ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Digital Visual Cryptographical Image Sharing Using DIM

Bhagyashri Machale[1], Padmashri Thorat[2], Prajakta Baravkar[3] , Tejshri Bavale[4] ,

Prof.Pankaj Agarkar[5]

UG Student, Dept. of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[1]

UG Student, Dept. of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[2]

UG Student, Dept. of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[3]

UG Student, Dept. of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[4]

Assistant Professor, Dept. of CSE, Dr.D.Y.Patil School of Engineering, Lohegaon Pune, Maharashtra, India[5]

ABSTRACT: In this paper, we search technique on how to improve the security of original data by hiding secret data in cover image (which may be digital or printed image) by using data hiding,cryptography and NVSS algorithm. The proposed system hides the secret data which is first encrypted and then is hidden behind a cover image and achieves the security by hiding image behind another image. The total effort of the proposed method is the achievement of hiding and extracting secret images. In proposed method, we have tried to increase the capacity of the original scheme by improving the capacity of hiding data and increasing security to send image through different media. The main aim of the proposed model is to improve security, efficiency and reliability of the secret image by using data hiding and cryptography method and NVSS algorithm.

KEYWORDS: Digital image sharing, Feature extraction, Secret image, VSS cryptography, Visual secret sharing

I.INTRODUCTION

In day to day life sharing information with each other is increasingly important Due to networking and communication media, it is used to share the important information like images, audio, video, pictures easily. Black Hackers tried to access unauthorized data/personal data. To solve this problem certain techniques are used. Today, in computer-aided environment sharing visual secrets images has becomes an important issue . Secret images can be of various types such as handwritten documents, photographs which are shortly called as digital images or printed images. Visual cryptography is a technique that encrypts a secret image into n shares with each participant holding one or more shares. This technique is used for provide security to important data by using NVSS algorithm. By using feature extraction of digital and printed image. After that it uses the main concept of visual cryptography. In that encryption of image, data hiding and decryption are done simultaneously.The major contribution is to reduce the transmission risk problem and provides the highest level of user friendliness. Major contributions are this is the first attempt to send secret image through various carrier media and for image. In enhanced system can segment the secret image and will perform the encryption process for all segmented regions, the same process will inversely perform in decryption, in order to achieve the efficient transformation of secret images.Visual Cryptography (VC) is a technique that encrypts a secret image into *n* shares, with each participant holding one or more shares. Anyone who holds fewer than *n* shares cannot reveal any information about the secret image. Stacking the *n* shares reveals the secret image and it can be recognized directly by the human visual system. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The original motivation of VC is to securely share secret images in non-computer-aided environments; however, devices with computational powers are ubiquitous (e.g., smart phones). Thus, sharing visual secret images in computer-aided. Environments have become an important issue today to reduce the intercepted risk during the transmission phase NVSS is proposed. Conventional VSS schemes use a unity carrier (e.g., either transparencies or digital images) for sharing images, which limits the practicality of VSS schemes. Proposed system explores the possibility of using diverse media for sharing digital images. The carrier media in the scheme contains digital images, printed images, hand-painted

DOI: 10.15680/IJIRCCE.2016. 0410075

pictures, and so on. Applying a diversity of media for sharing the secret image increases the degree of difficulty of intercepting the shares. The NVSS scheme can share a digital secret image over *n* - 1 arbitrary natural images (here after called natural shares) and one share. Instead of altering the contents of the natural images, the proposed approach extracts features from each natural share. These unaltered natural shares are totally innocuous, thus greatly reducing the interception probability of these shares. The generated share that is noise-like can be concealed by using data hiding techniques to increase the security level during the transmission phase.

II.LITERATURE SURVEY

Kai-Hui Lee and Pei-Ling Chiu proposed that Conventional visual secret sharing (VSS) schemes hide secret images in shares that are either printed on transparencies 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, they proposed a natural-image-based VSS scheme (NVSS scheme) that shares secret images via various carrier media to protect the secret and theparticipants during the transmission phase. The proposed (*n*, *n*) - NVSS scheme can share one digital secret image over *n* -1 arbitrary selectednatural images (called natural shares) and one noise-like share. The natural shares can be photos or hand-painted pictures in digital form or in printed form. The noise-like share is generated based on these natural shares and the secret image. The unaltered natural shares are diverse and innocuous, thus greatly reducing the transmission risk problem. They also propose possible ways to hide the noise like share to reduce the transmission risk problem for the share. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes [1].

Sunil G. Jare proposed that Visual Cryptography (VC) is a technique which can encrypts a secret image into *n* shares, with each participant holding one or more shares. One who has less number of shares than *n shares* cannot disclose any information about the secret image. Stacking the *n* shares disclosed the secret image and it can be recognized directly by the human visual system. Sharing and receiving secret images is also known as a visual secret sharing (VSS) scheme. The original propulsion of VC is to securely share secret images in non-computer-aided environments; however, devices with computational powers are omnipresent (e.g., smart phones).Conventional shares consisting many meaningless and random pixels, may satisfy the requirement for security required for protecting secret contents but they have drawbacks: first it has a high transmission risk. The reason behind it is it is holding noise-like shares which will cause attackers' dubitation and the shares may get intercepted. Hence, the risk of the sender and the shares increases, which will increase the probability of transmission failure. Second, the unmeaning shares may not user friendly.

G.Rajathi, G.Satodaha, D.Tamizharasi, S.Praveen Kumar proposed a natural-image-based VSS scheme (NVSS scheme) which shares secret data and one noise-like share. The natural share can be anything natural photos or hand-painted pictures in digital form or in printed form. The noise-like shares are created based on the natural shares and the secret data. The converted natural shares are diverse, thus greatly reducing the transmission risk problem .We have given different ways to hide the noise like share to reduce the transmission risk problem for the share. Experimental results show that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes [3].

Priyanka R. Pawar, Manjusha S. Borse, proposed Visual Secret Sharing scheme (VSS) which is implemented to hide secret images that are either printed transparencies or are encoded and stored in digital form and shares are easy to detect by naked eyes/unauthorized user. Hence to avoid problems generated by VSS, (n, n)-NVSS (Natural Image based VSS) Scheme encryption/ decryption algorithms to reduce the intercepted risk during the transmission phase is used. Regardless of the number of participants the value of n increases, the NVSS scheme uses only one noise share for sharing the secret image. It proposes a useful concept and method for using unaltered images as shares in a VSS scheme. A method to store the noise share as the QR code is used. The original motivation of NVSS scheme is to use printed images as sharing images and developing a method for storing the noise share [4].

Mayuri Sonkusare, Prof. Nitin Janwe proposed A natural-image-based VSS scheme (NVSS scheme) that shares secret images. A natural-image-based secret image sharing scheme (NSISS) which can share a color secret image over n - 1 arbitrary natural images and one noise-like share image. Instead of changing the contents of the natural images, the encryption process extracts feature images from each natural image. To protect the secret image from transmission phase. (n,n) - NVSS scheme shared secret image over n-1 natural share. By extracting the features of natural shares

they prepared noise-like share. After that encryption carried out with noise-like share and secret image. Proposed possible ways to hide the noise like share to reduce the transmission risk problem for the share.In this paper Initially Feature Extraction process has been performed for Natural Shares. This Encrypted result will be hided using Share-Hiding Algorithm where generated the QR code. In the Recovering of the secret image will be done by Share Extraction Algorithm and also decryption algorithm. Finally the secret image with all pixels has been obtained [5].
Dr. Prashant R. Deshmukh 1, Sejal V. Gawande emphasize on how to improve the capacity of carrier image by hiding secret data in it by using the combination of data hiding and cryptography. To fulfill the requirement, the proposed method highlights an approach of hiding secret data using diverse image media. The proposed system hides the secret data which is first encrypted and then is hidden behind a carrier image and achieves the security by hiding image behind another image. In this way the system achieves its encryption and decryption after going through visual cryptography. The overall effort of the proposed method is the achievement of hiding and extracting secret images. In proposed method, we have tried to increase the capability of the original scheme by improving the capacity of hiding data and increasing security. The main aim of the proposed model is to improve security, efficiency and reliability of the secret image by using the combination of data hiding and cryptography method [6].

Miss A A Naphade, Dr.R N Khobaragade, Dr.V M Thakareproposed *that* visual cryptography (VC) based on black-and-white or binary images. The shares can appear as noise-like pixels as meaningful images but it will produce dubitation and increase interception risk in transmission of the shares. This paper focused on five visual cryptography i.e. multiple image visual cryptography (MIVC),optimal gray scale reserving visual cryptography (GRVCS) , Embedded extended visual cryptography scheme (Embedded EVCS), simulated-annealing-based algorithm to use the VC construction problem to find the column vectors for the optimal VC construction , natural-image-based VSS scheme (NVSS scheme).The new proposed schemes is improved NVSS schemes ,it is more secure .the advantages are as the low pixel expansion[7].
Mr.Thanguganesh.M and Prof.Sarnaya R proposed system to protect important data from unauthorized illegal access and tampering various methods for data vague like visual cryptography, stenography,authentication have been developed our environment.They will be discussing one such data obscure technique called visual cryptography. Visual cryptography is the process of vague important data in any variant media to transfer it securely over the underlying unreliable and unsecured communication media by the usage of different image types like digital image, grey image, and natural image [8].

III. MODULE DESCRIPTION

A. IMAGE PROCESSING

In this Method Printed image will be preprocessed by cropping the input image. Cropping is performed by manually and stored for further processing. Resize the cropped image with predicted size.

B. FEATURE EXTRACTION

Feature Extraction is carried by Binarization of the natural share. Binarization performed by calculated with respect to the median value of the natural share. With the binarization result the stabilization process has been done. The stabilization process is used to balance the number of black and white pixels of an extracted feature image in each block. The process ensures that the number of black and white pixels in each block is equal. These clustered pixels have the same feature value. The chaos process is used to eliminate the texture that may appear on the extracted feature images and the generated share. The original feature matrix will be disordered by adding noise in the matrix.

C. ENCRYPTION

Before Encryption process pixels-swapping for printed image share performed which promotes tolerance of the image distortion caused by the image preparation process. The proposed (n, n)-NVSS scheme can encipher a true color secret image by n-1 innocuous natural shares and one noise like share. Input images include n-1 natural shares and one secret image. The output image is a noise-like share. Finally XOR operation performed for each color plane with the secret image.

D. DATA HIDING

In this section Quick-Response Code (QR code) techniques are introduced to conceal the noise-like share and further reduce intercepted risk for the share during the transmission phase. The code is printed on physical material and can be read and decoded by various devices, such as barcode readers and smart phones. It suitable for use as a carrier of secret communications. The string can be encoded to the QR code (a stego-share) by QR code generators.

E. DECRYPTION

By repeating the reversal process of encryption process to predict the secret image. Again feature extraction and pixel swapping performed to predict the secret image.

IV.EXISTING SYSTEM

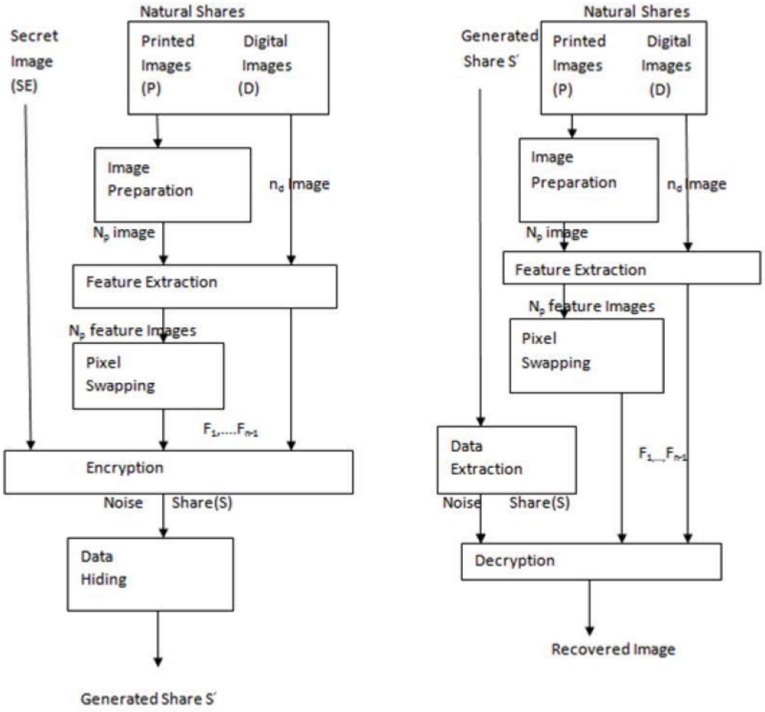

FIG NO 01. EXISTING SYSTEM

V. CONCLUSION AND FUTURE WORK

The paper proposes a VSS scheme, (n, n)-NVSS scheme, that can share a digital image using diverse image media. The media that include n-1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participants n increases, the NVSS scheme uses only one noise share for sharing the secret image. 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. This study provides four major contributions. First, this is the first attempt to share images via heterogeneous carriers in a VSS scheme. Second, we successfully introduce hand-printed images for images-haring schemes. Third, this study proposes a useful concept and method for using unaltered images as shares in a VSS scheme. Fourth, we develop a method to store the noise share as the QR code.

ACKNOWLEDGEMENT

We thank our guide Prof.Pankaj Agarkar (ME Coordinator of CSE) for his inspiration and guidance. We thank to our HOD of Comp Prof.Soumitra Das and Director DR.S.S.Sonawane.We also thanks tour family and friends for their help.

REFERENCES

[1] . Kai-Hui Lee and Pei-Ling Chiu,"Digital Image Sharing by Diverse Image Media", IEEE transactions on information forensics and security, vol. 9, no. 1, January 2014.

[2]. Sunil G. Jare, "Digital Image Sharing Using Visual Cryptography Techniques", Sunil G. Jare*et al*, International Journal of Computer Science and Mobile Computing, Vol.4 Issue.4, April- 2015, pg. 717-721

[3] .G.Rajathi, G.Sangeetha, D.Tamizharasi, S.Praveen Kumar, "Secret Image Sharing by Diverse Image Media".

[4] .Priyanka R. Pawar, Manjusha S. Borse, "transmission risk reduction in image sharing scheme with diverse image media"

[5]. Mayuri Sonkusare, Prof. Nitin Janwe,"Analysis of Digital Image Sharing By Diverse Image Media" ,Mayuri Sonkusare et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (4) , 2015, 3784-3786

[6]. Dr. Prashant R. Deshmukh 1, Sejal V. Gawande, "secrete image sharing by diverse image media".

[7] Miss A A Naphade, Dr.R N Khobaragade,Dr.V M Thakare,"Improved NVSS Scheme for Diverse image media".

[8] Mr.Thanguganesh.M and Prof.Sarnaya R.,''Assorted Image Based Obscure Techniques in Visual Cryptography".