# Diverse Visual Cryptography Schemes: A Glimpse

Sruthy K Joseph
Computer Science and Engineering
Adi Shankara Institute of Engineering & Technology
Kalady, India

Ramesh R
Computer Science and Engineering
Adi Shankara Institute of Engineering & Technology
Kalady, India

*Abstract*— **Visual cryptography scheme is a cryptographic process which allows visual information (e.g. images, printed text, and handwritten notes) to be encrypted in such a way that the decryption can be performed by the human visual system, without the help of computers. There are diverse visual cryptography schemes developed based on different factors like pixel expansion, meaningless or meaningful shares, contrast, security, type of secret image and the number of secret images encrypted. This paper discusses most of the visual cryptography schemes and the performance measures used to evaluate them.**

***Keywords — Visual cryptography, Meaningful share, random grid, pixel expansion, extended visual cryptography, progressive visual cryptography.***

## I. INTRODUCTION

To ensure fundamental data security requirements such as confidentiality, integrity, availability during data transmission over the Internet, conventional cryptography schemes were used in previous decades. It uses a secret key and complex mathematical computation to convert plain text into meaningless (cipher) text. Major disadvantage of cryptography is that a computer is required for the both process of encryption and decryption, resulting in wastage of computational resources and CPU execution time. Cryptography can be used only for the secure transmission of textual data but it cannot be used when the data to be secured is an image (picture or handwritten documents). For this a new visual secret sharing (VSS) scheme called visual cryptography (VC) was developed to protect sensitive images from rapacious behavior. It is initially proposed by Naor and Shamir [1] in 1994.

Visual cryptography is a powerful visual secret sharing scheme in which a secret image is distributed among some (say *n*) participants by dividing the secret image into two or more noise-like shares (or shadow images). When the shares on transparencies are stacked (superimposed) together, the original secret image will be revealed without any mechanical devices like a computer. Decryption can be done using the Human Visual System (HVS).

In the (*k*,*n*) threshold VSS scheme, a secret image is shared by generating *n* noise-like share images. Superimposing any *k (where* $k \leq n$*)* or more share images together, the secret image will get revealed using human visual system. On the other hand, if *k* - 1 participants attempt to reconstruct the secret, they will fail and the secret will never be revealed.VC is a simple mechanism for decrypting/ decoding the secret image with perfect security when computer resources are not available.

This paper provides an overview of various visual cryptography schemes. However, most of the available VC schemes use a pixel expansion method to decompose the secret image and so the generated share images become larger than the original secret image. The major drawbacks caused due to this enlargement are: it leads to the wastage of storage space, network bandwidth (unnecessary wastage of network resources while transmitting the share images) and distorts the image quality.

## II. LITERATURE SURVEY

The process of visual cryptography proposed by Naor and Shamir [1] discusses a technique for encrypting a binary secret image into *n* shares (printed on transparencies), where each pixel is expanded *m* times. Each participant will get a share image but the secret image cannot be revealed with any one share. Any n participants can compute the original secret when any *k* (or more) of them are stacked together. No group of *k-1* (or fewer) participants can compute the original secret.

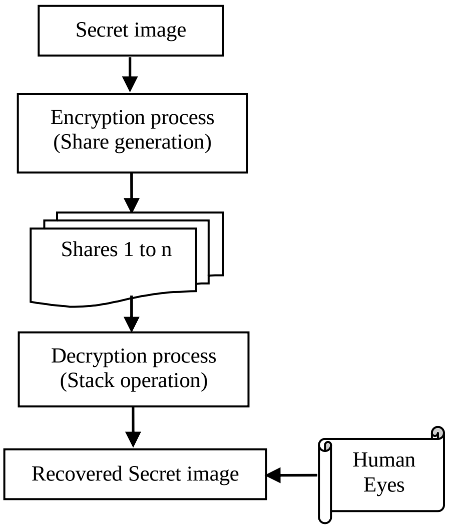


Fig 1: Basic flowchart of Visual Cryptography

The secret image cannot be seen from one transparency, but when *k* or more transparencies are stacked together the image will begin to emerge as the contrast between the black and white pixels becomes sufficient that the human eye will be able to recognize the secret image. Neither computational devices nor cryptographic knowledge are required for the decryption process. This approach is called *(k, n)*-threshold Visual Secret Sharing (VSS).

Initially the binary secret image is encoded (i.e. shares are generated) and during decoding the k or n shares are stacked together (according to the *(k, n)* or *(n, n)* scheme discussed later) to reveal the secret image. The secret image will get visible to the human visual system.

In the *(k, n)* visual cryptography scheme, two collections of *(n* x *m)* Boolean matrices (Basis matrices), C0 and $C_1$ are used. To share a white (black) pixel, the dealer randomly selects one row of the Boolean matrix $C_0$ ($C_1$) and assigns it to the corresponding share image. The gray level and contrast of the m sub-pixels in each of the n share images is defined by the chosen row (of the Boolean matrix).

$$C_0 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 1 & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 0 \end{bmatrix} \qquad C_1 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 1 \end{bmatrix}$$

The major drawbacks of visual cryptography include pixel expansion, loss of contrast, and share management difficulty (due to random or noise-like share images).

*Important parameters of the scheme are:*

- ***m*:** Pixel expansion (m) refers to the number of sub-pixels in the construcetd shares that represents a pixel of the original secret image. It signifies the loss in resolution from the original secret image to the shared one.
- **α:** Contrast (α) is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image.
- **γ:** the size of the collection of $C_0$ and $C_1$. $C_0$ refers to the sub-pixel patterns in the shares for a white pixel and $C_1$ refers to the sub-pixel patterns in the shares for a black pixel.

*Two basic VSS schemes:*

- *(n, n)* Visual Secret Sharing Scheme
  (n, n) Visual Secret Sharing Scheme is where the secret is divided into a total of *n* shares and all the *n* shares are overlapped to get visually read the secret message.
- *(k, n)* Visual Secret Sharing Scheme
  (k, n) Visual Secret Sharing Scheme is where the secret is divided into *n* shares and any *k* or more of these shares when overlapped reveals the secret.

*General Access Structures (GAS)*

In *(k, n)* scheme, using any of the 'k' shares someone can decode the secret image which in turn reduces security . 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.

*(2, 2) Visual Cryptography Scheme (VCS)*

The secret image is divided into two (*n*) share images so that the secret can be revealed only if both the shares are stacked together. The Boolean matrices to be dispatched can be designed as follows:

| Secret pixel | Share 1 | Share 2 | Stacked pixel (OR operation) |
|---|---|---|---|
| ■ | ■□<br>□■ | □■<br>■□ | ■■<br>■■ |
| □ | ■□<br>□■ | ■□<br>□■ | ■□<br>□■ |

$$S_0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \qquad S_1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

To encode the white secret pixel , one row from $S_0$ is selected and dispatched towards each share. The values 1 and 0 indicates the black and white pixels respectively. Two pixels from the first row is distributed to the first share and the remaining two pixels in the second row to the second share.

## III. DIVERSE VISUAL CRYPTOGRAPHY SCHEMES

Visual cryptography is paradigm of cryptography which allows visual information (e.g. images, printed text and handwritten notes) to be encrypted in such a way that its decryption can be done by the human eye, without the aid of computers. It avoids the need of complex mathematical computations during decryption and the secret image can be reconstructed using stacking (OR operation). There are diverse visual cryptography schemes based on the factors such as pixel expansion, contrast, security, meaningless or meaningful shares, type of secret image (either binary or color) and the number of secret images encrypted (single or multiple secret) etc. This paper discusses various schemes of visual cryptography and provides a brief overview.

The following are the diverse visual cryptography schemes:

1. Traditional Visual Cryptography
2. Extended Visual Cryptography
3. Halftone Visual Cryptography
4. Recursive Threshold Visual Cryptography Scheme
5. Random Grids based Visual Cryptography
6. Colour Visual Cryptography Schemes
7. Probabilistic Visual Cryptography
8. Region Incrementing Visual Cryptography
9. Progressive Visual Cryptography
10. Segment based Visual Cryptography Scheme
11. Cheating Immune Visual Cryptography Schemes
12. Size Invariant Visual Cryptography
13. User-friendly Visual Secret sharing scheme
14. Dynamic Visual Cryptography
15. OR and XOR Visual Cryptography

*Traditional Visual Cryptography*

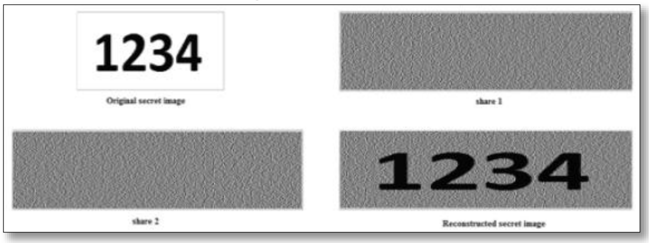
A secret is something which is kept from the knowledge of any but the initiated or privileged. Secret sharing defines a method by which a secret is distributed among a group of participants, whereby each participant is allocated a piece of the secret. This piece of the secret is known as a *share*. The secret can only be reconstructed when a sufficient number of shares are combined together. While these shares are separate, no information about the secret can be accessed. That is, the shares are completely useless while they are separated.

Within a secret sharing scheme, the secret is divided into a number of shares and distributed among n persons. When any *k* or more of these persons (where k ≤ n) bring their shares together, the secret can be recovered. However, if *k - 1* persons attempt to reconstruct the secret, they will fail. Due to this threshold scheme, we typically refer to such a secret sharing system as a *(k, n)*-threshold scheme or k-out-of-n secret sharing, where n is the number of Total Participant and k is the number of Qualified Participant The basic model for visual sharing of the k out of n secret image is such that;

- Any *n* participants can compute the original message if any *k* (or more) of them are stacked together.
- No group of *k-1* (or fewer) participants cannot compute the original message.

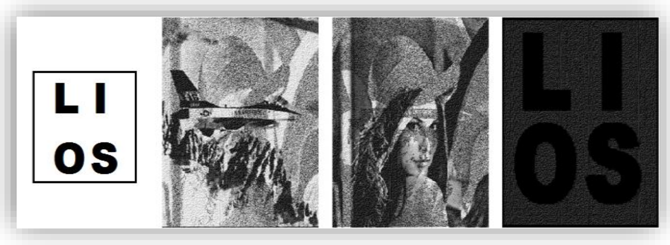
$$C_0 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 1 & 0 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 0 \end{bmatrix} \quad C_1 = \begin{bmatrix} 1 & 0 & 0 & . & . & 0 \\ 0 & 1 & 0 & . & . & 0 \\ . & . & . & . & . & . \\ 1 & 0 & 0 & . & . & 1 \end{bmatrix}$$

*A (k, n)* VSS scheme is a method by which the shared image (printed text, handwritten notes, pictures, etc.) is visible by k or more participants by stacking their transparencies with the help of an overhead projector. To share a white pixel, the dealer randomly chooses one of the matrices in $C_0$ and to share a black pixel, the dealer randomly chooses one of the matrices in $C_1$. The chosen matrix defines the colour of the *m* sub-pixels in each one of the *n* transparencies. The major drawback is the pixel expansion and low contrast of the reconstructed secret image.



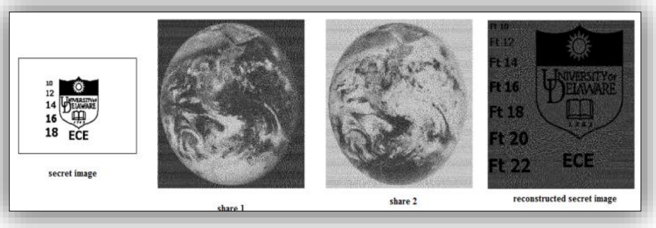
### Extended Visual Cryptography

Extended Visual Cryptography (EVC) takes the idea of visual cryptography further by creating shares which are meaningful to anyone who views them. This helps to alleviate suspicion that any encryption has taken place and also presents visually pleasing shares which incorporate all the previously mentioned features of VC. It allows the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. Meaningful shares avoid attention of hacker considering the security issues over the communication channels. EVCS can also be viewed as a method of steganography. One scenario of the applications of EVCS is to evade the custom inspections, because the shares of EVCS are meaningful images, hence there are fewer chances for the shares to be suspected and detected. In case of EVCS, shares were simply generated by replacing the white and black sub-pixels in a traditional VCS share with transparent pixels and pixels from the cover images, respectively. This scheme provides meaningful share images but endure pixel expansion problem.



### Halftone Visual Cryptography

The halftoning technique can be applied to both colour and gray-scale images. Halftoning simulates a continuous tone through the use of dots, varying either in size or in spacing. In general halftone visual cryptography framework, a secret binary image is encrypted into high-quality halftone images or halftone shares. It applies the rich theory of blue noise halftoning to the construction mechanism used in traditional VC to produce halftone shares, while the security properties are still maintained. The same contrast is obtained over the whole decoded image. The halftone shares bear significant visual information to the viewers, such as buildings, landscapes, etc. The visual quality attained by the new method is significantly better than that attained by extended VC or any other available VC method known to date. Halftone VC is built upon the basis matrices and collections available in conventional VC. This scheme is better than EVC in terms of contrast of the recovered secret but both the shares and the reconstructed secret suffer from pixel expansion.



### Probabilistic Visual Cryptography Schemes

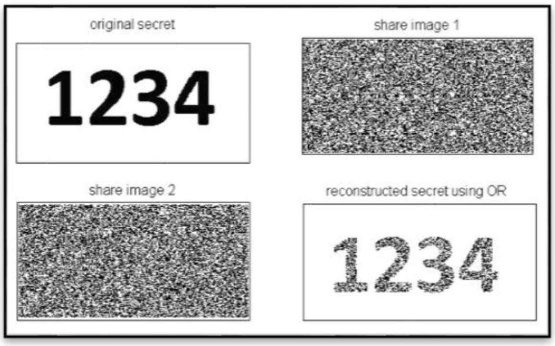
In this scheme, usually there is no pixel expansion, i.e., m is 1. The reconstruction of the image however is probabilistic, meaning that a secret pixel will be properly reconstructed only with a certain probability. On the other hand, in the deterministic model the reconstruction of an approximation of the secret pixel is guaranteed. But using probabilistic VCS [11], we can create shares with any pixel expansion m ≥ 1. In Yang's probabilistic model the secret pixel is appropriately reconstructed with some probability. Yang's aim is to provide schemes with no pixel expansion, which are obviously desirable. However the quality of the reconstructed pixel depends on how big the probabilities are of correctly reconstructing secret pixels.

*Recursive Threshold Visual Cryptography Scheme*

A recursive style of secret sharing takes into account a set of two shares which contain more than one secret. Recovering this secret requires rotation or shifting of the share to different locations on the corresponding share. In recursive hiding of secrets, the user encrypts additional information about smaller secrets in the shares of a larger secret without causing any expansion in the size of the latter, thereby increasing the efficiency of secret sharing. The idea here is to double the secret size at every step and so increases the information that every bit of share conveys to *(n-1)/n* bit of secret i.e. almost 100%.

*Random Grids based Visual Cryptography*

Random grid (RG) is a method to implement visual cryptography (VC) without pixel expansion. RG is defined as a transparency comprising a two-dimensional array of pixels, where each pixel can be fully transparent (white) or totally opaque (black), and the choice between the alternatives is made by a coin-flip procedure. Half of the pixels in a RG are white, and the remaining pixels are black. Encoding an image by random grids was introduced initially in 1987 by Kafri and Keren. A binary secret image is encoded into two noise-like transparencies with the same size of the original secret image, and stacking of the two transparencies reveals the content of the secret. Comparing RGs with basis matrices, one of the major advantages is that the size of generated transparencies is unexpanded. The RG scheme is similar to the probabilistic model of the VC scheme, but the RG scheme is not based on the basis matrices.



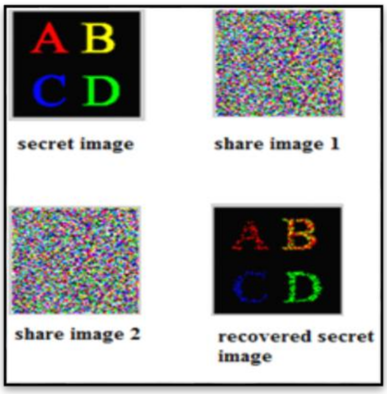
*Colour Visual Cryptography Schemes*

Up to 1996, visual cryptography schemes were only applied to binary images. Rijmen and Preneel have introduced a visual cryptography scheme for color images. In their scheme, each pixel of the color secret image is expanded into a 2×2 block in order to generate two share images. Each 2×2 block on the share image is filled with red, green, blue and white respectively, and thus no clue about the secret image can be recognized from any one of these two shares alone. Verheul and Van Tilborg introduced another method for encrypting a colored image, called *c*-colour (*k*, *n*)-threshold scheme. In this scheme one pixel is expanded into m sub-pixels, and each sub-pixel is partitioned into c color regions. In each sub-pixel, exactly one color region will be colored, and all the remaining color regions are black. The color of one pixel is based on the interrelations between colors of the stacked sub-pixels. For this colored visual cryptography scheme with c colors, the pixel expansion m is c x 3.

Basic Terminologies used in encrypting Colored Images via Visual Cryptographic method are discussed below.

*Half toning:* This method uses the density of the net dots to simulate the gray level is called "Halftone" and converts an image with gray level into a binary image before processing.

*Color Decomposition:* In this, every color on a color image can be decomposed into three primary colors: C, M, Y (if subtractive model is used) or R, G, B(if additive model is used). This method expand every pixel of a color secret image into a 2 x 2 block in the sharing images and keep two colored and two transparent pixels in the block.

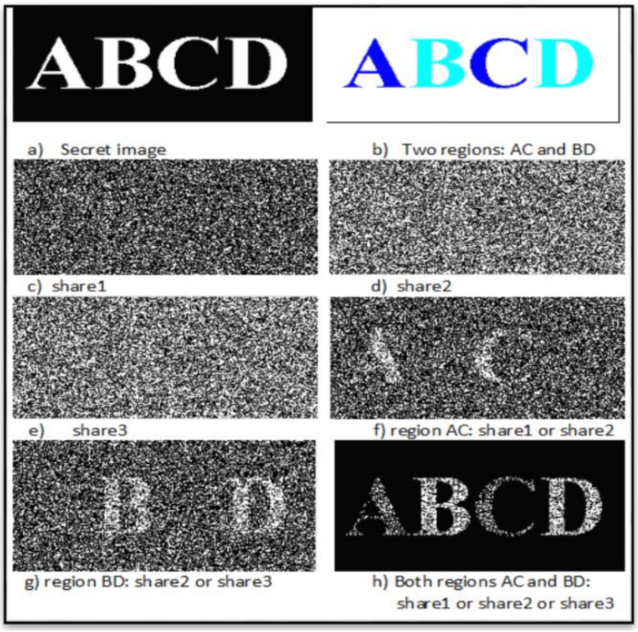


*Progressive Visual Cryptography*

Progressive Visual Cryptography takes into consideration the premise of perfect secret recovery and high quality secret reconstruction. Many of the schemes do require computational effort in order to perfectly reconstruct the secret. A new sharing concept emerged known as "Progressive Visual Cryptography" which revealed the secret image progressively as more and more number of shares were stacked together.

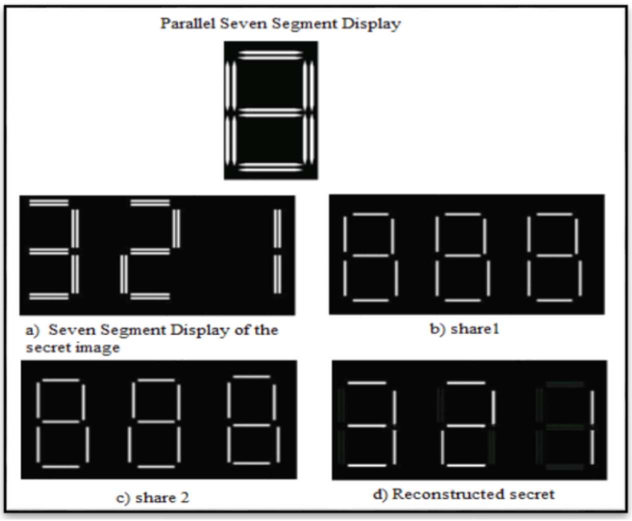
*Region Incrementing Visual Cryptography*

In traditional visual cryptography scheme, one whole image is considered as a single secret and same encoding rule is applied for all pixels of one image. So it reveals either entire image or nothing. It may be the situation that different regions in one image can have different secrecy levels, so we can't apply same encoding rule to all pixels. Ran-Zan Wang developed a scheme Region Incrementing Visual cryptography for sharing visual secrets of multiple secrecy level in a single image [9]. In this scheme, different regions are made of a single image, based on secrecy level and different encoding rules are applied to these regions.


a) Secret image
b) Two regions: AC and BD
c) share1
d) share2
e) share3
f) region AC: share1 or share2
g) region BD: share2 or share3
h) Both regions AC and BD: share1 or share2 or share3

### *Segment based Visual Cryptography Scheme*

Traditional visual cryptography schemes were based on pixels in the input image. The limitation of pixel based visual cryptography scheme is loss in contrast of the reconstructed image, which is directly proportional to pixel expansion. Bernd Borchert proposed a new scheme which is not pixel-based but segment-based. It is useful to encrypt *messages* consisting of symbols represented by a segment display. For example, the decimal digits 0, 1,..., 9 can be represented by seven-segment display. The advantage of the segment based encryption is that, it may be easier to adjust the secret images and the symbols are potentially easier to realize for the human eye and it may be easier for a non-expert human user of an encryption system to understand the working. The secret, usually in the form of digits is coded into seven segment display before encrypted. Two random share images will be generated during encryption. Decryption process involves the stacking of these two share images.


Parallel Seven Segment Display
a) Seven Segment Display of the secret image
b) share1
c) share 2
d) Reconstructed secret

### *Cheating Immune Visual Cryptography Schemes (CIVCS)*

A VSS scheme is said to be a cheating prevention scheme if the chance of successful cheating is negligible. Cheating can be prevented in visual secret sharing scheme if participants suspect that some shares or the reconstructed images are not genuine. There are two approaches in designing CIVCS schemes. One is based on share authentication where each participant is given an additional share to authenticate other shares. The other is based on blind authentication where some property of the secret image is used to authenticate the reconstructed image. Thus, the goal of share authentication is to provide the participants the ability to verify the integrity of the shares before reconstructing secret images, and the goal of blind authentication is to make it harder for the cheaters to predict the structure of the shares of the other participants. Prevention of cheating via authentication methods has been proposed which focus on identification between two participants to help prevent any type of cheating taking place. Another two types of cheating prevention designed; one type used an online trust authority to perform the verification between the participants. The second type involved changing the VC scheme whereby the stacking of two shares reveals a verification image; however this method requires the addition of extra pixels in the secret. Another cheating prevention scheme described by Horng et al. [6] is that if an attacker knows the exact distribution of black and white pixels of each of the shares of honest participants then they will be able to successfully attack and cheat the scheme. This method prevents the attacker from obtaining this distribution.

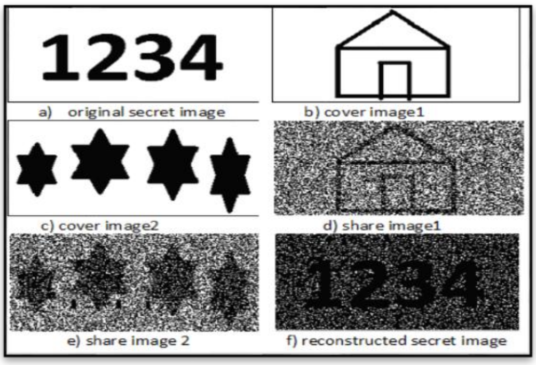
### *Size Invariant Visual Cryptography (Non-Expanded Visual Cryptography)*

Most of the traditional VCS suffer from pixel expansion, and hence it leads to over utilization of storage space and network bandwidth. Ito's scheme [8] removes the need for this pixel expansion. The scheme uses the traditional ($k$, $n$) scheme where $m$ (the number of sub-pixels in a shared pixel) is equal to one. The structure of this scheme is described by a Boolean $n$-vector V = $[v_1. . . v_n]^T$ , where $v_i$ represents the colour of the pixel in the $i$-th shared image. If $vi$ = 1 then the pixel is black, otherwise, if $vi$ = 0 then the pixel is white. The recovered secret can be viewed as the difference of probabilities with which a black pixel in the reconstructed image is generated from a white and black pixel in the secret image. Three major size invariant visual cryptography schemes are: *random grid*, *probabilistic* and *multi-pixel encoding*.

| Scheme | Advantage | Disadvantages |
|---|---|---|
| Probabilistic VC | No pixel expansion | Need to design complex matrices |
| Random grid VC | Perfect reconstruction of black pixels | White pixels is reconstructed only with ½ probability |
| Multi pixel Encoding | Fast Encryption | Some secret bits are omitted |

*User-friendly Visual Secret sharing scheme*

This scheme is used to generate meaningful size invariant share images during encryption. Unfortunately, in the two previous schemes (i.e., extended VC or halftone VC) that generate meaningful contents, the size of the shares generated during encryption were at least four times larger than that of the original secret image.Chen and Tsao [5] proposed a novel random grid based visual secret sharing scheme that has been skillfully designed to produce meaningful (user-friendly) share images without pixel expansion. It explains a procedure with different light transmissions based on the share images and the logo image (cover image) used to make the shares user-friendly. To implement meaningfulness, this scheme adjusts the respective contrasts of some areas of the two generated random grids $G_1$ and $G_2$ based on the cover image.

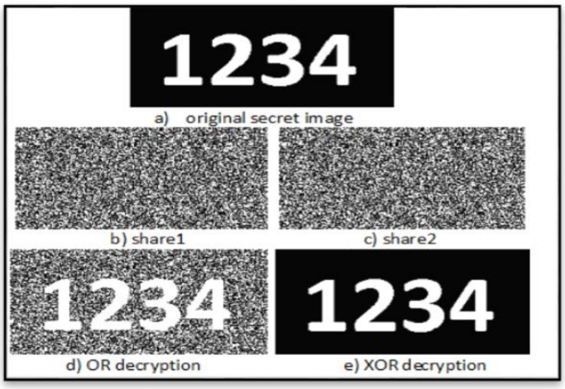


*Dynamic Visual Cryptography*

The core idea behind dynamic visual cryptography [6] is increasing the overall capacity of a visual cryptography scheme. This means that using a set of two or more shares, we can potentially hide two or more secrets. Multiple secret sharing is very useful when it comes to hiding more than one piece of information within a set of shares.

*OR and XOR Visual Cryptography*

A (k, n) visual cryptographic scheme encrypts a secret image into n share images (printed on transparencies) distributed among n participants. When any k participants stack their shares on an overhead projector (OR operation), the secret image can be visually discovered by a human visual system without the aid of computers (computation). But the monotone property of OR operation reduces the visual quality of reconstructed secret image for OR-based VCS. Generally all the conventional visual cryptography schemes (VCS) uses OR operation for stacking operations and so it is also called OR-based VCS. But it offers a poor visual quality image during decoding (stacking). Major advantage of XOR-based VCS (XVCS), is that since it uses XOR operation for decoding which results into exact recovery of the secret.



,

## IV. Performance Analysis

There are various parameters used to evaluate the performance of visual cryptography scheme.

- *Pixel expansion*- Pixel expansion m refers to the number of sub-pixels in the generated shares that represents a pixel of the original secret image. It represents the loss in resolution from the original secret image to the shared one.
- *Contrast*- Contrast is the relative difference in weight between combined shares that come from a white pixel and a black pixel in the original image. Contrast of the recovered secret image must be adjusted so that it is visible to the human eye.
- *Security*- Security is satisfied when each share individually discloses no information of the original image and the original image cannot be reconstructed with shares fewer than k in (k, n) scheme.
- *Accuracy*- Accuracy is measured to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR). Mean Squared Error (MSE) can also be used for accuracy evaluation.

## V. Conclusion

Visual cryptography offers perfect security for all the digitally transmitted secret images. This paper discusses various visual cryptography schemes and commonly used performance evaluation parameters. Diverse visual cryptography schemes were developed based on different factors like pixel expansion, meaningless or meaningful shares, contrast, security, type of secret image (either binary or colour) and the number of secret images encrypted. Also visual cryptography can be classified as *(n, n), (k, n) threshold* or general access structure based schemes.

## References

[1] Moni Naor and Adi Shamir, “Visual cryptography”. In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.

[2] G. Ateniese, C. Blundo, A. DeSantis, and D. R. Stinson, “Visual cryptography for general access structures”, Proc.ICAL96, Springer, Berlin, 1996, pp.416-428.

[3] T. Chen and K. Tsao, “User-friendly random-grid-based visual secret sharing”, IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 1693_1703, Nov. 2011.

[4] P. Tuyls, H. Hollmann, J. Lint, and L. Tolhuizen, “XOR-based visual cryptography schemes”, Designs, Codes, Cryptography, vol. 37, no. 1, pp. 169_186, 2005.

[5] Z. Zhou, G.R. Arce, and G. Di Crescenzo, “Halftone Visual Cryptography”, *IEEE Transactions on Image Processing*, vol. 15, no. 8, pp. 2441-2451, 2006

[6] http://bookboon.com/en/visual-cryptography-and-its-applications-ebook

[7] P. Tuyls, H. Hollmann, J. Lint, and L. Tolhuizen, “XOR-based visual cryptography schemes”, Designs, Codes, Cryptography, vol. 37, no. 1, pp. 169_186, 2005.

[8] R. Ito, H. Kuwakado, H. Tanaka, “ Image size invariant visual cryptography”, IEICETrans. Fundam. Electron. Commun. Comput. E82-A (10)(1999)2172–2177.

[9] R.-Z. Wang, “Region incrementing visual cryptography,” *IEEE Signal Process. Lett.*, vol. 16, no. 8, pp. 659–662, Aug. 2009.

[10] S. Cimato1, R. De Prisco∗ and A. De Santis, “Probabilistic Visual Cryptography Schemes”, *The Computer Journal*, December 1, 2005