Confidential Image Sharing Using Visual Secret Sharing Scheme

[1] Chaitanya Khoje [2] Akhil Bhosale [3] Vedang Bhide [4] Abhishek Bhavsar [5]S.P. Pattanaik
[1][2][3][4][5] Department of Computer Engineering
Savitribai Phule Pune University
[1]chaitanyakhoje9@gmail.com [2] akhilbhosale1468@gmail.com [3] vedangbhide0602@gmail.com
[4] bhavsar.abhishek.147@gmail.com [5] pattanaik.swapnalini@gmail.com

***Abstract*: Visual Secret Sharing Scheme deals with hiding a confidential/secret image in arbitrarily selected natural images called as shares. Sharing and delivering secret images is also known as a visual secret sharing scheme (VSSS). The standard VSSS suffers from a risk for the secret image being tampered during the transmission process. To address this problem, we are proposing a natural image-based Visual Secret Sharing Scheme that shares secret images via various carrier media to protect the secret and the participants during the transmission process. This scheme deals with the transmission of one digital secret image over n-1 arbitrary images that produce a noise image which is further concealed by embedding it into a Quick Response (QR) code image. The embedding process involves usage of an encoding/decoding technique. This allows us to transfer the secret image over insecure exchange media. During the decryption process the attacker has to read the QR code first and then he needs all the arbitrary shares used in the encryption process to reveal the concealed image as the output will be a noise image.**

***Key Words:* Quick Response (QR) codes, Visual Cryptography, Visual Secret Sharing Scheme, Extended visual cryptography scheme, Natural images.**

I. INTRODUCTION

The motivation of Visual Cryptography (VC) is to securely share secret images in non-computer-aided context/environments; however, devices with computational powers are ubiquitous (e.g., smart-phones). Therefore, sharing visual secret images in computer-aided environments has become an important issue today.

Traditionally for encrypting secret messages in the images, a standard technique known as steganography was used which had a drawback of being vulnerable to unauthorized access to the confidential data; as the images can easily be decrypted by the use of steg-analysis technique. Visual cryptography (VC) is a technique/methodology that encrypts a secret image into n shares (images given as input), with each participant holding one or more shares. So in fact, anyone who holds fewer than n shares won't be able to reveal any information about the secret image. By stacking the n shares the secret image is revealed and it can be recognized directly by the human visual system. Secret images can be of various types: handwritten documents, images, photographs, etc. Sharing and delivering secret images is also called as a visual secret sharing (VSS) scheme.

Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents, 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.

In this paper, we propose a VSS scheme, called the natural image– based VSS scheme (NVSS scheme), to reduce the intercepted risk during the transmission phase. Conventional VSS schemes use a unity carrier (e.g., either transparencies or digital images) for sharing images, which limits the practicality of VSS schemes. In the proposed scheme, we explore the possibility of using diverse media for sharing digital images. The carrier media in the scheme contains digital images, printed images, hand-painted pictures, and so on. Applying a diversity of media for sharing the secret image increases the degree of difficulty of intercepting the shares. The proposed NVSS scheme can share a digital secret image over *n*-1 arbitrary natural images (hereafter 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.

In this paper, we develop efficient encryption/decryption algorithms for the (*n*, *n*) -NVSS scheme. 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.
To summarize the major contributions of this paper:

- Efficient encryption/decryption algorithms for the (*n*, *n*) -NVSS scheme.
- 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 is highly user-friendly and has high manageability, but also reduces transmission risk and enhances the security of participants and shares.

II. DESCRIPTION

The objective of this study is to reduce the transmission risk of shares by using diverse and innocuous media. We make the following assumptions:

1. When the number of delivered shares increases, the transmission risk also increases.

2. The transmission risk of shares with a meaningful cover image is less than that of noise-like shares.

3. The transmission risk decreases as the quality of the meaningful shares increases.

4. The natural images without artificially altered or modified contents have the lowest transmission risk, lower than that of noise-like and meaningful shares.

In the NVSS scheme, the natural shares can be grey or colour photographs of scenery, family activities, or even flysheets, bookmarks, hand-painted pictures, web images, or photographs. The natural shares can be in digital or printed form. The encryption process only extracts features from the natural shares; it does not alter the natural shares. The innocuous natural shares can be delivered by participants who are involved in the NVSS scheme, by the owners of the photographs, or via public Internet. Because the natural shares are not altered, it is likely that they will not arouse suspicion during transmission. Even if the natural shares are intercepted, it will not be possible to verify that there is any hidden information in the images before reaching the decryption threshold. In such a scenario, the transmission of the innocuous natural shares is more secure than the transmission of shares in another form, such as noise-like or meaningful shares. Another share, which is generated by the secret image and features that are extracted from *n*-1 natural shares, can be hidden behind other media and then delivered by a disciplined person or via a high-security transmission channel.

III. SYSTEM ARCHITECTURE

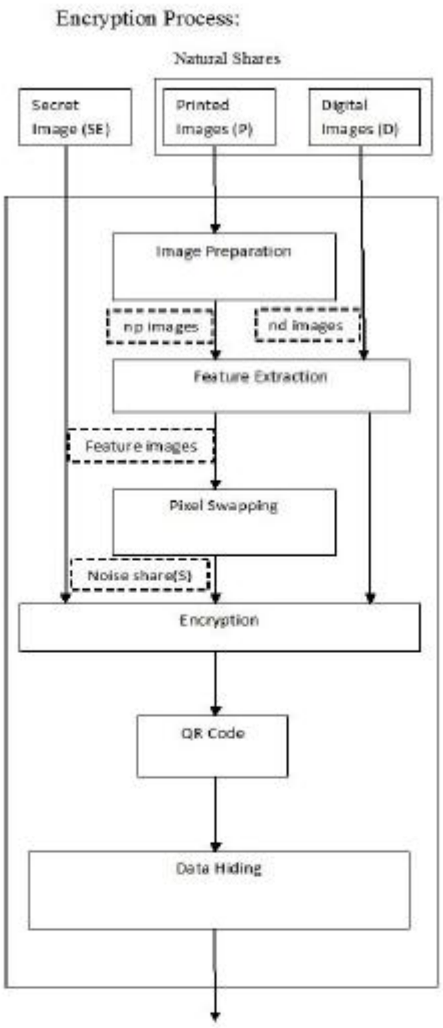

Fig. 1: System Architecture

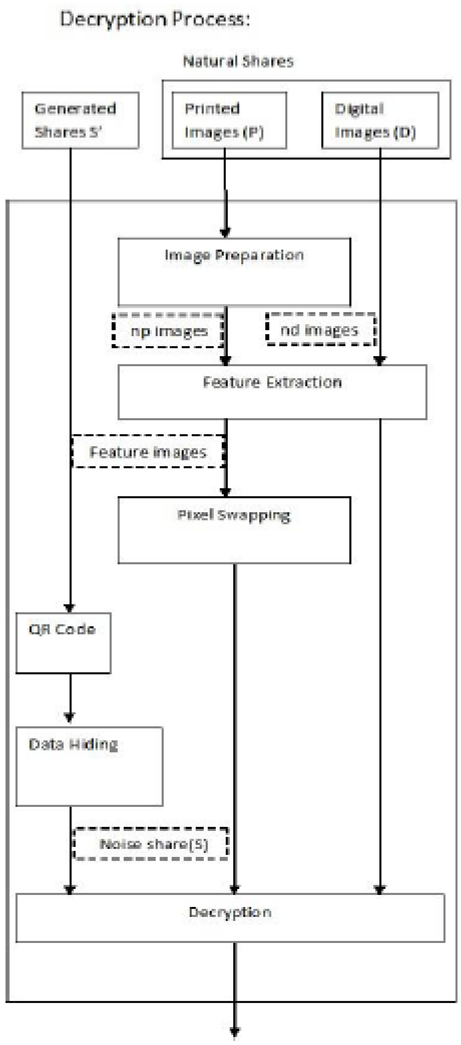

Fig. 2: System Architecture

IV. PROPOSED SYSTEM

In the process of encryption it only extracts features from the natural shares; but without altering the natural shares. In the image preparation and pixel swapping processes are used for pre-processing printed images and for post-processing the feature matrices that are extracted from the printed images. Image preparation process contains three small operations on printed image such as acquire image, crop image, resize image.

The methodologies are as follows;

A) Feature Extraction Process

1. The Feature Extraction Module

This module consists of 3 processes namely Binarization, stabilization, and chaos processes. Firstly, the task is a binary feature matrix is extracted from natural image N via the Binarization process. Then, the stabilization balances the occurrence frequency of values 1 and 0 in the matrix. At last, the chaos process scatters the clustered feature values in the matrix.

2. Image Preparation and Pixel Swapping Processes

These processes are used for pre-processing printed images and for post-processing the feature matrices that are extracted from the printed images. The printed images were selected for sharing secret images, but the contents of the printed images must be acquired by computational devices and then be transformed into the digital data.

B) Encryption/Decryption Process

Encryption: The input images include *n* -1 natural shares and one secret image. The output image looks like a noise-like share image. Decryption: Input images include *n*-1 natural shares and 1 noise-like share. The output image is a recovered image i.e. image with secret message.

C) Hide the Secret Noise-Like Share

The Quick-Response Code (QR code) technique is used to hide the secret image. The QR code is a two-dimensional barcode.

`A QR code uses four standardized encoding modes i.e. numeric, alphanumeric, byte / binary, and kanji to efficiently store data. A barcode is a machine-readable optical label that contains information about the item to which it is attached. This QR code encodes meaningful information. The noise-like share as the numeric type of the QR code. The encoding process consists of two steps:

1) Transform pixels on the share into binary values and represent the values in a decimal format.

2) Encode the decimal values into QR code format. Also the multiple QR can be used to encode more data bits.

The QR code generator is used to encode the secret image in the QR code i. e. stego share. The QR code can be read by using QR cod scanner and smart phone devices. It is necessary to provide security to the QR code also so that no one can easily read that particular QR code. That's why the concept of applying digital signature to the QR code is most important to provide security to QR code.

For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimer sender. In other word we can say that a Digital signature is a mathematical scheme for demonstrating the authenticity of a digital message/document.

V. MATHEMATICAL MODEL

Set theory:

System Description: Let S be the required System,

A system S is defined as a set such that:

System S = {Input, Output, constraint}

Input:
For Encryptor:-
Input = {Secret Image, Cover Image1, Cover Image2}
Secret Image SI = {SI1, SI2……………., SIn}
For Decryptor:-
Input = {QR Code Image, Cover Image1, Cover Image2}
Output:
For Encryptor:-
Output = {QR Code Image}
For Decryptor:-
Output = {Secret Image}
Constraint:
Constraint C = {C1, C2, C3}
Where,
C1 = "Secret Image, Cover Image 1 and Cover Image 2 should have same resolution"
C2 = "If the image is a square image then the square size should be in even numbers"
C3 = "Images with the extension .jpg and .png will be accepted by the system. Other image extensions will not be accepted."
SPACE COMPLEXITY:
The space complexity depends upon the storage space used in the database. In our system database isn't required at the back end the images are only stored on the internal HDD and SQL isn't required. So the space complexity is O (n).
TIME COMPLEXITY
The time complexity depends upon the time required for specific set of inputs to work in the procedure given in the system to produce the output.
In our system the best case time complexity can be given as O($n2$) when the input image is of the same resolution as expected by the system.
For average case time complexity: O($n2logn$) when input image has greater resolution than the expected, the image is rescaled to the system required resolution.

VI. CONCLUSION

The paper proposes a natural-image based Visual Secret Sharing (VSS) scheme, which can share a digital image using diverse image media. The media that include n-1 randomly chosen images are non-modified in the encryption phase. Therefore, they are totally innocuous. The NVSS scheme uses only one noise share for sharing the secret image. The proposed Natural-image based VSS scheme if compared with existing VSS schemes can considerably reduce transmission risk and provide the unquestionable level of user-friendliness, both for shares and for participants. This system provides three major contributions mentioned as followed. First, we successfully introduce hand-printed images for image-sharing schemes. Next, this system proposes a useful concept and method for using unaltered images as shares in a Visual secret sharing scheme. Lastly, we develop a method to store the noise share as the Quick Response (QR) code.

REFERENCES

[1] F. Liu and C. Wu, "Embedded extended visual cryptography schemes", IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307322, Jun. 2011.

[2] Kang, G. R. Arce, and H. K. Lee,"Color extended visual cryptography using error diffusion", IEEE Trans. Image Process., vol. 20, no. 1, pp. 132145, Jan. 2011.

[3] T. H. Chen and K. H. Tsao, User-friendly random-grid-based visual secret sharing, IEEE Trans. Circuits Syst. Video Technol., vol. 21, no. 11, pp. 16931703, Nov. 2011.

[4] T. H. N. Le, C. C. Lin, C. C. Chang, and H. B. Le, A high quality and small shadow size visual secret sharing scheme based on hybrid strategy for grayscale images, Digit. Signal Process, vol. 21, no. 6, pp. 734745, Dec. 2011.

[5] Archana B. Dhole*, Prof. Nitin J. Janwe, An Implementation of Algorithms in Visual Cryptography in Images, Volume 3, Issue 3, 2250-3153, March 2013.

[6] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Extended capabilities for visual cryptography, Theoretical Comput. Sci., vol. 250, nos. 12, pp. 143161, Jan. 2001.

[7] Kai-Hui Lee; Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media," in *Information Forensics and Security, IEEE Transactions on* , vol.9, no.1, pp.88-98, Jan. 2014.