

A Review of Image Steganographic Technique Based On Extended Visual Cryptography Scheme

Harshal S. Tekade¹, Dr. Baisa L. Gunjal²

^{1,2}Savitribai Phule Pune University, Amrutvahini College of Engineering, Sangamner, Maharashtra, India 422608

Abstract: Secret sharing techniques are required when important and sensible information is transferred from one end to another end. User shares data in form of text and images. There are lots of techniques for secret text sharing like encryption of text and sharing keys of decryption, hide text behind particular image known as steganography etc. When particular user wants to share image with another user then visual cryptography techniques are applied for sharing. Basic visual cryptography involves two images. After overlapping of these images properly, user will get secret image. Among these two images, one image containing random pixels and another information contains secret information. Required information cannot be retrieved unless and until both images are overlapped properly. User can print these images on semitransparent papers and later they can overlap it manually which is one of the advantages. These visual cryptographic techniques are having number of controlling parameters like image quality, image height and width while sharing etc. In this visual cryptography decoding part is done by human visual system without any computation. This visual cryptography can be extended by increasing the overlapping layers. By working on unfocused areas of this visual cryptography like maintaining contrast of reconstructed image, increase in size of original image, additional processing for colored images etc.

Keywords: Visual cryptography, steganography, decryption, secret sharing, overlapping.

1. Introduction

Secret sharing computation generally required additional computation and machines / computers for encryption and decryption which is overhead. Hence Shamir and Naor proposed solution for this by promoting visual cryptography technique.

Though it is not required any special computational logic and supporting computational device, it is having some serious problems like pixel expansion in which generated share images are larger. This cause extra consumptions of space required for storage also distortion in original image is also an issue. Hence this area should be focused. Some paper focused on it and approach towards solution with probability visual cryptography which is good for binary images and quality of image degrades in it due to random behavior of probability. Hence there must be techniques that generated unexpanded shared images. Random Grid Visual Secret Sharing techniques focused on useless expansions of shared images. One of the major things is unnoticed in it that numbers of meaningless shared images are generated which is difficult to manage keep track of it. Also meaningless image transaction can drag attention of outsider and he may guess that secret sharing is carried out. Hence they can try to decode it and security issue may arise. To rectify it "meaningful" secret sharing images are used. Processes used for it again faced pixel expansion problem. Hence there must be focus on process in which shared images must be meaningful with resolved pixel expansion problem.

2. Related Work

We have IEEE paper for reference and as base paper [1] which promotes and discussed modified scheme for visual cryptography.

Technique proposed by Naor and Shamir for visual

cryptography [2] is having some drawbacks like shared images are facing pixel expansion problem.

To avoid this pixel expansion problem paper [3] proposed a solution and land on solution of probability visual cryptography schemes. It propose (k, n) visual secret sharing scheme for black and white image encoding. In this they used probabilistic visual cryptography schemes and avoids pixel expansion problem. This technique is good for binary images and drawback is shared images has poor quality as far as display is concern. By using conventional visual secret sharing schemes paper [4] also discussed about pixel expansions and non-expandable schemes are implemented. These techniques are also facing low image quality problem. At the same time grey images have problems to encode and decode as black and white pixels are considered in it.

Paper [5] work on grey images visual cryptography, managed pixel expansion problem at certain extend and tried to improve the image quality. But this technique works well for grey scale images only.

New technique and solution to the pixel expansion problem is discussed in [6]. Technique is Random Grid Visual Secret Sharing (RGVSS). In this technique pixel is treated as grid and random variable is used to encrypt the secret image.

Paper [7] extends [6] and provides some models for encryption and random grid based visual secret sharing. These schemes are using 2 x 2 threshold schemes for encryption.

Further to make this scheme more complex in [8] same author proposed a 2 x n threshold schemes.

Later this idea is extended in [9] and n x n threshold schemes are proposed which is based on random grid and these are

used for encryption and generate grids which are cipher one.

These shared images are with great count and can generate image management problems as far as sharing of these secrets are concern also one more thing is that these meaningless share image sharing can drag the attention of hackers or security breakers. Hence new concept is discussed in which meaningful images are used for secret sharing. Here steganography is then utilized to generate meaningful share-images in visual cryptography. This idea is discussed in [10]. For meaningful colored/grey share images halftone and color decomposition and composition techniques are discussed in [11].

To improve the recovered image quality paper [12] proposed a halftone visual cryptography concept. In this cluster and void algorithm is used for binary image which is secret one and it then convert it into several halftone images having this secret information. It extends image quality to good level. Further two color images are used to hide one color image scheme in proposed for color secret image sharing in [13]. All of these techniques are using pixel expansion technique hence these shared images are four to nine times larger than original image. Hence efficient space management issue is generated.

Paper [14] proposed a progressive VC scheme which generates meaningful share images but suffering from pixel expansion problem in which 4 times larger share images are generated. [15] Also work for non-pixel expansion but it requires computation device to decode secret image from share images. [16] Presents solution for the management of lots of meaningless shared images. It designed user friendly random grid visual secret sharing it also deals with pixel expansion problem. Here basic drawback of system is in some situation if proper black pixels are not taken from secret images then it is impossible to show the content of secret image also in this only one picture is used as a cover image.

Watermarking and visual cryptography is used to provide copyright protection on black and white images [17]. This method ensures good transparency and robustness and does not allow pixel expansion.

Genetic Algorithm and Visual Cryptography is used along with steganography for enhancing the security on color images [18]. LSB insertion method is used to embed original message into the image. Genetic Algorithm is used to modify the pixel location of stego image. Using Genetic Algorithm's cross-over concept the column pixel shuffling and row pixel shuffling happens respectively which makes the detection of original message complex. The scheme shows pixel expansion.

[19] Also uses visual cryptography along with steganography and genetic algorithm. The scheme can be used for gray scale and colored images and is resilient against RS attack. [20] In this paper, HVC construction methods based on error diffusion are proposed. In this the contrast condition of the decoded image is satisfied. Furthermore, the shares do not suffer any interference from other shares.

The concept of Visual Information Pixel (VIP) synchronization is introduces along with error diffusion to attain a color visual cryptography encryption method to produce meaningful color shares having high visual quality [21]. This scheme considers relationship throughout color channels as well as the issue of colorful noise-like random patterns and pixel expansion.

[22] In this, the scheme uses (m, n) visual secrete sharing scheme which shares m binary secret images into n rectangular gray level share images. It uses Extended Visual Cryptography scheme (EVCS) to have meaningful shares that can be easily managed and reduce attention of unauthorized users. This scheme succeeds in improving contrast of recovered images with use of inspection function.

[23] This paper proposes a scheme which uses error diffusion halftoning for color visual cryptography encryption. This scheme reduces the time required for the process of encryption and decryption which results in fast execution time. The error diffusion used improves the visual quality of the encrypted shares as well as the decrypted secret image.

3. Analysis

From literature survey it is analyzed that there is misbehavior between qualities of secret image when it is recovered from shares images if there contrast is not perfect. Also if we modify the technique to enhance the security then pixel expansion problem is occurred and generates space management problem. Hence mismatched parameters like pixel expansion ration, image quality, pixel contrast should be balanced which is not the case in above papers.

4. Construction of Proposed System

There must be proposed system that firstly finds good solution for pixel expansion problem. Also we are sharing secret hence by balancing pixel expansion problem there should be focus on strong encryption or secret image technique. To achieve contrast of the shared image to great extend there must be probabilistic technique that helps to achieve high quality of recovered image.

Along with this proposed system must be user friendly. This system should not require heavy computational devices, gadgets etc. Meaningful shared images should be considered in proposed system so that hackers should not attract as they can be attracted if meaningless images are shared for secret sharing. Also these shared images are easy to carry and easy to manage and it must be light weight to transact. Also this system must consider every possible pixel in cover image and secret image for encryption so that contrast of stack and share images can be achieved which is good from recovered image quality point of view. Also encryption process must be very dynamic and flexible. It should not have restrictions on count of cover image selection and quantity of black pixel selection.

5. Conclusion

We have to adopt user friendly visual secret sharing. To make it popular we have to consider user friendly secret sharing schemes also. Random Grid Visual Secret Sharing should be extended having this adoptability of user friendly techniques with non-pixel expansion techniques achieving good quality of recovered image.

6. Acknowledgment

We would like to thank family members, friends and teachers for their support and precious guidance.

References

- [1] Young-Chang Hou, Shih-Chieh Wei and Chia-Yin Lin, "Random-grid-based Visual Cryptography Schemes", in IEEE Transactions on Circuits and Systems for Video Technology, vol. 24, no. 1, part 2, pp. 733-744, 2014.
- [2] M. Naor and A. Shamir, "Visual Cryptography", in Advances in Cryptology-EUROCRYPT '94, LNCS 950, Springer-Verlag, pp. 1-12, 1995.
- [3] R. Ito, H. Kuwakado and H. Tanaka, "Image size invariant visual cryptography," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E82-A, no. 10, pp. 2172-2177, 1999.
- [4] C. N. Yang, "New visual secret sharing schemes using probabilistic method," Pattern Recognition Letters, vol. 25, no. 4, pp. 481-494, 2004.
- [5] S. F. Tu and Y. C. Hou, "Design of visual cryptographic methods with smooth-looking decoded images of invariant size for gray level images," Imaging Science Journal, vol. 55, no. 2, pp. 90-101, 2007.
- [6] O. Kafri and E. Keren, "Encryption of pictures and shapes by random grids," Optics Letters, vol. 12, no. 6, pp. 377-379, June 1987.
- [7] S. J. Shyu, "Image encryption by random grids," Pattern Recognition, vol. 40, no. 3, pp. 1014-1031, 2007.
- [8] S. J. Shyu, "Image encryption by multiple random grids," Pattern Recognition, vol. 42, no. 7, pp. 1582-1596, 2009.
- [9] T. H. Chen and K. H. Tsao, "Visual secret sharing by random grids revisited," Pattern Recognition, vol. 42, no. 9, pp. 2203-2217, 2009.
- [10] G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson, "Extended capabilities for visual cryptography," Theoretical Computer Science, vol. 250, pp. 143-161, 2001.
- [11] Y. C. Hou and J. H. Wu, "An extended visual cryptography scheme for concealing color images," in Proceeding of The 5th Conference on Information Management and Police Administrative Practice, Taoyuan, Taiwan, pp. 62-69, 2001.
- [12] Z. Zhou, G. R. Arce and G. D. Crescenzo, "Halftone visual cryptography," IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2453, 2006.
- [13] C. C. Chang, W. L. Tai and C. C. Lin, "Hiding a secret color image in two color images," Imaging Science Journal, vol. 53, no. 4, pp. 229-240, 2005.
- [14] W. P. Fang, "Friendly progressive visual secret sharing," Pattern Recognition, vol. 41, pp. 1410-1414, 2008.
- [15] C. C. Thien and J. C. Lin, "An image-sharing method with user-friendly shadow images," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 12, pp. 1161-1169, 2003.
- [16] T. H. Chen and K. H. Tsao, "User-friendly random-grid-based visual secret sharing," IEEE Transactions on Circuits and Systems for Video Technology, vol. 21, no. 11, pp. 1693-1703, 2011.
- [17] Ren-Junn Hwang, "A Digital Image Copyright Protection Scheme Based on Visual Cryptography," Tamkang Journal of Science and Engineering, vol. 3, no. 2, pp. 97-106, 2000.
- [18] Rehana Begum R.D and Sharayu Pradeep, "Best Approach for LSB Based Steganography Using Genetic Algorithm and Visual Cryptography for Secured Data Hiding and Transmission over Networks," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 4, Issue 6, pp. 1-3, June 2014.
- [19] Ravindra Gupta, Akanksha Jain and Gajendra Singh, "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics," International Journal of Computer Science and Information Technologies, vol. 3, pp. 4366 - 4370, 2012.
- [20] Zhongmin Wang, Gonzalo R. Arce and Giovanni Di Crescenzo, "Halftone Visual Cryptography via Error Diffusion," IEEE Transactions on Information Forensics and Security, vol. 4, no. 3, pp. 383-396, Sept 2009.
- [21] Grishma R. Bhokare and C. J. Shelke, "Color Extended Visual Cryptography Using Error Diffusion with VIP Synchronization," International Journal of Engineering and Computer Science, vol 2. Issue 10, pp. 3066-3069, Oct 2013.
- [22] Aarti and Pushpendra K Rajput, "Multiple Secret Sharing Scheme with Gray-Level Mixing using EVCS," International Journal of Computer Applications on Issues and Challenges in Networking, Intelligence and Computing Technologies - ICNICT 2012, pp. 1-6, Nov 2012.
- [23] Anuprita Mande and Manish Tibdewal, "A Fast Encryption Algorithm for Color Extended Visual Cryptography," International Journal of Emerging Technology and Advanced Engineering, vol 3, Issue 4, pp. 1-8, April 2013.