IMPLEMENTATION OF VISUAL CRYPTOGRAPHY ON VIDEOS

Salma Bee
M.Tech Student, Teerthanker Mahaveer University ,Moradabad(India)

ABSTRACT

In Visual Cryptography is a new Cryptography technique which is used to secure the Videos. In Visual Cryptography the Image is divided into parts called shares and then they are distributed to the participants. The Decryption side just stacking the share Videos gets the image. The initial model developed only for the bi-level or binary Videos or monochrome Videos. Later it was advanced to suit for the Color Videos means Gray Videos and RGB/CMY Videos.This paper presents a study of implementation of algorithm of visual cryptography, Implementation of security level in Visual Cryptography Sharing Algorithm for Gray Level Videos and Comparison with previous approaches show the superior performance of the new method. Experimentation are conducted with standard synthetic and real data set Videos, which shows better performance of proposed color image visual cryptic scheme measured in terms of PSNR value and time with existing binary method.. The results showed that the PSNR values for proposed scheme is better than the existing scheme and maintains security.

Keywords - Cryptography, Encryption/Decryption, Security On Videos, Cryptography,Image Coding,Image Reconstruction, Matrix Algebra

I. INTRODUCTION

Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Naor and Shamir in 1994 proposed a new security technique named visual cryptography scheme. In this technique, a secret image of type binary is encoded in a cryptographically manner into random binary patterns which contains n shares in a k-out-of-n scheme. With the rapid advancement of network technology, multimedia information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial identifications are transmitted over the Internet. While using secret Videos, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret Videos, various image secret sharing schemes have been developed. Visual cryptography is introduced by first in 1994 Noar and Shamir.Visual cryptography is a cryptographic technique which allows visual information(e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers.

II. PROPOSED ENCRYPTION METHOD

1st Module: Study of Implementation of Visual Cryptography algorithm.

2nd Module: Implementation of security level in Visual Cryptography Sharing Algorithm for Gray Level Videos.

IJATES

III. DECRYPTION PROCESS

Ist Module: Implementation of Visual Cryptography Sharing Algorithm for Binary Videos. In this module of scheme the secret image which is to be converted into gray level then into binary level Videos. The image is to be divided in to 2 no. of shares by using visual cryptography algorithm. White Pixel processing and black pixel processing is done here.

Definition: Two matrices are called basis matrices, if the two collections and in Definition are obtained by permuting the columns of in all possible ways, respectively, and satisfy the following two conditions.

1) Contrast condition: if, the row vectors and, obtained by performing OR operation on rows of,

respectively and satisfy.

2) Security Condition: if, one of the two matrices, formed, respectively, by extracting rows from and , equals to a column permutation of the other. The construction of the basis matrices is a topic of study in conventional VC. Several design procedures, such as the method using cumulative arrays, are readily available

Example: The basis matrices and the collections of the encoding matrices in the conventional two- out-of-two scheme can be written as:

$$S0 = \begin{matrix} 0\ 1 \\ 0\ 1 \end{matrix} \qquad S1 = \begin{matrix} 0\ 1 \\ 1\ 0 \end{matrix}$$

$$C0 = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$$

$$C1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2nd Module: Implementation of security level in Visual Cryptography Sharing Algorithm for Gray Level Videos.

- In Gray scale image the value of each pixel carries only intensity information. Videos are known as black and white composed of gray. It is also known as monocrome.
- It has many shades of gray. Each pixel has 8 bit of information. Intensity of pixel is the range between minimum and maximum.
- The gray scale image is first decomposed into 8 bit binary codes by using bit planes that are equivalent to 8 binary Videos.
- It gives better approximation.
- If a bit on the nth bit plane on an m bit the dataset is set to 1, it contributes a value of 2(m-n), otherwise it contributes nothing.
- 8 bit value of bitplane.

Table-1: Binary representation of a no. 181.

Bit Plane	Value	Contribution	Running Total
1st	1	1*2 ^7=128	128
2nd	0	0*2 ^ 6=0	128
3rd	1	1*2 ^ 5 =32	160
4th	1	1*2 ^4=16	176
5th	0	0*2 ^ 3=0	176
6th	1	1*2 ^ 2=4	180
7th	0	0*2 ^ 1=0	180
8th	1	1*2 ^ 0=1	181

IV. DECRYPTION

In the decryption process the shares are stacked together to form the original Videos.

Bit planes are extracted first.

In bit plane decoding XOR operation is used.

V. ACKNOWLEDGMENTS

I would like to give this work to my parent, who have created the author of this thesis. I would like to thank professor .MISS MINI AGARWAL my advisor, for his understanding and research guidance. She has always been the one who guided me through difficulties to the final completion of my thesis. The idea of employing visual cryptography in video is in fact due to him and to the department staffs who has helped to create a computing environment that enabled us to work effectively.

REFERENCES

[1] W. Zeng, H. Yu, and C.-Y. Lin, Eds., Multimedia Security Technologies for Digital Rights Management. Orlando, Florida: Academic Press, Inc., 2006.

[2] A. Uhl and A. Pommer, Image and Video Encryption: From Digital Rights Management to Secured Personal Communication, ser. Advances in Information Security, vol. 15. Boston, USA: Springer Science + Business Media, Inc., 2005.

[3] B. Furht, E. Muharemagic, and D. Socek, Eds., Multimedia Encryption and Watermarking. New York: Springer, 2005.

[4] B. Furht, D. Socek, and A. M. Eskicioglu, "Fundamentals of multimedia encryption techniques," in Multimedia Security Handbook, B. Furht and D. Kirovski, Eds. CRC Press, LLC, 2004, ch. 3, pp. 93–131. [5] S. Li, G. Chen, and X. Zheng, "Chaos-based encryption for digital images and videos," in Multimedia Security Handbook, B. Furht and D. Kirovski, Eds. CRC Press, LLC, 2004, ch. 4, pp. 133–167, preprint available online at http://www.hooklee.com/pub.html.

[6] A. Servetti and J. C. D. Martin, "Perception-based selective encryption of G.729 speech," in Proc. IEEE Int. Conference on Acoustics, Speech, and Signal Processing (ICASSP'2002), vol. 1, 2002, pp. 621–624.

[7] "Perception-based partial encryption of compressed speech," IEEE Trans. Speech and Audio Processing, vol. 10, no. 8, pp. 637–643, 2002.

IJATES

[8] A. Torrubia and F. Mora, "Perceptual cryptography on MPEG layer III bit-streams," IEEE Trans. Consumer Eletronics, vol. 48, no. 4, pp. 1046–1050, 2002.

[9] M. V. Droogenbroeck and R. Benedett, "Techniques for a selective encryption of uncompressed and compressed images," in Proc. Advanced Concepts for Intelligent Vision Systems (ACIVS'2002), 2002, pp. 90–97. [10] A. Torrubia and F. Mora, "Perceptual cryptography of JPEG compressed images on the JFIF bit-stream domain," in Digest of Technical Papers of IEEE Int. Conference on Consumer Electronics (ICCE'2003), 2003, pp. 58–59.

[11] S. Lian, J. Sun, and Z. Wang, "Perceptual cryptography on SPIHT compressed images or videos," in Proc. IEEE Int. Conf. Multimedia & Expo (ICME'2004), vol. 3, 2004, pp. 2195–2198.

[12] "Perceptual cryptography on JPEG2000 compressed images or videos," in Proc. Int. Conf. Computer and Information Technology (CIT'2004). IEEE Computer Society, 2004, pp. 78–83. [13] S. Lian, X. Wang, J. Sun, and Z. Wang, "Perceptual cryptography on wavelet-transform encoded videos," in Proc. IEEE Int. Symp. on Intelligent Multimedia, Video and Speech Processing (ISIMP'2004), 2004, pp. 57–60.

[14] J. Dittmann and A. Steinmetz, "Enabling technology for the trading of MPEG-encoded video," in Information Security and Privacy: Second Australasian Conference (ACISP'97) Proc., ser. Lecture Notes in Com- puter Science, vol. 1270, 1997, pp. 314–324.

[15] Y. Bodo, N. Laurent, and J.-L. Dugelay, "A scrambling method based on disturbance of motion vector," in Proc. 10th ACM Int. Conference on Multimedia, 2002, pp. 89–90.

[16] M. Pazarci and V. Dipc¸in, "A MPEG2-transparent scrambling tech- nique," IEEE Trans. Consumer Eletronics, vol. 48, no. 2, pp. 345–355, 2002.

[17] C. Wang, H.-B. Yu, and M. Zheng, "A DCT-based MPEG-2 transparent scrambling algorithm," IEEE Trans. Consumer Eletronics, vol. 49, no. 4, pp. 1208–1213, 2003.

[18] A. Pommer and A. Uhl, "Selective encryption of wavelet packet subband structures for obscured transmission of visual data," in Proc. 3rd IEEE Benelux Signal Processing Symposium (SPS'2002), 2002, pp. 25–28.

[19] "Selective encryption of wavelet-packet encoded image data: Efficiency and security," Multimedia Systems, vol. 9, no. 3, pp. 279– 287, 2003.

[20] A. Pommer, "Selective encryption of wavelet-compressed visual data," Ph.D. dissertation, Department of Scientific Computing, University of Salzburg, Austria, June 2003.

IJATES