A Survey on Sharing Secret Image using NVSS Scheme

Sejal Patel
Research Scholar (Computer Engg.)
DYPIET (Pimpri)
Pune, India

Jyoti Rao
Assistant Professor (Computer Engg.)
DYPIET (Pimpri)
Pune, India

ABSTRACT
Secret sharing is of great importance for sharing secret or confidential information. This information can be in the form of documents, images, photographs and many more. Most of the previous visual secret sharing scheme uses shares to conceal secret images. The shares may be printed or in digital form. When the secret image is hidden into the shares, noise-like pixel appears which increase the risk of transmission. Attackers look at image having noise-like pixels with suspicion and try to intercept the image. Thus image having noise is not safe for transmission over network. Due to this transmission risk is involved in visual secret sharing. In order to overcome such problems some authors have presented another scheme known as Natural image based Visual Secret Sharing Scheme (NVSS Scheme). In this scheme the transmission of secret image occurs through different media in order to protect the secret. The n out of n NVSS scheme can transmit a digital secret image by randomly choosing n-1 natural images and one noise share. Natural images may be in digital or printed form. Noise-like share is produced by natural image and printed image. The natural shares which are unaltered minimize the risk associated during transmission.

Keywords
Natural images, transmission risk, visual secret sharing, Natural Image based Visual Secret Sharing.

1. INTRODUCTION
Rapid growth of Internet which is the collection of computer and communicating devices that are linked together via some media for the transmission of different information requires security. The conventional Cryptography is a method of converting the original data into an encrypted format called the cipher text. Visual cryptography (VC) [1] is a method that is used to encrypt a secret image into *n* shares. In this every participant can hold one or more shares. To reveal back the original secret image n shares are put together in (n, n) VC Scheme.

Visual secret sharing (VSS) [2] scheme is used for concealing a secret image. This scheme works by dividing the secret image into shares. Human visual system is used to decrypt the shares with great ease. Its idea is to encrypt the secret image into n meaningless share images. It is not able to reveal any information of the shared secret by any combination of the n share images except for all of images.

The drawback of VSS scheme is that it suffers from transmission risk as the shares are like noise which can seek the attacker's attention therefore the shares may be intercepted. The VSS scheme is not easy. The VSS limits its use as it depends on unity carrier medium for image sharing. In order to overcome the problem of VSS many authors came up with NVSS scheme. Further sections are organised as follows: Section 2 describes NVSS Scheme Section 3 gives related work. Section 4 compares various techniques, Section 5 concludes the paper.

2. NATURAL IMAGE BASED VISUAL SECRET SHARING
NVSS stands for Natural Image based Visual Secret Sharing scheme [15]. This scheme reduces possibility of intercepting shares while it is being transmitted. Earlier VSS schemes made use of unity carrier which may be either digital images or transparencies for image sharing. This is the main limitation of VSS schemes. Using NVSS scheme, it has become possible to use different medium to share images. The medium used as carrier in this technique can be the image which may be in printed form, or digital form, etc. Using diverse medium to share secret image lessens the probability of intercepting the shares.

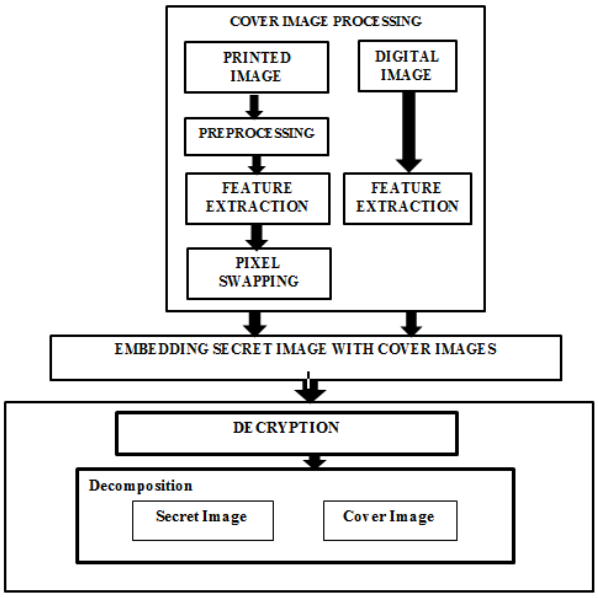

Fig. 1: NVSS Scheme

Fig. 1 shows NVSS Scheme. In this scheme the secret image is embedded into cover image. The cover image may be any of the printed or digital images. If the cover image is printed image then additional pre-processing is to be done. It is then followed by feature extraction and pixel swapping [15]. If the cover image is digital image then feature extraction is performed. There is no need to perform pre-processing in this case. The secret image is then embedded into cover image to generate the share. It is then sent through the network. As the share appears like meaningful image it does not attract the attackers. Hence the transmission of secret image with the cover image is secured. At the receiver end the share is decomposed into secret image and cover image. In this way the transmission of secret image is secured using NVSS scheme.

2.1 Cover Image Processing
This module is the core module which can use either digital or printed images. The printed image is pre-processed using image preparation and pixel-swapping modules.

2.1.1 Feature Extraction

This module performs feature extraction by extracting features from the natural shares. In this the natural shares are not modified. As there is no modification in the natural share, it will not seek the attackers' attention while transmission. In case, if the natural shares are captured, the attackers won't be able to figure out that there is some hidden information behind the image. Therefore, transmitting the innocent share is more secure than transmitting meaningful or noise-like share.

Wavelet transform is one of the methods that can be used for feature extraction. This can reduce the arbitrariness of share that is generated and as a result security is decreased. Another feature extraction method can be employed to produce noise like feature images from natural images so that it produces a noise-like share image. Feature extraction module works in three phases namely binarization process, stabilization process, and chaos processes. In first phase, a feature matrix is generated in binary format from natural image. In second phase, the stabilization is used to equalize the frequency of occurrence of 0 and 1 in the matrix. Lastly in the third phase, the chaos process distributes the clustered feature values in the matrix [15].

2.1.2 Image Preparations and Pixel Swapping Processes

These processes are applied before processing printed images and also after processing the feature matrices. The contents of the printed images must be first given to computational devices before converting into digital data [15].

2.2 Embedding Technique

This technique combines the cover images and secret image to generate share for security purpose. The generated share appears as natural share. Therefore, it does not give any clue that some secret image or secret data is embedded with it. Hence, the security is increased. After embedding the secret image with cover image the generated natural share is transmitted over network to the receiver.

2.3 Decryption Module

Decryption takes place at the receiver side. When the generated share is received by the receiver, it performs the decryption to get the secret image. At this stage the generated share is decomposed into cover image and secret image. In this way, receiver can receive the secret image securely.

3. RELATED WORK

Moni Naor et al. presented a VSS technique which was termed as (k, n) secret sharing problem. They made assumptions that the image consists of B&W pixels where every pixel is controlled independently. The white pixel signifies the transparent color. The drawback is that the deciphering process results in loss of contrast [1].

Yang et al. presented new techniques of coloured VSS schemes. The construction methods are dependent on the extension of the black & white VSS schemes. It has seen that presented coloured VSS schemes can improve the block length [2].

Yang et al. also has suggested novel (k, n) Probabilistic VSS schemes with non-expandable shares size which was dependent on probabilistic technique. He also presented (2, 2), (2, n) and (k, n) schemes depending on the probabilistic technique. The contrast level of this method is same as the traditional VSS scheme. Furthermore, they also illustrated that the traditional VSS scheme can be converted to Prob VSS scheme by using transfer function. Thus, Prob VSS scheme has a distinct view than the traditional VSS scheme. For reconstructing the secret; the process is same as those of non-probabilistic schemes [3].

Zhou et al. presented halftone visual cryptography technique for performing VC via halftoning. In order to encrypt the binary secret image into n halftone image that is intended to contain some important visual information, this method uses void and cluster algorithm [17]. The result of simulation reveals that the generated halftone shares have better visual quality [4].

Chen et al. has introduced (n, n) and (2, n) scheme for secret sharing of image dependent random grids. While encrypting and decrypting the image no pixel expansion takes place which adds as an advantage for this method. In this method encryption process utilizes code book. At the receiver end the decryption takes place by overlapping all n shares in (n, n) scheme and at least 2 shares in (2, n) scheme. This process does not require any computation rather it uses human visual system to regenerate the image. The quality of regenerated secret image is good by using this process [5].

Lin, T.L et al. presented multiple secrets sharing scheme with no pixel expansion in 2010. They presented two secrets in which there is no pixel expansion. Also, it does not need codebook to encode the secret images. It was observed that the pixel expansion was 4 times less as compared to the earlier schemes after applying aspect ratio constraints. Through the separation and disguising processes, two shares where meaningless images individually. They did not disclose any data of the secret images. Therefore, the security rule of VSS schemes is obeyed. For recovering the secret, both shares were overlapped and HVS was able to identify the recovered image. This scheme resolved the serious pixel expansion problem. Authors also carried out a new study that differs from the former schemes [6].

Lou et al introduced a VSS scheme in which two meaningful image known as cover image is used to conceal a secret image. The shares obtained using this technique does not suffer from pixel expansion. To check the validity of the secret image at the receiver side, an additional confidential image is embedded in the two share images. The secret image can be revealed by overlapping them. This does not require any complex computation. This scheme is also used for sharing color image securely [7]

Alex et al. presented different methods for error diffusion in order to enhance the quality of image in the halftone shares. The halftoning VC is used to introduce the pixels of secret information into an uncoded halftone shares that existed before. VC is applied with halftoning in which the continuous-tone image is initially converted into a binary image followed by applying VSS to it. Conversion of secret image into halftone share is performed by acquiring meaningful visual information by simultaneously applying error diffusion to halftone shares. The complexity with using error diffusion is less. It also provides halftone shares having good quality image. The secret image regenerated is gained by putting together the qualified shares and it does not suffer from cross interference of share images. [8]

Shyu et al. presented a scheme to define some of the operations onto a share or transparency which based upon either turning over or flipping around. Then the author has introduced visual cryptographic schemes which have ability to encrypt two or four secrets into shares of two rectangular

shapes as well as gives up to eight number of secrets into shares of two square shapes but the secrets can't be achieved from any one or single image share, where as they are released by merging the two shares under different combinations of various operations such as turning or flipping operations. The introduced scheme explains the relationship among the encrypted shares and also the shared secrets, expanded the research scope and enriched the applicability and flexibility of VC scheme or image encryption process theoretically as well as practically. The scheme for sharing four and eight secrets is also examined [9]

Sasaki et al. provided the formulation of VSS encryption for multiple secret. The restriction with EVCS Scheme was that each share had additional secret image associated with it. Even the restriction with VSS-*q*-PI was that multiple secret images are accompanied with the corresponding shares in qualified sets but the shares in forbidden sets must be similar. Therefore they presented a generalized VSS scheme for encrypting multiple secret image [10].

Askari et al. provided the extension to the previous VSS was given by presenting (2, 2) VSS scheme without causing size expansion. This approach aims to encrypt a secret block having four pixels into two shares based on the distribution of B&W pixels. This can permit the restoring of secret image with XOR operation. This technique is applicable to binary as well as halftone images. It does not cause pixel expansion [11].

Xiao-Yi Liu et al. proposed a new color VCS that is based on the modified VC. Such type of scheme can share secret images such as a color secret image using various random natural images and one noise share image. Rather than alteration of natural image features, the encryption method take the features from every natural image. This is how the proposed scheme can efficiently decrease the transmission risk problem and also overcome the share management problems. This scheme overcomes the problem of expansion of pixel and creates the ease to regenerate secret images without quality loss. Due to this, the suggested scheme can share black & white pixels, gray-level VC or color images VC in secret manner easily [12].

Tso et al. introduced a novel image sharing method to overcome various issues such as low quality of recovered image, problem related to pixel expansion, and generating meaningless shares for image sharing. This method starts with decomposing the secret image and encoding them into n shares. These shares are then embedded into cover images. This technique can be used to construct meaningful shares for image sharing. The size of original secret image and the constructed share is same. On the receiver end when all the shares are stacked the quality of the regenerated image is clearer and has no distortion [13].

Chen et al. proposed the quality-adaptive RG-based VSS scheme which enhances the visual quality of reconstructed images thus securing the transmission. This can be applicable to many VSS techniques. The proposed scheme is feasible to encrypt binary secret images as well as grey level and colour secret images. The the light transmission of constructed shares is greater as compared to earlier technique and also the visual quality of regenerated secrets is better.[14]

Kai-Hui Lee et al. proposed (*n*, *n*) NVSS scheme which enables us to share a secret image in digital form image using *n* - 1 different natural images and one noise-like share. The natural image may be in any format like printed, digital etc. The natural shares are not altered. These natural shares and the secret image are used to produce the noise-like share. These shares are different and natural, therefore it decreases the risk related with transmission. They also proposed some technique to hide the noise-like share for securing its transmission. They carried out experiment and revealed that their presented approach is the best way to solve the problem of transmission in VSS [15].

Lin et al. designed the hybrid codebook, approach such that any two shares can be used to regenerate the original image and verification image. The hybrid codebook was designed such that the two codebooks (2, 2) and (2, 3) were combined for encryption process. The concept of verification image in this system is used for checking the legitimacy of the shares. Any two shares are able to regenerate the verification image by shifting the generic shares in various locations to hide the verification images into it. Hence, this system can detect fake shares. This hidden verification images itself in the generic created shares removes the need of maintaining extra verification shares with the low computational costs. [16]

4. COMPARISION

Table 1 shows comparison of various VSS techniques.

Table 1. Comparison of Various VSS Techniques

Schemes	Encryption Techniques	Meaningful shares	Color Secret Shares	Quality of recovered image	Pixel Expansion
[3]	Probabilistic	No	No	Recognizable	No
[4]	Halftone	No	No	Recognizable	Yes
[5]	Random Grids	No	No	Recognizable	No
[6]	Multiple Secrets	No	No	Recognizable	No
[7]	Cover Image	Yes	Yes	Recognizable	No
[8]	Error Diffusion	No	No	Recognizable	Yes
[12]	NVSS	Yes	Yes	Recognizable	No

[13]	(n, n) VSS	Yes	Yes	Recognizable	No
[14]	Random Grids	Yes	Yes	Recognizable	No
[15]	NVSS	Yes	Yes	Recognizable	No

5. CONCLUSION

This paper gives the review of various VSS and NVSS techniques. It can be concluded from the above survey that NVSS scheme can be applied to share image using different image media. This scheme reduces possibility of intercepting shares while it is being transmitted. This scheme uses diverse media to avoid risk of transmission. This scheme can be useful in sharing a color secret image using natural image. Using this approach the risk associated with transmission as well as share management problems is solved. Future scope must be to hide the secret into video.

6. REFERENCES

[1] Naor, Moni, and Adi Shamir. "Visual cryptography." *Advances in Cryptology—EUROCRYPT'94*. Springer Berlin/Heidelberg, 1995.

[2] Yang, Ching-Nung, and Chi-Sung Laih. "New colored visual secret sharing schemes." *Designs, Codes and cryptography* 20.3 (2000): 325-336.

[3] Yang, Ching-Nung. "New visual secret sharing schemes using probabilistic method." *Pattern Recognition Letters* 25.4 (2004): 481-494.

[4] Zhou, Zhi, Gonzalo R. Arce, and Giovanni Di Crescenzo. "Halftone visual cryptography." *Image Processing, IEEE Transactions on* 15.8 (2006): 2441-2453.

[5] T.H. Chen, K.H. Tsao, "Visual secret sharing by random grids ", *Pattern Recognition*, vol. 42, no.9, pp.2203–2217, 2009.

[6] Lin, Tsung-Lieh, et al. "A novel visual secret sharing scheme for multiple secrets without pixel expansion." *Expert systems with applications* 37.12 (2010): 7858-7869.

[7] Lou, Der-Chyuan, et al. "A novel authenticatable color visual secret sharing scheme using non-expanded meaningful shares." *Displays* 32.3 (2011): 118-134.

[8] Alex, Nitty Sarah, and L. Jani Anbarasi. "Enhanced image secret sharing via error diffusion in halftone visual cryptography." *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*. Vol. 2. IEEE, 2011.

[9] Shyu, Shyong Jian, and Kun Chen. "Visual multiple secret sharing based upon turning and flipping." *Information Sciences* 181.15 (2011): 3246-3266.

[10] Sasaki, Motoharu, and Yoshihiro Watanabe. "Formulation of visual secret sharing schemes encrypting multiple images." *Acoustics, Speech and Signal Processing (ICASSP), 2014 IEEE International Conference on*. IEEE, 2014.

[11] Askari, Nazanin, Cecilia Moloney, and Howard M. Heys. "A novel visual secret sharing scheme without image size expansion." *Electrical & Computer Engineering (CCECE), 2012 25th IEEE Canadian Conference on*. IEEE, 2012.

[12] Liu, Xiao-Yi, Ming-Song Chen, and Ya-Li Zhang. "A new color visual cryptography scheme with perfect contrast." *Communications and Networking in China (CHINACOM), 2013 8th International ICST Conference on*. IEEE, 2013.

[13] Tso, Hao-Kuan. "Secret Sharing Using Meaningful Images." *Journal of Advanced Management Science* 1.1 (2013).

[14] Chen, Tzung-Her, et al. "Quality-adaptive visual secret sharing by random grids." *Journal of Systems and Software* 86.5 (2013): 1267-1274.

[15] Lee, Kai-Hui, and Pei-Ling Chiu. "Digital image sharing by diverse image media." *Information Forensics and Security, IEEE Transactions on* 9.1 (2014): 88-98.

[16] Lin, Chih-Hung, et al. "Multi-factor cheating prevention in visual secret sharing by hybrid codebooks." *Journal of Visual Communication and Image Representation* 25.7 (2014): 1543-1557.

[17] Ulichney, Robert. "The void-and-cluster method for dither array generation."*SPIE MILESTONE SERIES MS* 154 (1999): 183-194.