International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 08 | August -2020 ISSN: 2582-3930

A Survey on Visual Secret Sharing Scheme for Digital Image Watermarking

Tabassum Nakhawa, Dr.K.T.Belerao

Dept of Computer Engineering, KJEI, TCOER, Pune
Dept of Computer Engineering, KJEI, TCOER, Pune

Abstract— Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies or are encoded and stored in a digital form. The shares can appear as noise-like pixels or as meaningful images; but it will arouse suspicion and increase interception risk during transmission of the shares. Hence, VSS schemes suffer from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To address this problem, proposed a novel technique for digital watermarking using a texture and also a natural-image-based VSS scheme (VSS scheme) that shares secret images via various carrier media to protect the secret and the participants during the transmission phase. Contrive the texture synthesis process into digital image to hide secret messages. In comparison to using an existing cover image to hide messages, our algorithm hides the source texture image and embeds secret messages through the process of watermarking. The natural shares can be photos or hand-painted pictures in digital form or in printed form. We also propose possible ways to hide the secret to reduce the transmission risk problem for the share.

.

.**Keywords**— Data Security, high security, visual secret sharing scheme, Watermarking.

F

I. INTRODUCTION

In most of the image watermarking methods, uses the existing image as their cover medium. This leads to two drawbacks. Since the size of the cover image is fixed, embedding a large secret message will results in the distortion of the image. Thus a compromise should be made between the size of the image and the embedding capacity to improve the quality of the cover image.

In the most years no of advances have been made in the range of computerized media, and much more concern has developed with respect to watermarking for computerized media. Watermarking is a solitary system for data hiding strategies. It implants messages into a host medium keeping in mind the end aim to cover secrete

messages so as not to excite doubt by a meddler. A normal technique incorporates secretive correspondences between two gatherings whose presence is unclear to a conceivable attacker and whose achievement based on upon identifying the presence of this correspondence [1].

The VSS scheme uses diverse media as a carrier; hence it has many possible scenarios for sharing secret images. For example, assume a dealer selects n -1 media as natural shares for sharing a secret image. To reduce the transmission risk, the dealer can choose an image that is not easily suspected as the content of the media (e.g., landscape, portrait photographs, hand-painted pictures, and flysheets). The digital shares can be stored in a participant's digital devices (e.g., digital cameras or smart phones) to reduce the risk of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent via postal or direct mail marketing services. In such a way, the transmission

channels are also diverse, further reducing the transmission risk.

II. Related Work

In this paper [1], introduces a prototype for Digital Image Authentication System (DIAS). This system can perform visible and invisible watermarking on image. DIAS is applicable for colour and grey images. The input image could be of any size, and the resultant image size would be same as input image. DIAS identifies the ownership of digital image using Digital Watermarking. The Digital watermarking concept is used to hide and detect information from image. It is the best way to copyright protection of the user. By the use of digital watermarking, user can blame on faker for ownership. This is known as an Authentication System for ownership identification. The complete system consists of two functions, one for hiding information inside image and other for detecting information from image. In this approach, digital watermarking performed using Discrete Wavelet Transform (DWT) and analysed its results. This research paper introduces a prototype for Digital Image Authentication System (DIAS).

In this paper [2], the digital information is stored in a digital form or transmitted from one place to another through an electronic media. This digital information may fall in the hands of sniffers who may use or misuse that information for their intended use. Therefore, it is necessary to hide/embed very critical/important digital information (digital media) covertly in a cover digital data (image/audio/video) known as watermarked digital media before its storage or transmission without distorting the cover data. The digital information may be in the form of an image, a text file, and an executable program. To verify the authenticity or ownership, the digital watermarks may also be embedded in the copyrighted digital information. This Visual Secret Sharing Scheme for Digital Image Watermarking research work discusses the basic idea of steganography and implements Least Significant Bit (LSB) algorithm in MATLAB to hide text as well as an image in a cover image by the means of digital watermarking. It verifies the authenticity or ownership, the digital watermarks may also be embedded in the copyrighted digital information. It also shows the basic idea of steganography and implements Least Significant Bit (LSB) algorithm.

In this paper [3], A (k, n) visual cryptographic scheme (VCS) encodes a secret image into n shadow images (printed on transparencies) distributed among n participants. When any k participants superimpose their transparencies on an overhead projector (OR operation), the secret image can be visually revealed by a human visual system without computation. However, the monotone property of OR operation degrades the visual quality of reconstructed image for OR-based VCS (OVCS). Accordingly, XOR-based VCS (XVCS), which uses XOR operation for decoding, was proposed to enhance the contrast. In this paper, it is proved that the two theorems (Theorem 1 and Theorem 2) are given to show that an OVCS is also a XVCS and vice versa. Also, it is theoretically prove that the contrast of XVCS is 2(k1) times greater than OVCS.

In this paper [4], A QR code based blind digital image watermarking technique with an attack

detection feature is described here. The technique describes a key based framework to incorporate image, server port address or website address as watermark data; which increases the extended usability of the embedded data and the adaptability of the verification application. The watermarking problem is formulated as a signal communication problem with watermark data representation, embedding of watermark and attack detection as a source encoding, channel encoding and attenuation detection problems respectively. The mathematical aspects of the respective signal processing problems are extended to digital image watermarking with sufficient background support. In this paper the key based approach and the attack resistant embedding domain makes this method robust against visually invariant attacks. The testing results show the compliance of the method with all the proposed aspects.

In this paper [5], QR barcodes are used extensively due to their beneficial properties, including small tag, large data capacity, reliability, and high-speed scanning. However, the private data of the QR barcode lacks adequate security protection. In this article, we design a secret QR sharing approach to protect the private QR data with a secure and reliable distributed system. The proposed approach differs from related QR code schemes in which it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. The secret can be split and conveyed with QR tags in the distribution application, and the system can retrieve the lossless secret when authorized participants cooperate. General browsers can read the original data from the marked QR tag via a barcode reader, and this helps reduce the security risk of the secret.

Based on our experiments, in this paper, the new approach is feasible and provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. The proposed approach differs from related QR code schemes in that it uses the QR characteristics to achieve secret sharing and can resist the print-and-scan operation. In this paper [6], the quick response (QR) code was designed for storage information and high-speed reading applications. In this paper, we present a new rich QR code that has two storage levels and can be used for document authentication. This new rich QR code, named two-level QR code, has public and private storage levels. The public level is the same as the standard QR code storage level; therefore, it is readable by any classical QR code application. The private level is constructed by replacing the black modules by specific textured patterns. It consists of information encoded using q-ary code with an error correction capacity. This allows us not only to increase the storage capacity of the QR code, but also to distinguish the original document from a copy. This authentication is due to the sensitivity of the used patterns to the print-and-scan (PS) process. It is based on maximizing the correlation values between PS degraded patterns and reference patterns. In this paper, the storage capacity can be significantly improved by increasing the code alphabet q or by increasing the textured pattern size. The experimental results show a perfect restoration of private information. It also highlights the possibility of using this new rich QR code for document authentication.

In this paper [7], Quick response (QR) code has become one of the more popular two-dimensional barcodes because of its greater data capacity and

higher damage resistance. The barcode scanners can easily extract the information hidden in the QR code while scanning the data modules. However, some sensitive data directly stored in QR codes are insecure in real-world QR applications, such as the e-ticket and e-coupon. To protect the sensitive data, this paper explores the characteristics of QR barcodes to design a secret hiding mechanism for the QR barcode with a higher payload compared to the past ones. For a normal scanner, a browser can only reveal the formal information from the marked QR code. The authorized user/scanner can further reveal the sensitive data from the marked QR tag. The experiments demonstrates a satisfactory secret payload and the feasibility of the proposed scheme. The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication.

In this paper [8], with the rapid development of digital information age, digital watermarking technology is gradually becoming a useful way to protect the copyright of multimedia vendors. Robustness and imperceptibility of watermarked image are two important properties of Digital Watermarking. So they must be taken into consideration. In this paper, a watermarking algorithm of colour image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD). First convert host colour image from RGB colour space to YUV colour space. Then a layer of discrete wavelet transform is applied to the luminance component Y, and divided the low frequency and into blocks by using discrete cosine transform, and conducted SVD with every block. Finally embed watermark to the cover image. The experimental results show that the algorithm is good invisibility and strong robust, and can effectively resist common watermark attacks. In this paper, a watermarking algorithm of colour image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWT-DCT-SVD).

In this paper [9], a novel spatial domain colour image watermarking technique is proposed to rapidly and effectively protect the copyright of the colour image. First, the direct current (DC) coefficient of 2D-DFT obtained in the spatial domain is discussed, and the relationship between the change of each pixel in the spatial domain and the change of the DC co-efficient in the Fourier transform is proved. Then, the DC coefficient is used to embed and extract watermark in the spatial domain by the proposed quantization technique. The novelties of this paper include three points: 1) the DC coefficient of 2D-DFT is obtained in the spatial domain without of the true 2D-DFT; 2) the relationship between the change of each pixel in the image block and the change of the DC coefficient of 2D-DFT is found, and; 3) the proposed method has the short running time and strong robustness. The paper shows on two publicly available image databases (CVG-UGR and USC-SIPI) have shown that the proposed method not only has satisfied the needs of invisibility but also has better performance in terms of robustness and real-time feature, which show the proposed method has both advantages of spatial domain and frequency domain.

In this paper [10], information security is on its top priority for all organizations. The individuals, government officials, and military with the rapid development of Internet technologies like the

Internet of Things (IoT), Big Data and Cloud Computing facing data security problems. As the massive rate of data growth, its challenging task for the researchers, that how to manage the vast amount of data safely and effectively while designing smart cities. It has been quite easy to produce an illegal copy of digital contents. The verification of digital content is one of the major issues because digital contents are generated daily and shared via the internet. Limited techniques are available for document copyright protection. However, most of the existing techniques produce distortion during watermark insertion or lack of capacity. In the said perspective, a digital watermarking technique is proposed for document copyright protection and ownership verification with the help of data mining. The techniques of data mining are applied to find suitable properties from the document for embedding watermark. The proposed system provides copyright protection to text documents on local and cloud computing paradigm. For the evaluation of the proposed technique, twenty different text documents are used to perform many attacks such as formatting, insertion and deletion attacks. The proposed technique attained is robust and resists from formatting attacks and capacity of the proposed technique is also improved as compared to the previous techniques.

III. Visual Secret Sharing Scheme Method

This method is expressed as k-out-of-n secret sharing. The concept of this scheme is illustrated as follows; the secret image is divided into n shares so that the original image is visible if any k of these shares are stacked together. The image remains hidden if fewer than k shares are superimposed together [8]. The construction of shares can be done by using a codebook to encode a binary image with different pixel expansion. **Visual Secret Sharing** (VSS) is a sub class of **Secret Sharing** (SS) scheme of 1970s, called threshold schemes, to encode a **secret** into pieces (“shadows” or “shares”) so that the pieces can be distributed to participants at different locations. So in general it is something like a **secret** picture to be shared among n number of participants. The picture is divided into n transparencies (shares) such that if any k transparencies are placed together, the picture becomes visible, but if fewer than m transparencies are placed together, nothing can be seen. Such a scheme is constructed by viewing the **secret** picture as a set of black and white pixels and handling each pixel separately. The schemes are perfectly secure and easily implemented without any cryptographic computation. Because a **secret** kept in a single scheme could be easily lost or damaged or even been detected, and later replaced to give wrong information at receiver end as well. Thus multiple schemes may be preferred. A further improvement allows each transparency (share) to be an innocent picture (e.g. a picture of a landscape or a picture of a building), thus concealing the fact that **secret sharing** is taking place.

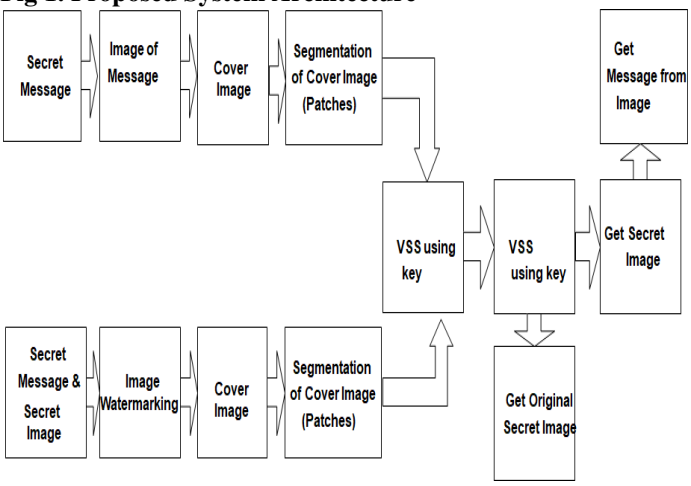
IV. Proposed Approaches

Proposed system working to facilitate the data security in getting secure transmission of data over social media which maintain the data hiding inside texture image. Hence this system is suitable for

maintaining high level security for data transmission or image preservation in the network. In proposed work, watermarking is used to hide the secret message in image and also extract the secret message from texture image.

Also we develop efficient encryption/decryption algorithms for the (*n, n*) -VSS scheme using cover image's shares. The Proposed algorithms are applicable to digital and printed media. The possible ways to hide the generated share are also discussed. The proposed NVSS scheme not only has a high level of user friendliness and manageability, but also reduces transmission risk and enhances the security of participants and shares.

Fig 1. Proposed System Architecture



- Sender
  - Enter Public Message / Private Message
  - Generate QR code image with hide message
  - Generate n shares/patches of QR code using visual secret sharing scheme
  - Transfer the shares to the receiver
  - Logout
- Receiver
  - Receiver must select accurate n-1 shares and combine it.
  - After retrieve the QR code
  - Decode QR code
  - Read public/private message

On the sender's side, the secret message of the sender is hidden under a cover message. The cover image is then segmented or is divided into shares/patches using VSS (visual secret sharing scheme).These shares are then transferred to the receiver.

While on the receiver's side, the receiver selects n-1 shares and combines them and retrieves the cover image. This cover image then helps in retrieving the original secret message.

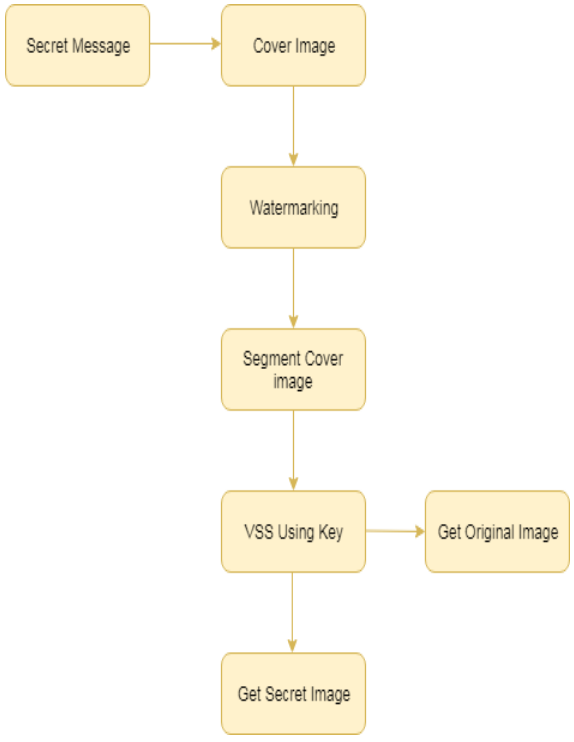


Fig 2. Flow Diagram

The message and image is loaded by using GUI format. Watermarking process is used to hide the

secret message in image and also extract the secret message from texture image in our system. Secret message will extract by receiver. Proposed methodology uses waterma≤input the texture image pattern for hiding text in the data. The proposed VSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness for shares and for secret image.

- Algorithms
  - Text Embedding Algorithm

Encoding:-

Representation of each letter in secret message by its equivalent ASCII code.

1. Conversion of ASCII code to equivalent 128 bit binary number.
2. Division of 8 bit binary number into two 4 bit parts. Choosing of suitable letters corresponding to the 4 bit parts.
3. Meaningful sentence construction by using letters obtained as the first letters of suitable words.
4. Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.

4. Encoding is not case sensitive.

Decoding:-

Steps:

1. First letter in each word of cover message is taken and represented by corresponding 4 bit number.
5. 4 bit binary numbers of combined to obtain 8 bit number.
2. ASCII codes are obtained from 8 bit numbers.
3. Finally secret message is recovered from ASCII codes.

Techniques achieved in existing system	Techniques that will be achieved in the proposed system
In existing system, the technique proposed is 99.9% robust against formatting attacks such as cut, copy, paste, font size, font colour and also alignment. And it proves that it is robust and tolerates most of the possible attacks and watermark is extracted with higher accuracy.	In proposed system, we are working on providing more security to the watermarked image by using the VSS (Visual Secret Sharing) technique which helps in segmenting the cover image in several shares which attempts in better security of the watermarked image. And we are also trying to increase the storage capacity.

V. Acknowledgement

It gives me great pleasure in presenting the dissertation report on ‘Visual Secret Sharing Scheme for Digital Image Watermarking’. I would like to take this opportunity to thank my internal guide Dr. K.T.Belerao for helping me in providing all the necessary information regarding my dissertation. I am also thankful to Dr. Geetika Narang (Head of Department) for providing me with the required facilities and helping me in

carrying out this seminar work. Finally I wish to thank all our faculties and friends for their constructive comments and suggestions.

VI. Conclusion

The message and image is loaded by using GUI format. Watermarking process is used to hide the secret message in image and also extract the secret message from texture image in our system. Secret message will extract by receiver. Proposed methodology uses watermarking for hiding data inside the image which input the texture image pattern for hiding text in the data. The proposed VSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness for shares and for secret image.

VII. References

[1] Shahnawaz Uddin "Digital watermarking of text/image using least significant bit algorithm," IJARSE, vol. no.2, issue no. 02, february 2013.

[2] Neeraj Bhargava, M. M. Sharma, Abhimanyu Singh Garhwal, Manish Mathur, "Digital image authentication system based on digital watermarking", IEEE 07, February 2013.

[3] C. N. Yang, D. S. Wang, "Property Analysis of XOR- Based Visual Cryptography," IEEE Transactions on Circuits Systems for Video Technology, vol. 24, no. 12 pp. 189-197, 2014.

[4] P. P. Thulasidharan, M. S. Nair, "QR code based blind digital image watermarking with attack detection code," AEU - International Journal of Electronics and Communications, vol. 69, no. 7, pp. 1074-1084, 2015.

[5] P. Y. Lin, "Distributed Secret Sharing Approach with Cheater Prevention Based on QR Code," IEEE Transactions on Industrial Informatics, vol. 12, no. 1, pp. 384-392, 2016.

[6] I. Tkachenko,W. Puech, C. Destruel, et al., "Two-Level QR Code for Private Message Sharing and Document Authentication," IEEE Transactions on Information Forensics Security, vol. 11, no. 13, pp. 571-583, 2016.

[7] P. Y. Lin, Y. H. Chen, "High payload secret hiding technology for QR codes," Eurasip Journal on Image Video Processing, vol. 2017, no. 1, pp. 14, 2017.

[8] Yuqi He, Yan Hu, "A Proposed Digital Image Watermarking Based on DWT- DCTSVD", IEEE 27 may 2018.

[9] Qingtang Su, Decheng Liu, Zihan Yuan, Gang Wang, Xiaofeng Zhang, Beijing Chen,Tao Yao, "New Rapid and Robust Color Image Watermarking Technique in Spatial Domain". December 2018.

[10] Umair Khadam, Muhammad Munwar Iqbal, Muhammad Awais Azam, Shehzad Khalid, Seungmin Rho, Naveen Chilamkurti, "Digital Watermarking Technique for Text Document Protection Using Data Mining Analysis", April 15 2019.