

A Review on Visual Cryptography Schemes

Vijay Kumar S Karwande¹, Ashok P Kankale², Pravin G Thakare³

¹P.G. Scholar, Department of Computer Science and Engineering, RSCE, Buldana, India

²HoD, Department of Computer Science and Engineering, RSCE, Buldana, India

³Assistant Professor, Department of Computer Science and Engineering, STC, Shegaon, India

Abstract—In our daily life Information is increasingly important. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. There are lots of security related issues. Hacker's may try to access unauthorized data and misuse it. Various techniques are required to solve this problem. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. Visual cryptography (VC) is a technique used for protecting image-based secrets. This paper presents a detail survey of different visual cryptography scheme used for visual cryptography. The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are necessary to combine to reveal the secret image. We discuss different visual cryptography scheme like Halftone Visual Cryptography Scheme, Multiple Secret Sharing Scheme, Extended Visual Cryptography Scheme, Visual secret sharing, Natural Image Based Visual Secret Sharing etc.

Index Terms—Secret sharing scheme, Visual Cryptography, Data hiding

I. INTRODUCTION

Nowadays, information gets more value when shared with others. Due to internet, it is possible to share information like audio, video, images easily. There are security related issues. Hacker's access unauthorized data. Various techniques can be used to solve this problem. Today, in computer-aided environment sharing visual secrets images has become an important issue today. The secret images can be various types such as handwritten documents, photographs and others. Naor and Shamir [1] proposed the concept of Visual cryptography (VC) which allows the encryption of secret information in the image form. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares. By using the concept of visual cryptography, a secret image was broken up into some shares and then distributed to the n participants. By stacking their n shares, the secret information can be revealed and visually recognized by human visual system. There has been a steadily growing interest in visual cryptography. Visual cryptography is simple,

Secure, effective cryptographic scheme and very easy to implement.

II. CRYPTOGRAPHY

Cryptography is derived from Greek word „Krypto“ which means hidden and “Grafo”, which means written. It is the study and implementation of techniques to hide information, or simply to protect a message or text from being read. The information that is protected can be written text, electronic signals, and e-mail messages or data transmissions. The process of making the information unreadable is encryption or enciphering and the result of encryption is a cipher text or cryptogram. Reversing this process and retrieving the original readable information is called decryption or deciphering. To encrypt or decrypt information, an algorithm or so called cipher is used. Ever since mankind has existed, people have had secrets, and other people have wanted to know these secrets. The earliest forms of cryptography were performed by pencil and paper, and were available only to those who had access to proper education. Today our lives are completely digitized and cryptography has become an integral part of nearly everyone's daily life, and it's used to protect confidential information from hackers. Nearly all our private information is stored in one of the many databases from the government, banks, and health care services and so on. Cryptography protects the right to privacy and the right to communicate confidentially secure communications can protect one's intimate private life, business relations, and social or political activities.

1) Background on visual cryptography

Cryptography has a long and fascinating history, and it is one of the most important fields within the security profession. Visual cryptography uses the characteristics of human vision to decrypt encrypted images and in it the secret image is split into two or more separate random images called shares. To decrypt the encrypted information, the shares are stacked one on top of the other, and the hidden secret image appears. Due to its simplicity, anyone can physically manipulate the elements of the system, and visually see the decryption process in action without any knowledge of cryptography and without performing any cryptographic computations. With the near universal use of the Internet in every field, the need to share important documents from one office to other via this medium

becomes increasingly more necessary. With the coming era of the electronic commerce, there is an immediate need to solve the problem of ensuring information safety in today's increasingly open network environment. To protect the security of information, various encrypting technologies of traditional cryptography are usually used. With such technologies, the data can become disordered after being encrypted and later it can be recovered by a correct key. Without the correct key, the encrypted source content can hardly be detected even though unauthorized persons steal the data.

2) Traditional secret sharing

When important secret information is managed by individuals, secrets may leak. Suppose there is a vault that must be opened every day in a bank. Although the bank employs three senior tellers, management may not trust any individual teller. Therefore, it is necessary to find a possible solution to design a system whereby any two of the three senior tellers can gain access to the vault, but no individual teller can do so. This problem can be easily solved using a secret sharing scheme.

In a more general situation one may need to specify exactly which subsets of participants should be able to determine the key and which should not. Secret sharing schemes are useful in many situations that require the concurrence of several chosen people as in launching a missile or entering an area of restricted access (e.g., a bank vault).

3) Secret sharing scheme

A secret sharing scheme divides (sharing) a secret key K among a finite set of n participants in such a way that only certain specified subsets (qualified subsets) of participants can compute the secret key K by gathering their information. It was discovered independently by G.R. Blakley and Adi Shamir [3, 13]. Shamir's secret sharing scheme is an interpolating scheme based on polynomial interpolation while Blakley's secret sharing scheme is geometric in nature. Both of the schemes are k -out-of- n schemes but they represent two different ways of constructing such schemes, based on which more advanced secret sharing schemes can be designed. The biggest motivation for secret sharing is secure key management. In particular situations, there will be only one secret key that provide access to many important files. If such a key is lost, then all the important files become inaccessible. The basic model for secret sharing is called a k -out-of- n scheme (or sometimes referred as (k, n) threshold scheme). In this scheme, there is a sender and n participants. The secret information is divided into n parts by the sender, and gives each participant one part so that any k parts can be put together to recover the secret, but any $k - 1$ parts reveal no information about the secret. The pieces are usually called shares or shadows. Different choices for the values of k and n reflect the tradeoff between security and reliability. A secret sharing scheme is perfect if any group of at most $k - 1$ participants (insiders) has no advantage in guessing the secret over the outsiders.

4) Visual-threshold scheme

In a threshold scheme the secret can be any type of data. For example, it might be an image I , consists of black and white pixels. The secret image I could be encoded as a binary string $K=K(I)$, where 1 represents a black pixel and 0 represents a white pixel. By using any convenient secret sharing scheme, shares for K could be constructed. K would later be reconstructed using the appropriate algorithm for the secret sharing scheme. The image I is converted back using there sulting binary string. In this basic secret sharing scheme, however, cryptographic computations using computer are necessary to share a secret and decode the secret from shared data. In all the secret sharing schemes, a great deal of complexity is necessary to encrypt and decode a secret, and therefore computers are essential. The following question was asked by Kafri and Keren: [1] Is it possible to create a secret sharing scheme in which the secret image I that can be reconstructed visually by superimposing random grids? Each grid would consist of a transparency, made up of black and white pixels. Later Naor and Shamir: [2] introduced a specific implementation that was named visual secret sharing (VSS). This method can securely share image information (printed text, handwritten notes, pictures etc.), and it is possible to decode shared secrets by the human visual system. Based on the secret message (the original image) the VSS scheme generates n images (known as shares) which can be printed on n transparencies. In a k -out-of- n scheme, there would be n transparencies, and if any k or more than k transparencies are superimposed, the original secret image I should appear, but no information about the original image can be gained if fewer than the threshold number of k transparencies are stacked ($k - 1$ shares). The main difference between a traditional threshold scheme and a visual threshold scheme is how the secret is recovered. A traditional threshold scheme typically involves computations in a finite field; in a visual threshold scheme, the computation is performed by the human visual system [8]. In both types of schemes the security conditions is the same.

5) Recursive hiding of secrets

Recursive hiding of secrets was first introduced by M. Gnanaguruparan and SubhashKak [5], with applications to both images and printed text, to increase the efficiency of visual cryptography and to make it possible to incorporate additional secret information that serves as a stenographic channel [6]. The idea involved in recursive hiding secret is that several multiple message can be hidden is one of the share of the original secret image. The secret images that are to be hidden are taken according to their sizes from the smallest to the largest (i.e., secret size doubling at every step). The smallest secret image is divided into n shares using the basic idea of visual cryptography. These n shares are placed below each other, and they now represent the first share of the secret image. The second share is accomplished in such a manner that if the n shares are overlaid, then the secret image is revealed under consideration. This process is repeated recursively. Important thing to be noticed is that the share of the original secret image

that contains the recursively-hidden information must also contain both the shares of the last hidden secret image [5]. With respect to the original secret image this enforces a compulsion on the size of the secret images.

6) *Gray scale images*

In a gray scale image the value of each single pixel carries intensity information. Images of this kind are also known as black-and-white. These are exclusively composed of gray shades and are thus distinct from one-bit black and white images. The darkest possible shade is black, which is the total absence of transmitted or reflected light and the lightest possible shade is white.

III. REVIEW OF LITERATURE

1) *Visual cryptography*

Visual cryptography is a powerful encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. It uses two or more transient images (called shares). One image contains random pixels and the other image contains the secret information. It is impossible to retrieve the secret information from one of the images. Either transparent images or layers are required to reveal the secret information. The easiest way to implement visual cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as one-time pad system and will offer unbreakable encryption. In the overlay animation it can be observed by sliding the two layers over each other until they are correctly aligned and the hidden information appears.

2) *How visual cryptography works*

Each pixel of the image is divided into smaller blocks and always has the same number of black and white (transparent) blocks. For example if a pixel is divided into two parts (2 sub pixels), there will be one white and one black blocks. Similarly if the same pixel is divided into four equal parts (4 sub pixels), there will be two white and two black blocks. Here is a simple example that explains the idea of how visual cryptography works.

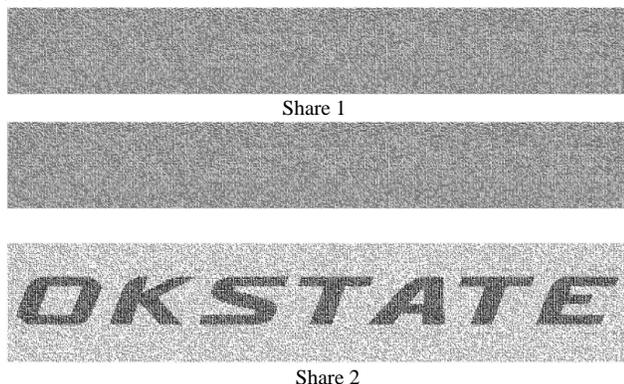


Fig. 1. Example to show how VC works

From Figure-1 we can observe that the original image is broken up into two parts which are its shares. Separately these shares look like random noise but when combining reveals an image. Every single pixel is split into sub pixels and the human vision still perceives them as one pixel. To try this, one can copy the share 1 and 2 and print them onto a transparent sheet or thin paper. Always use a program that displays both the black and white pixels aligned correctly and set the printer so that all pixels are printed accurate.

3) *Two-out-of-two scheme (2 sub pixels)*

The encoding scheme is to share a binary image into two different shares Share 1 and Share 2. Each pixel is divided into a black and white sub pixel placed next to each other. For the case of white pixel, one of the two combinations of sub pixels will be chosen with a probability of 0.5 to represent the pixel in each of the shares. When these shares are placed one on top of the other, the pixel are visually ORed and hence a white pixel looks gray (half black and half white) to the human eye. The pixels are chosen in a similar manner for the case of a black pixel. But when the sub pixels are visually ORed, the two black sub pixels placed next to each other appear as a single black pixel. This idea can be applied to images to develop a basic Two-out-of-Two scheme by using 2 sub pixels.

The 2 out of 2 visual secret sharing problem can be solved by the following collection of $n \times n$ matrices:

- $C_0 = \{ \text{all the matrices obtained by permuting the columns of} \}$
- $C_1 = \{ \text{all the matrices obtained by permuting the columns of} \}$

4) *Two-out-of-Two Scheme (4 sub pixels)*

The original problem of visual cryptography is the special case of a Two-out-of-Two visual secret sharing problem. It can be solved with 2 sub pixels per pixel, but in practice this can distort the aspect ratio of the original image. It is thus recommended to use 4 sub pixels arranged in a 2×2 array where each share has one of the visual forms in Figure-4. A white pixel is shared into two identical arrays from the list, and a black pixel is shared into two complementary arrays from the list. Any single share is a random choice of two black and two white subpixels, which looks medium grey. When two shares are stacked together, the result is either medium grey (which represent white) or completely black. Note that the horizontal, vertical and diagonal shares described in Figure-4, is used to solve the following 3-out-of-3 scheme. The six shares described below by the rows of C_0 and C_1 are exactly the six 2×2 arrays of sub pixels. By stacking all the three transparencies from C_0 and C_1 we can observe C_0 is only $\frac{3}{4}$ black whereas a C_1 is completely black.

$C_0 = \{ \text{all the matrices obtained by permuting The columns of} \}$



$C_0 = \{ \text{all the matrices obtained by permuting the columns of} \}$



Pixel		Share 1	Share 2	Result
	$P =$			
	$P =$			
	$P =$			
	$P =$			

Fig. 2. Partitions for black and white pixels for 2- out-of scheme (2subpixels)

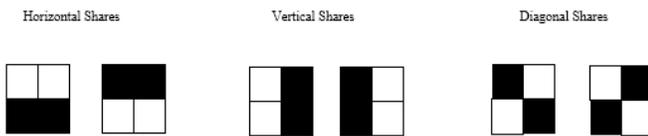


Fig. 3. Partitions for black and white pixels for 2- out-of scheme (4subpixels)

In Figure-2: it can be seen that a pixel, divided into four parts, can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel. If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all the requirements for true randomness are fulfilled, Visual cryptography offers absolute secrecy according to the information. The sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a secret message he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing any mathematical calculations by hand. The whole system is unbreakable, as long as both layers don't fall in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information. In general there are four criteria's, used to evaluate the performance of a (k, n) Visual secret sharing scheme. The first criterion is security: fewer k shadows offer no information about the secret image, where $k \leq n$. The second criterion is accuracy: it is similarity between the reconstructed image and the original one. The next criterion is computational complexity: the number of operations is required to produce shadows and to generate the reconstructed image. The last criterion is the size of a shadow, which is also called the pixel expansion problem.

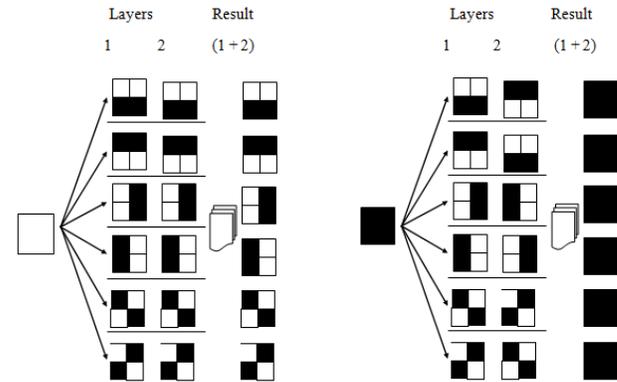


Fig. 3. Superimposition of black and white pixels for 2- out-of scheme (4subpixels)

5) Importance of aspect ratio in visual cryptography

Pixel expansion plays a vital role in visual secret sharing schemes. Here I used m , the pixel expansion, and sub pixels to represent a pixel. Suppose the secret image is a solar system symbol earth and m is not a square value, i.e., the aspect ratio is changed. After performing visual secret sharing scheme, the original symbol will be changed to an ellipse and consequently lead to loss of information.

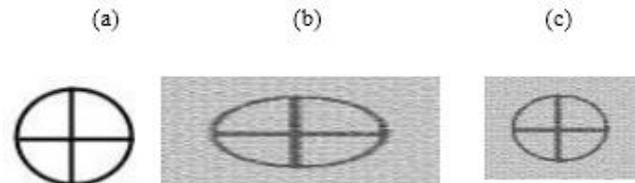


Fig. 4. Distortion to the variant expect ratio (a) Original secret image, (b)The aspect ratio is changed (c)The aspect ratio is unchanged

To avoid distorting the image, the dummy sub pixels are added to keep the aspect ratio unchanged. In the 3-out-of-5 scheme any single share contains 4 black and 4white pixels, so to make it a complete square array without distorting their aspect ratio, we need to add one more pixel. It should be either black or white

IV. CONCLUSION

A. Visual cryptography provides a secure way to transfer images. The advantage of visual cryptography is that it exploits human eyes to decrypt secret images with no computation required. Visual Cryptography allows easy decoding of the secret image by a simple stacking of the printed share transparencies. However, there are some practical issues that need careful consideration. The transparencies should be precisely aligned in order to obtain a clear reconstruction of the secret image. There is also some unavoidable noise introduced during the hiding technique can be applied to many applications in real and cyber world. For gray-scale images I proposed a new scheme that gives perfect printing process. Furthermore, the stacking method can only simulate the OR operation which always leads to a loss in contrast. The loss of contrast can be rectified by further processing. As visual cryptography schemes operate at the pixel levels, each pixel on one share must be

matched correctly with the corresponding pixel on the other share. Superimposing the shares with even a slight change in the alignment results in a drastic degradation in the quality of the reconstructed image.

REFERENCES

- [1] Kafri, O and Keren, E. 1987. Encryption of pictures and shapes by random grids. *Optics Letters* 12: 377-379.
- [2] Naor, M. and Shamir, A. 1995. Visual Cryptography. *Advances in Cryptography-Eurocrypt*, 950: 1-12.
- [3] Shamir, A. 1979. How to Share a Secret. *Communications of the ACM*. 22: 612-613.
- [4] Horng, G., Chen, T. and Tsai, D. 2006. Cheating in Visual Cryptography. *Design, Codes and Cryptography* 38: 219-236.
- [5] Gnanaguruparan, M. and Kak, S. 2002. Recursive Hiding of Secrets in Visual Cryptography. *Cryptologia* 26:68-76.
- [6] Parakh, A. and Kak, S. 2008. A Recursive Threshold Visual Cryptography Scheme. *Cryptology ePrint Archive*, Report 2008/535.
- [7] Ching-Nung, Y. and Tse-Shih, C. 2004. Aspect Ratio Invariant Visual Secret Sharing Schemes with Minimum Pixel Expansion. *Pattern Recognition Letters* 26: 193-206.
- [8] Stinson, D. 1995. *Cryptography Theory and Practice*. CRC Press.
- [9] Kato, T. and Imai, H. 1996. Some Visual Secret Sharing Schemes and Their Share Size. *Joint Conference of 1996 International Computer Symposium, Kaohsiung, Taiwan, R.O.C.*, pages 19-21
- [10] Sandeep Katta Recursive information hiding in visual cryptography
- [11] Kak, S. 1982. On Asymmetric Secret Sharing. *LSU ECE Technical Report*. May.
- [12] Alon, N. and Spencer, J. 1992. *The Probabilistic Method*, Wiley-Interscience, 2nd edition.