www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 4 April 2015, Page No. 11615-11620

Visual Secrete Sharing by Diverse Image Media

Aparna Bhosale [1], Jyoti Rao [2]

[1] *Dept. of CSE, D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune, India*
[1]aparnabhosale39@yahoo.co.in
[1] *Dept. of CSE, D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune, India*
[2]jyoti.aswale@gmail.com

Abstract*: Conventional visual secret sharing schemes hide secret images in shares and the image may be printed on transparencies or encoded and also stored in a digital form. The shares of the image can appear like noise pixels or as meaningful images; but it will suspicion and increase interception risk during transmission of the shares. Hence, VSS schemes have limitation that it suffers from a transmission risk problem for the secret itself and for the participants who are involved in the VSS scheme. To overcome the problem of transmission risk, we proposed a natural image based VSS scheme (NVSS scheme) which can shares secret images via different carrier media to protect the secret and the participants during the transmission phase. The above proposed (n, n) - NVSS scheme can share digital secret image over n-1 arbitrary selected natural images (called natural shares) and one noise-like share. The natural shares or natural images can be photos or hand-painted pictures in digital form or in printed form. The shares that look like noisy share can be generated based on these natural shares and the secret image. The unaltered natural shares are various and inoffensive, thus considerably reducing the transmission risk problem.*

Keywords: Cryptography scheme, extended visual cryptography, natural images, transmission risk, Visual secret sharing.

1. Introduction

A technique that encrypts a secret image into *n* shares, with each participant holding one or more shares is visual cryptography (VC). Secret images can be of different types: images, handwritten documents, photographs etc. Sharing and delivering secret images is also known as a visual secret sharing (VSS) scheme. The 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).Conventional shares, which consist of many random and meaningless pixels, satisfy the security requirement for protecting secret contents, but they suffer from two drawbacks: a) 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. b) The meaningless shares are not user friendly. If the number of shares of image increases, it becomes more difficult to maintain the shares, which never give any information for identifying the shares.

In the process of encryption plain text will be encrypted to hide secrete message. A key will be provided to encode it and send that encoded text from source to destination. Other side in decryption process received encoded message will be decoded by using the key and original message will be decrypted. The secrete message extracted from encrypted message. The shared secrete key plays an important role in whole encryption-decryption process.

2. The Classification Of The Existing VSS

Visual cryptography is not much in use in spite of possessing several merits. One of the reasons for this is the difficulty of use in practice. There is need to be superimposed in case of shares of visual cryptography are printed on transparencies. It is not very easy to do precise superposition due to the fine resolution as well as printing noise. Scanning of the share is necessary in many visual cryptography applications need to print shares on paper. The print and scan process can introduce noise. Also consider the problem of precise alignment of printed and scanned visual cryptography shares. Due to the susceptibility in the spatial domain, a frequency domain alignment scheme will be developed. So there is need of employ the Walsh transforms to embed marks in both of the shares so as to find the alignment position of these shares. The experimental results show that the technique can be useful in print and scan applications.

Below fig. shows the classification of VSS schemes from the carriers' viewpoints. Existing research focuses only on using transparencies or digital media as carriers for a VSS scheme. The transparency shares have either a noise-like or a meaningful appearance.

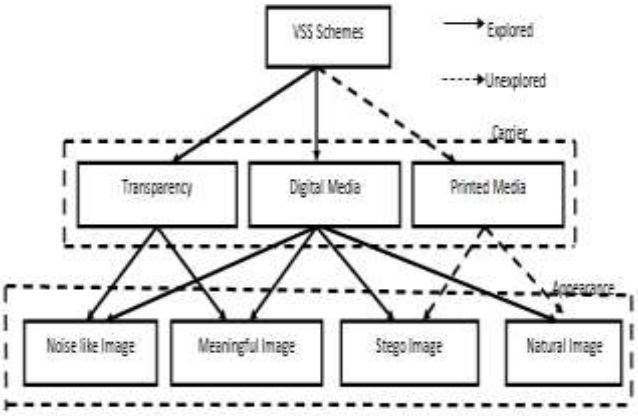

Figure 1: The classification of the existing VSS research from the viewpoints of carriers.

Various VSS schemes are important in the visual cryptography That use images and text messages to hide secrets and provide secure communication. Carrier is the medium that used to transfer the message e.g. digital media, printed media, and transparency. Second is appearance which can be used to display the image in different formats such as noise like image, meaningful image, stego image and natural image. These images are used to hide secrete message and make the communication secure.

3. Literature Survey

Visual cryptography concept came into focus to hide the secret text or image behind another image also this concept used by M. Naor and A. Shamir. These can be done by generating the different shares of the image. Then apply the process of encryption to encrypt that image and send to the proper destination. Other side that received shares can be merged to get the original image. But it suffers from the problem of share management, because they generate more than one share to hide the secret image [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 a by using the stamping algorithm. As this VC scheme uses binary image they are not able to maintain the quality of recovered image [3].

The purpose of such schemes to generate noise-like random pixels on shares to hide secret images which can be done in the conventional visual secret sharing. But it suffers a management problem, because of which dealers cannot visually identify each share. This management problem is solved by the extended visual cryptography scheme (EVCS), which adds a meaningful cover image in each share. However, the previous approaches involving the EVCS for general access structures suffer from a pixel expansion problem [4].

A construction of EVCS which is realized by embedding random shares into meaningful covering shares, and we call it the embedded extended visual cryptography scheme (embedded EVCS). A construction of EVCS which was realized by embedding the random shares into the meaningful covering shares. A method to improve the visual quality of the share images. Embedded EVCS has many specific advantages against different well-known schemes, such as can deal with grey-scale input images, has smaller pixel expansion, always unconditionally secure, does not require complementary share images, one participant only needs to carry one share and can be applied for general access structure [5].

Extended VCS is that where hyper graph colorings are used in constructing meaningful binary shares. Since hyper graph colorings are constructed by random distributed pixels, the resultant binary share contains strong white noise leading to inadequate results. An encryption method to construct color EVCS with VIP (Visual information pixel) synchronization and error diffusion for visual quality improvement. [6].

Gray level visual cryptography is invented to provide the better quality image in the VC scheme. Here they applying adaptive order dither technique as well as existing visual cryptography scheme for binary image to construct the shares. This method reduces the size of decrypted images. The quality of decrypted image will be improved than the ECVS scheme. But this technique suffers from the pixel expansion problem [7].
Pixel expansion problem can be further considered in the Halftone VC scheme. This technique uses Halftone error diffusion method 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 [8].

Technique used for halftone technique is error diffusion method. Which take one gray scale image and convert it into binary image by applying halftone technique? In this binary share images, put secret image pixel in to each share image by applying void and cluster algorithm. The reconstructed image is obtained by superimposing two share images. It is a very good method but still there is a tradeoff between pixel expansion and contrast loss of original image. this method size of pixel is same as original image pixel size. That means relieved secret image size and original image size is same so it reduces the problem of pixel expansion. In this method random grid R is defined as a two dimensional array of pixels. Each pixel is either transparent (white) or opaque (black) by a coin flip procedure The numbers of transparent pixels and opaque pixels are probabilistically same and the average opacity of a random grid is 50% [9-11].

Color image with natural shadow visual cryptography scheme Use the natural image to hide the secret information and one noise-like share image. For the encryption process its need to alter the natural image. So that this type of VC scheme suffers from texture problem i.e. original texture of the image will be lost [12].

In order to guarantee the secret image that transmits through the network will not be stolen, the secret images must be encrypted, the concept of this process is called secret image encryption. The random grid algorithm to encrypt the secret image. The scheme can adjust distortion to infinitesimal it also improve on the problems of decoding. The secret image consists of a collection of pixels, where to each pixel is associated a grey level ranging from white to black and each pixel is handled separately. Any set of qualified participants stack their transparencies they can correctly recover the image shared by the dealer. The security of the scheme, since it implies that, even by inspecting all their shares, any set of forbidden participants cannot gain any information on the value of the grey level of the shared pixel. [13-15].

4. Flow of Visual Cryptography

Visual cryptography proposed by Naor and Shamir discloses the possibility for using human visual ability to perform the decryption process. Specifically, one secret image is encoded into two shares which are seemingly random pictures. The

dealer distributes the two random transparencies to two participants. No any participant tells the secret from his own transparency, but when the two participants overlap their transparencies according to pixel, they recognize the secret from the overlapped result by their visual system. No any type of computational devices or cryptographic knowledge is required for the decryption process.

Color Visual Cryptography is the latest phenomenon for encrypting color secret images. Such secret messages are converted into number of color halftone image shares.

The previous extended visual cryptographic schemes focused on gray scale and black and white visual cryptography schemes. Such type of schemes is not suitable for color shares because they have different structures. There are some actual color visual cryptography schemes that might produce either meaningful or meaningless shares that produce less visual quality which lets people to suspect any kind of encryption involved in producing such shares. Such type of problems can be overcome by recently introduced error diffusion and the Visual Information Pixel (VIP) synchronization techniques to achieve color visual cryptography that can produce meaningful shares besides making the shares in such a way that they are pleasant to human eyes. We also build a prototype application that demonstrates the proof of concept. The experimental results inform that the proposed color visual cryptography can be used in real world applications.

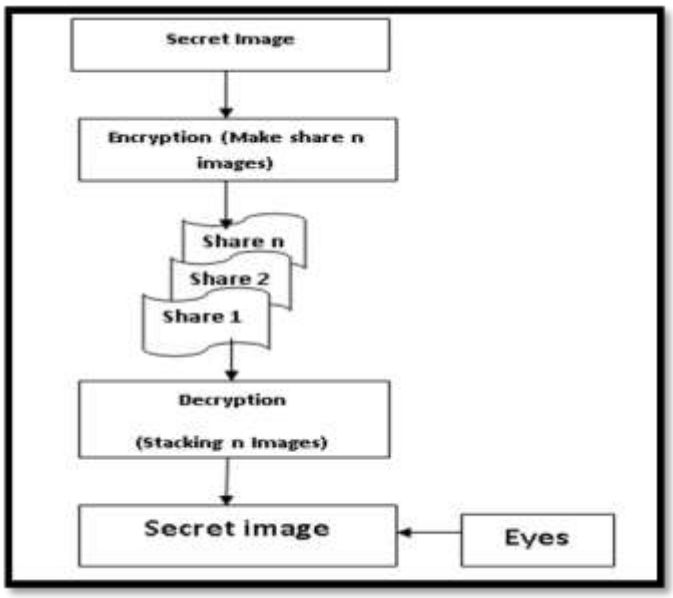

Figure 2: Flow of visual cryptography

Visual cryptography technology, the end user fined an image, which is going to act as the carrier of data. The data file is also selected and then to achieve greater speed of transmission the data file and image file are compressed and sent. Previous to this the data is fixed into the image and then sent. The image if hacked by a third party user will open up in any image previewed but not displaying the data. This protects the data from being invisible and hence is secure during transmission. On the other side the user uses another piece of code to retrieve the data from the image.

The scope of the System provides a friendly environment to deal with images. The tools supports only one kind of image formats. This application supports .gif and .png (portable network graphics) formatted images and the application has been developed using swing and applet technologies, hence provides a friendly environment to users. VCS is a kind of secret sharing scheme that focuses on sharing secret images. The visual cryptography model proposed in is to split a secret image into two random shares (printed on transparencies) which separately reveals no information about the secret image other than the size of the secret image. The secret image can be regenerate by stacking the two shares. The operation of this scheme is logical operation. A VCS with random shares the traditional VCS or simply the VCS. An existing VCS takes a secret image as input, and outputs shares that satisfy two conditions:

1) Any qualified subset of shares can recover the secret image;
2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image.

An example of traditional VCS where, generally speaking, a VCS means any out of shares could recover the secret image. Shares (1) and (2) are distributed to two participants secretly, and each participant cannot get any information about the secret image, but after stacking shares (1) and (2), the secret image can be observed visually by the participants. There are many applications of VCS, for example, transmitting military orders to soldiers who may have no cryptographic knowledge or computation devices in the battle field. Many other applications of VCS, other than its original objective (i.e., sharing secret image), have been found, for example, authentication and identification, watermarking and transmitting passwords etc.

5. The Proposed Scheme

In the below diagram it shows the whole process of encryption. In this process 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 preprocessing 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.

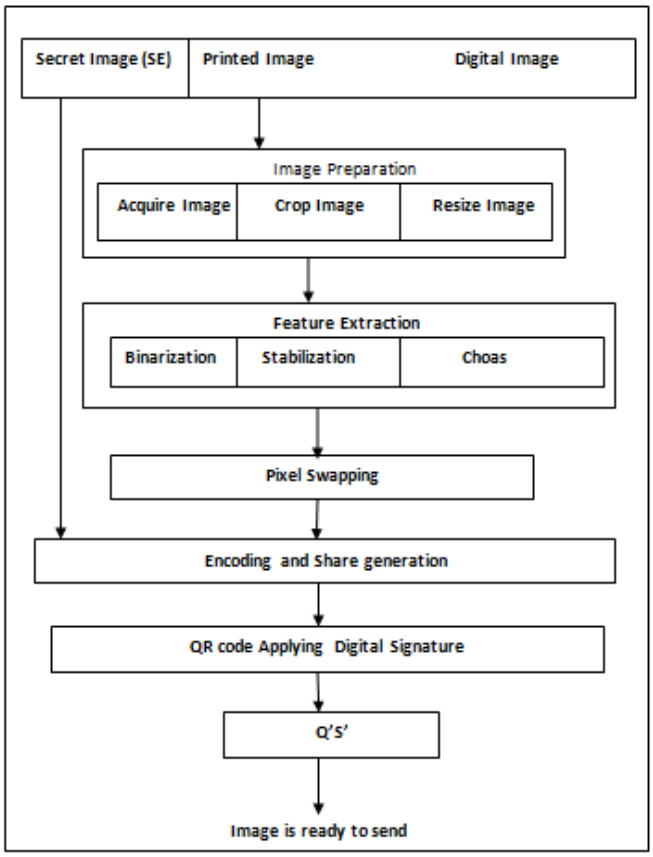

Figure 3: Encryption Process

The feature extraction process is used to extract feature from the natural image by doing the three operations namely Binarization, stabilization, chaos. Binarization process used to extract feature matrix from natural image. Balancing the occurrence frequency of values 1 and 0 in the obtained feature matrix can be done in the process of stabilization. The process named chaos is used to eliminate the texture of the extracted feature images and the generated share. In this process, the original feature matrix will be disordered by adding noise in the matrix.

Image distortion caused by the image preparation process can be tolerated in the pixel swapping process. The image distortions were introduced in the image preparation process was spread in a feature matrix, and the noise also is distributed in the recovered image without clustering together. Lots of the image distortions result in noise that appears in the recovered images and if there is large amount of noise clusters together, then the image is severely disrupted which may cause a bad effect on recovered image that it makes impossible task for the naked eye to identify it. The pixel swapping process is the solution for this problem.

XOR operation used to do the encryption process. Before applying the XOR operation the stacking process of input image S and feature images FI1,…, FI*n*--1 can be done after that the XOR operation can be apply on in each color plane. Then the resultant image S is the share image ready to send to the destination place. This generated share is secure because the share was generated by stacking a secret image and *n*-1 feature images as well as the pixel values in each feature image are distributed randomly and uniformly. These feature images (FI) can be used as *n*-1 one-time pads (OTP). An important OTP system used which is difficult to break. The length of each one-time pad is equal to the length of the secret image. The encryption operation uses the logical XOR operator. By using these different methods the generated share must be secure.

By applying the feature extraction algorithm the generated shares of image have the properties like the new generated share is secure along with the pixel expansion free.

6. Methodology

A) Feature Extraction Process

1. The Feature Extraction Module

The feature extraction module consists of three processes Binarization, stabilization, and chaos processes. First, 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. The Image Preparation and Pixel Swapping Processes

The image preparation and pixel swapping processes are used for preprocessing 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 digital data [1].

B) Encryption/Decryption Process

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

C) Hide the Secret Noise-Like Share

The Quick-Response Code (QR code) technique is used to hide the secrete 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 secrete 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.

Digital signatures employ a type of asymmetric cryptography. For messages sent through a nonsecure 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 or document.

7. Expected Result

In the traditional visual cryptography schemes suffers from share management, quality of shares, quality of recovered image, pixel expansion, transmission risk, texture of image. These problems can be overcome in this proposed NVSS schemes. Here in this scheme it will produce only one share that's why it cannot face the share management problem. This proposed NVSS scheme uses the natural images so that the problem of quality maintenance can be overcome. By using the digital images, hand printed pictures, scan photos etc these are high quality images so that they can avoid the image or share quality problems. The amount of information required for the generated share is the same as for the secret image. So that the generated share is expansion free. 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.

As this scheme work on the unaltered natural images, due to this there is no any possibility of loss in image texture. The widely used concept i.e. QR code can be used with the generated share to transfer over the various channels i. e. from source to destination without any risk. Here an important concept digital signature is applied to the QR code to provide more security the QR code.

Hence this proposed scheme gives the better result over the traditional VSS schemes. It uses the secure share with QR code which reduces the transmission risk and gives the better quality of recovered image i.e. secrete image.

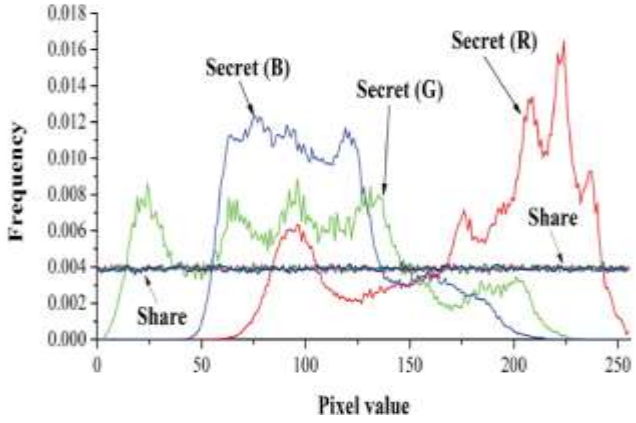

Figure 4: Pixel distribution in share image

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.

8. Conclusion

The proposed VSS scheme, (*n, n*)-NVSS scheme, that can share a digital image using diverse image media. The media that include *n*-1 randomly chosen images are unaltered in the encryption phase. Therefore, they are totally innocuous. Regardless of the number of participant's *n* increases, the NVSS scheme uses only one noise share for sharing the secret image. Compared with existing VSS schemes, the proposed NVSS scheme can effectively reduce transmission risk and provide the highest level of user friendliness, both for shares and for participants. This provides four major contributions.

1) This is the first attempt to share images via heterogeneous carriers in a VSS scheme.

2) Successfully introduce hand-printed images for images-haring schemes.

3) This proposes a useful concept and method for using unaltered images as shares in a VSS scheme.

4) Develop a method to store the noise share as the QR code with digital signature.

Acknowledgment

I express my gratitude towards Prof. Jyoti Rao, of Department of Computer Engineering, Padmashree Dr. D. Y. Patil Institute of Engineering and Technology, Pimpri, Pune who guided and encouraged me. No words are sufficient to express my gratitude to Prof. Pramod Patil for their unwavering encouragement.

References

[1] Kai-Hui Lee and Pei-Ling Chiu, "Digital Image Sharing by Diverse Image Media" ," IEEE Trans. Inf. Forensics Security, vol. 9, no. 1, pp. 88–98, Jan. 2014.

[2] M. Naor and A. Shamir, "Visual cryptography," in Advances in Cryptology,vol. 950. New York, NY, USA: Springer-Verlag, 1995, pp. 1–12.

[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. 879–898, 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] 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.

[7] 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. 201.

[8] 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.

[9] 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.

[10] 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. 4242–4249, Nov. 2010.
[11] 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.
[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] 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,
[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.