International Journal of Current Engineering and Technology
E-ISSN 2277 – 4106, P-ISSN 2347 – 5161

Available at http://inpressco.com/category/ijcet

Research Article

Visual secret sharing scheme for digital image watermarking

Miss.Tabassum Nakhawa and Dr.K.T.Belerao

Department of Computer Engineering Trinity College of Engineering and Research, Pune Savitribai Phule Pune University Pune, India

Received 10 Nov 2020, Accepted 10 Dec 2020, Available online 01 Feb 2021, **Special Issue-8 (Feb 2021)**

Abstract

Traditional visual secret sharing (VSS) strategies hide secret imagesin shares that are either imprinted on transparencies or are encoded and put away in a digital form. The shares can appear as noise-like pixels or as significant pictures; but it will arouse suspicion and increase interception risk during transmission of the shares. Subsequently, VSS schema experience from a transmission risk problem for the secret itself and for the members who are associated with the VSS conspire. To address this issue, proposed a advanced technique for advanced 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. Devise 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 regular offers can be photographs or hand-painted pictures in computerized structure or in printed structure. We likewise propose potential approaches to conceal the key to diminish the transmission chance issue for the offer. Test results demonstrate that the proposed approach is an amazing answer for taking care of the transmission chance issue for the VSS technique.

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

Introduction

In a large portion of the picture watermarking techniques, utilizes the current picture as their spread medium. This prompts two downsides. Since the size of the spread picture is fixed, implanting a huge mystery message will brings about the contortion of the picture. Subsequently a trade off ought to 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.The VSS conspire utilizes different media as a transporter; subsequently it has numerous potential situations for sharing secret images. For example, assume a seller chooses n - 1 media as natural shares for sharing a secret image. To diminish the transmission risk, the vendor can pick a picture that isn't effectively associated as the substance with the media (e.g., scene, representation photos, hand-painted pictures, and flysheets). The computerized offers can be put away in a member's advanced gadgets (e.g., computerized cameras or PDAs) to decrease the danger of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent by means of postal or regular postal mail showcasing administrations. In such a way, the transmission channels are also diverse, further reducing the transmission risk.

To diminish the transmission hazard, the vendor can pick apicture that isn't effectively associated as the substance with the media (e.g., scene, representation photos, hand-painted pictures, and flysheets). The computerized offers can be put away in a member's advanced gadgets (e.g., computerized cameras or PDAs) to decrease the danger of being suspected. The printed media (e.g., flysheets or hand-painted pictures) can be sent by means of postal or regular postal mail showcasing administrations. In such a manner, the transmission channels are additionally differing, further lessening the transmission hazard.

A. Motivation

1) Image watermarking technique embeds an authorized mark information in the digital image to protect the ownership of digital image.

2) The motivation of the work is to propose the storage capacity can be significantly improved by increasing the code alphabet q or by increasing the textured pattern size.

B. Objectives

1) To protect copyright, production, illegal distribution, unauthorized manipulation, theft using image watermarking.
2) To hide information in digital image and transmission of private information into watermarking.
3) To provide security for message using visual secret sharing scheme.
4) To distinguish the original printed document from its copy.

Literature Survey

In [1] paper, a watermarking algorithm of color image is proposed based on Discrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition (DWTDCT-SVD). First convert host color image from RGB color space to YUV color space. At that point a layer of discrete wavelet change is applied to the luminance part Y, and isolated the low recurrence and into hinders by utilizing discrete cosine change, and directed SVD with each square. At last install watermark to the spread picture.
In [2] paper, a new digital watermarking model is proposed for the medical images. An improved SMQT is used for image enhancement and the image is being segmented using OTSU thresholding. Discrete Wavelet Transform (DWT) and Inverse DWT are used to embed and extract the watermark on the host image. The goal of our scheme is to make the watermarking more robust against attacks and secure the image from privacy threats.
In [3] paper, presents a Wavelet change Singular Value Decomposition based hearty zero watermarking system for clinical pictures to address the protection and security issues. Dissimilar to regular watermarking, the proposed technique saves the unwavering quality of the spread picture without bringing any ancient rarities and with no adjustment in the basic data contained in the clinical picture. The performance of the scheme is assessed with teleophthalmological images. The simulation results reveal the robustness of the proposed technique against various image processing attacks and indicate its suitability for safe exchange of medical images among remote medical practitioners.
In [4] paper, This exploration is done to locate the best advanced watermarking procedure to exceptionally make sure about computerized picture structure the unlawful duplicates. The examination work additionally done to investigate the potential outcomes of double watermarking. Different standard research articles were contemplated and it is discovered that double watermarking is conceivable with some circumstance. This research work motivates and offers different combinations on digital watermarking techniques in near future for efficient output of watermarking.
In [5] paper, proves that the contrast of XVCS is 2((k-1)) times greater than OVCS. 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. Advantages are: Easily decode the secret image by stacking operation. XVCS has better reconstructed image than OVCS. Disadvantages are: Proposed algorithm is more complicated.
In [6] paper, present a visually impaired, key based watermarking method, which inserts a changed double type of the watermark information into the DWT area of the spread picture and uses a remarkable picture code for the location of picture twisting. The QR code is installed into the assault safe HH part of 1stlevel DWT area of the spread picture and to identify malevolent obstruction by an aggressor. Focal points are: More data portrayal per bit change joined with blunder rectification abilities. Expands the ease of use of the watermark information and keeps up power against outwardly invariant information expulsion assaults. Inconveniences are: Limited to a LSB bit in the spatial space of the picture power esteems. Since the spatial space is progressively powerless to assaults this can't be utilized.
In [7] paper, plan a mystery QR sharing way to deal with ensure the private QR information with a safe and solid disseminated framework. The proposed approach varies from related QR code plots in that it utilizes the QR qualities to accomplish mystery sharing and can oppose the print-and-sweep activity. Advantages are: Reduces the security risk of the secret. Approach is feasible. It provides content readability, cheater detectability, and an adjustable secret payload of the QR barcode. Disadvantages are: Need to improve the security of the QR barcode. QR technique requires reducing the modifications.
In [8] paper, The two-level QR code (2LQR), has two public and private storage levels and can be used for document authentication. 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 qr code with an error correction capacity. Advantages are: It increases the storage capacity of the classical QR code. The textured patterns used in 2LQR sensitivity to the PS process. Disadvantages are: Need to improve the pattern recognition method. Need to increase the storage capacity of 2LQR by replacing the white modules with textured patterns.
In [9] paper, By using data mining a digital watermarking technique is proposed here for

document copyright protection and ownership. Data mining techniques are applied to find appropriate properties from document for embedding watermark. The work shows us that even after applying formatting attacks on the document the proposed algorithm proves to be robust and tolerates the formatting attacks, and also extracts the watermark with high accuracy. In cloud computing environment it also shows the same results to ensure the security of the text documents.

Proposed Methodology

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.

A. Architecture

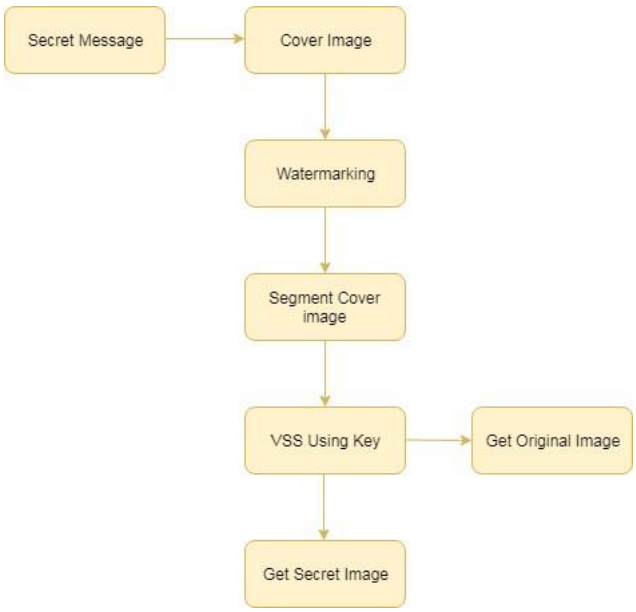

Fig. 1. Proposed System Architecture

B. Algorithm

1) Text Embedding Algorithm

Encoding:-

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

a) Conversion of ASCII code to equivalent 128 bitbinary number.

b) Division of 8 bit binary number into two 4 bit parts.Choosing of suitable letters corresponding to the 4 bit parts.

c) Meaningful sentence construction by using lettersobtained as the first letters of suitable words.

d) 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.

e) Encoding is not case sensitive.

Decoding:Steps:

a) First letter in each word of cover message is takenand represented by corresponding 4 bit number.

b) 4 bit binary numbers of combined to obtain 8 bitnumber.

c) ASCII codes are obtained from 8 bit numbers.

d) Finally secret message is recovered from ASCIIcodes.

2 Sharing Algorithm: t = 1

t = 1 secret sharing is trivial. The secret can simply be distributed to all n participants.

t = n

There are several (t, n) secret-sharing schemes for t = n, when all shares are necessary to recover the secret: Encode the secret as an arbitrary length binary number s. Give to each player i (except one) a random number pi with the same length as s. Give to the last player the result of (s XOR p1 XOR p2 XOR ... XOR pn1) where XOR is bitwise exclusive or. The secret is the bitwise XOR of all the players' numbers (p).

Additionally, (a) can be performed using any linear operator in any field. For example, here's an alternative that is functionally equivalent to (a). Let's select 32bit bit integers with well-defined overflow semantics (i.e. the correct answer is preserved, modulo 232). First, s can be divided into a vector of M 32-bit integers called vsecret. Then (n 1) players are each given a vector of M random integers, player i receiving vi. The remaining player is given vn = (vsecret v1 v2 ... vn1). The secret vector can then be recovered by summing across all the player's vectors.

Results And Discussion

This section demonstrates the performance of the NVSS scheme by using the Watermarking to hide the secret image using n natural shares. Input secret message to generate the QR code image is shown in Fig2, generated QR code image is shown in Fig3, the natural shares are as shown in Fig4 and NVSS encryption and decryption of image using n natural shares is shown in Fig5 and Fig6 respectively.

Fig. 2. Input Secret Message

Fig. 3. QR Secret Image

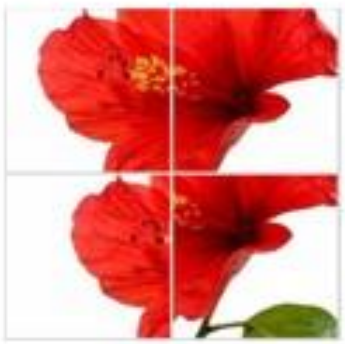

Fig. 4. Natural Shares of Cover Image

Fig. 5. Encrypted Secret Image

Fig. 6. Decrypted Image

Conclusion

The message and image is s stacked by utilizing GUI position. Watermarking process is used to hide the secret message in image and also extract the secret message from texture image in our framework. Secret message will extricate by recipient. Proposed procedure utilizes watermarking for hiding data inside the image which input the texture image pattern for hiding text in the data. The proposed VSS plan can successfully decrease transmission chance and give the most significant level of ease of use for shares and for secret picture.

References

[1]. Yuqi He, Yan Hu,"A Proposed Digital Image Watermarking Based on DWT-DCT-SVD"2018 2nd IEEE Advanced Information Management,Communicates,Electronic and Automation Control Conference(IMCEC 2018).

[2]. Shaekh Hasan Shoron,Monamy Islam,Biprojit Mondal,Jia Uddin,"A Digital Watermarking Approach using SMQT,OTSU, DWT and IDWT"IEEE Conference 2018.

[3]. Abhilasha Singh, 2 Malay Kishore Dutta," Lossless and Robust Digital Watermarking Scheme for Retinal Images" International Conference on

[4]. "Computational Intelligence and Communication Technology" (CICT 2018)

[5]. Etti Mathur, Manish Mathuria," Unbreakable Digital Watermarking using combination of LSB and DCT" International Conference on Electronics, Communication and Aerospace Technology ICECA 2017

[6]. 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.

[7]. 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.

[8]. 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.

[9]. 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.