International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 23, 2017 ISSN: 2348-6600
Reference ID: IJCS-266 PAGE NO: 1701-1706
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

A feasibility paradigmatic of (t n) visual cryptography codification with vitalizing group

K.Nithya Kalyani

M.Phil Scholar J.J College of Arts and Science, Pudukottai.

Abstract – 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. This project discusses the additions and deletions of users in a dynamic user group. To reduce the overhead of generating and distributing transparencies in user changes, this project proposes a (t,n) VC scheme with unlimited n based on the probabilistic model. The proposed scheme allows n 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 (t,∞) 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 project.

Keywords: visual cryptography, Encoding Algorithm, transparencies, probabilistic, dynamic user

INTRODUCTION

This work proposes a novel scheme for lossy compression of an encrypted image with flexible compression ratio. A pseudorandom permutation is used to encrypt an original image, and the encrypted data are efficiently compressed by

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 23, 2017 ISSN: 2348-6600
Reference ID: IJCS-266 PAGE NO: 1701-1706
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

discarding the excessively rough and fine information of coefficients generated from orthogonal transform. After receiving the compressed data, with the aid of spatial correlation in natural image, a receiver can reconstruct the principal content of the original image by iteratively updating the values of coefficients. This way, the higher the compression ratio and the smoother the original.

SCOPE OF THE PROJECT

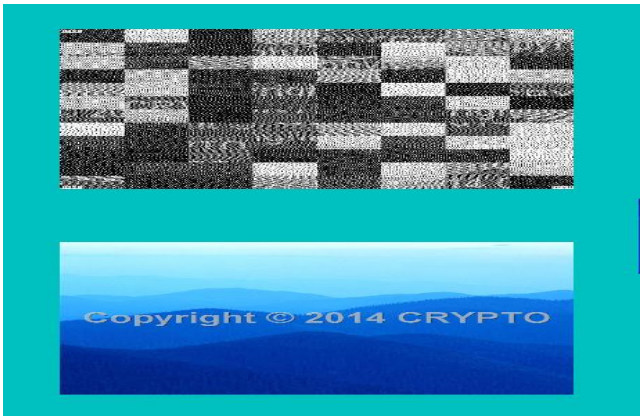
The goal of the project is data hiding for binary images in morphological transform domain. This project process the images based on 2*2 pixel blocks and combine two different processing cases that the flippability conditions of one are not affected by flipping the candidates of another for data embedding, namely “orthogonal embedding”.

SWAP EMBEDDING

This project flips an edge pixel in binary images, equivalent to shifting the edge location horizontally one pixel and vertically one pixel. A horizontal edge exists if there is a transition between two neighboring pixels vertically and a vertical edge exists if there is a transition between two neighboring pixels horizontally. This project swap an morphological images.

WATERMARKED IMAGE

The watermarked image is obtained by computing the inverse for the main processing block to reconstruct its candidate pixels. Using this module the original watermarked image can be seen.



- Proof of ownership
- Transcation Tracking
- Content authentication

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 23, 2017 ISSN: 2348-6600
Reference ID: IJCS-266 PAGE NO: 1701-1706
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

- Modification and multiple Watermark

THE SCHEME

The proposed scheme consider security of image in terms of encrypting it with the help of symmetric key, hence if someone access all the shares in unauthorized way, he/she can't decrypt it completely without symmetric key. This scheme manages security as well as decrypted images are of same size as original. The scheme is divided into three parts:

- Encryption of original image using symmetric key.
- Generation of Shares
- Decryption of Overlapped shares.

ENCRYPTION PROCESS

- Divide images into blocks such that block size equals to key size.
- Each block is XORed with key and then placed again in its original position. Now, encrypted image is divided into shares using visual cryptography.

DECRYPTION PROCESS

- Divided into blocks such that block size equals to key size.
- Each block is XORed with key and then placed again in its original position. Now original secret image is recovered.

COMPARISON

The existing Visual Secret Sharing schemes increases size of decrypted image and security gets ruined if someone has access to all shares. The proposed scheme improves with respect to size and security with a limitation of aspect ratio of original image cannot be maintained.

COMPARISON OF PROPOSED SCHEME WITH OTHER VCS

	Original Image	Each share of Naor and Shamir (2,2) Scheme	Each share of Basis (2,2) Scheme	Each Share of Proposed VCS
No. of Pixel	100	400	200	100
Security	Not Secure	Secure until all shares are not intercepts	Secure until all shares are not intercepts	More than all VCS until key is not known.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 23, 2017 ISSN: 2348-6600
Reference ID: IJCS-266 PAGE NO: 1701-1706
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

FUTURE ENHANCEMENT

The project will cover almost all the application requirements. Further requirements and improvements can easily be done since the coding is mainly structured or modular in nature. Further enhancements can be made to the application, so that the web site functions very attractive and useful manner than the present one. At present this project runs only in the systems, which has Microsoft ASP.Net & SQL server 2005 and it should contain internet information services. The system can be made attractive by enhancing more flexible. For this reason, as well, super resolution remains an ill-posed problem in a family of enhancement problems whose ultimate goal is to elucidate sharp edges and distinct borders while maintaining texture continuity.

ADVANTAGES

The third party cannot access the data hided image .Embedding data using real-valued coefficients requires more memory space. We observe that the morphological binary wavelet transform can be used to track the transitions in binary images by utilizing the detail coefficients. One rather intuitive idea in employing the morphological binary wavelet transform for data hiding is to use the detail coefficients as a location map to determine the data-hiding locations.

CONCLUSION

This project proposes a 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 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

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 23, 2017 ISSN: 2348-6600
Reference ID: IJCS-266 PAGE NO: 1701-1706
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

verification for the lower bound proved by Krause and Simon. 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.

BIBLIOGRAPHY

[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 cryp-tography," 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 expan-sion," J. Vis. Commun. Image Represent., vol. 21, pp. 900–916, Nov.

[5] G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryp-tography 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,

[7] Z. Zhou, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptog-raphy," IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453,

[8] Z. Wang, G. R. Arce, and G. Di Crescenzo, "Halftone visual cryptog- raphy 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 cryptog- raphy," IEEE Trans. Image Process., vol. 16, no. 1, pp. 36–45, Jan.

International Journal of Computer Science
Scholarly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
http://www.ijcsjournal.com Volume 5, Issue 1, No 23, 2017 ISSN: 2348-6600
Reference ID: IJCS-266 PAGE NO: 1701-1706
Alagappa University, Karaikudi, India 15th -16th February 2017
IT Skills Show & International Conference on Advancements in Computing Resources (SSICACR-2017)
http://aisdau.in/ssicacr ssicacr2017@gmail.com

[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.

[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

[15] C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast op-timal threshold visual cryptography schemes,"SIAM J. Discrete Math.,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

[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