Design and Implementation of K-Split Segmentation Approach for Visual Cryptography

Puja Devi Rana*, Anita Singhrova, Suman Deswal*****

*Department of Computer Science, Deenbandhu Chhotu Ram University of Science and Technology, India
**Department of Computer Science, Deenbandhu Chhotu Ram University of Science and Technology, India
***Department of Computer Science, Deenbandhu Chhotu Ram University of Science and Technology, India

Abstract: Visual Cryptography is a special type of encryption technique which is used to hide the information and data in images. In this technique the decryption process is done without any complex cryptographic computation. The encrypted data is decrypted using Human Visual System (HVS). This is the benefit of the visual secret sharing scheme. The encryption technique requires a cryptographic computation to divide the image into a number of parts or we can call it shares. We divide the image into n number of shares. In this paper we have proposed a new k-n secret sharing visual cryptographic scheme for black and white images in which encryption of the image is done by using Random Number generator. This k-n secret sharing scheme uses at least a group of k shares out of n shares to reveal the secret information and less of it will not reveal any information.

Index Terms: Encryption, Decryption, Visual Cryptography, Image Processing.

I. Introduction

Any web based computer system is susceptible to attacks from system hackers who could attempt to control and intrude a computer 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 like false base station attack, middle man attack, intrusion etc. To counter these attacks there are different authentication and encryption techniques like authentication and encryption techniques.

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 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.

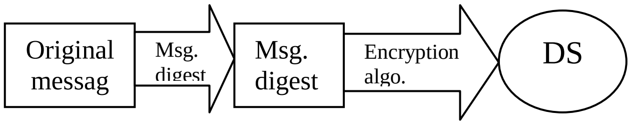
Password guessing requires the hacker to have known usernames and suitable password guesses, by persistently trying the guessed passwords into the system, the attacker could finally break in, and this is mainly due to poor passwords being chosen by users. The best way to protect a system from this form 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. 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. 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.

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.

Process at sender's end:



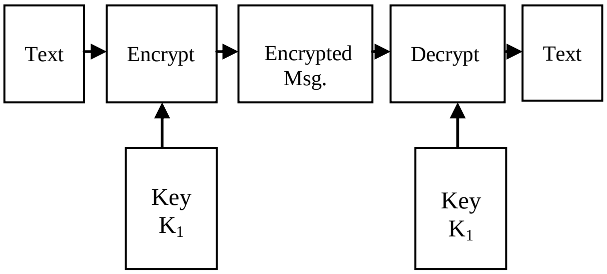
Encrypted Communication

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, there by 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.

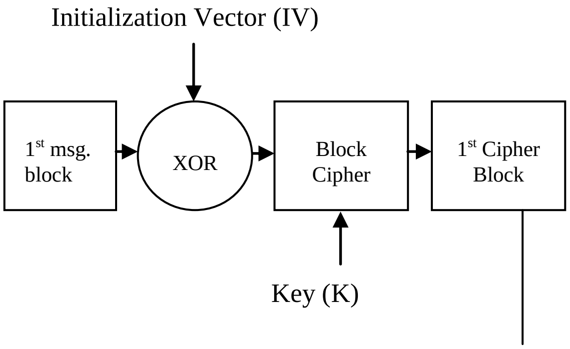
Symmetric Key Cryptography

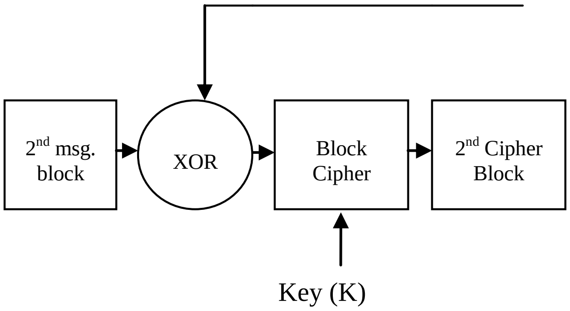
This form of encryption is also known as the secret key cryptography. Symmetric key cryptography makes use of the same private key while performing an encrypted communication between two users. The same secret key is used for the encryption and decryption of data being transmitted between the two or 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.



Block Ciphers

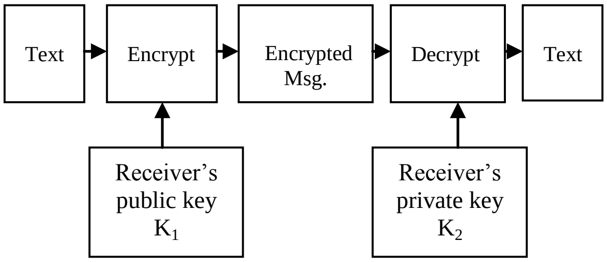
A block cipher is an encryption method which encrypts large blocks of text; the block cipher regards the input stream for encryption as blocks of fixed sized bytes which can be up to 128 bits long. The block cipher can encrypt a 128 bit plaintext and generate a 128 bit cipher text as the output result. 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.





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.



II. LITERATURE SURVEY

Alfre Jo De Santk et.al [1] proposed visual cryptography schemes in which two pixels combine in various arbitrary ways and then analyze the pixel expansion. In this scheme each share has some information of the secret image but only the required n number of shares will reconstruct the image. The combination of shares can be done by using any Boolean function like "OR" "XOR" etc. Chin-Chen Chang et.al [2] has proposed an effective and generalized scheme of hiding a color image. This scheme uses a color index table to hide and recover the image. In recovering a secret image, very small memory space and simple computations are required. Chin-Chen Chang et.al [3] has proposed colored visual cryptography schemes based on modified visual cryptography. This uses very few additional computations to hide a colored secret image into some shares. Size of the shares and the implementation complexity in this scheme depends on the number of colors appearing in the secret image. More efficient way is to hide a gray image (256-colors) in different shares. The size of the shares is fixed and does not vary with the number of colors appearing in the secret image. The newly proposed scheme has the advantage of low computation and it also avoids the drawbacks of the previous approach, it is very much suitable for today's requirement of low power. Stelvio Cimato et.al [4] has proposed another visual cryptography scheme that allows 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 contains pixels from a given set of c colors. This paper shows the c-color (k, n)-threshold visual cryptography schemes. Zhi Zhori and Gonzalo et.al [5] has proposed a scheme in which the secret image, SI is encoded into n shares of random patterns. This scheme decodes the secret image by superimposing the required number of shares onto transparencies, but no secret information can be obtained from the superposition of a forbidden subset. This scheme is mathematically secure. Wei-Qi Yan, Duo Jin [6] proposed the applications of Visual Cryptography on print and scan images**.** There are many difficulties in printing or scanning the secret image shares. The main reason for this is the difficulty of use in practice. The shares are printed onto transparencies and then needs to superimpose them. But it is not very easy to do precise superposition due to the fine resolution and the printing noise. There must be some criteria to find the alignment of all the shares in order to avoid any difficulty in superimposition. This paper uses Walsh transform to embed marks in all the shares to find the alignment position of these shares. Experimental results shows that it is very useful in print and scan applications. Chih-Ming Hu and Wen-Guey Tzeng [7] proposed the method of detection the cheating prevention in visual cryptography**.** In this paper various cheating problems in the area of visual cryptography are discussed. This paper presented three cheating methods and applied them on extended VC schemes and improved one cheat-preventing scheme. This paper proposed a generic method that converts one VCS to another VCS that has the property of cheating prevention. The overhead of the conversion is near optimal in both the cases contrast digression and pixel expansion. It only added two sub pixels for each pixel in the secret image and the contrast is reduced only slightly. Zhi Zhou, et.al [8] has proposed Halftone Visual Cryptography scheme. Visual cryptography encrypts the secret image into random shares of binary patterns. The shares are xeroxed onto transparencies and the secret image can be revealed by superimposing the qualified sets of transparencies. But no information can be revealed by superimposing any forbidden sets of transparencies. The binary patterns of the shares do not have any visual meaning and hinders the objective of visual cryptography. To avoid any further problem due to binary pattern of the shares, extended visual cryptography was proposed. In this paper, a technique named halftone visual cryptography is proposed to achieve visual cryptography via half toning. It is based on the blue-noise dithering principles. It utilizes the void and cluster algorithm to encode a secret binary image into halftone shares. The result shows that the visual quality of the obtained halftone shares was better than that attained by any available visual cryptography method known to date. This new scheme can be broadly used in a number of visual secret sharing applications where high-quality visual images are required, 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. The proposed scheme uses a simple codebook for generating a watermark image. It does not need to expand the watermark image. Experimental results shows that the proposed method can verify the ownership of the copyright and is also robust to resistant the variety of attacks. Debasish Jena1 et.al [10] has proposed a method of Data hiding in halftone images using conjugate ordered dithering (DHCOD) algorithm. This algorithm is a modified version of Data hiding in halftone images using conjugate error Diffusion technique (DHCED). This scheme generates the shares using basic visual cryptography model and then embed these shares into a cover image using a DHCOD technique, so that the shares will be more secure and meaningful.

III PROPOSED WORK

Visual cryptography is a cryptographic technique which uses visual information like Image, text, etc. and encrypts them in such a way so that the decryption can be done by combination of the image shares. As we all know image is a multimedia component which is sensed by human and its smallest element is pixel. For example if we take an image of 32 bit then each pixel of the image contains 32 bits, which is divided mainly into four parts, namely Alpha, Red, Green and Blue; each containing 8 bits. The Alpha part represents the degree of transparency. The image is fully transparent if all bits of Alpha part are ‘0’.

In this paper we have proposed an algorithm which divides the digital image into n number of shares out of which minimum k number of shares can reconstruct the image. If we take k numbers of shares to reconstruct the image then (n-k) shares are left. If in the image certain position of a pixel is 1, then in (n−k) +1 number of shares there will be a 1 in that position of the pixel. In the remaining shares there will be a 0 in that position of the pixel. The (n−k) +1 number of shares can be identified by using a random number generator.

In the case of visual cryptography, decryption is done by human visual system in which a minimum number of shares are used to reconstruct the original image. For computer generated programs decryption can be done by using OR function. The human visual system acts as an OR function.

Input to the computer is the number of shares the image would be divided (n) and number of shares to reconstruct the image (k). All the shares are of equal height and width as the source image because they all are created from the same image. Then the bitwise OR operation is performed on the shares and the final value is stored in an array.

First of all the encryption of the original image is done using the proposed algorithm. The image is divided into various number of shares say N. out of these N number of shares a group of some shares can reveal the image say K. These K numbers of shares are sufficient to reconstruct the image.

The algorithm which is used to divide the image into N shares is as follows:

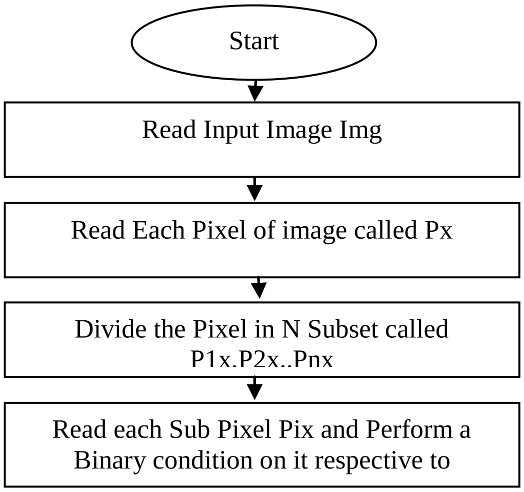
Encryption Algorithm

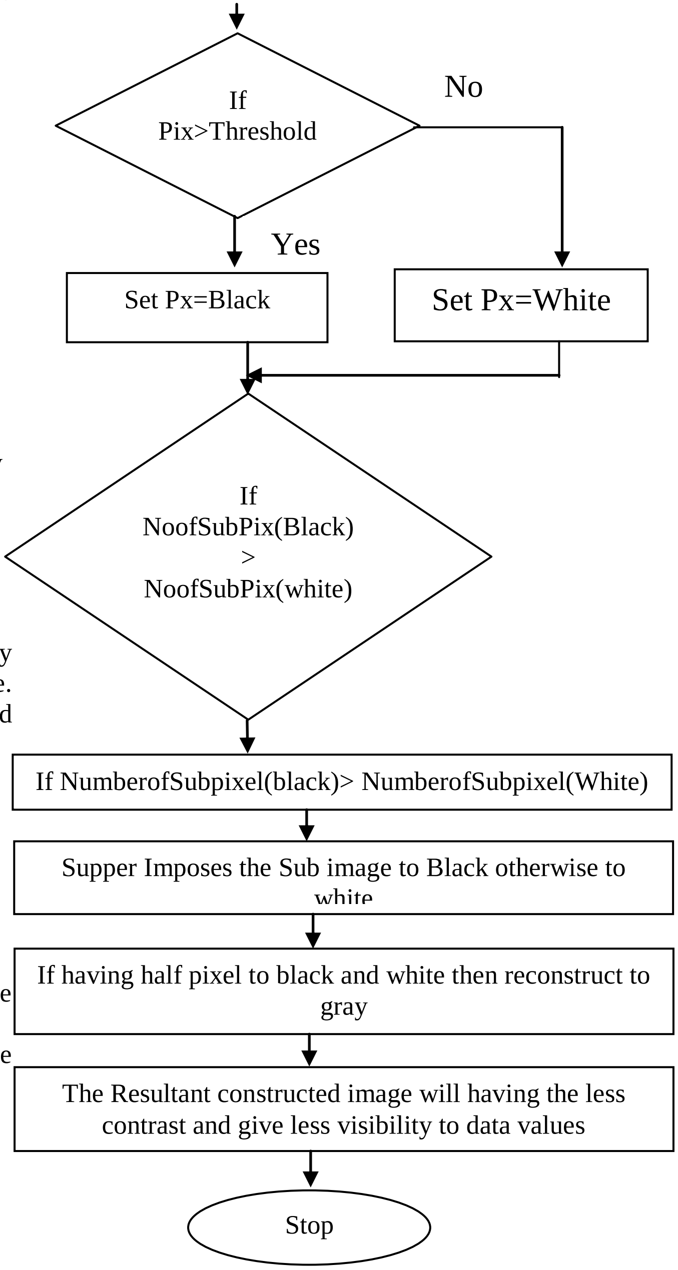
- Divide the pixels of the image into N number of sub pixels or we can say divide the data sets into N sub data sets.
- Now the original data set can be constructed from any K data sets out of N data sets.
- The K-1 data sets can represent the information of the original data set.
- Write K data sets out of N data sets.
- A pixel P is split into two sub pixels in each of the two shares.
- If P is white, then a coin is tossed. Then the pixel P is encrypted as two sub pixels in each of the two shares. Every pixel is encrypted using a new coin toss.
- If pixel P is black, then we get both sub pixels black when we superimpose the two shares;
- If P is white, then we get one sub pixel black and one sub pixel white when we superimpose the two shares.
- Thus, we can say that the reconstructed pixel has a grey level of 1 if P is black and a grey level of 1/2 if P is white. There will be a loss of 50% contrast in the reconstructed image, but it will be still visible.

The decryption algorithm decrypts the shares into the original image. The decryption algorithm is as follows:

Decryption Algorithm

1. Read the Encrypted Image called Img
2. read the image Pixel by pixel called Px(i,j) is the current pixel
3. Decompose the pixels in n sub block relative to the Encryption algorithm.
4. Perform the Decoding on each sub block
5. Marge the sub blocks Extract 8 valid bits
6. Reform the image from these pixels
7. Return the result image.


Start
Read Input Image Img
Read Each Pixel of image called Px
Divide the Pixel in N Subset called P1x.P2x..Pnx
Read each Sub Pixel Pix and Perform a Binary condition on it respective to


If Pix>Threshold
No
Yes
Set Px=Black
Set Px=White
If NoofSubPix(Black) > NoofSubPix(white)
If NumberofSubpixel(black)> NumberofSubpixel(White)
Supper Imposes the Sub image to Black otherwise to white
If having half pixel to black and white then reconstruct to gray
The Resultant constructed image will having the less contrast and give less visibility to data values
Stop

Flow Chart of Encryption Algorithm

IV CONCLUSION

In this paper we have proposed a technique of well-known k-n secret sharing on grey scale images. We use a new technique called random number generator to divide the secret image into N number of shares. This technique uses very less mathematical computation in comparison with any other visual cryptography techniques. The proposed technique checks '1' at the bit position of the pixel and divide the '1' into (n-k) +1 shares using random numbers. In most of our experimental results, each share reflects very little or even no information of the secret image which is not easily visible by human eye.

REFERENCES

[1] AlfreJo De Santk, “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.