Research Paper | Engineering | E-ISSN No : 2454-9916 | Volume : 1 | Issue : 4 | Nov 2015

A SURVEY ON ENHANCING VISUAL CRYPTOGRAPHY USING NATURAL SHARES

Rekha Sarawade [1] | Ashish Manwatkar [2]

[1,2] Department of computer engineering, Indira College of Engineering and Management, Pune, India.

ABSTRACT

In visual cryptography reducing the pixel expansion and improving the display quality of recovered images are still major issues. Secret images are covered in shares by using conventional visual secret sharing schemes (VSS). Shares can appear as meaningful images or noise like pixels; but transmission of such a shares increase difficulties. In this paper we have propose survey on natural image based visual secret sharing scheme (NVSS). In this carrier image is using to recover the secret image and protect the participant during transmission phase. So we can hide the noisy shares and also propose possible ways to reduce the transmission risk problem for the shares.

Keywords: Natural shares, visual cryptography, transmission risk, visual secret sharing

I. INTRODUCTION

Visual cryptography is a scheme that encrypts a secret image into n shares and these shares handled by one or more participant. Each participant hold one or more than one shares. Sharing the secret image securely without any transmission risk is important part of visual secret sharing scheme. In conventional scheme for security it consists of meaningless pixel. It is better for security to protect the secured content [1] but it suffers from transmission risk problem. It consist of noise like shares so will cause attackers so there is chances of transmission failure. Again here used a meaningless shares these shares are not user friendly [2]. When number of shares increase then it is very difficult to manage such shares and also identify the shares. In previous research into the thresholds visual cryptography scheme reducing the pixel expansion and improved the display quality of recovered images [3] but the main problem in such techniques is secret images is easily detect by attacker. Image size visual cryptography show the display quality of recovered images is superior to other techniques [4] but it can easily detect by the hacker.

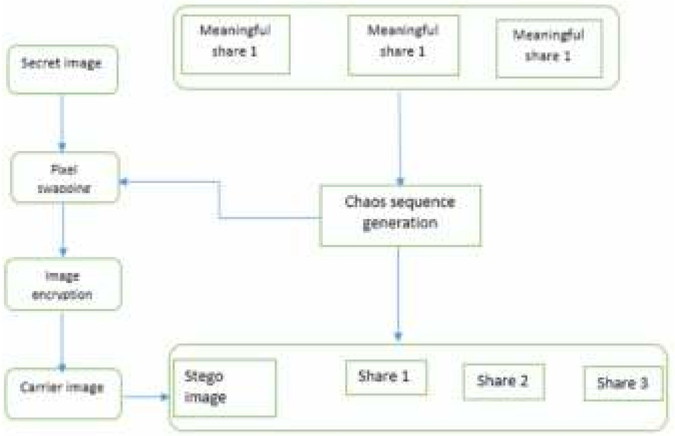

Fig. Architecture for Visual cryptopgraphy using natural shares

The Extended Visual Cryptography Scheme (EVCS) or the user-friendly VSS scheme provided some effective solutions to deal with the management issue [5]–[6]. The shares display low-quality images or contain many noise-like pixels. Such shares are easy to detect by hacker, and participants who transmit the share can easily lead to suspicion by others. By using steganography techniques, secret images can be concealed in cover images that are halftone gray images and true-color images [7]–[8] However, the stego-images still can be detected by steganalysis methods [9]. Therefore the existing VSS schemes still must be investigated for reducing the transmission risk problem for carriers and shares. A method for reducing the transmission risk is an important issue in VSS schemes. As shown in above fig 1. Secret image is used as input and this secret image is encrypted using natural shares. This encrypted image again recovered with carrier image to provide the more security and finally this encrypted image is send to receiver.

II. SURVEY

In this paper propose the visual cryptography that encrypts the secret image into n shares. Security is important issue when we transmit the secret image. Secret image contain the important information so to hide such information from hacker we need to provide security to the secret image in shares. Here shares are nothing but the meaningful images or noise like pixels but it increases interception risk during the transmission of shares. Hence VSS scheme suffers from transmission risk problem. So in this paper propose natural secret share scheme. Natural shares are in digital form or printed form using this NVSS scheme can share one digital secret image over n-1 arbitrary selected natural shares thus greatly reducing the transmission risk problem for the share.

In general process it consist many random and meaning pixels, it satisfy the security requirement but it creates the transmission risk [1] some shares contain low display quality images are easily detected [4].

In extended visual cryptography it is user friendly but it contain low quality images [7] so it is easy to detect. In halftone visual cryptography pixel expansion of generated shares increases rapidly it creates the transmission risk problem [9].

III. PERFORMANCE REVIEW

Performance analysis shows the behaviour and performance of this particular algorithm. And Quality of Services achieved by that algorithms or protocols. As like same here we have done performance review for different algorithms used in survey section of this paper. The bellow given table of Performance Review contains. The Paper Reference Number, Algorithms or Techniques, Parameters achievement and Working as well as Use of this algorithm in that paper. This table is created after analysis of papers result and algorithms. And using papers included in survey.

Table 1. Performance Review Table for Different Algorithms.

PR NO	ALGORITHAMS	PARAMETERS ACHIEMENT	WORKING AND USE
1	Enhancing visual cryptography-hanon algorithm	1. High Reliability. 2. Better Feasibility	1.Encryption on secret image and provides security
2	Asymmetric RSA Cipher encryption	1. High security 2. Prevent Attacks & Tapping.	1.Attack Prevention 2. RSA Public Key Uses.
3	Implement Public Key Cryptosystem.	1. Integrity. 2.Confidentiality 3.Non-repudiation	1.Use PKI 2.Provide Security to key
4	RSA & ELGamal & Elliptive Curve encryption	1. Security with small Key. 2. High Reliability	1. Improve Security. 2.Reduce Processing Time

IV. CONCLUSION AND FUTUR SCOPE

In this paper we have do the survey of previous and new encryption as well as decryption application and algorithms. In this paper NVSS scheme is used that can share digital image using diverse image media. In this NVSS scheme only one noise share is used to transmit the secret image. In comparison with existing system NVSS scheme reduce the transmission risk of secret image and having friendliness with shares as well as participant. In future work we have doing survey of the more encryption and decryption algorithms. And develop stronger, secure, and easy new algorithm for encryption and decryption for transmission of the secret image using natural shares.

ACKNOWLEDGEMENT

The authors gracefully acknowledge the helpful comments and suggestions of reviewers and appreciate the anonymous reviewers for their valuable comments.

REFRENCES

[1] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia,"Incrementing visual cryptography using random grids," *Opt. Commun.*,vol. 283, no. 21, pp. 4242–4249, Nov. 2010.

[2] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology*, vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[3] P. L. Chiu and K. H. Lee, "A simulated annealing algorithm for general threshold visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 992–1001, Sep. 2011

[4] K. H. Lee and P. L. Chiu, "Image size invariant visual cryptography for general access structures subject to display quality constraints," *IEEE Trans. Image Process.*, vol. 22, no. 10, pp. 3830–3841, Oct. 2013

[5] C. N. Yang and T. S. Chen, "Extended visual secret sharing schemes: Improving the shadow image quality," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 21, no. 5, pp. 879–898, Aug. 2007.

[6] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, "Extended capabilities for visual cryptography," *Theoretical Comput. Sci.*, vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.

[7] Z. Zhou, G. R. Arce, and G. D. 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. D. Crescenzo, "Halftone visual cryptography via error diffusion," *IEEE Trans. Inf. Forensics Security*, vol. 4, no. 3, pp. 383–396, Sep. 2009

[9] F. Liu and C. Wu, "Embedded extended visual cryptography schemes," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 2, pp. 307–322, Jun.2011