Biosc.Biotech.Res.Comm. Special Issue Vol 13 No 14 (2020) Pp-268-272

BBRC
Bioscience Biotechnology Research Communications

A Review on Visual Secret Sharing Schemes for Binary, Gray & Color Image

Vishal V. Panchbhai[1*] and Suchita W. Varade[2]
[1,2]*Department of Electronics & Telecommunication, Priyadarshini College of Engineering, Nagpur, India*

ABSTRACT

Today's fast growing world of the internet is acquiring more attention of people. People are using more services provided by e-commerce and social sites, they exchange multimedia data over the internet thus there is need of data confidentiality, integrity and availability. Cryptography is used to solve some of above problems. Visual Secret Sharing (VSS) schemes capable to handle the problem related with sharing of visual data. But display quality, variations in share sizes, insecurity in transmission of shares, originality of share, pixel expansion, etc. are still open problems. The aim of this paper is to review and examine numerous existing visual secret sharing schemes, which tries to solve above problems. This information will be useful to researchers who would like to work in this area.

KEY WORDS: VISUAL SECRET SHARING SCHEME (VSSS), VISUAL CRYPTOGRAPHY (VC), VSSS PERFORMANCE MEASURES

INTRODUCTION

Today many people are using the internet to transfer their multimedia data. This data transfer on an open network environment is not safe because an intruder tries to check, alter or access your confidential data so there is an urgent need to provide security to this data. Security will be provided in terms of confidentiality, integrity and an availability of data. Confidentiality limits access to data and which is managed by encryption of data. Integrity is related to reliability of data and which is managed by hashing algorithm and availability is assurance of getting unbreakable service from a reliable source. In order to tackle the problem of data encryption and hiding, cryptography and stegnography techniques are used respectively.

Visual Secret Sharing Scheme (VSSS) is the cryptography technique for visual sharing of secret images. Naor M. et al.(1994) invented this cryptography technique in year 1994. They proposed and demonstrate k out on n VSSS. In this scheme 'n' shadows / shares are generated by a dealer on transparencies. When 'k' shadows out of 'n' shadows are stack together then only secret data will be visible otherwise not. Following figure 1 shows an example of 2 out of 2 visual cryptography scheme (VCS) by putting four sub-pixel in the shadow image for each pixel in a secret binary image. Secret will be reconstructed using Boolean OR operation. It will increase the size of output image.

Visual data may be monochrome image, gray image or color image. Many researchers work on different visual data to solve various existing problems such as a quality of reconstructed image, variations in share sizes, insecurity in transmission of shares, originality of share, etc. In this paper, we study and analysis various VSS schemes based on some performance parameters.

ARTICLE INFORMATION

*Corresponding Author: vishalpanchbhai82@gmail.com
Received 18th Oct 2020 Accepted after revision 29th Dec 2020
Print ISSN: 0974-6455 Online ISSN: 2321-4007 CODEN: BBRCBA

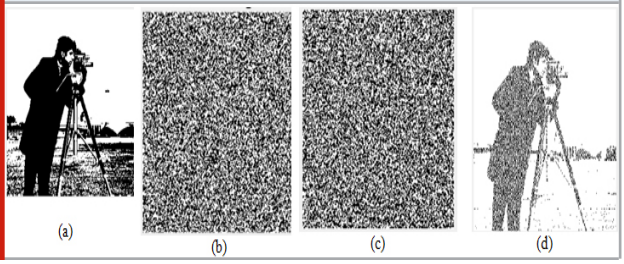
Thomson Reuters ISI Web of Science Clarivate Analytics USA and Crossref Indexed Journal

NAAS Journal Score 2020 (4.31)

Online Contents Available at: http//www.bbrc.in/
Doi: http://dx.doi.org/10.21786/bbrc/13.14/63

Various Visual Secret Schemes: Visual secrete sharing scheme is a method of generating two or more shadows with or without making changes and retrieving visual data by combining all or some of them. The existing VSS schemes are mainly classified based on black and white, gray scale & color images (secret image type) and discuss in the next section.

Figure 1: a) Cameraman image as a secret image (256 x 256) b) share 1 (512 x 512) c) share 2 (512 x 512) d) reconstructed Secret image (512 x 512)



i) VSS schemes on black and white image: The VSS scheme based on a black and white image contains secret image in black and white format. The OR based visual cryptography is mostly used in the scheme stated above. Naor et al. (1994) proposed cryptographic scheme based on black and white image, in this scheme, 'n' number of noise like shares created by dealer and it is distributed among the ' n' number of users, secret image can be visualized by overlapping at least 'k' numbers of user shares otherwise not. This scheme is called as (k,n) VSSS. Kumar et al. (2014) proposed (2,n) threshold based approach for a visual cryptography scheme on black and white image using hadamard matrices. In this scheme two groups of shares are available namely qualified set and forbidden set, secrete data will be discovered through overlapping at least two shares from a qualified set without any cryptographic computation.

Lee et al. (2013) define General Access Structure (GAS) based VCS approach to solve the problem of increased size of generated shares through encryption of pixels in a secret image by column vectors. In GAS the dealer specified reasonable combinations of shares to be used for decryption. Hou et al. (2011) tried to solve a pixel expansion problem by using progressive VCS. To solve the problem of increased size of generated shares, Lee et al. (2012) proposed simulated annealing based algorithm for encryption and use stamping algorithm for adding cover to a black and white secrete image. To address the above problem Fan et al. (2018) proposed random grid and XOR based VSSS.

As noise like share is not user friendly and it gives suspiciousness to intruder thus some researchers worked on the generation of meaningful share. To address above problem Liu et al. (2011) proposed VSS scheme based on embedded extended visual cryptography, S. Shyu (2014) proposed (k,n) VCS based on integer linear programming, Yang et al. (2016) proposed scheme in which shares are generated by (k, n) VSSS and then color pixels are added in shares to generate meaning full shares.

ii) VSS schemes on the gray scale / color images: The VSS scheme based on the gray scale / color image contains secret image in gray scale or color image format. Boolean functions such as OR, EX-OR, EX-NOR, AND & NOT based visual cryptography operations are performed in this. Luo et al. (2014) proposed a VSS technique, based on transfer of color, in which secret color image is braked into red, green and blue 8-bit planes then halftone algorithm is used to generate shares from this planes. To recover secrete color image computer computations are required. Another approach using Floyd's halftoning proposed by Kar et al. (2018) this scheme is based on the CMY color model. In this scheme secrete image is decomposed into cyan, magenta and yellow planes first then halftoning algorithm is used to generate shares.

To address the problem of pixel expansion and to increase security of black and white, gray and color image shares Wu et al. (2014) proposed two solution methods for GAS based scheme, first is XOR based VC which is useful to solve an expanded size problem of shares and second is based on an adaptive area enhancing VC using the boolean EXOR operation which is useful to increase security of share. Another solution based on sharing matrix and encryption of an image proposed by Bao et al. (2017) which is useful to generate lossless (k,n) VSSS. Lee et al. (2014) proposed binocular VCS for black and white & gray secret image without increasing the size of shares and hide the shared pixel in another image.

To increase contrast of a recovered gray scale image, Wang et al. (2013) developed VC scheme using basis matrices and reversing techniques. Another approach is proposed by Wu et al. (2013) based on a generalized random grid. To increase the visual appearance of recovered image various researchers proposed different approaches which will be discussed here. To address above problem, Mhala et al. (2018) suggested solution based on block-based progressive VSS and additional data hiding techniques for gray and color secret image. Deepa et al. (2014) suggested a color image based VSS scheme using the artificial bee colony algorithm to resolve the above problem.

To address the problem of secure transmission of color secret image shares, Lee et al. (2014) proposed algorithm that uses various carrier media to send shares of a secret image generated through the natural share based VSSS. Another method provided by Abdelfatah (2020) uses two stage encryption, elliptic curve encryption based on first stage and XOR operation is carried out between the first stage output and a pseudorandom sequence generated by multi chaotic pseudo random generator algorithm. Visual cryptography can be pooled with steganography for a meaningful share generation in order to improve the security of secret messages. Least Significant Bits (LSB) based approach is suggested by Gupta et al. (2012) to encode a secret message by using genetic algorithm and it is useful to retain an original characteristics of the images.

VSS Performance Analysis Parameters: Performance of visual secret sharing schemes can be evaluated based on the some of the following parameters.

1) Peak Signal to Noise Ratio (PSNR): PSNR is the most commonly used metric to check the visual appearance of a recovered image (Ahmed et al., 2016). It gives the peak of error between an original and recovered image. Ideally PSNR value should be infinity and practically as large as possible. PSNR value of a reconstructed image should be greater than 30 dB is acceptable.

2) Mean Squared Error (MSC): MSE (Ahmed et al., 2016) gives a mean square of the differences between the respective pixels of the two images. Ideally MSE value should be zero and practically as small as possible.

3) Correlation Coefficient (CC): The quality of cryptosystem is determined by correlation coefficient metric (Ahmed et al., 2016). It is ideally one for an indistinguishable image and zero for an uncorrelated image. CC value should be minimum (towards zero) recommended.

Table 1. Performance Analysis of Various VSS Schemes

Reference	Secret Image Format	Encryption Method	No. of shares	Noiselike / Meaning-ful Shares	Pixel expansion
(Value of m) (Naor et al., 1994)	Binary	Boolean matrix based	2,3,4	Noiselike	4 & 9
(Kumar et al., 2014)	Binary	Threshold based VCS using Hadamard matrices	2	Noiselike	4
(Lee et al., 2013)	Binary	GAS based VC algorithm	5	Noiselike	NIL
(Lee et al., 2012)	Binary	progressive VC algorithm	6	Noiselike	NIL
(Fan et al., 2018)	Binary	Random grid and XOR based VC algorithm	2	meaningful	NIL
(Shyu, 2014)	Binary	Threshold based VCS with meaningful shares	2 to 7	Meaningful	4 to 77
(Yang et al., 2016)	Binary	Colored black and white visual cryptography scheme	2, n	Meaningful	4, 2n
(Lee et al., 2014)	Binary	binocular VCS	2 to 10	Noiselike	NIL
(Wu et al., 2013)	Binary	Generalized random grid based VC algorithm	2, n	Noiselike and meaningful	NIL
(Jana et al., 2014)	Binary	Self defined algorithm with stego data for fake share identification	4	Noiselike	4
(Gupta et al., 2012)	Binary (text to binary)	VC based on pseudorandom number and pixels exchange.	3	Noiselike	NIL
(Liu et al., 2018)	Gray	Embedded extended VCS algorithm	2, 3	Meaningful	Present
(Wang et al., 2013)	Gray	Reversible VCS (GRVCS) by using basis matrices	2, m	Noiselike	Present
(Hou et al., 2011)	Gray and color	Halftoning and color decomposition based	2, 3	Noiselike	4
(Kar et al., 2018)	Gray and color	Self generated algorithm is used on halftone image	3	Noiselike	4
(Mhala et al., 2018)	Gray and color	Block based progressive VC with additional data embedding facility using DCT technique	4 to n	Noiselike and meaningful	NIL
(Luo et al., 2014)		Color VCS based on color transfer and halftone method	2,3	Noiselike	2
(Deepa et al., 2014)	Color	Visual Cryptography Scheme using Artificial Bee Colony algorithm	2	Meaningful	4
(Bao et al., 2017)	Binary, gray and color	Sharing matrix and image encryption based algorithm	4,6,8,	Noiselike	NIL

4) Pixel Expansion: In most of VSSS, shares are generated by placing m sub-pixels in shares for each pixel in a secret image. This will increase the size of each share by m times as compared to a secrete image is called as pixel expansion.

5) Structural Similarity Index quality Measure (SSIM): SSIM is used for measuring the resemblance between an original & recovered image. SSIM value ranges from zero to one. Ideally SSIM value should be one but practically it should be nearer to one.

Performance Analysis of Various VSS Schemes: Following table – 1 shows performance analysis of various VSS schemes based on secret image format, encryption / share generation method, number of shares, generated shares are meaningful or noise like and pixel expansion. From this table it is found that various researchers work on different techniques to solve the problem in existing VSS schemes such as an increase size of generated share, a meaningful share generation, secure data transmission, fake share identification, etc. It is also found that many researchers work on binary secret image format only and very few works on gray and color secret image.

DISCUSSION

From the study and analysis of different research work, on the visual secret sharing scheme based on performance measure, helps us to find the limitation / area where research may be carried out to get the better result. The visual secret sharing schemes with meaningful shares are more user-friendly and secure for transmission than noise-like shares thus it encourages to develop algorithm for generation of meaningful shares. Cheating prevention / fake share identification based VSS is required to increase security, very few works is done in that direction. Whatever data is embedded in shares it will create the blocking artifact in a recovered secret image, thus there is need to eliminate this artifact to increase the visual appearance of a recovered secret image. Most of the VSS schemes based on gray and color image use large computation at receiver side to decrypt the secret image which should be minimized to get the better result as limited power and processor capability is available with most of handheld devices now a days.

CONCLUSION

In today's world of the internet, a significant role played by the visual secret sharing scheme for data confidentiality over an open network environment. In this paper various existing schemes on visual secret sharing is studied and analyzed. It is found that various researcher contributed their best to solve the existing problems in VSS schemes such as increase in size of generated share, a meaningful share generation, secure data transmission, originality of share , etc.. Still problems are open to do research as most of work done on binary visual data and very little work done on grayscale and color visual data.

REFERENCES

Ahmed, N., Asif, H.M., & Saleem, G. 2016. A Benchmark for Performance Evaluation and Security Assessment of Image Encryption Schemes. International Journal of Computer Network and Information Security, 8, 18-29.

Abdelfatah, R.I. 2020. Secure Image Transmission Using Chaotic-Enhanced Elliptic Curve Cryptography. IEEE Access, 8, 3875-3890.

Bao, L., Yi, S., & Zhou, Y. 2017. Combination of Sharing Matrix and Image Encryption for Lossless (k,n) -Secret Image Sharing. IEEE Transactions on Image Processing, 26, 5618-5631.

Fan, T., & Chao, H. 2018. User-friendly XOR-based visual secret sharing by random grid. IET Inf. Secur., 12, 398-403.

Deepa, A., & Bento, B. 2014. Embedded Extended Visual Cryptography Scheme for Color Image using ABC algorithm. 2014 12th International Conference on Signal Processing (ICSP), 653-657.

Gupta, R., Jain, A., & Singh, G. 2012. Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics, International journal of computer science and information technologies, 3, 4366-4370.

Hou, Y., & Quan, Z. 2011. Progressive Visual Cryptography with Unexpanded Shares. IEEE Transactions on Circuits and Systems for Video Technology, 21, 1760-1764.

Kar, C., Kar, S.K., & Banerjee, S. 2018. An Approach for Visual Cryptography Scheme on Color Images, 501-508.

Jana, B., Mallick, M., Chowdhuri, P., & Mondal, S. 2014. Cheating prevention in Visual Cryptography using steganographic scheme. 2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), 706-712.

Kumar, M., & Singh, R. 2014. A (2, n) and (3, n) Visual Cryptography Scheme for Black and White Images, International journal of science and research, vol. 3, pp.574-577

Lee, K., & Chiu, P. 2013. Image Size Invariant Visual Cryptography for General Access Structures Subject to Display Quality Constraints. IEEE Transactions on Image Processing, 22, 3830-3841.

Lee, K., & Chiu, P. 2012. An Extended Visual Cryptography Algorithm for General Access Structures. IEEE Transactions on Information Forensics and Security, 7, 219-229.

Lee, K., & Chiu, P. 2014. Sharing Visual Secrets in Single Image Random Dot Stereograms. IEEE Transactions on Image Processing, 23, 4336-4347.

Liu, F., & Wu, C. 2011. Embedded Extended Visual Cryptography Schemes. IEEE Transactions on Information Forensics and Security, 6, 307-322

Lee, K., & Chiu, P. 2014. Digital Image Sharing by Diverse Image Media. IEEE Transactions on Information Forensics and Security, 9, 88-98.

Luo, H., Chen, H., Shang, Y., Zhao, Z., & Zhang, Y. 2014. Color transfer in visual cryptography. Measurement, 51, 81-90.

Mhala, N.C., Jamal, R., & Pais, A.R. 2018. Randomised visual secret sharing scheme for grey-scale and colour images. IET Image Process., 12, 422-431.

Naor, M., & Shamir, A. 1994. Visual Cryptography.

EUROCRYPT, 1-12.
Shyu, S.J. 2014. Threshold Visual Cryptographic Scheme with Meaningful Shares. IEEE Signal Processing Letters, 21, 1521-1525.
Wu, X., & Sun, W. 2014. Extended Capabilities for XOR-Based Visual Cryptography. IEEE Transactions on Information Forensics and Security, 9, 1592-1605.
Wang, D., Song, T., Dong, L., & Yang, C. 2013. Optimal Contrast Grayscale Visual Cryptography Schemes With Reversing. IEEE Transactions on Information Forensics and Security, 8, 2059-2072.
Wu, X., & Sun, W. 2013. Generalized Random Grid and Its Applications in Visual Cryptography. IEEE Transactions on Information Forensics and Security, 8, 1541-1553.
Yang, C., Sun, L., & Cai, S. 2016. Extended color visual cryptography for black and white secret image. Theor. Comput. Sci., 609, 143-161.