International Journal of advancement in electronics and computer engineering (IJAECE)
Volume 1, Issue 9, December 2012, pp.167-171, ***ISSN 2278 -1412***

A Probabilistic Model of Visual Cryptography

Swati Yadav[1], Rajesh Kumar rai[2]
;
[1]*M. Tech Scholar, NIIST, RGTU, swati_yadav87@rediffmail.com, Bhopal (M.P.) India;*
[2]*Professor, Electronics Department, NIIST, RGTU,raj.rai1008@gmail.com, Bhopal (M.P.) India;*

Abstract- *The visual cryptography (VC) is a secret sharing scheme where a secret image is encoded into transparencies, and the stacking of any out of transparencies reveals 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 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 VC scheme, and then the VC scheme achieving maximal contrast can be designed by using the derived equation.*

Key words: *visual cryptography, Probabilistic scheme*

I. 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 -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 or fewer number of transparencies cannot retrieve any information other than the size of the secret image. Naor and Shamir [1] proposed a –threshold VC scheme based on basis matrices, and the model had been further studied and extended. The related works include the VC schemes based on probabilistic models [2]–[4], general access structures [5], [6], VC over halftone images [7], [8], VC for color images [9], cheating in VC [10], [11], the general formula of VC schemes [12], and region incrementing VC [13]. 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. Based on the definition of contrast, there are studies attempting to achieve the contrast bound of VC scheme [4], [14]–[20]. For instance, Blundo *et al.* [17] give the optimal contrast of VC schemes. Hofmeister *et al.* [19] provide a linear program which is able to compute exactly the optimal contrast for VC schemes. Krause and Simon [20] provide the upper bound and lower bound of the optimal contrast for VC schemes. Moreover, there exist VC related researches using differential definitions of contrast [21]–[23]. Another

important metric is the pixel expansion denoting the number of sub pixels in transparency used to encode a secret pixel. The minimization of pixel expansions has been investigated.

II. System study

II.1. Feasibility Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.
Three key considerations involved in the feasibility analysis are

- ECONOMICAL FEASIBILITY
- TECHNICAL FEASIBILITY
- SOCIAL FEASIBILITY

II.2. Economical Feasibility

This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchase

II.3. Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

II.4. Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

III. System Analysis

III.1. 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.

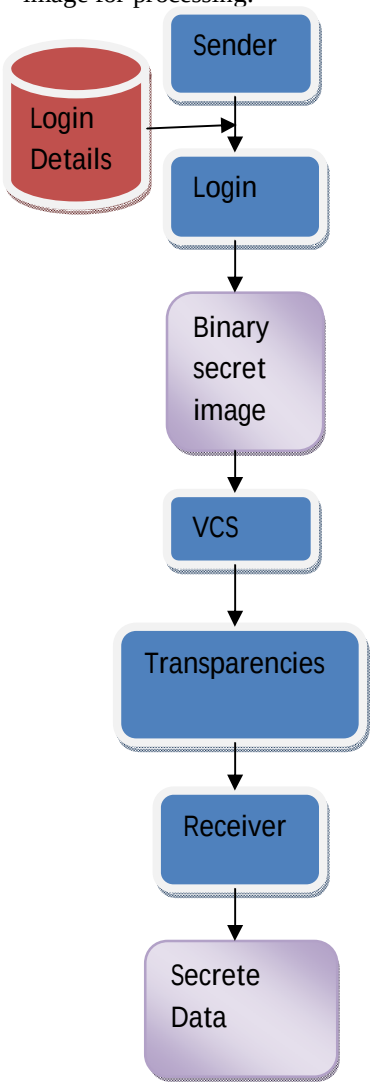
III.2. Proposed System

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.

IV. Implementation

IV.1. Input Image 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 to vyfvs 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. After logging in, in this module we design to take the input image for processing.



IV.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.

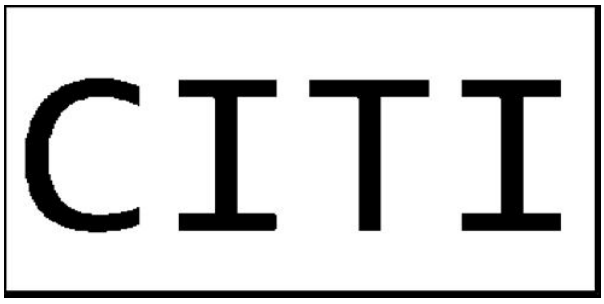
IV.3. VC Scheme Method

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.

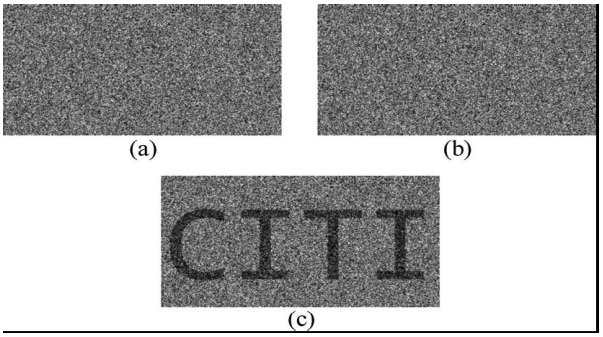
IV.4. Encoding Algorithm Method

For a given value of (t), the transparencies can be continuously generated with the Opt Pr VC 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.

V. Result



Binary image



Results of Opt Pr VC scheme. (a) T1 (b) T2 (c)T1 (+) T2

VI. Conclusion

We have proposed a 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 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, 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.

[16] M. Bose and R. Mukerjee, "Optimal visual cryptographic schemes," *Designs, Codes, Cryptography*, vol. 40, no. 3, pp. 255–267, Sep. 2006.

[17] C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," *J. Cryptology*, vol. 12, no. 4, pp. 261–289, 1999.

[18] S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," *Designs, Codes, Cryptography*, vol. 35, no. 3, pp. 311–335, Jun. 2005.

[19] T.Hofmeister,M. Krause, andH. U. Simon, "Contrast-optimal out of secret sharing schemes in visual cryptography," *Theoretical Comput. Sci.*, vol. 240, no. 2, pp. 471–485, Jun. 2000.

[20] M. Krause and H. U. Simon, "Determining the optimal contrast for secret sharing schemes in visual cryptography," *Combinatorics, Probability, Comput.*, vol. 12, no. 3, pp. 285–299, May 2003.

[21] E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of out of visual secret sharing schemes," *Designs, Codes, Cryptography*, vol. 11, no. 2, pp. 179–196, May 1997.

[22] P. A. Eisen and D. R. Stinson, "Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels," *Designs, Codes, Cryptography*, vol. 25, no. 1, pp. 15–61, 2002.

[23] F. Liu, C. K. Wu, and X. J. Lin, "A new definition of the contrast of visual cryptography scheme," *Inf. Process. Lett.*, vol. 110, no. 7, pp. 241–246, Mar. 2010.

[24] C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," *Theoretical Comput. Sci.*, vol. 369, no. 1, pp. 169–182, Dec. 2006.

[25] H. Hajiabolhassan and A. Cheraghi, "Bounds for visual cryptography schemes," *Discrete Appl. Math.*, vol. 158, no. 6, pp. 659–665, Mar. 2010.

Author's Profile

Swati Yadav*, received B.tech. From P.I.R.M.E. College JNTU Hyderabad (A.P.) in 2008 and currently pursuing M.Tech. in Digital Communication from NIIST, affiliated to RGTU, Bhopal. His area of interests is Digital Communication, Image Processing and WIMAX.*

Rajesh Kumar Rai *received M. E. (Elect) Degree with specialization in Digital Techniques & Instrumentation from S.G.S.I.T.S. Indore. His Research interests are Image Processing, Embedded System & Communication. He is Ph.D scholar in JJT University, Rajasthan. He has worked as a Assistant Professor & Head of Electronics Department in Siddhant College of Engineering, Pune, affiliated to University of Pune, Pune (India).Presently he is associated with NIIST, RGTU, Bhopal as a Associate professor in Department of Electronics & Communication.*
Life time member of IETE , IEEE & ISTE.