct the Result Pixel Image
    12. Return Image
        }
```

The number of shares the image would be divided (n) and number of shares to reconstruct the image (k) is also taken as input from user. The encryption, i.e. division of
the image into n number of shares such that k numbers of shares are sufficient to reconstruct the image; is done by the following.

## IV. Conclusions

In this paper we have proposed a technique of well known k-n secret sharing but on images. At the time of dividing an image into n number of shares we have used random number generator, which is a new technique not available till date. This technique needs very less mathematical calculation compare with other existing techniques of visual cryptography on color images. This technique only checks '1' at the bit position and divide that '1' into (n-k+1) shares using random numbers. In most of our experimental results, each share reflects very little or even no information regarding the original image to human eye

## References

[1] AlfreJo De Santk , "On Visual Cryptography Schemes", ITW Killarney, Ireland, 1998.

[2] Chin-Chen Chang, Chwei-Shyong Tsai, Tung-Shou Chen, "A New Scheme for Sharing Secret Color Images in Computer Network", Taiwan, 2000.

[3] Chin-Chen Chang et.al , " Sharing a Secret Gray Image in Multiple Images"2002.

[4] Stelvio Cimato ,Roberto De Prisco, Alfred0 De Santis, " Contrast Optimal Colored Visual Cryptography Schemes, ITW 2003, Paris, France, March 31 -April 4, 2003.

[5] Zhi Zhori and Gonzalo et.al, "Halftone Visual Cryptography" New Jersey, 2003.

[6] Wei-Qi Yan, Duo Jin, " Visual Cryptography For Print And Scan Applications", 2004.

[7] Chih-Ming Hu, Wen-Guey Tzeng, "Cheating Prevention in Visual Cryptography", Ieee Transactions On Image Processing, Vol. 16, No. 1, January, 2007.

[8] Zhi Zhou, et.al, "Halftone Visual Cryptography scheme", 2006.

[9] Geum-Dal Park, Eun-Jun Yoon , Kee-Young Yoo "A New Copyright Protection Scheme with Visual Cryptography", 2008 Second International Conference on Future Generation Communication and Networking Symposia, 2008.

[10] Debasish Jena, Sanjay Kumar Jena, "A Novel Visual Cryptography Scheme", International Conference on Advanced Computer Control, 2008.

[11] Hsien-Chu Wu, Hao-Cheng Wang, and Rui-Wen Yu, "Color Visual Cryptography Scheme Using Meaningful Shares", Eighth International Conference on Intelligent Systems Design and Applications, 2008.

[12] Hao Luo, Faxin Yu, "Data Hiding in Image Size Invariant Visual Cryptography", The 3rd International Conference on Innovative Computing Information and Control (ICICIC'08), 2008.