International Engineering Journal For Research & Development

Vol.4
Issue 6

E-ISSN NO:-2349-0721

Impact factor : 6.03

DIGITAL IMAGE SHARING BY USING QR CODE TECHNOLOGY

Prof. Ekeshwari A. Rangari
Asst. Prof.
Elect. & Telecom. Engg
ekeshwari.rangari@gmail.com

Prof. Vishwajit K. Barbudhe.
Asst. Prof.
Elect. & Telecom. Engg
vbarbudhe@gmail.com

Dr. Anirudha D. Shelotkar
Head Of Department
Elect. & Telecom. Engg.
JCET, Yavatmal, India
anishelotkar@gmail.com

Prof. Vinay U. Kale
Asst. Prof.
Elect. & Telecom. Engg.,
PRMIRT, Amravati

Abstract-

In the previous methods of sharing the digital image i.e. Visual Secret Sharing (VSS) scheme and Extended Visual Cryptography Scheme (EVSS) arises a transmission risk problem while sharing the secret data. To reduce this unavoidable problem, the solution is given in this paper. This paper introduces a natural-image-based Visual Secret Sharing scheme (NVSS scheme) which is the proposed technique used to reduce the transmission risk problem and also to protect the participant while sharing the data. Here, the data is in the form of digital image. In such a NVSS scheme, one digital image, one printed image i.e. n-natural images and one secret image in the form of digital are needed. All the images are converted into one noise-like share for sharing the secret image. By performing the process of extraction, the secret image will be encrypted by using (n-1) natural shares. This generated data will be hiding by using the QR code technology. At the receiver end, the secret image will be received through the decryption process by performing the XOR operation. The transmission risk is reduced here by transmitting the natural images using a variable secure media.

Keywords— Visual Secret Sharing Scheme, Extended Visual Secret Sharing Scheme, digital images, natural shares, noise-like share, etc.

I. INTRODUCTION

The conventional Visual Secret Sharing (VSS) scheme is not secure to share the secret data. Extended Visual Cryptography Scheme (EVCS) is a user-friendly scheme. Visual Cryptography (VC) is a special image encryption technique. The Visual Cryptography does not need complex computation in the decryption phase. In the decryption at the receiver, the secret data is decrypted without any complex cryptographic computation. It is a simple method which can provide high security for confidential information. In EVCS technique, to construct a set of noise-like shares that is pixel expansion free. Then a cover image directly adds on each share via a stamping algorithm. So, the pixel expansion can be removed entirely and the message is encoded into a binary pattern. In each secret image, each message pixel is represented by a fixed size binary pattern which is called as a share. In this share, which two of the four sub pixels selected randomly are black. The pixel expansion problem arises due to sub pixels.

The problem arises to use of Extended Visual Cryptography Scheme (EVCS) are as follow:

(i) The decryption process need not require complex computation; it may be difficult to analyze every share without computers.

(ii) It would not investigate combinations and statistical data of pixels in shares.

(iii) Storage and transmission of the shares requires an amount of storage and bandwidth resources which equivalent to the size of the secret times the number of shares.

(iv) Expansion of the original pixels on the secret images in encryption phase, which makes lower level of contrast of the reproduced images at the receiver.

In Halftone Visual Cryptography Scheme (HVCS), the 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. The shares contain many noise-like pixels or display low-quality images. Such types of shares are easy to detect by the naked eye. This meaningless shared data were embedded into the cover image to form stego images.

In this paper, a natural-image-based Visual Secret Sharing (NVSS) scheme i.e. (n, n)-NVSS is proposed which is shown in fig. 1.

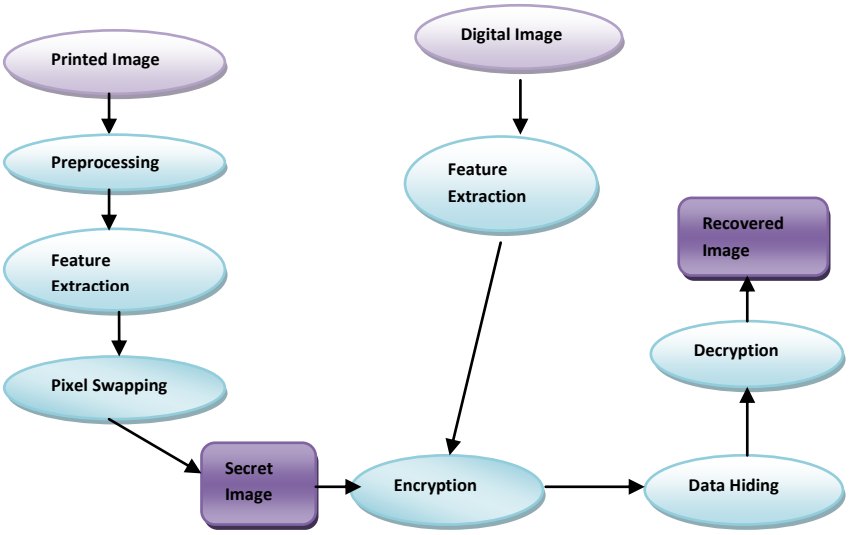

Fig. 1.The flow of (n, n)-NVSS scheme

The (n, n)-NVSS scheme is that technology which shares the secret image through various carrier media to protect the secret and the participants during the transmission. To protect the secret image during the transmission phase, the (n, n)-NVSS scheme shares the secret image over n-1 natural share. Here 'n' represents the number of natural shares and one secret image. For e.g., if n = 5, here the number of natural shares are n-1 = 5-1 = 4 and one secret image i.e. 4 + 1 = 5. The secret image can be of various types i.e. images, handwritten documents, photographs, etc and the natural shares will be photos or hand-painted pictures in digital form or in printed form. The sharing and delivering the secret images is also known as Visual Secret Sharing Scheme (VSS). Then the feature extraction process has been performed to prepare the noise-like share. This process is used to detect the various shapes or features of a digital image. After that the encryption process is carried out for noise-like share and secret image. In this process, the extracted features of the digital image and the printed image are encoded with the secret image by using the (n, n)-NVSS scheme. This encrypted or encoded image will be hided by using data hiding algorithm. In this data hiding process, the Quick Response (QR) code technique is used to hide the noise-like share which reduces the intercepted risk for the share during the transmission phase. Finally, the decryption algorithm is used to recover the secret image in the decryption process at the receiver. In the decryption process, the hidden information or secret image is extracted from the stego-share i.e. covered data which is in the QR code format.

II. RELATED WORK

The Visual Secret Sharing (VSS) scheme uses the transparency and digital media, but it was unable to use the printed media. The existing research focuses only on using the transparencies or digital media as carriers. The transparency shares are either a noise-like or a meaningful. The conventional noise-like shares are not friendly, hence researchers tried to overcome these drawbacks and enhance the friendliness of VSS schemes to the participants. The cover images are added to noise-like shares for secret communication. In a Simulated Annealing Algorithm for General Threshold Visual Cryptography scheme, an optimization technique is used to encrypt the binary secret images but which maximizes the contrast of recovered images. The Extended Visual Cryptography Scheme (EVCS) is a user-friendly scheme which constructs the noise-like shares but reduces the display quality of the recovered image. In this scheme, a stamping algorithm is used to cover each share directly. The research has also focused on gray-level and color secret images to develop a user-friendly VSS scheme. In this technique, the cover image adds into the meaningless shares [2]-[8].

The Halftone Visual Cryptography generates halftone shares carrying the significant visual information and improves the quality of the shares more than the quality of the recovered images. But these techniques has the serious drawbacks of pixel expansion and contrast loss of original image, although the display quality of the shares has enhanced [9], [10].

The Color Extended Visual Cryptography Using Error Diffusion method produces meaningful color shares with high visual quality but the colorful secret messages having low contrast. The random grid algorithm encrypts the secret image. It can adjust the distortion to extremely small and also improves the problems of decoding. Here, each pixel is associated with a grey level ranging from white to black and each pixel is handled separately. The participants can correctly recover the secret image at the receiver phase. Any of the set of forbidden participants cannot gain any information on the value of the grey level of the shared pixel. [11]-[13].

The Steganography Technique issued to hide the secret images in cover images which make the invisible communication. The digital secret shares have been successfully hidden by using the steganography technique. Therefore, the hidden information and the participant can be protected but each shadow reveals no information about the original image. Although the shares are totally prevented from being seen and the stego-images have a high level of user friendliness, the shared information and the stego-images remain intercepted risks during the transmission phase [14]-[16].

III. THE PROPOSED SCHEME

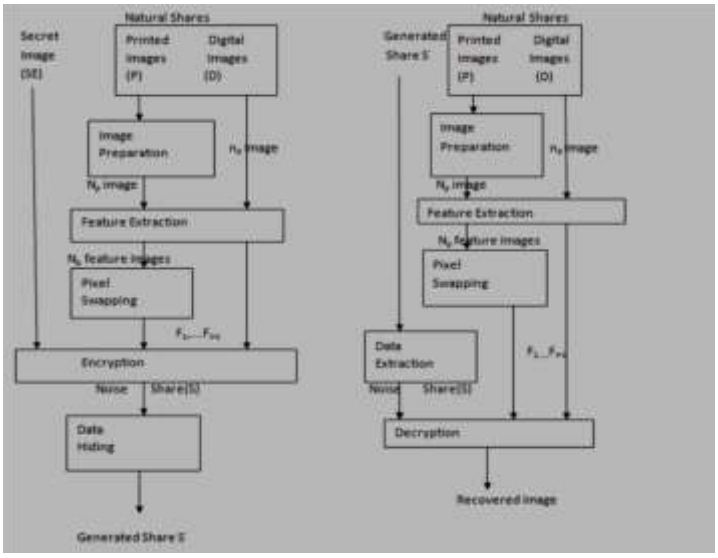

Fig. 2. The encryption and decryption process in (n, n)-NVSS scheme

The fig. 2 shows the encryption and decryption process in (n, n)-NVSS scheme. Here, the encryption process is shown by first part of fig. 2. This includes two main phases (i) Feature extraction, and (ii) Encryption.

In the first phase, the natural shares are taken as the input in the form of printed images (P) and digital images (D). The image preparation process is performed only for printed image, here some portion of the printed image is cropped manually and the digital image is taken as it is. In the second phase, the feature extraction process is carried out. In this process, the 24-bit binary feature images are extracted from each natural share. Here, 'np' and 'nd' should be greater than or equal to '1', and n = np + nd + 1. The feature images that were extracted from natural images are combined to make one feature image with 24-bit/pixel color depth. Then, the pixel swapping process will be performed. In this process, the feature values of a pair of the coordinates is exchanged into a feature matrix, so the pixels are exchanged here from '0' to '1' and '1' to '0'.

In the encryption phase, the n-1 feature images (F1----Fn-1) and the secret image (SE) execute the XOR operation to generate one noise-like share 'S' with 24-bit/pixel color depth. To reduce the transmission risk of the share 'S', this share is hide behind the cover media by the data hiding process. For this data hiding process, the Quick Response (QR) code technology is used. QR code is a two-dimensional code. The QR Code is more advantageous than UPC barcodes because of the fast readability and greater storage capacity. The resultant share is called the generated share. The n-1 natural shares and the generated share 'S' are 'n' shares in the (n, n)-NVSS scheme.

The second part of the fig. 2 shows the decryption process. In this process, the share extraction algorithm is used. When all 'n' shares i.e. n-1 natural shares and 'S' generated share received at the receiver, the decryption process extracts n-1 feature images from all natural shares. Then XOR operation is performed with the generated share 'S' to obtain the recovered image.

The objectives of the Natural-image-based Visual Secret Sharing Scheme are as follows:

- To preprocess the natural shares.
- To extract the features in the natural shares.
- To encrypt the secret image with the extracted features of natural shares.
- To perform data hiding and share extraction process.
- To decrypt and retrieve the original secret image.

IV. THE MODULES AND DESCRIPTION

The five modules are used in the (n, n) - NVSS scheme; (i) Image Preprocessing, (ii) Feature Extraction, (iii) Encryption, (iv) Data Hiding, (v) Decryption. They are described here,

4.1 Image Preprocessing

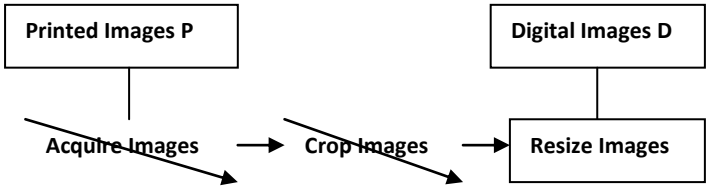

Fig. 3: Flow of the image preparation process

The flow of the image preparation process is shown in the fig. 3. It is simply a process, no algorithm is used here.

In the first step, the contents of the printed image can be obtained by digital scanners and captured by digital cameras. To reduce the difference in the contents of the obtained images during the encryption and decryption processes, the parameters i.e. resolution and image size of the devices should be the same in both process. The next step is to crop the extra portion of the images. This cropping process is done manually.

Finally, the images are resized so that they have the same dimensions as the natural shares n. The distortions introduced with this image. Because of this distortion, the different distortions are caused during the encryption and decryption process. The obtained digital image during the encryption and decryption phase is not same. To remove this distortion, the pixel-swapping process is used.

4.2 Feature Extraction

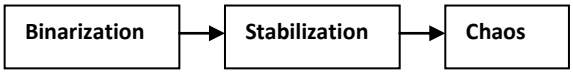

Fig. 4: The block diagram of the feature extraction process

The fig. 4 shows the feature extraction process. In this process, the feature extraction algorithm is used. The feature extraction is carried by three processes: (i) Binarization, (ii) Stabilization and (iii) Chaos process.

First, a binary feature matrix is extracted from natural images n via the binarization process. The median value of the natural share is calculated during this process by using the formula,

- The pixel value is the sum of RGB color values of pixel (x, y) in natural share N, it given as
  $H^{x,y} = P_R^{x,y} + P_G^{x,y} + P_B^{x,y}$
- The Extraction function of pixel (x,y) of N is given as,
  $f^{x,y} = F(H^{x,y}) = 1$, for $H^{x,y} > M$ and

  $= 0$, Otherwise

Where, F = Feature matrix of N, M = The median of all pixel values in the block of N

Then in the stabilization process, the occurrence frequency of values 1 and 0 in the matrix are balanced as the number of black and white pixels are balanced by using the formulas,

- The no. of unbalanced black pixels Q_s is calculated as,
  $Q_s = \Sigma f^{x,y} - b^2/2$

  Where, b = block size
- The no. of unbalanced white pixels Q_c is calculated as,
  $Q_c = b^2/2 \ xP_{noise}$

  Where, b = block size, P_{noise} = Pixel noise

Finally, the chaos process is used to eliminate the texture of the extracted feature images and the generated share. The original feature matrix will be disordered by adding noise in the matrix.

4.3 Encryption

The encryption module uses the encryption algorithm. The proposed (n, n)-NVSS scheme can encoded a true- color secret image by n-1 natural shares and one noise-like share. For one image, a bit is denoted with the same color as a bit plane. So, the color secret image has 24 bit planes. Thus, the feature images and the noise-like share are also extended to 24 bit planes. Before encryption of each bit plane of the secret image, the proposed algorithm first extracts n-1 feature matrices from n-1 natural shares. Then the bit plane of the secret image and n-1 feature matrices execute the XOR operation to obtain the bit plane of the share image. The XOR operation is that for same inputs, the output will be '0' and for variable inputs, the output will be '1'.

4.4 Data Hiding

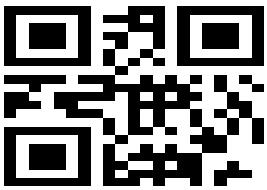

Fig. 5: The QR code

In the data hiding process, the share-hiding algorithm is used to hide the secret share. In this process, the Quick Response (QR) code technique is introduced to hide the noise-like share which is shown in fig. 5. By using this technique for data hiding, the intercepted risk for the secret share reduces during the transmission phase. In the proposed (n, n)-NVSS scheme, a sender can hide the generated share by using existing stegnography technique, but this has the drawback of the limited information hiding. Due to this drawback of stegnography technique, the QR code technique is used in the proposed scheme. The QR code is a two-dimensional code first designed for the automotive industry. The QR code encodes the meaningful information in both the dimensions and the vertical-horizontal directions.

The QR code is advantageous than the barcodes because of fast readability and better storage capacity. It can carry the several hundred times the amount of data than barcodes. The QR code is printed on physical material and can be read and decoded by barcode readers and smart phones. In the proposed scheme, the numeric type QR code is used to hide the secret share. In this step, 16 binary feature bits are converted into 5-digit decimal value ranges from 0 to 65,535, then to encode the decimal values into QR code format. Here, the generated QR code is 128128130 as per the input given.

4.5 Decryption

In the decryption phase, the share-decryption algorithm is used to extract the hidden information from the stego-share which is in the QR code format. This algorithm extracts a feature matrix F from numeric string which is in QR code format. Then these numeric characters converted into binary form. This binary string converts to the resultant feature matrix F. The share-hiding algorithm alters some of the pixel values which introduce the noise into the recovered image in the decryption phase. The recovered image will get at the receiver stage.

V. RESULTS

The MATLAB Image Processing Tool is used for image processing purpose. It evaluates the performance of the proposed technique.

The stepwise procedure of the (n, n)-NVSS scheme is given below.

Step 1: At first, the digital image and the printed image shown in fig. 6 & 7 are taken as an input. The printed image is the hand-painted picture which is scanned by the scanner or captured by the smart phone and converted into the digital image

.

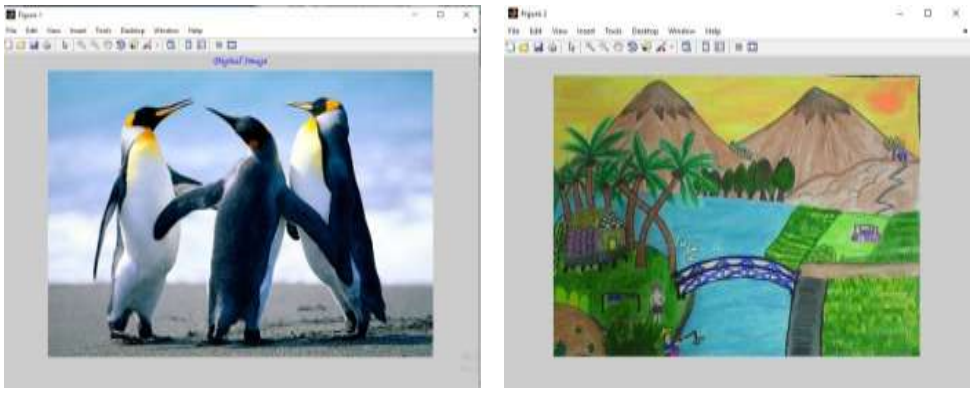

Fig. 6 & 7: The digital image and the printed image as an input

Step 2: Some portion of the printed image is cropped by manually which is given in fig. 8.

Fig. 8: The cropped image of the printed image

Step 3: The filtered digital image and the printed image are given in fig. 9 & 10 which gets after the feature extraction process.

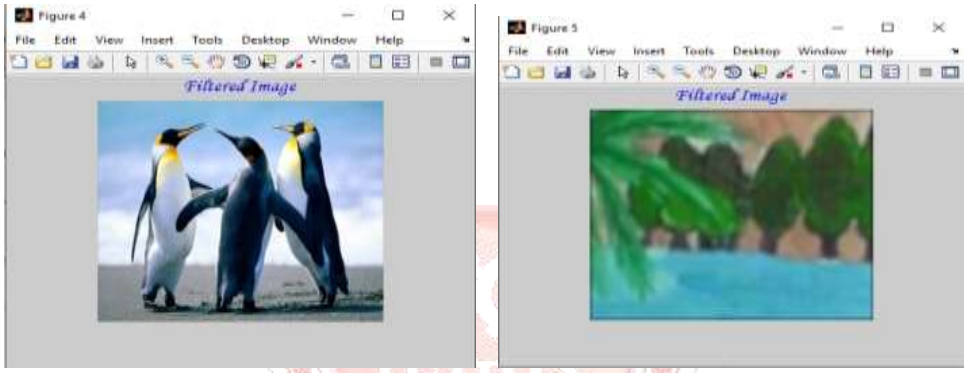

Fig. 9 & 10: The filtered digital image and the printed image

Step 4: The digital image is taken as a secret image which is shown in fig. 11. This secret image is then encrypted and hided in the QR code for the secret communication.

Fig. 11: The digital image is taken as a secret image

Step 5: The natural shares is encrypted with the secret image in the encryption process by performing the XOR operation as shown in fig. 13 and then the secret image is hide by the QR code which is shown in fig. 12. The secret image is decrypted by performing the same XOR operation at the receiver. The encryption and decryption processes are shown in fig. 13 & 14.

Fig. 12: The QR generated to hide the secret image

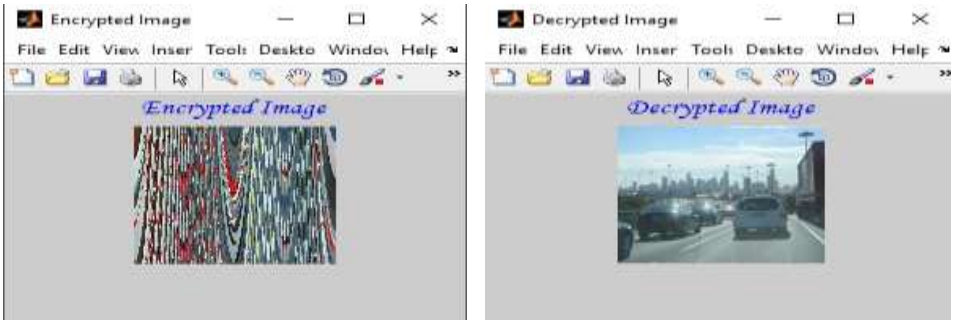

Fig. 13 & 14: The encryption and the decryption process

The comparison of the pixel values of the secret image with RGB colors in the base paper and the proposed scheme is given below in the fig. 15 & 16.

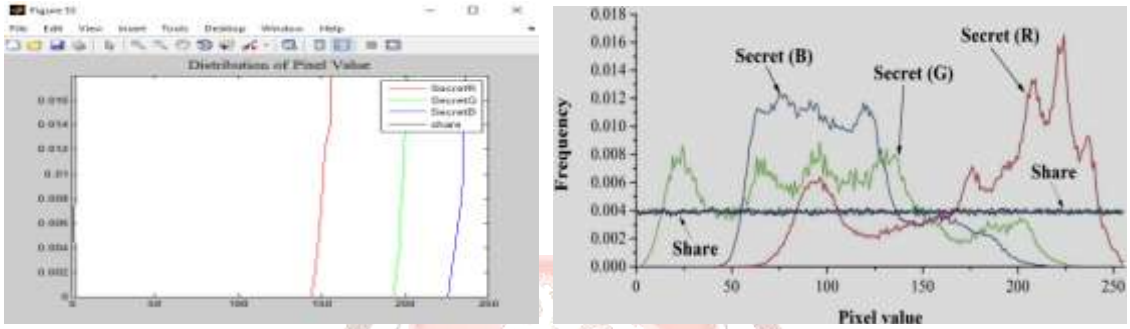

Fig. 15 & 16: Pixel values of secret image with RGB colors in the base paper and the proposed scheme

VI. CONCLUSION

In this paper, the (n, n)-NVSS scheme shares a digital image using the various media. For the increasing number participants n, this scheme uses only one noise-like share for sharing the secret image. The n-1 shares are unaltered in the encryption phase.

As compared to the existing Visual Secret Sharing (VSS) scheme, the proposed NVSS scheme can reduce the transmission risk problem and provide the highest level of user friendliness. There is a trade-off between the contrast at the encrypted shares and the decrypted shares. The proposed scheme can recognize the colorful secret messages even having low contrast. The major advantage of this study is that it reduces the pixel expansion problem and to increase the contrast. And also reduces the transmission risk problem because of diverse image media selected to share the secret image.

REFERENCES

[1] Kai-Hui Lee and Pei-Ling Chiu, “Digital Image Sharing by Diverse Image Media” in IEEE Transactions on Information Forensics and Security, vol. 9, No. 1, pp. 88-98,Januaary 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] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

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

[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, pp. 1693–1703, Nov. 2011.

[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," Digital 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] X. Wu, D. Ou, Q. Liang, and W. Sun, "A user-friendly secret image sharing scheme with reversible steganography based on cellular automata," *J. Syst. Softw.*, vol. 85, no. 8, pp. 1852–1863, Aug. 2012.