IPHV2I10007X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

OPTIMISED MODELS FOR HANDLING TRANPARENCIES IN VISUAL CRYPTOGRAPHY

P.Nimilitha[1], T.P Shekar[2]

[1]Pursuing M.Tech, Department of Computer Science, Vivekananda Institute of Technology

[2]Assistant Professor, Department of Computer Science, Vivekananda Institute of Technology

ABSTRACT:

Now a days data security common concern to every application systems. While transferring the data over the network in a encoded format. Visual cryptography is a specialized secret sharing scheme. We consider data (images) transparencies with different dynamic user groups. The (t,n)visual cryptography (VC) is a secret sharing scheme where a secret image is encoded into (n) transparencies, and the stacking of any out of transparencies reveals the secret image. The stacking of (t-1) 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 (n) based on the probabilistic model. The proposed scheme allows (n) changing 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.

INTRODUCTION

Visual cryptography

is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that decryption becomes a mechanical operation that does not require a computer.

One of the best-known techniques has been credited to Moni Naor and Adi Shamir, who developed it 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 implement a one-time pad encryption, where one transparency is a shared random

pad, and another transparency acts as the ciphertext.

(2, N) Visual Cryptography Sharing Case

Sharing a secret with an arbitrary number of people N such that at least 2 of them are required to decode the secret is one form of the visual secret sharing scheme presented by Moni Naor andAdi Shamir in 1994. In this scheme we have a secret image which is encoded into N shares printed on transparencies. The shares appear random and contain no decipherable information about the underlying secret image, however if any 2 of the shares are stacked on top of one another the secret image becomes decipherable by the human eye.

Every pixel from the secret image is encoded into multiple subpixels in each share image using a matrix to determine the color of the pixels. In the (2,N) case a white pixel in the secret image is encoded using a matrix from the following set:

{all permutations of the columns of} : $\mathbf{C_0} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 1 & 0 & \dots & 0 \\ \dots & & & \\ 1 & 0 & \dots & 0 \end{bmatrix}$.

While a black pixel in the secret image is encoded using a matrix from the following set:

{all permutations of the columns of} : $\mathbf{C_1} = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & & & \\ 0 & 0 & \dots & 1 \end{bmatrix}$.

For instance in the (2,2) sharing case (the secret is split into 2 shares and both shares are required to decode the secret) we use complimentary matrices to share a black pixel and identical matrices to share a white pixel. Stacking the shares we have all the subpixels associated with the black pixel now black while 50% of the subpixels associated with the white pixel remain white.

Cheating the (2,N) Visual Secret Sharing Scheme

Horng et al. proposed a method that allows colluding parties to cheat an honest party in visual cryptography. They take advantage of knowing the underlying distribution of the pixels in the shares to create new shares that combine with existing shares to form a new secret message of the cheaters choosing.

We know that 2 shares are enough to decode the secret image using the human visual system. But examining two shares also gives some information about the 3rd share. For instance colluding participants may examine their shares to determine when they both have black pixels and use that information to determine that another participant will also

IPHV2I10007X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

have a black pixel in that location. Knowing where black pixels exist in another party's share allows them to create a new share that will combine with the predicted share to form a new secret message.

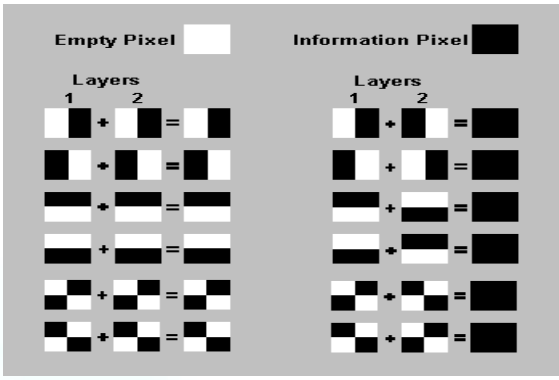
In this way a set of colluding parties that have enough shares to access the secret code can cheat other honest parties.

What is Visual Cryptography

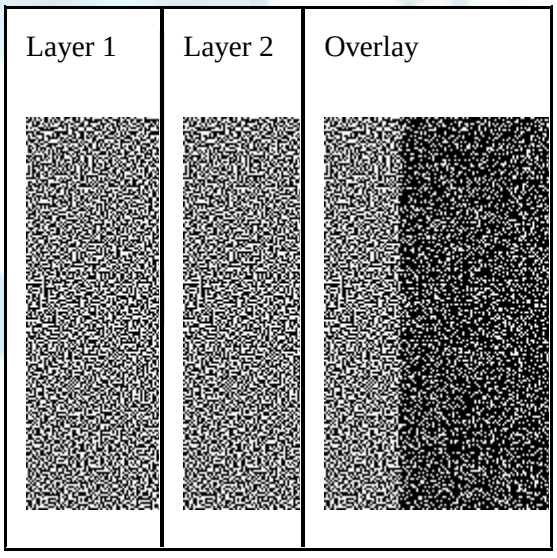
Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir in 1994.

Visual Cryptography uses two transparent images. 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. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

When the random image contains truely random pixels it can be seen as a **one-time pad system** and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper.



Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and past them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.



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 overlayed pixel will be half black and half white. Such overlayed pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlayed version will be completely black. This is an information pixel.

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 overlayed. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlayed, 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. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

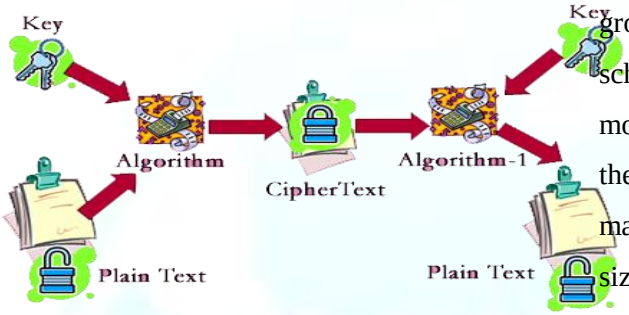
If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, Visual Cryptography offers absolute secrecy according to the Information Theory.

If Visual Cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a 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 calculations by hand. The system

IPHV2I10007X
International Journal Of Advanced Research and Innovation -Vol.II, Issue .1
ISSN Online: 2319 – 9253
Print: 2319 – 9245

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.

ARCHITECTURE:



EXISTING SYSTEM:

In visual cryptography, the decoding process is performed directly by the human eyes; while in existing the shared images need some processing to reconstruct the secret image. The increasing numbers of possibilities to create, publishes, and distribute images calls for novel protection methods, new sharing and access control mechanisms for the information contained in the published images. Secure image sharing techniques overcome the traditional cryptographic approach, providing new solutions for the development of new and secure imaging applications.

PROPOSED SYSTEM:

We have proposed a (t, n) VC scheme with flexible value of (n). 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.

MODULES:

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

MODULE DESCRIPTION:

1. LOGIN MODULES:

Login or logon (also called logging in or on and signing in or on) is the process by which individual access to a computer system is controlled by identification of

the user using credentials provided by the user.

A user can log in to a system tovyfvs and can then log out or log off (perform a logout / logoff) when the access is no longer needed.

Logging out may be done explicitly by the user performing some action, such as entering the appropriate command, or clicking a website link labeled as such. It can also be done implicitly, such as by powering the machine off, closing a web browser window, leaving a website, or not refreshing a webpage within a defined period.

2. MATRICES (BLACK AND WHITE) METHOD:

The basis matrices of VC scheme were first introduced, a white-and-black secret image or pixel is also described as a binary image or pixel. In the basis matrices, to encode a binary secret image, each secret pixel white black will be turned into blocks at the corresponding position of transparencies, respectively. Each block consists of subpixels and each subpixel is opaque or transparent. Throughout this paper, we use 0 to indicate a transparent subpixel and 1 to indicate an opaque subpixel. If any two subpixels are stacked with matching positions, the representation of a stacked pixel may be transparent, when the two corresponding pixels are both transparent.

3. VC SCHEME METHOD:

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 (B0)and(B1) are both constructed and described as H0 and H1, respectively.

VC scheme with flexible value of (n) 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.

4. ENCODING ALGORITHM METHOD:

For a given value of (t), the transparencies can be continuously generated with the OptPrVC scheme. However, practical applications require the algorithm to terminate within finite steps. To meet the requirement, a finite number is used to specify the number of transparencies in the algorithm.

CONCLUSION

We provide the Visual cryptography 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 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. The proposed scheme also provides the alternate verification for the lower bound proved by Krause and Simon [20]. For , 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.

REFERENCES

[1] M. Naor and A. Shamir, "Visual cryptography," in *Proc. Advances in Cryptography (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.

[10] G. Horng, T. Chen, and D. S. Tsai, "Cheating in visual cryptography," *Designs, Codes, Cryptography*, vol. 38, no. 2, pp. 219–236, Feb. 2006.

[11] C. M. Hu and W. G. Tzeng, "Cheating prevention in visual cryptography," *IEEE Trans. Image Process.*, vol. 16, no. 1, pp. 36–45, Jan. 2007.

[12] H. Koga, "A general formula of the - threshold visual secret sharing scheme," in *Proc. 8th Int. Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology*, Dec. 2002, pp. 328–345.

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

[14] M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes for general ," *Designs, Codes, Cryptography*, vol. 55, no. 1, pp. 19–35, Apr. 2010.

[15] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM J. DiscreteMath.*, vol. 16, no. 2, pp. 224–261, Feb. 2003.