TRANSMISSION RISK REDUCTION IN IMAGE SHARING SCHEME WITH DIVERSE IMAGE MEDIA

Priyanka R. Pawar[1], Manjusha S. Borse[2]

[1] PG Student, [2] Assistant Professor, Department of Electronics & Telecommunication Engineering, Kalyani Charitable Trust's- Late G. N. Sapkal College of Engineering, Nashik, Maharashtra.

.

ABSTRACT

The main 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 digital form. VSS scheme increases interception risk during transmission of the shares because the shares can looks like noise-like pixels or as meaningful images. For the secret itself and for the participants who are involved in the VSS scheme, VSS schemes suffer from a transmission risk problem. To avoid this problem, we proposed a natural-image-based VSS scheme (NVSS scheme). To protect the secret and the participants during the transmission phase, NVSS schemes shares secret images via different carrier media. NVSS scheme involved can share one digital secret image over arbitrary selected natural images (called natural shares) and one noise-like share. The noise-like share is initiated based on these natural shares and the secret image. The unaltered natural shares greatly reducing the transmission risk problem because the natural shares are diverse and safe. We also proposed possible ways to conceal the noise-like share to decrease the transmission risk problem for the share.

Keywords : Data Hiding. Natural-Image-Based VSS Scheme, Transmission Risk, Visual Secret Sharing Scheme

I INTRODUCTION

In day today life information is increasingly important, but securely sharing this information is more important. Security is important issue in today's world and securing useful data is very essential, so that the data cannot be intercepted or misused by any kind of unauthorized use. The hackers are always ready to get personal data or important information of a person or an organization and use them in various unauthorized ways. Various techniques are used to overcome this problem. A method of transforming message into an unreadable format which is called as cipher text known as "Traditional Cryptography". To read the original data the receiver has to decrypt the message with the secret key. Cryptography makes use of hash function that uses some mathematical function to encode the data which protects the data during transmission. It is basically used in ecommerce, military and to transmit confidential data over the communication media. The original data is then decrypted by calculating some hash function.

A technique called visual cryptography that encrypts a secret image into n shares with each holding one or more shares. Any information about the secret image cannot be understand if anyone holds less than n shares. The secret can be understand when the n shares of the image are put together. Secret images sharing and delivering over the network is known as visual secret sharing (VSS) scheme. VSS scheme has two drawbacks; first, transmission risk is high because holding noise-like shares. Thus probability of transmission failure is increases. Second, the meaningless shares are not user friendly. It would be difficult to manage the shares, as the number of shares increases, which does not provide any information for identifying the shares. A method called natural-image-based VSS scheme (NVSS scheme) is proposed. The interception risk during transmission phase is reduced by using this method. Traditional VSS scheme uses a unity carrier for sharing images. But in this technique diverse media are used for sharing digital images. The data hiding techniques are used to hide the obtained share i.e. noise-like share, to increase the security during transmission of shares.

II RELATED WORK

Major issues in visual cryptography schemes (VCSs) are reducing the pixel expansion and improving the display quality of recovered images particularly for large k and n. Moreover, the development of a systematic and practical approach for threshold VCSs is a challenge. In this paper, in order to encrypt binary secret images, a pixel-expansion-free threshold VCSs approach based on an optimization technique is proposed. In addition to contrast, in the evaluation of the display quality of recovered images we consider blackness as a performance metric. In order to maximize the contrast of recovered images that are subject to density-balance and blackness constraints, we first formulate the problem as a mathematical optimization model. We then develop a simulated-annealing-based algorithm to solve this problem. Furthermore, we try to promote the contrast by slightly relaxing the density-balance constraint. The experimental results show that the proposed optimization-based approach significantly outperforms previous methods in terms of both the pixel expansion factor and the display quality of recovered images.

Conventional visual cryptography (VC) suffers from a pixel-expansion problem, or an uncontrollable display quality problem for recovered images, and lacks a general approach to construct visual secret sharing schemes for general access structures. To address these issues we propose a general and systematic approach without sophisticated codebook design. This approach can be used for binary secret images in non-computer-aided decryption environments. To avoid pixel expansion, to encrypt secret pixels rather than using the conventional VC-based approach we design a set of column vectors. We begin by formulating a mathematic model for the VC construction problem to find the column vectors for the optimal VC construction, after which we develop a simulated-annealing-based algorithm to solve the problem. The experimental results show that the display quality of the recovered image is superior to that of previous papers [1, 2].

The problem occurred in the VC scheme that can be overcome by the extended visual cryptography scheme. This VC schemes work on the Share management problem. To get the better solution Kai-Hui Lee and Pei-Ling

Chiu uses a meaningful cover image concept. This type of VC scheme uses binary images. For the purpose of managing shares this technique first construct the meaningful share using an optimization technique. And in the next step it will uses cover images that can be added in each share directly by using the stamping algorithm. As this VC scheme uses binary image they are not able to maintain the quality of recovered image [3-5].

In the Halftone VC scheme Pixel expansion problem can be further considered. Halftone error diffusion method is used in this technique, to convert secret image and the visible image in to the halftone image. Halftone shares are generated, because the secret information is embedded into the halftone shares and it will give the result as recovered good quality of image. This technique can avoid the transmission risk problem [7].

III SYSTEM DETAILS

3.1 Block Diagram of Proposed System

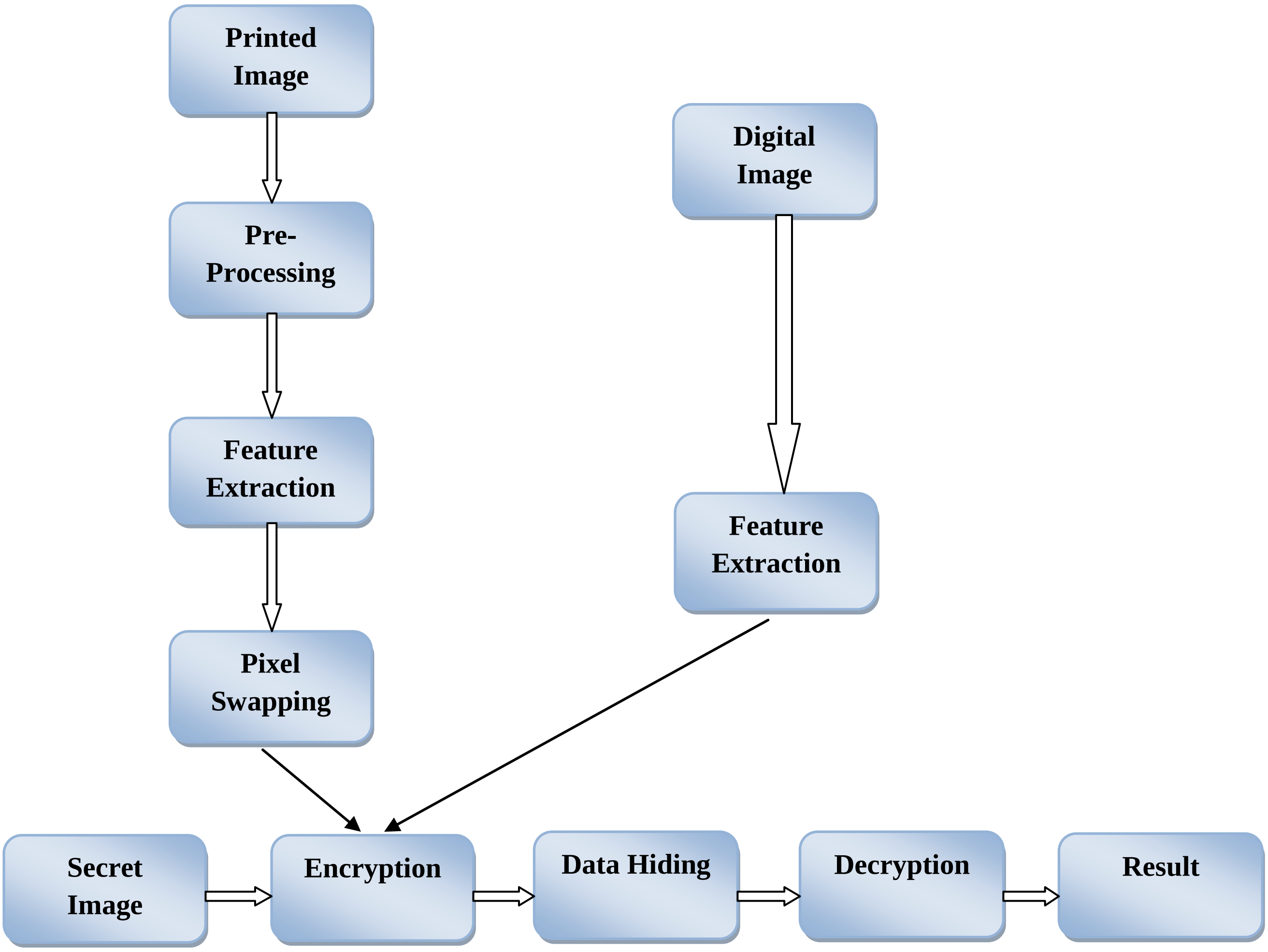

Fig. 1 Generalized block diagram of the system.

In our proposed system (n, n) - NVSS scheme has been implemented. To generate the noise-like share here both printed image and digital image have been taken into account. For further process this natural image needed to be extracted feature. Encryption process can perform with the featured image and secret image. Feature extraction has been performed for two natural shares, so as the natural share's pixels are more efficiently compressed. These extracted features are encrypted with Secret Image. This process is performed by (n, n) – NVSS scheme. Using share hiding algorithm the encrypted image will be hided. The transmission risk of the conventional VSS schemes increases rapidly. On the contrary, the proposed NVSS scheme always requires only one generated share, regardless of the increasing number of shares. Share extraction algorithm performed in decryption process and decryption algorithm applied to recover the Secret image.

3.2 Advantages of NVSS scheme

- In order to implement the natural share by feature extraction and pixel swapping can effectively improve the performance of encryption process.
- The NVSS scheme uses diverse media as a carrier; hence it has many possible ways for sharing secret images.
- 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.

3.3 Applications of NVSS scheme

- Secure Web browsing using Secure Socket Layer (SSL) or Transport Layer Security (TLS) protocols, the use of encryption may be transparent to users.
- Encrypting entity needs to share the key with a separate decrypting entity, the key must be transported to the decrypting entity in a secure manner.
- It also applied in the field of ecology, biometrics and medical applications.

IV EXPECTED RESULT

Conventional visual cryptography schemes suffers from share management, quality of shares, quality of recovered image, pixel expansion, high transmission risk, texture of image. As the number of shares increases, it would be difficult to manage the shares, which does not provide any information for identifying the shares. The proposed NVSS scheme is used to solve these problems. For sharing images traditional VSS scheme use a unity carrier, which limits the practicality of the VSS scheme. But in the proposed method diverse media are used to transmit digital images. The carrier media contains digital images, printed images, hand painted pictures and so on. Using diverse media for sharing the secret image would make hacker's job more difficult. NVSS scheme cannot suffer from share management problem, as it will produce only one share.

The problem of quality maintenance can be overcome as the proposed NVSS scheme uses the natural images. By using the high quality images such as digital images, hand printed pictures, scan photos etc they can avoid the image or share quality problems. The generated share is expansion free as the amount of information required for the generated share is the same as for the secret image. Next is the texture problem of the image as the proposed NVSS scheme uses or work on natural images there will be no any texture problem occurs.

The proposed scheme extracts features from each natural share, rather than altering the contents of the natural images. As this scheme work on the unaltered natural images, due to this there is no any possibility of loss in image texture. These unaltered natural shares are totally safe, hence highly reducing the interception probability of these shares.

Hence this proposed scheme gives the better result over the traditional VSS schemes. It uses the secure share with reversible data hiding which reduces the transmission risk and gives the better quality of recovered image i.e. secrete image. The proposed scheme has a high level of user friendliness and manageability; it also reduces transmission risk and increases the security of participants and shares.

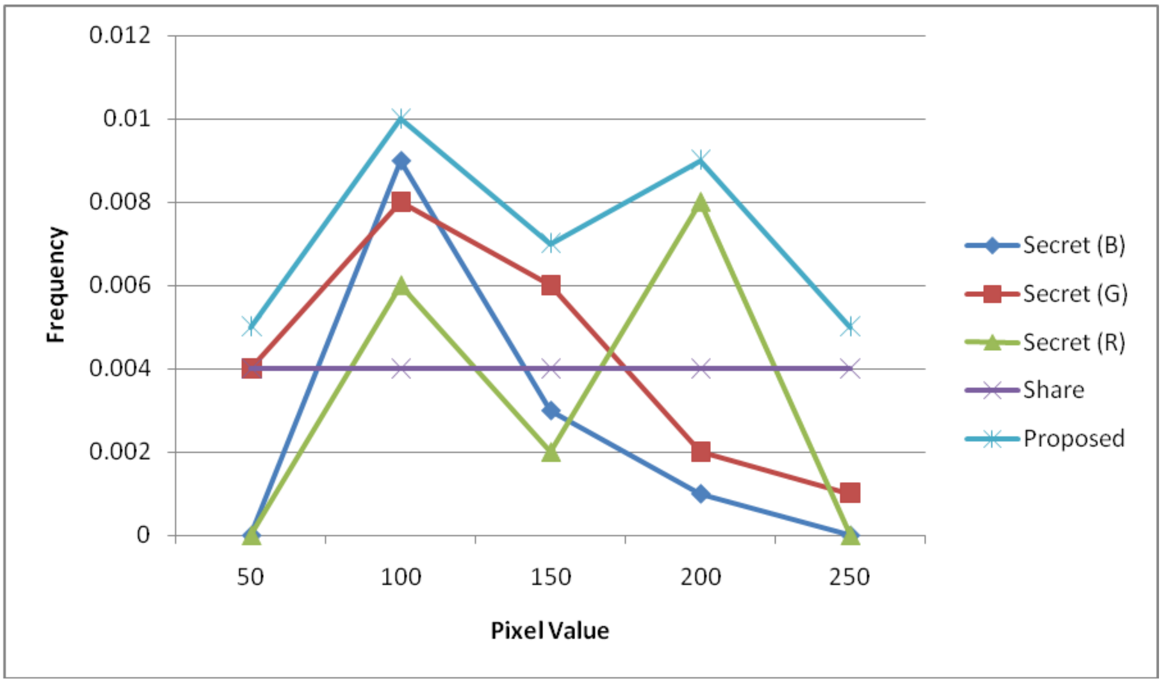

Fig. 2 The distribution of pixel value in share S and secret image SE1.

Table 1 Results of proposed system.

	Secret (B)	Secret (G)	Secret (R)	Share	Proposed
50	0	0.004	0	0.004	0.005
100	0.009	0.008	0.006	0.004	0.01
150	0.003	0.006	0.002	0.004	0.007
200	0.001	0.002	0.008	0.004	0.009
250	0	0.001	0	0.004	0.005

In the above figure the graphic representation showing the statistical results on the distribution of pixel values in share S and secret image (SE1). The distributions in SE1 in the red, green, and blue color planes are denoted as Secret (R), Secret (G), and Secret (B), respectively. The distribution in share S, in each color plane is random, which is totally different from the distribution in secret image SE1. Hence, it is difficult to obtain any information related to SE1 from share S.

V FUTURE WORK

We can segment the secret image, in enhanced system. For all the segmented regions, we will perform the encryption process. In order to achieve the efficient transformation of secret images, in decryption part the same process will inversely perform.

VI CONCLUSION

It can be concluded from the above discussion that the NVSS scheme is effectively used to reduce the transmission risk problem by using natural image as shares and data hiding techniques such as reversible data hiding technique. NVSS scheme is also a user friendly technique for the participants and shares.

REFERENCES

[1] M. Naor and A. Shamir, Visual cryptography, in Advances in Cryptology, *vol. 950.New York, NY, USA: Springer-Verlag, 1995, pp. 112.*

[2] R. Z.Wang, Y. C. Lan, Y. K. Lee, S. Y. Huang, S. J. Shyu, and T. L. Chia, Incrementing visual cryptography using random grids, *Opt. Commun., vol. 283, no. 21, pp. 42424249, Nov. 2010*.

[3] C. N. Yang and T. S. Chen, Extended visual secret sharing schemes: Improving the shadow image quality, *Int. J. Pattern Recognit. Artif.Intell., vol. 21, no. 5, pp. 879898, Aug. 2007.*

[4] K. H. Lee and P. L. Chiu, An extended visual cryptography algorithm for general access structures, *IEEE Trans. Inf. Forensics Security, vol. 7,no. 1, pp. 219–229, Feb. 2012.*

[5] F. Liu and C. Wu, Embedded extended visual cryptography schemes, *IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 307–322, Jun.2011.*

[6] I. 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.*

[7] Z. Zhou, G. R. Arce, and G. D. Crescenzo, Halftone visual Cryptography, *IEEE Trans. Image Process. vol. 15, no. 8, pp. 2441–2453, Aug. 2006.*

[8] Z. Wang, G. R. Arce, and G. D. Crescenzo, Halftone visual cryptography via error diffusion, *IEEE Trans. Inf. Forensics Security, vol. 4,no. 3, pp. 383–396, Sep. 2009.*

[9] P. L. Chiu and K. H. Lee, A simulated annealing algorithm for general threshold visual cryptography schemes, *IEEE Trans. Inf. Forensics Security, vol. 6, no. 3, pp. 992– 1001, Sep. 2011.*

[10] 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.*

[11] Kai-Hui Lee , Pei-Ling Chiu, Digital Image Sharing by Diverse Image media, *IEEE Transactions on Information Forensics and Security, vol 9, No. 1,pp.88-98,January 2014.*

[12] K. H. Lee and P. L. Chiu, Image size invariant visual cryptography for general access structures subject to display quality constraints, *IEEE Trans. Image Process., vol. 22, no. 10, pp. 3830–3841, Oct. 2013.*

[13] G. Ateniese, C. Blundo, A. D. Santis, and D. R. Stinson, Extended capabilities for visual cryptography, *Theoretical Comput. Sci., vol. 250, nos. 1–2, pp. 143–161, Jan. 2001.*

[14] 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. 734–745, Dec. 2011.*

[15] 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, *Inf. Sci., vol. 179, no. 19, pp. 3247–3254, Sep. 2009.*

[16] C. Guo, C. C. Chang, and C. Qin, A multi-threshold secret image sharing scheme based on MSP, *Pattern Recognit. Lett., vol. 33, no. 12, pp. 1594–1600, Sep. 2012.*

[17] P. L. Chiu, K. H. Lee, K. W. Peng, and S. Y. Cheng, A new color image sharing scheme with natural shadows, *in Proc. 10th WCICA, Beijing, China, Jul. 2012, pp. 4568–4573.*