ISSN: 2321-7782 (Online)
Volume 3, Issue 12, December 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

A Review on Various Digital Image Secret Sharing Schemes

Minal Bodke[1]
ME Student in Information Tech., PCCOE
Pune, India

Nilam Kate[2]
ME Student in Information Tech., PCCOE
Pune, India

J. V. Katti [3]
Prof., Information Tech., PCCOE
Pune, India

Abstract: ***In today's world, secret data is more pretended to hack easily by unauthorized user. These hacked data may be misused in various ways. So, the field of Cryptography plays an important role to secure data. There are various security media's used to transmit secret information from one location to another, and one of them is image media. The intent of this paper is to study different approaches of sharing secret digital images.***

Keywords: Visual Cryptography, Visual secret sharing, Diverse media, Digital image.

I. INTRODUCTION

In today's emerging world of privatization, liberalization, globalization almost every field has become computerized and technologically more advanced for showing of secret images, one of the best techniques with less computation effort is Visual Cryptography. Visual Cryptography is one of the cryptographic techniques. Basically cryptography means converting plaintext (readable text) into cipher text (unreadable text) by using some encryption algorithm and vice versa so that only intended user can read and process the information[1][2].

Visual cryptography was developed by Moni, Naor and Adi Shamir in 1994[3].Visual Cryptography is a secret sharing technique that encrypts the secret images into n shares, and stacking of thus n shares can only reveal the original secret, image. The secret images can be of various forms like images, handwritten documents, photography etc. Sharing delivering such secret image is called as Visual Secret Sharing.

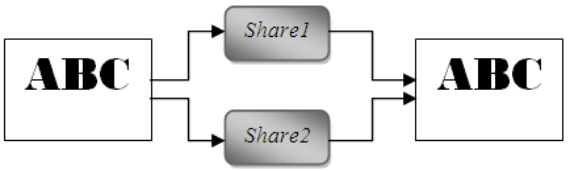

Fig1: Traditional Visual Cryptography Scheme. Original image is divided into two shares and stacking these shares reveals again original image

Visual cryptography for gray level images

Previous efforts in visual cryptography were restricted to binary images which is insufficient in real time applications. Chang- ChouLin, Wen-HsiangTsai proposed visual cryptography for gray level images by dithering techniques. Instead of using gray sub pixels directly to constructed shares, a dithering technique is used to convert gray level images into approximate binary images. Then existing visual cryptography schemes for binary images are applied to accomplish the work of creating shares. The effect of this scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

Visual cryptography for general access structures

In (k,n) Basic model any „k shares will decode the secret image which reduces security level. To overcome this issue the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, where an access structure is a specification of all qualified and forbidden subsets of „n shares. Any subset of „k or more qualified shares can decrypt the secret image but no information can be obtained by stacking lesser number of qualified shares or by stacking disqualified shares. Construction of scheme is still satisfactory in the aspects of increase in relative size and decoded image quality, even when the number of gray levels in the original image still reaches 256.

Halftone Visual Cryptography

The meaningful shares generated in extended visual cryptography proposed by Mizuho NAKAJIMA and Yasushi YAMAGUCHI was of poor quality which again increases the suspicion of data encryption. Zhi Zhou, Gonzalo R. Arce, and Giovanni Di Crescenzo proposed halftone visual cryptography which increases the quality of the meaningful shares. In halftone visual cryptography a secret binary pixel „P is encoded into an array of Q1 x Q2 („m in basic model) sub pixels, referred to as halftone cell, in each of the „n shares. By using halftone cells with an appropriate size, visually pleasing halftone shares can be obtained. Also maintains contrast and security.

Recursive Threshold Visual Cryptography

The (k,n) visual cryptography explained in section I needs „k shares to reconstruct the secret image. Each share consists at most [1/k] bits of secrets. This approach suffers from inefficiency in terms of number of bits of secret conveyed per bit of shares. Recursive threshold visual cryptography proposed by Abhishek Parakh and SubhasKak eliminates this problem by hiding of smaller secrets in shares of larger secrets with secret sizes doubling at every step. When Recursive threshold visual cryptography is used in network application, network load is reduced.

Visual Cryptography for color images

The researches in visual cryptography leads to the degradation in the quality of the decoded binary images, which makes it unsuitable for protection of color image .F.Liu,C.K. Wu X.J. Lin proposed a new approach on visual cryptography for colored images.

Visual Cryptography Regional incrementing

VC schemes mentioned above usually process the content of an image as a single\ secret i.e all of the pixels in the secret image are shared using a single encoding rule. This type of sharing policy reveals either the entire image or nothing, and hence limits the secrets in an image to have the same secrecy property. Ran-Zan Wang proposed Region Incrementing Visual cryptography for sharing visual secrets in multiple secrecy level in a single image.

Extended Visual Cryptography for natural images

All of the VC methods suffer from a severe limitation, which hinders the objectives of VC. The limitation lies in the fact that all shares are inherently random patterns carrying no visual information, raising the suspicion of data encryption. Mizuho NAKAJIMA and Yasushi YAMAGUCHI proposed Extended visual cryptography for natural images constructs meaningful binary images as shares. This will reduce the cryptanalysts to suspect secrets from an individual shares. While the previous researches basically handle only binary images, establishes the extended visual cryptography scheme suitable for natural images.

Progressive Visual Cryptography

The application of digital halftoning techniques results in some downgrading of the original image quality due to its inherently lossy nature and it is not possible to recover the original image from its halftone version. Duo Jin Wei-Qi Yan

,Mohan S, Kankanhalli proposed a new encoding method that enables us to transform gray-scale and color images into monochrome ones without loss of any information. Incorporating this new encoding scheme into visual cryptography technique allows perfect recovery of the secret grayscale or color image.

VSS technique have been developed only for black and white images, there are different approaches for gray scale image, and color image have been proposed but these earlier works resulted in a lower quality of the decrypted image into n-shares that are either encoded, printed on transparency and stored in a digital form[4]. These shares may appear as meaningful images or as a noisy like pixel but it will increase interception risk and arouse suspicion during transmission of these secret shares. It cannot leak any confidential or critical information of the shared secret by any combination of the n-shares images except for all of images.

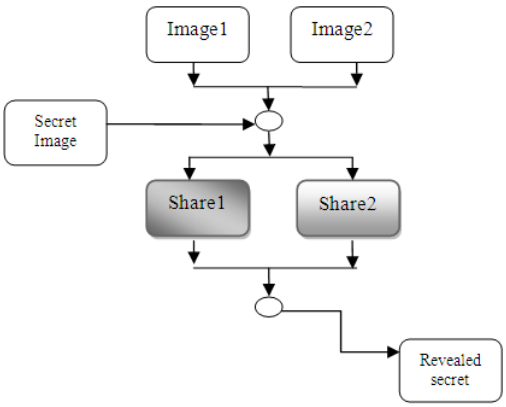

Fig2: Visual Secret Sharing Scheme

Below mentioned are some of the applications of VSS by embedding of an extra confidential image with pair key structure.

- Halftone conversion: In these method the two input images, secret image and the extra confidential image has to be converted into halftone image in order to diffuse the secret image and the extra confidential image in the two input images. Hence halftone conversion can be done by using the Floyd Steinberg dithering process.
- Diffusion: Diffusing the secret image and the extra confidential image into two input image to create share image A and B. Therefore this can be done by swapping each of pixels in the image.
- Pair key structure: The two input image and one secret image has been converted to halftone image. When converting these extra confidential image to halftone and diffuse it with input image, a pair key should be given in order to sender and receiver to get paired mutually.
- Stacking: The two share image that are transmitted via Internet holds secret image, hence to reveal secret image both the share image has to be stacked.
- Shifting: Shifting is the process of placing first share constantly and shifting the second share image to certain unit N/2 to reveal extra confidential image.

Diverse media: Diverse media is used in digital image, printed image and hand-printed pictures.

II. Related Work

The first approach on how to support query operations on encrypted data with bucketization, after the data is encrypted, the ciphertext is concatenated to a bucket number, which is assigned to a specific range that includes the data. When a user requests a query operation, the server uses the bucket numbers to execute the query operation. For example, if a client program wants to retrieve the data in the range between 100,000 and 200,000, it first calculates the numbers of buckets whose union is the

smallest set that covers the queried range. The client program sends the bucket numbers to the database server. The database server searches all the encrypted data whose bucket number is one of the received numbers. The server then, sends the data back to the client. The client can obtain the correct result by filtering out the data that are not in the range after decrypting them. In this case, a larger amount of data transmitted between the client and server than in the case where the database stores unencrypted data items due to the false positives that occur in cases where a bucket has both the data the client wants to retrieve and data that it does not want. In OPE, the order of the underlying plaintexts can be compared only with the computation of sub-linear complexity from the ciphertexts without decrypting them. Owing to such efficiency, more efficient range queries can be supported with OPE compared to the case of using OB. Moreover, the result of range queries on ciphertexts encrypted by OPE does not produce false positives because the comparison ability on ciphertexts can distinguish whether a ciphertext has the plaintext in a specified range when the server has an encryption of two borders of the range being queried in the plaintext space.

III. A Broad Review on Sharing Secret Image Techniques

A. Review based on enhanced VC scheme for secret image retrieval using average filter.

These approach increase the quality of color decode image. In these approach sender takes one secret image which is encoded into n shares, by applying Jarvis halftoning and encoding table and for the decoding process, the share images are used along with decoding table to obtain original secret image. In these approach basically average filter method has been apply to decrease the noise produce during encoding operation so that the quality of the decoded secret image has been increased [8].

So 15-20% of noise gets reduced by using average filter scheme. But in these approach pixel expansion problem is been arised, to overcome the problem further, inverse halftoning can be applied at the time of decoding of the image.

B. Review based on a new color VC scheme with perfect contrast.

For security purpose, researcher has made some technique for color image visual cryptography. In these techniques a new color VC scheme is based upon the modified VC. These approach can share a color secret image over n-1 arbitrary natural images and one noise like share images. Natural image can be grayscale or live photos, landscape photos. In these scheme it does not alter the content of natural images, instead it extract feature images from each natural image during encryption process [7].

These propose technique can effectively reduce the transmission risk problem, and also avoid the pixel expansion problem, and makes it possible to obtain original secret image without any distortion. Hence the proposed scheme can share black and white gray-level or color images in a secure way. But the drawback of the scheme is that it cannot work on the threshold type and multiple images vc.

C. Review based on Information hiding in gray scale images using pseudo-randomized VC algorithm for visual information security.

Security has gained more important information technology has become more popularly. In these schemes a novel method of VC has been used for halftoning images which represent the resultant image in the same size as that of original secret image. Halftone image are nothing but continued stored images, photograph that has been converted into black-white images. So hiding of visual information scheme is based on pseudo randomization and pixel reversal [9].Pseudo random is nothing but a deterministic random bit generator generating a sequence of no whose property approximately the properties o sequence of random numbers.

The proposed scheme reveals pixel expansion and the quality of image. But the drawback of the scheme is that dividing pixel into two or more sub pixel, help secret picture required with additional impairments and poor resolutions.

D. Review based upon Linear equation based VSS

Linear equation is an algebraic equation in which each term is constant or product of constant it can have one or more variables. In this scheme Linear equation of Hill Cipher divide the image into sub images and then the method of random grid is used for sub images construction of an encrypted images. In this scheme Linear Equation are used along with Hill Cipher. Hill Cipher is a substitution technique based on multiplication to encrypt the given plain text[6].

These scheme overcome the security issues and it is more secure and effective .But the drawback of the scheme is it is only used or single secret sharing.

E. Review based on digital image sharing by diverse image media.

In Visual Cryptography secret data is hidden in the shares, these shares are either printed on transparencies or are encoded and stored in a digital form. The shares can be noise-like pixels or as meaningful images, but it will increase interception risk during transmission of shares. Hence VSS schemes suffer from transmission risk problem, so to avoid this problem NVSS.

In these approach it uses (n, n)-NVSS scheme that can share digital secret image over (n-1) arbitrary selected natural image (natural share) and one noise –like share. Natural images such as hand-printed picture or photos, I digital form or in printed form. The natural share which are generated using these schemes remains unaltered which are diverse and innocuous, hence reducing the transmission risk issues. This approach also uses different ways to hide the noise–like share (QR-CODE) to greatly reduce the transmission risk problem or the share [5].So these scheme compared with the existing VSS, these scheme provides highest level of user friendliness for shares and for participant .By transmitting secret image via heterogeneous carrier media thus reducing transmission risk.

IV. Performances Analysis of Various Secret Sharing Scheme.

Performance of VSS is evaluated on the basis of some parameter which is recommended by researchers they are pixel expansion, contrasts, transmission factor or security, quality of image.

Reference	A	B	C	D	E
Quality	Yes	Yes	No	No	No
Contrast	No	No	Yes	Yes	Yes
Pixel Expansion	Yes	Yes	No	No	No
Transmission Factor	Yes	No	Yes	No	No

V. Conclusion

According to the analysis done, Enhanced scheme VC using average filter has reduced the problem of noise by 15-20% ,but it has increased pixel expansion problem. The referred Color VC scheme with perfect contrast has removed the pixel expansion problem. The method Information hiding in gray scale images using pseudo-randomized VC, also overcomes the pixel expansion problem but it has reduced quality of recovered images. Linear equation based VSS scheme has overcome the security issues but it only used with single secret sharing methods. Digital image sharing using diverse image media schemes can effectively reduce the transmission risk problem and provide highest level of user-friendliness both for shares and for participants.

VI. Directions For Future Research

The performance reviews help us to find the drawbacks and future needs of VSS. As a result, the survey work will be supportive for researcher to focus on the suggested various VSS techniques.

References

1. Gajendra Singh ,Vishwa gupta, and Ravindra Gupta," Advance cryptography algorithm for improving data security", Volume 2, Issue 1, January 2012, ISSN: 2277 128X.International Journal of Advanced Research in Computer Science and Software Engineering.
2. Alfred J. Menezes, Paul C. van Oorschot , and Scott A. Vanstone "Handbook of Applied Cryptography" CRC Press 1996.
3. M. Naor and A. Shamir "Visual cryptography " in Advances in Cryptology, vol. 950. New Yark, NY, USA: Springer-Verlag, 1995, pp. 1-12.
4. N.Krishna Prakash and Prof.S.Govindaraju," Visual Secret Sharing Schemes for Color Images using Halftoning", International Conference on Computational Intelligence and Multimedia Applications 2007.
5. Kai-Hui Lee and Pei-Ling Chui. "Digital image sharing by Diverse Image Media" IEEE transactions on information forensics and security, vol. 9,no. 1, January 2014.
6. S. C. Bunker, M. Barasa, A. Ojha, "Linear Equation Based Visual Secret Sharing Scheme" Advance Computing Conference (IACC), 2014 IEEE International
7. Xiao-Yi Liu, Ming-Song Chen, and Ya-Li Zhang, "A New Color Visual Cryptography Scheme with Perfect Contrast", 2013 8th International Conference on Communications and Networking in China (CHINACOM).
8. V. G. Pujari, Prof. S. R. Khot, Prof. K. T. Mane, "Enhanced Visual Cryptography Scheme for Secret Image Retrieval using Average Filter", 2014 IEEE Global Conference on Wireless Computing and Networking (GCWCN).
9. Ch. R. Babu, M.Sridhar, Dr. B. R. Babu, "Information Hiding in Gray Scale Images using Pseudo - Randomized Visual Cryptography Algorithm for Visual Information Security", 978-1-4673-5986-3/13/$31.00 ©2013 IEEE.
10. T Dinesh Babu and G Sujatha ,"Data security for Image Shares by 2- Level Authentication in Visual Cryptography", 2014 IJEDR | Volume 2, Issue 2 | ISSN: 2321-9939.
11. Neha Sharma,Ajay Goyal,Anil Suryavanshi,"Improved NVSS Scheme for Diverse Image Media",2014 International conference on Control,Instrumentation,Commuincation,Computational technologies(ICCICCT).
12. K. H. Lee and P. L. Chiu, "An extended visual cryptography algorithm for general access structures," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 219–229, Feb. 2012.

