ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 7, Issue 2, pp: (142-147), Month: April - June 2019, Available at: www.researchpublish.com

A Secured Image Sharing Encyption Watermarking Schemes

[1]Miss. S. V. Kale, [2]Dr. V. M. Thakare

[1,2]SGBAU, Amravati, India.Author

Email: [1]*snehakale009@gmail.com*, [2]*vilthakare@yahoo.co.in*

Abstract: **Images from various sources are frequently utilized and to be transmitted through the internet for various applications, such as online personal photograph albums, confidential enterprise archives, document storage systems, medical imaging systems, and military image databases are used. These images usually contain private or confidential information so that they should be protected from leakages during the secure transmissions. This paper focuses on different schemes, such as Robust Watermarking Technique based on Texture Matching of the Watermark with the Host Image, A new blind authentication method based on the secret sharing technique with a data repair capability for gray scale document images via the use of the Portable Network Graphics (PNG) image, Integral imaging is a three-dimensional (3D) imaging technique. But some problems exists in each method, So as to overcome the problems that are given in analysis and discussion, The improved "Secured Image Sharing watermarking Technique" sharing method for secure transformation is proposed using the analysis of the various mobility models.**

Keywords: **Encryption, Decryption, Mutation, symmetric Key, Cryptography, Visual security.**

I. INTRODUCTION

The growth of the Internet along with the increasing availability of multimedia applications has given rise to the number of issues in medical science and defence applications. The ease of communication has given rise to several privacy problems which can be addressed by watermarking [1]. Conventional VSS schemes is a technique that encrypts a secret image into *n* shares, Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents [2], but they suffer from two drawbacks: first, there is a high transmission risk because holding noise-like shares will cause attackers' suspicion and the shares may be intercepted. Thus, the risk to both the participants and the shares increases, in turn increasing the probability of transmission failure. Second, the meaningless shares are not user friendly. As the number of shares increases, it becomes more difficult to manage the shares, which never provide any information for identifying the shares[3].

This paper, discusses different secret image sharing schemes such as Robust Watermarking Technique based on Texture Matching of the Watermark with the Host Image[1], A new blind authentication method based on the secret sharing technique with a data repair capability for gray scale document images via the use of the Portable Network Graphics (PNG) image [2], Image encryption technology based on optics is an effective measure to ensure the information security and has gained great interest in the rapid development of communication technologies. Optical encryption methods own many intrinsic advantages, such as high speed and difficulty of unauthorized access. Integral imaging is a three-dimensional (3D) imaging technique which comprises of two optical processes: pickup process and reconstruction process[3].

But these methods also have some problems. To overcome such problems improved version of sharing scheme that is "Secured Image Sharing watermarking Technique" sharing method for secure transformation is proposed using the analysis of the various mobility models.

II. BACKGROUND

Many studies on sharing models have been done to develop the more secured sharing scheme in recent past years. Such schemes are:

Robust Watermarking Technique based on Texture Matching of the Watermark with the Host Image. The watermark is texturized using Arnold transform and matching is found using histogram of gradient and Log Gabor filter. The watermark is inserted at several places in the image to ensure the security of the image in smaller parts. The efficacy of the algorithm is tested in terms of PSNR (peak signal to noise ratio) and NCC (normalized correlation coefficient). [1].

This paper introduces sharing scheme i.e. a new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is proposed[2].

The paper is organized as follows: **Section I** Introduction. **Section II** discusses Background. **Section III** discusses previous work. **Section IV** discusses existing methodologies. **Section V** discusses attributes and parameters and how these are affected on mobility models. **Section VI** proposed methodology. **Section VII** outcome of results. Finally **Section VIII** Conclusion.

III. PREVIOUS WORK DONE

In research literature, many sharing models have been studied to provide various secret sharing schemes and improve the performance in terms of more secured transmission, also method for image watermarking which improves the (i) capacity, and (ii) imperceptibility of the watermarked image.

Palak Jaina et al., (2017) [1] have worked on Protecting the confidentiality of information and to ensure the security of the image in smaller parts.

Che-Wei Lee et al., (2012) [2] has proposed the a new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image.

Long Bao et al., (2017) [3] has proposed a Integral imaging is a three-dimensional (3D) imaging technique which comprises of two optical processes: pickup process and reconstruction process. With the growth of the Internet and the increase of the requirement for image transmission, image encryption and watermarking are becoming more and more important.

M.Karolin et al., (2018) [4] has presented the Cryptography is one of the mathematical techniques that are used to protect images from adversaries and increase the security of communications. Encryption is done by the sender to convert the original grayscale image to encrypted image before sending it via the internet to the other user (recipient). Decryption is done by the receiver to return the ciphered image back to the original image.

Yodai Watanabe et al., (2015) [5] have shown the impact of to maximize the range of the access control of visual secret sharing (VSS) schemes encrypting multiple images. This scheme uses SIRDSs as cover images of the shares of VCSs to reduce the transmission risk of the shares. The encryption algorithm alters the random dots in the SIRDSs according to the construction rule of the *(*2, *n)*-BVCS to produce nonpixel expansion shares of the BVCS.

IV. EXISTING METHODOLOGIES

Many sharing schemes have been implemented over the last several decades. There are different methodologies that are implemented for different secret sharing models i.e Robust Watermarking Technique based on Texture Matching of the Watermark, Visual Secret Sharing Schemes for Plural Secret Images (VSS-q-PI), Threshold Multiple-secret Visual Cryptographic Schemes (MVCS), Secret Image Sharing Procedure, Secret Image Retrieving Procedure, The Two-Phase Encryption Procedure.

A] Robust watermarking technique for textured images: These watermarks can be used to verify the authenticity or integrity of the carrier signal or can be used to show the identity of its owner. The images can be stored in cloud based storages. Here the privacy has to be taken into account. Thus, the image is encrypted using homomorphic encryption scheme and can be accessed by intended persons by decrypting it using homomorphic decryption scheme. Now, Homomorphic cryptosystem has been widely used all over the public cloud. In homomorphic cryptosystem, the user can perform operations on the encrypted data without decrypting the data and get the same result as performed on the original data. Thus, it maintains confidentiality over the cloud based storages [1].

B] Portable Network Graphics (PNG) image: In this a new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares usingthe Shamir secret sharing scheme [2].

C] Integral imaging is a three-dimensional (3D) imaging technique: Integral imaging is a three-dimensional (3D) imaging technique which comprises of two optical processes: pickup process and reconstruction process[3].

D] Visual cryptography schemes (VCSs):

A secret image is encrypted into two shares. Each share is indistinguishable from noise images, and so leaks no information about the secret. On the other hand, the secret image can be reconstructed when both of the shares are superposed. This can be constructed as follows. A pixel in the secret image is encrypted into two sub pixels in each of the two shares. In this proposed scheme, scheme is a (2, 2) secret image sharing scheme, which should guarantee that none of the shadow images can leak any useful information about the secret image [4].

V. ANALYSIS AND DISCUSSION

A robust watermarking technique solve Authentication and integrity verification issues in the images. A Robust Watermarking Technique is based on texture matching of the watermark with the host image. The watermark is texturized using Arnold transform and matching is found using histogram of gradient and Log Gabor filter. The watermark is inserted at several places in the image to ensure the security of the image in smaller parts [1]. A new blind authentication method based on the secret sharing technique with a data repair capability for grayscale document images via the use of the Portable Network Graphics (PNG) image is proposed. An authentication signal is generated for each block of a grayscale document image, which, together with the binarized block content, is transformed into several shares usingthe Shamir secret sharing scheme [2]. Secret sharing (SS) scheme is a cryptosystem which encrypts a secret into multiple shares so that any qualified combination of shares can reconstruct the secret, while any forbidden combination of shares reveals no information about the secret [3].Visual cryptography schemes (VCSs) uses half toning technique to construct meaningful binary images as shares carrying significant visual information. sharing secret images via high quality shares. The visual quality of the halftone is significantly better than that attained by extended VC [4].

TABLE 1: Comparisons between different schemes.

Mobility scheme	Advantages	Disadvantages
Robust Watermarking Technique	This method uses image watermarking which improves the (i) capacity, and (ii) imperceptibility of the watermarked image. Number of issues in medical science and defense applications, rise to several privacy problems which can be addressed by watermarking.	Different algoritham techniques is used to measure efficacy of the algorithm in terms of PSNR (peak signal to noise ratio) and NCC (normalized correlation coefficient).
Portable Network Graphics (PNG) image	Simple to implement. Lower computational cost. Propose an authentication method that deals with binary-like greyscale document images instead of pure binary ones and simultaneously solves the problems of image tampering detection and visual quality keeping.	The image authentication problem is difficult for a binary document image because of its simple binary nature that leads to perceptible changes after authentication signals are embedded in the image pixels.

Integral imaging is a three-dimensional (3D) imaging technique.	Image encryption technology based on optics is an effective measure to ensure the information security and has gained great interest in the rapid development of communication technologies. Optical encryption methods own many intrinsic advantages, such as high speed and difficulty of unauthorized access.	The drawback of this method cannot predict the interference beyond the Gaussian. Due to more complex and dynamic nature of method it takes more time.
Visual Cryptography Schemes (VCS)	The advantages of this method are its simplicity, high imperceptibility and high capacity.	This method is a very fragile method and does not tolerate any manipulation. Even slightest modification to the image or change of format destroys the hidden data.

VI. PROPOSED METHODOLOGY

Secret image sharing scheme is important and difficult task to analyse and discuss about various methods based on different parameters i.e accuracy, transmission, time, throughput, delay, capacity, pixel value etc for different sharing models. There are still problems which trouble in this field. New sharing method called “secret image sharing with encryption decryption” model for secret sharing model is propose here to overcome the problems of this model. This section describes the feature extraction module that extract feature images from the natural shares. The proposed system consists of a original-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. For this process the share contain arbitrary number of original natural images and one noise like share. Visual cryptography is a method used to encrypt a secret image into n shares (share1, share2,..) in which every participant holding one or more shares.

The proposed (n, n)-NVSS scheme can encipher a truecolor secret image by n- 1 natural shares and one noise like share. Before encryption (resp. decrypt) of each bit-plane of the secret image, the encryption algorithm first extracts n-1 feature matrices from n - 1 natural shares. Then the bit-plane of the reconstruct (secret image) feature matrices execute the XOR operation. Therefore, to encrypt (resp. decrypt) a true-color reconstruct (secret image), the encryption (resp. decryption) procedure must be performed iteratively on the 24 number of bit-planes. The input natural shares (N1,…..,Nn+1_)of the scheme include np printed images and nd digital images (np > 0, nd > 0, and n =np +nd + 1). The np printed images must be processed and transformed into digital form in the image preparation process.

Encryption:

Step 1: Preprocessing -Embedding.

The cover image is divided into blocks of size 64×64.Then the following embedding algorithm is performed which consists of six main stages:

1) Firstly basic texture segmentation is done to distinguish between textured regions and non-textured regions in the cover image.

2) In textured region, adaptive logo scrambling is done by Arnold Transform and lossless rotations and in non-textured region only lossless rotation is performed .

3) The dissimilarity between the host blocks and logo images are found by histogram of gradient (Hog) and Log Gabor filters (Log).

4) The perfect match of texturized logo image corresponding to each host block is obtained.

5) Embedding is done by using Discrete Cosine Transform (DCT)for host image and weighted Singular Value Decomposition (SVD) for logo image.

6) Watermark Extraction is done by the inverse process.

Step 2: Watermark embedding

The watermark embedding algorithm consists of following stages:

Step 1: Firstly the 2-D DCT of the host image is taken.

Step 2: SVD of the logo image is taken.

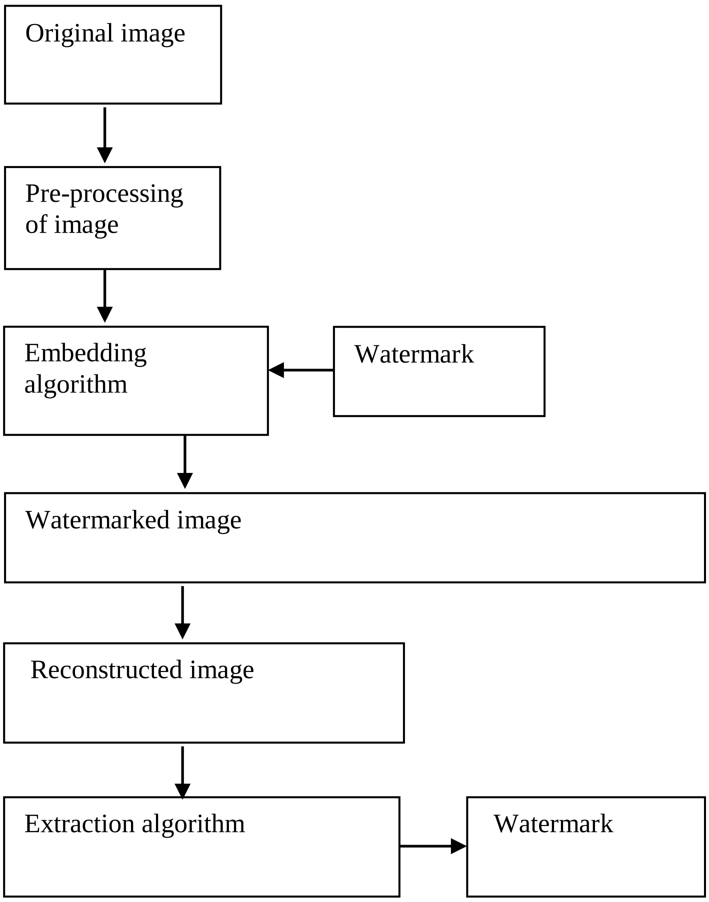
Step 3: Weights selection.

Step 4: Embedding of the logo image in the host image is done by modifying the DCT coefficient of the host image.

Step 3: Extraction. 'Embedding' is performed to hide the logo at the transmitting side and 'extraction' is performed at the receiving side to judge the ownership.

The imperceptibility of the proposed algorithm is very high on different types of images.

Diagrammatic representation of proposed method is shown below:



VII. OUTCOME AND POSSIBLE RESULTS

In this way the proposed method is performing for the secure transformation model when image moves out of network. With the help of the Low-complexity algorithms will ensure efficiency in terms of computation time for embedding and extraction. Robust watermark is a digital watermark that resists a selected class of transformations. Robust watermarks are used in copy protection applications, authentication and secure information.

VIII. CONCLUSION

This paper focused on robust watermarking in frequency domain based on DCT-SVD. Various type of of cover images are hidden in to a cover images. The study of various secret sharing scheme i.e. Extended

Portable Network Graphics (PNG) image, Visual secret sharing (VSS), Integral imaging is a three-dimensional (3D) imaging technique. But there are some problems in secure image transmission so to improve this “secret image sharing with encryption decryption” sharing method for secure transmission is proposed here. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants.

IX. FUTURE SCOPE

From observations of the proposed method the future work will include security analysis more simpler and more practical, reduce the transmission risk problem for participants and shares.

Future studies may be directed to choices of other block sizes and related parameters (prime number, coefficients for secret sharing, number of authentication signal bits, etc.) to improve data repair effects.

REFERENCES

[1] Palak Jaina, Umesh Ghanekarb,“ Robust watermarking technique for textured images”, Procedia Computer Science Vol. 12, Iss. 8, December 2017.

[2] Che-Wei Lee and Wen-Hsiang Tsai,,“ A Secret-Sharing-Based Method for Authentication of Grayscale Document Images via the Use of the PNG Image With a Data Repair Capability”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 21, NO. 1, JANUARY 2012.

[3] Long Bao and Yicong Zhou, “Combination of Sharing Matrix and Image Encryption for Lossless (k,n)-Secret Image Sharing”, *IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 26, NO. 12, DECEMBER 2017.*

[4] M.Karolin, Dr. T. Meyyappan,” Encryption and Decryption of Color Images using Visual Cryptography,” International Journal of Pure and Applied Mathematics VOL 118 No. 8 2018.

[5] Pei-Ling Chiu,“ Sharing Visual Secrets in Single Image Random Dot Stereograms”, IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 23, NO. 10, OCTOBER 2014.

Author’s Profile:

	Snehal Kale has completed B.E. Degree in computer science and engineering from Sant Gadge Baba Amravati University, Amravati, Maharashtra. She is persuing Master’s Degree in Computer Science and Information Technology from P.G. Department of Computer Science and Engineering, S.G.B.A.U. Amravati. (e-mail id: snehakale009@gmail.com)
	Dr. Vilas M. Thakare is Professor and Head in Post Graduate department of Computer Science and engg, Faculty of Engineering & Technology, SGB Amravati university, Amravati. He is also working as a coordinator on UGC sponsored scheme of e-learning and m-learning specially designed for teaching and research. He is Ph.D. in Computer Science/Engg and completed M.E. in year 1989. He has done his PhD in area of robotics, AI and computer architecture. His (e-mailid: vilthakare@yahoo.co.in)