Secured Digital Image Sharing by Using NVSS

Pramod Shimgekar[1], Kishor Wane[2]

[1]Department of ENTC, Dhole Patil College of Engineering, Savitribaiphule University, Pune, India

[2] Professor, Department of ENTC, Dhole Patil College of Engineering, Savitribaiphule University, Pune, India

Abstract: ***Conventional visual secret sharing schemes hide secret images in the form of shares that are printed on transparencies and stored in a digital form. The generated shares appear as noise-like pixels; but it will stimulate suspicion and increase the interception risk during transmission of the generated shares. Hence, visual secret sharing schemes experience from a transmission risk problem for both the secret data image and for the participants who are involved in the sharing process. To tackle this transmission risk problem, we proposed a natural-image-based visual secret sharing scheme (NVSS scheme) which can share the secret data images via various transporter media to protect the secret data image and the participants during the transmission process. The proposed NVSS scheme can share a digital secret data image over n - 1 randomly selected natural images (natural shares) and one noise-like share. The natural images can be of different types such as camera photos or hand-painted pictures in digital or in printed form. The noise-like share is generated based on these natural shares and the secret data image. The unchanged natural shares are diverse and harmless, thus greatly reducing the transmission risk problem. Experimental results will indicate that the proposed scheme is an admirable way out for solving the transmission risk difficulty for the visual secret sharing schemes***.

Keywords: visual cryptography, visual secret sharing, natural image based visual secret sharing.

1. Introduction

Visual Cryptography (VC) is a technique that divides a secret data image into n shares, with each participant holding one share or more than one shares. Anybody who has shares which are fewer than than the generated n shares will fail to expose any information about the final secret data image. To reveal the secret image we have to stack the generated n shares and after regeneration of the image even the human eye can be able to recognize it. The Cryptography is a technique of converting the original data into a scribbled encrypted format called the cipher text. The technique to encode the secret data which will protect it while transmission can be achieved by making use of cryptography, it makes use of hash function that uses some mathematical function to achieve the technique to encode the secret data. This technique is basically used in military, ecommerce and to transmit confidential data. Secret data images can be of different types: photographs, images, handwritten documents, etc. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme.

Sharing secret images has become an important issue today. The generated shares consist of many arbitrary and meaningless pixels which satisfies the security requirement for protecting secret contents to be transmitted, but they will experience two drawbacks: first, high transmission risk is present because of generated noise-like shares will cause attackers‘ doubt and the shares may be detected. Thus, the risk to both the participants and the shares increases, in turn increasing the possibility of transmission failure. Second, the meaningless shares are not user friendly.

2. Proposed Theory

We propose a visual secret sharing (VSS) scheme, called the natural image–based VSS scheme (NVSS scheme), to reduce the interception risk during the transmission phase. In the proposed scheme, we are using various media for sharing digital data images. The various carrier media in the scheme includes digital images, printed images, hand-painted pictures, and images taken from a camera etc. The difficulty degree to intercept the shares is increased by using different ways to share the secret data image. The proposed NVSS scheme can share one digital secret image over n - 1 randomly selected natural images or natural shares and one noise-like share. Here instead of altering thenatural shares content we just extracts the features of the natural shares.These unaltered natural shares are totally harmless and it reduces the probability of these share interception to a great extent. To increase the level of security and making it more easy and secure to transmit during the transmission phase the generated share which is noise-like can be hidden by using different techniques present to hide data.The NVSS scheme makes use of different media as a shipper, hence to reduce the transmission risk the trader can choose an image which cannot be suspected easily as the content of the media.The generated digital shares can be easily stored in a digital devices of participant (e.g., smart phone, digital cameras, laptops, tablets, computers) reducing the risk of being suspected. We can send the printed media (e.g., digital images, hand-painted pictures) through direct mail marketing services, by post or even by e-mail services. In such a way, to increase the security for the shared images the different transmission channels are used, further reducing the transmission risk. Thus the proposed NVSS scheme has a high level of user friendliness and manageability, reducing the transmission risk and enhancing the security of both participants and shares.

3. Literature Survey

According to chengguo, chin-chenchang, chuanqin [1] by using the multi-threshold access sharing of secret image in groups can be achieved. Using this approach multiple secret images can be shared with different group of participants and each image is associated with different access structure. To propose a multi-threshold secret image sharing scheme author has used Hsu et al’s multi secret sharing scheme which is based on MSP (Monotone Span Program). In this scheme corresponding access structure are pre-defined. According to these access structures shadow data can be achieved from multiple secret images by using Hsu et al's method by making use of Least Significant Bit (LSB) replacement can be used to embed the shadow data into the cover images. By collecting a corresponding subset of shadow images each lossless secret image can be reconstructed. The proposed scheme first generates the shadow data. These shadow data is then embedded in the cover image. The integrity of the shadow image is verified in order to avoid the false shadow image transfer to participant during the recovery of the secret image. Then the secret image is retrieved. Thus this scheme is feasible and can achieve high visual quality of shadow image and high embedding capacity.

Kai-hui lee and pei-ling chiu [2] has proposed an extended visual cryptography algorithm for general access structure.The previous approaches suffer from pixel expansion problem. The extended visual cryptography add meaningful cover images in each generated share. The proposed scheme can be used for binary secret images present in non-computer environment. The proposed approach consists of two phases. The first phase is based on given access structure in which meaningless shares are generated using an optimization technique. In the second phase stamping algorithm is used to directly add the cover image in each generated share. Hence by using the proposed approach the pixel expansion problem of EVCS for general access structure is achieved. The display quality of the recovered image is also good.

Tzung-Her Chen and Kai-Hsiang Tsao [3] proposed that in 1987 kafri and keren stated the visual secret sharing technique which was based on random grid. In this scheme pixels of secret image and natural image are divided into two grades grade1 and grade2 depending on which pixel is move on which grade. And at the receiving end grade1 and grade2 is combined, then depending on which pixel belong to which grade move the pixel in grade1 and grade2.In this paper they propose that the pixel expansion is not introduced in random grid visual secret sharing the first random grid G1 is achieved by selecting the white or black color. Then it is provided to a certain private pixel to resolve the grid pixel of G1 and grid pixel of G2. G1 and G2 stacked results are always fully black although the private is black and white or black with ½ probabilities although the private is white. In this way the private is recognizable through stacked random grid.

Pei-Ling Chiu and Kai-Hui Lee [4] has proposed that a threshold visual cryptography scheme is considered of more than one secret data image and n-number of natural images. Only binary image is consideredin Threshold visual cryptography scheme. In order to increase the computation cost and degrade the performance, In the proposed paper, an optimization technique is in order to encipher unseen binary images. Blackness is recognized as a resourceful metric in the display quality measurement of an output image. The problem is first solved as a mathematical optimization in order to exploit the contrast of the output image. To solve this problem they establish a encouraged annealing based algorithm.

InkooKang,Gonzalo.R.Arce and H.K.Lee [5] proposed that the meaningful shares are generated due to encoding of secret image in generated shares by using a visual cryptography encryption method. Color visual cryptography is depended on two principle, one is error diffusion and another is visual information pixel synchronization. Error diffusion is for image halftone generation and synchronization which improves the contrast of shares. The error diffusion in general generates the shares which are pleasant to the human eyes, by synchronizing the visual information pixels beyond the color channels visual contrast of shares can be made better. The paper states the encryption method which improves the visual quality by constructing color extended visual cryptography with VIP synchronization and error diffusion.the original VIP values and the shares of visually high quality is present in before encryption VIP synchronization and after encryption VIP synchronization also.

Z. Zhou, G. R. Arce, and G. D. Crescenzo [6] proposed a framework of common halftone visual cryptography (HVS), where a personal binary image is hidden into halftone share. Blue noise halftone technique is applied in order to generate the halftone shares. These generated half tone are used to transfer the important visible data to the participant like photography, scenery, paintings, and images. The visible character obtained through this current plan is better in comparison made to the extended visual cryptography. In the reviewed paper the technique used to obtain visual cryptography through half tone,is half tone visual cryptography technique. In this method the void and cluster algorithm is used to encrypt a binary personal image into 'n' number of halftone shares which includes the significant visual information. The proposed method generates the visually attractive halftone shares which carry important data better Visual quality is obtained than other available visual cryptography method.

4. Methodology

Initially Secret Image and Natural Images is being selected by the user. Natural Images could be in painted or in the digital image form . The image preparation processes is used for preprocessing of printed images and for post-processing of the feature matrices that are extracted from the printed images. In theImage Preparation process the contents of the printed images can be acquired by popular electronic devices, such as digital scanners and digital cameras. This image is croped in the paint to remove the extra images. Finally, the images are resized in order to have the same dimensions as the natural shares have. In order to be used in an encryption module and decryption module without any fault. Then the pixel swapping is performed to randomize the spatial correlation of pixels present in a printed image. The generated shares are encrypted in the encryption process in order to be transmitted. This shares after receiving are decrypted by the decryption module and we get the secret shared image.

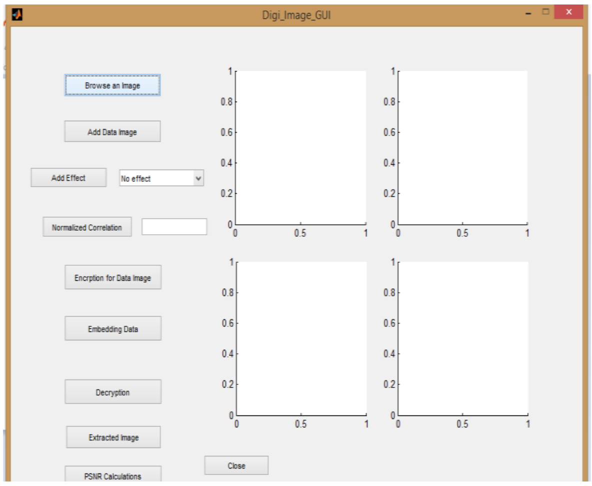

Figure 1: Basic GUI

5. Conclusion

The proposed natural image based visual secret sharing scheme can share a digital image using a diverse media of images. The media includes the randomly chosen images which are unaltered in the encryption phase. Therefore they are totally inoffensive. No matter as the number of participants increases the proposed NVSS scheme make use of only one noise like share for sharing the secret data image. As compared to the existing visual secret sharing schemes the proposed scheme can effectively reduce the transmission risk and provide the high level of user friendliness for both, the shares and the participants.

References

[1] 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.

[2] 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.

[3] Tzung-Her Chen and Kai-Hsiang Tsao,” User-Friendly Random-Grid-Based Visual Secret Sharing,” ieee transactions on circuits and systems for video technology, vol. 21, no. 11, november 2011.

[4] Pei-Ling Chiu and Kai-HuiLee,”A Simulated Annealing Algorithm for General Threshold Visual Cryptography Schemes,”ieee transactions on information forensics and security, vol. 6, no. 3, september 2011.

[5] 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. 132–145, Jan. 2011.

[6] Z. Zhou, G. R. Arce, and G. D. Crescenzo“Halftone visual cryptog- raphy,” IEEE Trans. Image Process., vol. 15, no. 8, pp. 2441–2453, Aug. 2006.

[7] A. Nissar and A. H. Mir, ―Classification of steganalysis techniques: A study,‖*Digit. Signal Process.*, vol. 20, no. 6, pp. 1758–1770, Dec. 2010.

[8] 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.

[9] 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.

Author Profile

Pramodshimgekar received a bachelor’s degree in Electronics and Telecommunication from SipnashikshanPrasarakMandal’s College of Engineering and Technology, SantGadge Baba Amravati University, Amravati in 2012.He is now pursuing his master’s degree in VLSI and Embedded Systems from Dhole Patil College of Engineering and Technology, SavitribaiPhule University, Pune