ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

A Survey on High Capacity Reversible Data Hiding in Encrypted Images

Rutuja Sharad Warule[1], Himani Wadnere[1], Mayuri Wagalgave[1], Gayatri Wagh[1], Prof. Sanjay B. Waykar[2]

B. E Students, Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala, India[1]

Professor, Department of Computer Engineering, Sinhgad Institute of Technology, Lonavala, India.[2]

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, we proposed a novel technique for steganography using a texture and also a natural-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. We contrive the texture synthesis process into steganography 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 stenography. 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. Experimental results indicate that the proposed approach is an excellent solution for solving the transmission risk problem for the VSS schemes.

KEYWORDS: visual secret sharing (VSS), steganography, natural-image-based VSS scheme (NVSS scheme), OR Code.

I. INTRODUCTION

In most of the image steganographic 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.

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. Secret images can be of various types: images, handwritten documents, photographs, and others. 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.

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 steganography for computerized media. Steganography 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 steganographic 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 NVSS 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

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

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 Initially Feature Extraction process has been performed for Natural Shares. Here Digital image and Printed image have been used as Natural Shares. With that extracted features secret image will be encrypted by (n, n) - NVSS scheme where process carried by (n-1) natural shares [1].
Natural-image-based VSS scheme (NVSS scheme) which shares secret image via various carrier media to protect the secret and the participants during the transmission phase. This Process involved sharing a secret image over arbitrary selected natural images (called natural shares) and one noise-like share [2].
This Process involved sharing a secret image over arbitrary selected natural images (called natural shares) and one noise-like share. Natural-image-based VSS scheme (NVSS scheme) which shares secret image via various carrier media to protect the secret and the participants during the transmission phase [3].
Aim of this project is to avoid the transmission risk problem during sharing an image in a network.Regular visual secret sharing (VSS) schemes hide secret images in shares that are encoded or stored in digitalform [4].

One such data obscure technique called visual cryptography. This survey is on various data obscure techniques in cryptography that are in practice today along with the comparative analysis of these techniques [5].

Visual cryptography i.e. multiple image visual cryptography (MIVC),optimal grayscale reserving visual cryptography (GRVCS) are studied. 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) [6].
This research had used steganography techniques to securely share the secret image to avoid data lost [7].
The proposed (n, n) – NVSS scheme can share one digital secret image using n - 1 arbitrary selected shares and one share which is noise share. The natural shares can be photos as well as hand painted pictures in digital form as well as in printed form. The noise-like share is generated based on these natural shares and the secret image. The natural shares which are not altered are diverse and innocuous, thus greatly reducing the transmission risk problem [8].
In this work, HVC construction methods based on error diffusion are proposed. The secret image is concurrently embedded into binary valued shares while these shares are half toned by error diffusion—the workhorse standard of half toning algorithms. Error diffusion has low complexity and provides halftone shares with good image quality. A reconstructed secret image, obtained by stacking qualified shares together, does not suffer from cross interference of share images [9].

III. PROPOSED SYSTEM

We have worked 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, stenography 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*) -NVSS 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.

ISSN(Online): 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Proposed System Architecture

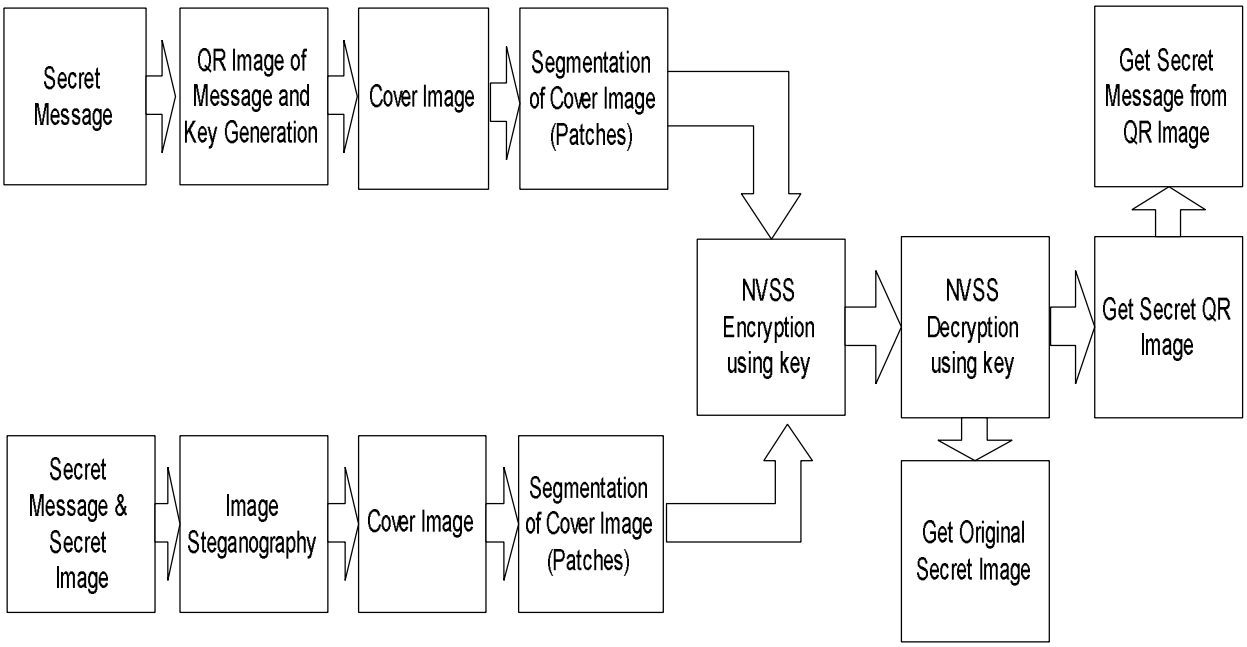

Fig: Proposed System Architecture

IV. CONCLUSION

The message and image is loaded by using GUI format. Stenography 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 stenography for hiding data inside the image which input the texture image pattern for hiding text in the data.

The proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness for shares and for secret image.

REFERENCES

[1] 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.
[2] R.H. adekar, N.M. jadhav, N.D. Pergad, "Digital image sharing by diverse image media using nvss technique", IJARIIE-ISSN (O)-2395-4396, Vol-2 Issue-1, 2016.
[3] G.Rajathi, G.Sangeetha, D.Tamizharasi, S.Praveen Kumar, "Secret sharing schemes by diverse image media". International Journal of Innovative Research in Computer and Communication Engineering an ISO 3297: 2007 Certified Organization Vol.3, Special Issue 1, February 2015.
[4] Priyanka R. Pawar, Manjusha S. Borse, "Transmission risk reduction in image sharing scheme with diverse image media". International Conference on "Recent Research Development in Science, Engineering and Management",2016.
[5] Thanuganesh.M, Saranya.R, "Assorted Image Based Obscure Techniques in Visual Cryptography", International Journal of Computer Science and Information Technologies, Vol. 5 (6), 2014.
[6] Miss A.A.Naphade Dr. R.N.khobaragade Dr.V.M.Thakare, "Improved nvss scheme for diverse image media". International Conference on Science and Technology for Sustainable Development, Kuala Lumpur, MALAYSIA, May 24-26, 2016.
[7] D. S. Tsai, G. Horng, T. H. Chen, and Y. T. Huang, "A novel secret image sharing scheme for true-color images with size constraint".
[8] Gayathri Soman, Mr. Jyothish K John,"Secure Digital Image Sharing Using Diverse Image Media". International Journal of Innovations & Advancement in Computer Science IJIACS ISSN 2347 – 8616 Volume 4, Special Issue September 2015.
[9] Z. Wang, G. R. Arce, and G. D. Crescenzo, "Halftone visual cryptography via error diffusion", IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 4, NO. 3, SEPTEMBER 2009.