1. **problem definition**

Visual secret sharing is the technique that divide the secret image into n multiple shares. Each share constitute some information and when k shares out of n stack together the secret will reveal. The beauty of the visual secret sharing scheme is its decryption process i.e., to decrypt the secret using Human Visual System without any computation. Halftone visual cryptography is one method that achieves visual cryptography via halftoning. This method uses void and cluster to encrypt a secret binary image into n halftone shares each carrying significant visual information.

**Problem:**

An image of size mxn pixels is given. Each pixel is represented by an 8-bit data. Design Halftone Visual Cryptography model that encodes given image into a two tone binary image.

**Example:**



1. **sOLUTION**

**2.1 EXISTING METHODOLOGIES**

Naor and Shamir proposed a new cryptography area, visual cryptography, in 1994.Visual Cryptography is a secret-sharing method that encrypts a secret image into several shares but requires neither computer nor calculations to decrypt the secret image. Instead, the secret image is reconstructed visually: simply by overlaying the encrypted shares the secret image becomes clearly visible. It helped us in overcoming the disadvantage of complex computation required in the traditional cryptography

**2.1.1 Basic Model\_ (k, n) secret sharing scheme**

The basic model of visual cryptography proposed by Naor and Shamir accepts binary image ‘I’ as secret image, which is divided into ‘n’ number of shares. Each pixel of image ‘I’ is represented by ‘m’ sub pixels in each of the ‘n’ shared images. The resulting structure of each shared image is described by Boolean matrix ‘S’ Where S= [Sij] an [n x m] matrix Sij=1 if the jth sub pixel in the ith share is Black Sij=0 if the jth sub pixel in the ith share is White When the shares are stacked together secret image can be seen but the size is increased by ‘m’ times. The grey level of each pixel in the reconstructed image is proportional to the hamming weight H (V) of the OR – ed Vector ‘V’, where vector ‘V’ is the stacked sub pixels for each original pixel. A solution of the ‘n’ out of ‘n’ visual secret sharing consists of two collections of n x m Boolean Matrices C0 and C1 .To share a white pixel, randomly choose one of the matrices from C0, and to share a black pixel, randomly choose one of the matrices from C1.The following conditions are considered for the construction of the matrices: 1. For any ‘S’ in C0, the OR-ed ‘V’ of ‘n’ rows satisfies H(V) \_n-\_m. 2. For any ‘S’ in C1, the OR-ed ‘V’ of any ‘n’ rows satisfies H (V) \_n.

By stacking fewer than ‘n’ shares, even an Infinitely powerful cryptanalyst cannot gain any advantage in deciding whether the shared pixel was white or black. Let us describe the construction of matrix for (n, n) visual cryptography for n=3. C0= {all the matrices obtained by permuting the columns complement of [BI]} C1= {all the matrices obtained by permuting the columns of [BI]} Where, B is the matrix of order n x (n-2) which contains only ones I is the identity matrix of order n x n





The basic model was then extended to (k, n) threshold cryptography where any ‘k’ or more shares will reveal the secret image. The construction of ‘k’ out of ‘n’ visual secret sharing is similar to the basic model with one difference. That is in basic model the threshold value is n where

**2.1.2 Visual cryptography for general access structures**

In (k,n) Basic model any ‘k’ shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson [2], where an access structure is a specification of all qualified and forbidden subsets of ‘n’ shares . Any subset of ‘k’ or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of k out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion than Basic Model

**2.1.3 Visual cryptography for gray level images**

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

**2.1.4** **Recursive Threshold visual cryptography**

The (k,n) visual cryptography needs ‘k’ shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and Subhash Kak eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

**2.1.5** **Extended visual cryptography for natural images**

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI proposed Extended visual cryptography for natural images constructs meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, establishes the extended visual cryptography scheme suitable for natural images.

**2.2 PROPOSED APPROACH**

Assume the pixel is located at the ith row and jth column. These are the values associated with that pixel

• PV(i,j) : pixel value 8-bit input

• CPV(i,j): Corrected pixel value 8-bit intermediate value

• e(i,j): error of the pixel 8-bit intermediate value

• E\_av(i,j): Average error 8-bit intermediate value

• HTPV(i,j): Halftone pixel value 1-bit output

Calculation of Average Error:

Equation for calculating average error

w1\*e(i-1,j) + w2\*e(i-1,j-1) + w3\*e(I,j-1) + w4\*e(i+1,j-1)

E\_avg = -------------------------------------------------------------------------------------------

w1+w2+w3+w4

****

**Floyd-Steinberg Algorithm:**

For each pixel

CPV = PV(I , j) + E\_avg;

If CPV < CPV\_thresh

HTPV(I , j) = 0;

e(I , j) = CPV;

else

HTPV(I , j) = 1;

e(I , j) = CPV - CPV\_max;

CPV\_thresh = 128 & CPV\_max = 255

Procedure for obtaining halftone pixel value matrix is described in the pseudo code section.

1. **SOLUTION ANALYSIS (PROS AND CONS)**

**3.1 Pros**

1. Decryption Algorithm is not required. So a person unknown to cryptography can easily decrypt the message.
2. We can send cipher text through FAX or email
3. Lower computational cost, since secret message is recognized only by human eyes and not a cryptosystem
4. Halftone Cryptography retains all advantages of traditional visual cryptography techniques.. Cheating is possible to some extent in Traditional visual cryptography. Cheater generates fake shares and a fake image appears on the stacking of genuine shares and fake shares. In halftone cryptography, Stacking involves only XORing. Therefore, honest participants who present their shares for recovering the secret image will be able to distinguish fake shares from genuine shares. Hence cheating is solved to some extent in Halftone Cryptography.
5. Easy Implementation
6. Halftone Cryptography is used with short messages. Therefore it can be used to strengthen other cryptographic techniques (ex: Encrypting public keys)
   1. **cons**
7. The background image in the decoded image can be eliminated and the hidden binary visual pattern can be revealed precisely.
8. The contrast of reconstructed image is not properly maintained
9. Perfect alignment of transparencies is nearly impossible

**4. IMPLEMENTATION**

* 1. **S/W AND HARDWARE REQUIREMENTS**

**4.1.1** **Software Requirements**

The algorithm is as follows.

The whole image is considered as a matrix with each entry the corresponding pixel value. Each entry of the matrix is associated with

• PV(i,j) : pixel value 8-bit input

• CPV(i,j): Corrected pixel value 8-bit intermediate value

• e(i,j): error of the pixel 8-bit intermediate value

• E\_av(i,j): Average error 8-bit intermediate value

• HTPV(i,j): Halftone pixel value 1-bit output

The input to the Floyd-Steinberg Algorithm is the pixel value and the output will be the halftone pixel value.

This can be implemented easily in programming languages like c, c++, java etc..

**4.2.2 Hardware Requirements**

The hardware implementation requires four processing units, a memory and a set of registers

**4.2** **PSEUDO CODE**

for(k=1;k<N;k++) {Err[k][0]=0;}

for(k=0;k<=M;k++) {Err[0][k]=0;Err[N+1][0]=0;} //boundary initialization for(j=1;j<M;j++)

{

for(i=1;i<N;i++)

{

E\_av = (7\*Err[i-1][j]+1\*Err[i-1][j-1]+5\*Err[i][j-1]+3\*Err[i+1][j-1])/16;

CPV = PV[i][j]+E\_av;

CPV\_round = (if CPV<T then 0 else 255); //T is thresh=128;

HTPV[i][j] = if(CPV\_round==0 then 0 else 1);

Err[i][j] = CPV-CPV\_round;

}

}

**5. APPLICATIon areas**

**5.1**  Maintaining Biometric Privacy

BIOMETRICS is the science of establishing the identity of an individual based on physical or behavioral traits such as face, ﬁnger prints, iris, gait, and voice. Halftone visual cryptography can be used for imparting privacy to biometric data such as ﬁngerprint images, iris codes, and face images

* 1. Digital Watermarking

A binary logo is used to represent the ownership of the host image. The logo is used to generate a private sharing image and a public sharing image by visual cryptography algorithms. We use the public sharing image as the watermark embedded in the host image. An error correction-coding scheme is also used to protect the watermark

**5.3** Visual Steganography

 Visual steganography is one of the most secure forms of steganography available today. It is most commonly implemented in image files. However embedding data into image changes its color frequencies in a predictable way. The data will be encrypted into a cipher and the cipher will be hidden into a multimedia image file in encrypted format. It combines the features of cryptography, steganography along with multimedia data hiding.

**5.4** Bank Customer Identification (E-banking)

Bank sends customer a set of keys in advance. Bank Website

displays cipher, Customer applies overlay and reads transaction

keys and then he/she enters the transaction key and access

his/her account.

**5.5**  Electronic Balloting System

Nowadays, most of the voting are managed with computer systems. These voting machines expected voters to trust them, without giving proof that they recorded each vote correctly. One way to solve this problem is to issue receipts to voters to ensure them their votes are counted. However, this could improperly influence the voters, which produces coercion or vote selling problems .To solve this dilemma, Visual cryptographic technique can be used. Voting machine generates an encrypted receipt to every voter which allows her to verify the election outcome - even if all election computers and records were compromised. At the polling station, you will receive a double-layer receipt that prints your voting decision. You will be asked to give one of the layer to the poll worker who will destroy it immediately with a paper shredder. The remaining one layer will now become unreadable. To make sure that your vote is not altered or deleted, you could querying the serial number on your receipt on the election Web site. This will return a posted receipt that looks identical to yours in hand. First of all, a receipt that is not properly posted can act as a physical evidence of the failure of the election system. Secondly, voters are ensured that their vote is correctly recorded at the polling station, but after surrendering a layer of the receipt, no one can decode it unless he somehow know the decryption algorithm and obtained all secret keys, which are typically held by different trustee. Thirdly, even if all election computers were compromised, there are only limited ways that the system could alter the voting. For example, the system could print a wrong layer and hope that the voter will choose another one. However, the chances that it would go undetected is 1/2 for one vote, and hence (1/2)^10 for 10 ballots, which is considered negligible for a voting population of, say 30,000 people

**6. FUTURE ENHANCEMENT**

* 1. **Extend the method with colour images.**

There have been many published studies of visual cryptography. Most of them, however, have concentrated on discussing black-and-white images, and just few of them have proposed methods for processing gray-level and color images. In the approach of a visual cryptography for color images each pixel of the color secret image is expanded into a 2×2 block to form two sharing images. Each 2×2 block on the sharing image is filled with red, green, blue and white (transparent),respectively, and hence no clue about the secret image can be identified from any one of these two shares alone. Because human eyes cannot detect the color of a very tiny subpixel, the four-pixel colors will be treated as an average color.When stacking the corresponding blocks of the two shares, there would be 242 variations of the resultant color for forming a color image.

* 1. **Extend the method with 3D images.**
  2. **Extend the method for natural images.**

Previous works on the extended visual cryptography deal with binary images such as text images, but natural images such as photographs are difficult to handle in such scheme. There is a straightforward way to extend this scheme to colour images. Generally in printing, colour images can be separated into channels of three primary colours, i.e., cyan, magenta and yellow, and each channel can be treated as an independent grayscale image. In a very naive approach, the system applies the encryption to each channel and merges the result to get the coloured output. Under the ideal subtractive colour mixing model, stacking the two coloured sheets reveals the coloured target1. In reality, however, such ideal subtractive colour mixture is unlikely due to the properties of ink, transparencies, etc. With extended visual cryptography for natural images, we can improve the problem to get the desired output.

* Improving the contrast and reduce the pixel expansion in the resultant secret image
* Improving the pixel shape from dots to a continuous tone
* Overcoming the security issues

For further improvement we can use three stage pre-processing cycle and divide the phase I (used for producing the share 1) into three stages and process the image.

**7. CONCLUSion**

Undoubtedly, Visual Cryptography provides one of the secure ways to transfer images on the Internet. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required.  With the halftone technology, we can transform a gray-level image into a binary one suitable for generating visual cryptography. As the traditional schemes for black-and-white visual cryptography, our methods expand every pixel of a color secret image into a 2×2 block in the sharing images and keep two color and two transparent pixels in the block. As mentioned earlier Visual Cryptography has got so many interesting applications in private and public sectors of our society since decoding a visually encoded image or message is much simpler as compared to other cryptographic techniques. So deep study on this method will undoubtedly add one more powerful tool to the pool of cryptographic techniques which can ensure the security goals of cryptography like Integrity, Confidentiality and Availability of data.

**8. REFERENCES**

1. An overview of visual cryptography by Chandramathi .S , Ramesh Kumar .R , Suresh .R , Hareesh .S
2. Visual cryptography by Naor .M and Shamir .A
3. Halftone visual Cryptography by Zhi Zhou, Gonzalo .R Arce and Giovanni Di Crescenzo
4. Visual Cryptography An introduction visual srcret sharing scheme by C.N Yang