Visual Cryptography Scheme for Secret Image Retrieval

M. Sukumar Reddy†, S. Murali Mohan††

†M.Tech, Sri Venkateswara College Of Engineering & Technology Chittoor(Dist),Andhra-Pradesh India.
††M.Tech (Ph.D) ASSOCIATE PROFESSOR, Sri Venkateswara College Of Engineering & Technology , Chittoor(Dist),Andhra- Pradesh,India.

Abstract
The (t, n) visual cryptography (VC) is a secret stacking of t-1 any out of transparencies reveals the sharing scheme where a secret image is encoded into transparencies, and the secret image. The stacking of or fewer transparencies is unable to extract any information about the secret. We discuss the additions and deletions of users in a dynamic user group. To reduce the overhead of generating and distributing transparencies in user changes, this paper proposes a (t,n) VC scheme with unlimited based on the probabilistic model. The proposed scheme allows to change dynamically in order to include new transparencies without regenerating and redistributing the original transparencies. Specifically, an extended VC scheme based on basis matrices and a probabilistic model is proposed. An equation is derived from the fundamental definitions of the (t,n) VC scheme, and then the VC scheme achieving maximal contrast can be designed by using the derived equation. The maximal contrasts with t=2 to 6 are explicitly solved in this paper.

Keywords
Visual Cryptography(VC), Random Grids(RGs), Secret Sharing , Contrast

1. Introduction

Visual cryptography (VC) is a branch of secret sharing. In the VC scheme, a secret image is encoded into transparencies, and the content of each transparency is noise-like so that the secret information cannot be retrieved from any one transparency via human visual observation or signal analysis techniques. In general, a (t, n) threshold VC scheme has the following properties: The stacking of any out of those VC generated transparencies can reveal the secret. by visual perception, but the stacking of any t-1 or fewer number of transparencies cannot retrieve any information other than the size of the secret image. Naor and Shamir [1] proposed a (t, n)–threshold VC scheme based on basis matrices,and region incrementing VC. Contrast is one of the important performance metrics for VC schemes. Generally, the stacking revelation of the secret with higher contrast represents the better visual quality, and therefore the stacking secret with high contrast is the goal of pursuit in VC designs. Naor and Shamir [1] define a contrast formula which has been widely used in many studies.

Manuscript received June 5, 2014
Manuscript revised June 20, 2014

Architecture

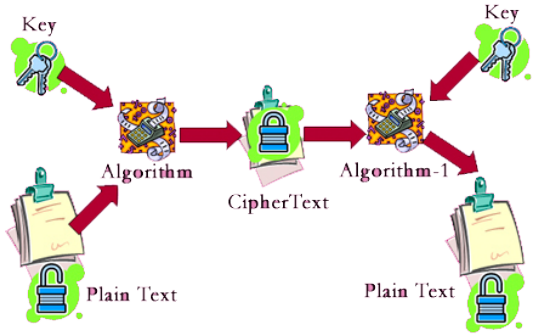

Fig .1.architecture of visual cryptography

1.1 Modules

a. Login modules.
b. Matrices (Black and White) Method.
c. VC Scheme Method.
d. Encoding Algorithm Method.

2. How Visual Cryptography works

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example images from above uses pixels that are divided into four parts.
In the table on the right we can see 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.

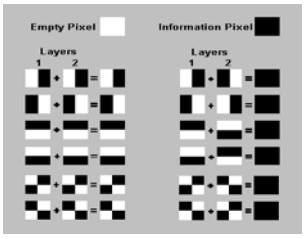

Fig.2. In the table on the right we can see that a pixel, divided into four parts, can have six different states

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.The system of pixel can be applied in different ways. In our example, each pixel is divided into four blocks. However, you can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically.

3. Previous work

Encrypting an image by random grids (RGs) was first introduced by Kafri and Keren [26] in 1987.
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. The recent studies include the RG for color image.

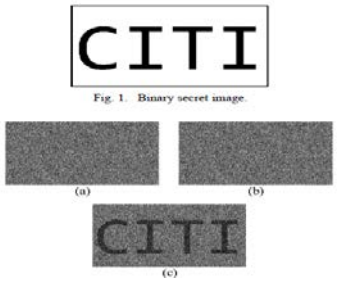

Fig.3. (a) T1,(b) T2 , (c)T1+ T2

4. Visual Cryptography schemes

4.1Visual cryptography for general access structures

In (t, n) Basic model any ‘t’ 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 t out of n threshold visual cryptography scheme for general access structure is better with respect to pixel expansion than .

a.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 [3] 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.

b.Recursive Threshold visual cryptography

The (t, n) visual cryptography explained in section I needs ‘t’ 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.

4.2 Halftone Visual Cryptography

The meaningful shares generated in Extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI [5] was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel ‘P’ is encoded into an array of Q1 x Q2 (‘m’ in basic model) sub pixels, referred to as halftone cell, in each of the ‘n’ shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

5. Visual cryptography Background

In order for the benchmarking scheme to be properly developed and executed, a developer needs to have an awareness of the history of Visual Cryptography. The developer also needs an understanding of the underlying concepts of Visual Cryptography and how they are used to generate shares of binary images. Recently, Visual Cryptography has been extended to accommodate shares of gray and color images, further extending its capabilities and versatility. This understanding of Visual Cryptography is necessary to allow an objective comparison of all the different types of algorithms.

5.1 History of Visual Cryptography

The field of Visual Cryptography has evolved over the past several years. The first Visual Cryptography method was proposed by Moni Naor and Adi Shamir in 1994 [12]. Their paper focused on a process for perfectly encrypting digital media that could be decoded using solely the human visual system. This idea would allow written material to be digitally transmitted without concern that the message could be intercepted and accidentally revealed to unauthorized parties. The primary description associated with Visual Cryptography is the message being encoded into two shares. When looked at individually, these shares reveal no information about the message contained in them and resemble random noise. However, when these shares are printed on transparencies, overlaid, and perfectly aligned, the message contained in the shares is revealed. The message is revealed without additional calculation or manipulation. This feature assures that the secure process can be used by someone who has no previous knowledge of Visual Cryptography, programming background, or cryptographic analysis experience.

5.2 Proof of Concept - Binary Images

The process behind Visual Cryptography allows messages to be contained in seemingly random shares. The generation of these shares demonstrates the concept of Visual Cryptography along with its strengths and limitations. Assuming that the message being encrypted is a binary image with p pixels, each of these pixels are separately encoded with a sub pixel grouping with s pixels. This allows n shares to be generated using these sub pixel groupings. Each share is a collection of m black and white sub pixels, which are printed in close proximity to each other so that the human visual system averages their individual black/white contributions." [12] These sub pixel groupings are typically square to not distort the aspect ratio of the original image. However, sub pixel groupings that are not square do happen in Visual Cryptography algorithms and the aspect ratio of the image is altered accordingly.

The most frequently used sub-pixel groupings in Visual Cryptography algorithms. The image is encoded in n shares and the message can be revealed by stacking k of those n shares. However, if k-1 shares are stacked together, the encoded message cannot be seen. This provides security by the fact that the messages cannot be revealed unless a minimum number of shares are stacked together, in addition to the security of seemingly random shares. The generation of the shares is based on the value of the pixel and the probability of a sub-pixel group occurring. A share generation scheme corresponding to k = 2 and n = 2. This is applied to a binary image by assigning the corresponding sub-pixel grouping to the pixels throughout the image. This results in two random shares where the message cannot be identified. The mathematical proof of this scheme and its perfect encryption are shown in the original paper by Naor and Shamir \Visual Cryptography" .

5.3 Extension to Gray and Color Images

The process of Visual Cryptography, as developed through the original algorithm [12], was designed to be used with binary images. This is illustrated from the nature of the shares and the encryption process documented previously. If the secret messages being encoded contain text or binary images, the process shown in the original algorithm works well. However, the world is not composed of solely black and white pixels. With the increasing production of images in the digital age, gray and color images have a pressing need for encryption and protection as much, or more, as binary images.

5.3.1 Gray Images

While Naor and Shamir did focus most of their paper on the development of an algorithm to encrypt binary images, they were also aware of the eventual need to encrypt gray and color images. In the last section of their paper, they proposed a technique which involved printing each of the pixels in an image as half black - half white circles. This allowed the rotation angle of the corresponding circles to vary and which would reveal a range of gray tones throughout the overlapped shares. If the rotation angle of the first share pixel is chosen at random, then the relative change in rotation of the corresponding share pixels would result in uniformly gray shares with no information about the original image being revealed.

5.3.2 Color Images

Just as images in the world cannot be solely represented by binary images, gray images are not sufficient either. Representation of the world in color images is important for our understanding of the world and allows the storage of information linked to the human visual system's interpretation of the world. The incorporation of color into Visual Cryptography would offer security to a majority of the digital media being generated today.

5.4 Observations and Additional Information

While these techniques provide an approximate binary representation of gray and color images, none of these techniques provide a perfect reconstruction of the original gray and color images. The result of overlapping the shares is only an approximation to the original image. This is due to the nature of the original Visual Cryptography algorithm that was designed. Because there is no way to perfectly construct gray or color image shares using current Visual Cryptography techniques, this will be a loop hole that can be exploited and does not provide the same security for gray and color images as it does for binary images. In order to achieve the same level of security, the Visual Cryptography technique would need to be modified to properly accommodate gray and color image pixels and a modified generation of the shares.

6. Result & Discussion

The proposed method is based on the basis matrices and the idea of probabilistic model.
For a (t,n) VC scheme, the “totally symmetric” form of and B0 and B1 are both constructed and described as and , respectively.
For a column bi randomly selected from with uniform distribution, let Pj,i be the probability that consists of zeros and (n-j)ones.
We have seen that in the case of visual cryptography schemes, the 6result of stacking of transparencies, can be completely characterized by the Boolean "OR" operation. We know that it favors 1s to 0s. i.e., If we "OR" two random bits, the result is more likely towards 1 than 0. When more random bits are involved, it will be more and more likely that the result is 1. So, when k increases, the distinguishing threshold for 0 bit and 1 bit will beat a higher level. So, it is natural that as k increases, the blowing factor also increases. This threshold will not affect the security of the system. Its purpose is only to distinguish the two bits from one another. So, if one could reduce the distinguishing threshold, the blowing factor may decrease. Since "XOR" does not favor either 0 or 1, it could be a better choice to "OR". This is the difference between traditional Visual Cryptography and Modified Visual Cryptography. This cannot be implemented in the case of images, where as for binary strings it can be done. It is easy to see that, in modified visual cryptography, the blowing factor will never increase, (if not decreased) compared with ordinary visual cryptography.

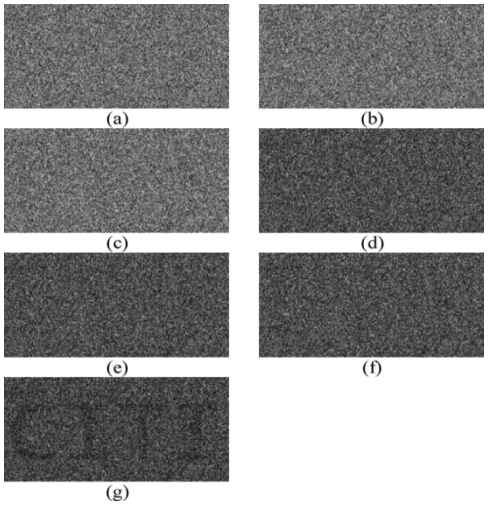

Fig.4. proposed system(a).T1,(b).T2 ,©.T3, (d).T1+T2 , (e).T1 + T3 , (f).T2+T3 , (g). T1+T2+T3

6.1 A Modified scheme for (k; k) Visual Cryptography

We now describe a general construction which can solve any (k; k) modified visual secret sharing problem, having a blowing factor, one. Let Bi; X; and Y be the matrices defined in section 3.5. In Modified Visual Cryptography we perform instead of V.

6.1.1 Comparison of the schemes

While both the schemes are equally secure, in the former scheme, the result of combining shares varies on r, where as in latter one, it is a fixed value This phenomena does not enhance or reduce the security of the system. So, we suspect that the former scheme has done some extra effort for unnecessarily distinguishing the number of shares combined, which is insignificant. So we strongly believe that the blowing factor could be reduced, by striking at a better modified visual cryptography scheme, than the corresponding one. When the secret is recovered by combining all the k shares, in the former, we have to search for the single 0 present, in case, the secret bit is 0. Where as in the latter one, because the result is either all zeros or all 1s, one can recover the secret bit just by looking at the first bit itself. So, though both are equally

secure, the modified cryptographic scheme is at least more efficient in the combining process.

7. Permutation Ordered Binary Number System

In the course of our research work we have formulated a new number system. This number system is found to be very useful and more efficient than the conventional number systems under use. We have used this number system in some of our newly introduced secret sharing schemes.

7.1 A new number system

We consider a general number system, called, Permutation Ordered Binary (POB) Number System with two non negative integral parameters, n and r, where n =>r.

7.2 POB-representation is unique

We prove that the POB-representation is unique in the sense that the binary correspondence of a POB-number is unique.

7.3 Visual cryptography

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to been crypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography was pioneered by Moni Naorand Adi Shamir in 1994. They demonstrated a visual secret sharing scheme, where an image was broken up into n shares so that only someone with all n shares could decrypt the image, while any n-1 shares revealed no information about the original image. Each share was printed on a separate transparency, and decryption was performed by overlaying the shares. When all n shares were overlaid, the original image would appear. Using a similar idea, transparencies can be used to implemental one-time pad encryption, where one transparency is a shared random pad, and another transparency acts as the cipher text cryptography and steganography are well known and widely used techniques that manipulate information (messages) in order to cipher or hide their existence

7.4 Halftone Visual Cryptography

The two-out-of-two visual threshold scheme demonstrates a special case of -out-of- schemes [3], [4], [8]–[10]. A more general model for visual sharing schemes based on general access structures has been recently studied in [11], [12], where all qualified and forbidden subsets of the participants are defined. The participants in a qualified subset can recover the secret image while the participants in a forbidden subset cannot. The properties of a -out-of- scheme including the conditions needed for optimal contrast and the minimum pixel expansion attainable can be found in [8]–[10]. The concepts of VC have been recently extended such that the secret image is allowed to be a grey-level image rather than a binary image [13], [14]. Although the secret image is grey scale, shares are still constructed by random binary patterns. In [15] and [16], the concepts are further generalized where a secret color image is encrypted into shares consisting of randomly distributed color pixels.

Applications

1. Secrecy in Transmission
2. Secrecy in Storage
3. Integrity in Transmission
4. Integrity in Storage
5. Authentication of Identity
6. Credentialing Systems

Conclusion

We have proposed a (t, n) VC scheme with flexible value of. From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of (t, n) VC with unlimited. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic model is adopted in the scheme. As the results listed in Table I, the proposed scheme also provides the alternate verification for the lower bound proved by Krause and Simon [20]. For t=4, the contrast is very low so that the secret is visually insignificant. Therefore, in practical applications, the values of 2 or 3 for are empirically suggested for the proposed scheme.

Future Scope

1. Visual Cryptography provides a secure way to Transfer Images.
2. It exploits human eyes to decrypt secret images with no computation required.
3. It uses XOR operation so, computation is easy.
4. We can generate infinite number of shares dynamically.

5. Proposed Method performs accurately Stacking mechanism without Regeneration and Redistribution of Shares.

References

[1] M. Naor and A. Shamir, "Visual cryptography," in Proc.AdvancesinCryptography(EUROCRYPT'94), 1995, vol. 950, LNCS, pp. 1–12.
[2] R. Ito, H. Kuwakado, and H. Tanaka, "Image size invariant visual cryptography," IEICE Trans. Fundam. Electron., Commun., Comput. Sci.,vol. 82, pp. 2172–2177, Oct. 1999.
[3] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognit.Lett., vol. 25, pp. 481–494, Mar. 2004.
[4] S. J. Lin, S. K. Chen, and J. C. Lin, "Flip visual cryptography (FVC) with perfect security, conditionally-optimal contrast,and no expansion,"J. Vis. Commun. Image Represent., vol. 21, pp. 900–916, Nov.2010.
[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inf. Computat., vol. 129, no. 2,pp. 86–106, Sep. 1996.
[6] F. Liu, C. Wu, and X. Lin, "Step construction of visual cryptography schemes," IEEE Trans. Inf. Forensics Security, vol. 5, no. 1, pp. 27–38, Mar. 2010.
[7] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.
[8] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptography via error diffusion," IEEE Trans. Inf. Forensics Security, vol. 4, no. 3, pp. 383–396, Sep. 2009.
[9] F. Liu, C. K.Wu, and X. J. Lin, "Colour visual cryptography schemes,*IET* Inf. Security,"vol. 2, no. 4, pp. 151–165, Dec. 2008.

Mannuru Sukumarreddy received the B.Tech Degree in Electronic Engineering from JNTU Univercity,Ananthpur in 2007-2011.Presently I am studying M.Tech(DECS) at Sri Venkateswara College Of Engineering & Technology in chittoor .My native place is Rly-kodur,Kadapa Dist,Andhra pradesh ,India.

S. Murali Mohan is received M.Tech degree in Electronic Enginnering and doing P.hD.Now he is act as a ASSOCIATE PROFESSOR in Sri Venkateswara College Of Engineering & Technology, chittoor,Andhra pradesh,India.