Available onlinewww.ejaet.com

European Journal of Advances in Engineering and Technology, 2022, 9(4s):199-203
International Conference on Tech Trends in Science & Engineering (ICTTSE) 2022
Suryodaya College of Engineering & Technology, Suryodaya Polytechnic, Nagpur, Maharashtra, India

Research Article ISSN: 2394 - 658X

# Encryption Scheme for Color Visual Cryptography using Random Grids without Pixel Expansion

**Prof. Veena K. Katankar, Prof. Shilpa D. Chindamwar**

Asst. prof Department of Computer Engineering, Suryodaya college of Engg. & Tech., Nagpur, India
veenakatankar@gmail.com, shilpaijmulwar@gmail.com

**ABSTRACT**

Visual cryptography is a cryptographic technique which allows visual information (pictures, text, etc.) to be encrypted in such a way that the decryption can be performed by humans (without computers). Visual cryptographic schemes to share a binary secret image among n participants. Specifically, secret image is encoded into n transparencies, called shares, which are distributed to the n participants one by one, such that k (or more) participants can recognize secret image from the superimposed result of their shares, while less than k participants obtain no information about secret image. It involved breaking up the image into n shares by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. This is more general than a (k, n)-VCS and may be applied to different applications. The deception process relies on human visual ability without any computation.

The proposed visual cryptography scheme by random grids resolves the problem of secret sharing without pixel expansion and can be extended to cope up with colour images, without disturbing the quality of picture.

**Key words:** Visual cryptography, Random grid, Secret sharing

## INTRODUCTION

The first visual cryptographic technique was developed by Moni Naor and Adi Shamir in 1994, which defined and designed threshold k-out-of-n visual cryptographic schemes ((k, n)-VCSs to share a binary secret image P among a set P of n participants. Specifically, P is encoded into n transparencies, called shares, which are distributed to the n participants one by one, such that k (or more) participants can recognize P from the superimposed result of their shares, while less than k participants obtain no information about P. It involved breaking up the image into n shares by printing each share on a separate transparency and then placing all of the transparencies on top of each other. In their technique n-1 shares reveals no information about the original image. This can achieve this by using one of following access structure schemes.

1: (2, 2) – Threshold VCS: This is a simplest threshold scheme that takes a secret image and encrypts it into two different shares that reveal the secret image when they are overlaid. No additional information is required to create this kind of access structure.

2: (2, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3: (n, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that only when all n of the shares are combined will the secret image be revealed. The user will be prompted for n, the number of participants.

4: (k, n) – Threshold VCS: This scheme encrypts the secret image into n shares such that when any group of at least k shares are overlaid the secret image will be revealed. The user will be prompted k, the threshold, and n, the number of participants.

A visual cryptography scheme using random grids is an extension to the threshold (k, n)-VCS. It encodes P into n transparencies for the n participants in such a way that only the participants in qualified subsets of P can visually recover P by superimposing their shares, but those in forbidden subsets of P cannot acquire any information about P. This is more general than a (k, n)-VCS and may be applied to different applications.

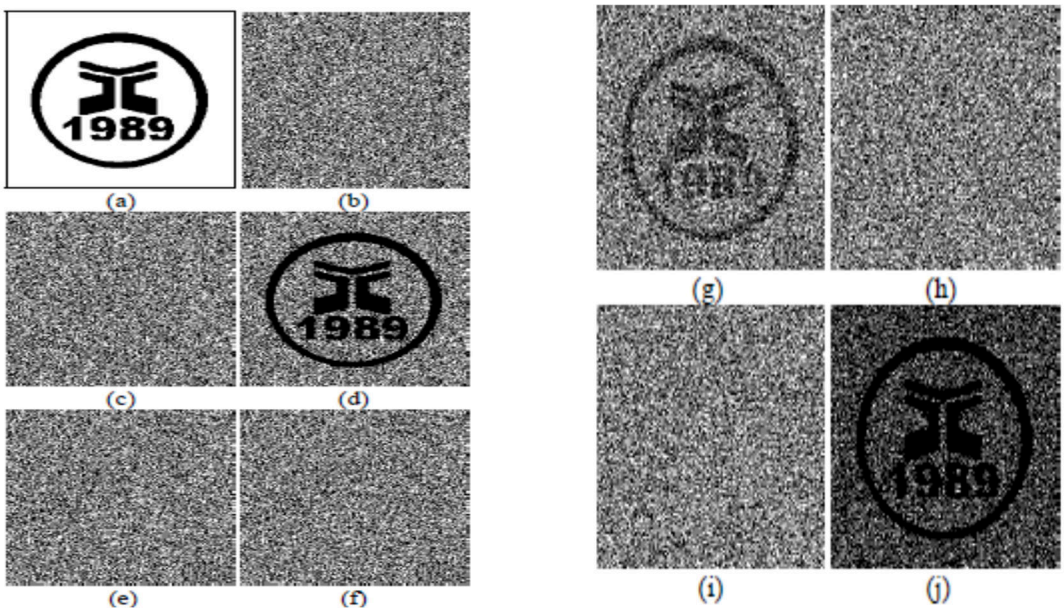


**Fig. 1** Kafri and Keren's picture encryption example. The two encoded shares and their superimposing result by Kafri and Keren's algorithms are shown in (b)−(d), (e)−(g), and (h)−(j), respectively.

## RELATED WORK

The new type of cryptographic scheme which can decode concealed image without any cryptographic computation. This scheme is perfectly secure and easy to implement. M. Naor and Shamir defined and designed threshold k-out-of-n visual cryptographic schemes ((k, n)-VCSs) to share a binary secret image P among a set P of n participants. Specifically, P is encoded into n transparencies, called shares, which are distributed to the n participants one by one, such that k (or more) participants can recognize P from the superimposed result of their shares, while less than k participants obtain no information (in an information-theoretic sense) about P [1].

Cimato, R. De Prisco, and A. De Santis presented characterization of contrast optimal c colour (k, n) –threshold visual cryptography scheme it satisfy the strong symmetry property and they are achieving optimal contrast [16]. The techniques of halftone technology and color decomposition to construct three methods that can deal with both gray-level and color visual cryptography. Based on the theory of color decomposition, every color on a color image can be decomposed into three primary colors: C, M, and Y. With the halftone technology, they transform a gray-level image into a binary one suitable for generating visual cryptography. The methods expand every pixel of a color secret image into a 2×2 block in the sharing images and keep two color and two transparent pixels in the block [15, 17].

Random grid is a transparency comprising a two-dimensional array of pixels that are either transparent or opaque determined in a totally random way. S. J. Shyu, encrypt a secret picture or shape into the random grids which are printed on transparencies such that the areas containing the secret information in the two grids are inter- correlated. When the transparencies are superimposed together, the correlated areas will be resolved from the random background due to the difference in light transmission so that the secret picture or sharp can be seen visually [5, 6].

Two common drawbacks of the visual cryptography scheme (VCS) are the large pixel expansion of each share image and the small contrast of the recovered secret image. A step construction to construct VCS (or) and VCS (xor) for general access structure by applying (2, 2)-VCS recursively, where a participant may receive multiple share images. Step construction generates VCS (or) and VCS (xor) which have optimal pixel expansion and contrast for each qualified

set in the general access structure in most cases. A technique to simplify the access structure, which can reduce the average pixel expansion [2, 3].

Askari, H.M. Heys, and C.R. Moloney [18] proposed visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques. In this paper, we propose a method for processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

## SCOPE OF WORK

- As seen from the existing work, the secured data hidden in shares seems to poor the quality of the shares. Therefore, there is a need to increase the quality of shares.
- The SNR value as per the existing system is low. Hence the Peak signal to Noise Ratio of the share can be improved before encryption and decryption.
- Most existing system shares intend something is hidden below. The quality itself shows a major scope for implementation of strong algorithm that will hide the secured data not identified by human naked eyes.
- Efficient Post processing for the shares for soft error diffusion across the shares.
- The previous work shows a difference in the decrypted secret image with respect to the original secret image. There is enough work to be done to improve reconstruction ability of the system.

## PROPOSED SYSTEM

**a) Preprocessing module -** The basic secret image can have any color components such as RGB, CMY etc and can be a additive or subtractive model. The primary colors in subtractive model are cyan (c), magenta (m), and yellow (y). It can generate all other color space by linear combination. Basically information to be encrypted is first converted to binary i.e. black and white [0/1]. After converting it into binary scale pixels in sequence or encoded pixels are extracted from the image.

**b) Sharing and distribution module -** Secret images shared by the participants. In this scheme it encodes secret data into transparencies, which are distributed over the participants.

**c) Encoding using random grids module -** For encoding the secret data random grids is used so that the data can be encoded without pixel expansion.

**d) Post processing module -** Once data is send over the participants, to get the actual secret data there is need of post – processing so that the high quality of image shares can be achieved.

**e) Decoding -** By superimposing the transparencies the secret data is recovered.

Method to encrypt a binary image O in two RGs, G1 and G2, in such a way that each RG singly reveals no secret information about O, but superimposing G1 and G2 pixel by pixel can reveal the patterns on O.

**Step 1 -** Generate G1 as a RG with same scale as O by assigning value 0 (transparent dot) or 1 (black dot) to each pixel of G1 randomly, with the probabilities for the two alternatives are the same, i.e., Prob (0) = prob(1)=1/2.

**Step 2 -** Generate G2 as a RG with same scale as O using one of the following two substeps:

**Step 2.1 -** If the pixel at position (i, j) of O has value 0, the pixel located on (i, j) of G2 is copied from the pixel at position (i, j) of G1.

**Step 2.2 -** If the pixel at position (i, j) of O has value 1, the pixel located on (i, j) of G2 takes the complement value of the pixel at position (i, j) of G1.

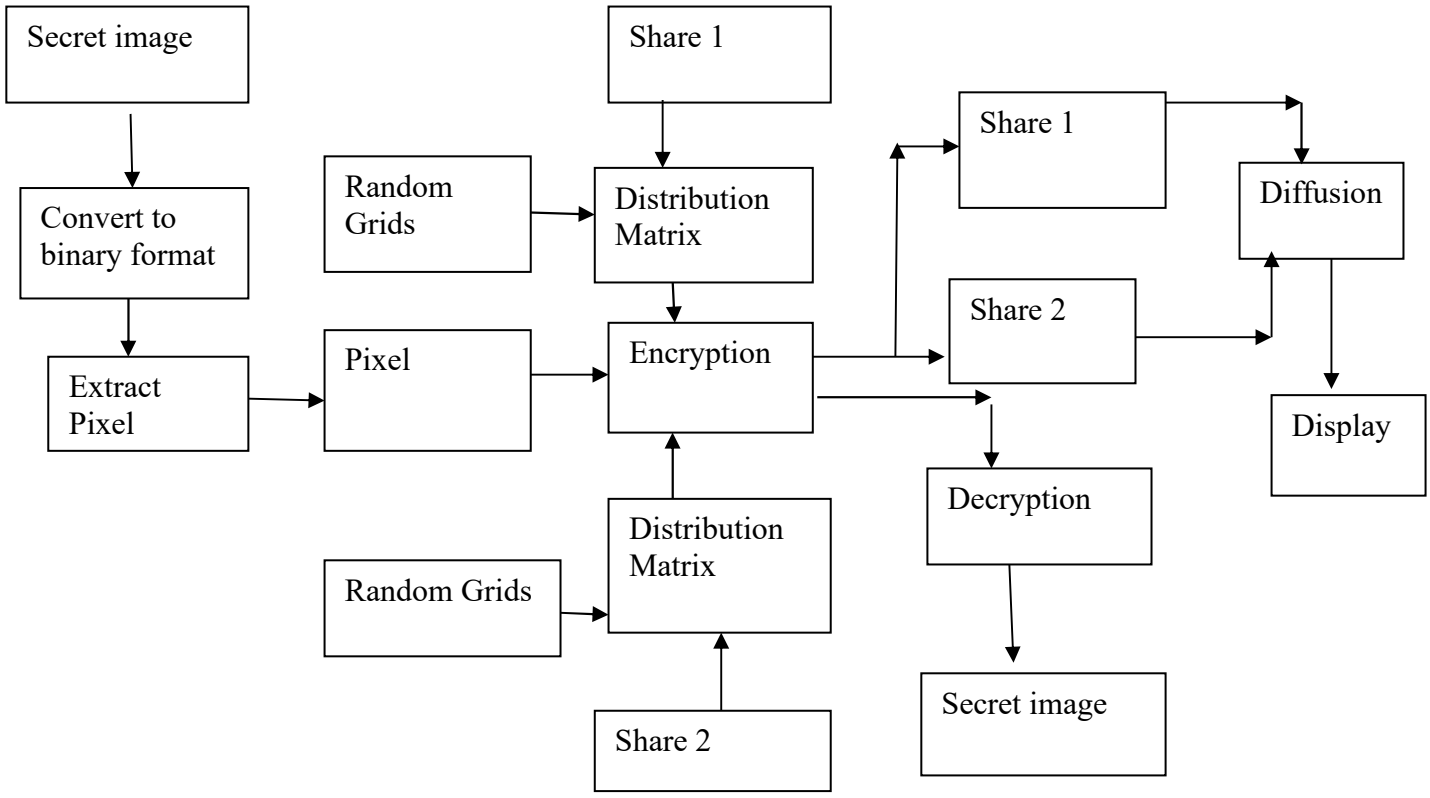


**Fig. 1** Structure of Proposed scheme

To encrypt the color image by using random grids, integrating some feature of colors with the encryption abilities of random grids on the binary image. The color features includes color model, color mixture and color decomposition. Color model are additive model or the subtractive model. The additive model mainly describes the colors are originated from lights while the subtractive model defines the mixture of colors when the colors are made of dyes, pigments, paints, or other natural colorants. Research work is mainly focused on the subtractive model. According to light transmission random grids were formed.

## CONCLUSION

For developing an efficient color visual cryptography scheme using Random Grids which will hide information to be secured in participants without actual pixel expansion with strong access structure maintaining visual quality and will hide the information that will not appear to be visual with naked eyes. Proposed work will be -implementing comparison of Existing systems and based on performance parameters.

## REFERENCES

[1]. M. Naor and A. Shamir, “Visual cryptography,” in Proc. Advances Cryptology (Eurpocrypt), LNCS 950. 1995, pp. 1–12.

[2]. S. J. Shyu and M. C. Chen, “Optimum pixel expansions for threshold visual secret sharing schemes,” IEEE Trans. Information Forensics Security, vol. 6, no. 3, pp. 960–969, Sep. 2011.

[3]. F. Liu, C. Wu, and X. Lin, “Step construction of visual cryptography schemes,” IEEE Trans. Information Forensics Security, vol. 5, no. 1, pp.27–38, Mar. 2010.

[4]. “Visual cryptography,” M. Naor and A. Shamir, in Proc. EUROCRYPT, 1994, pp. 1-12

[5]. S. J. Shyu, “Efficient visual secret sharing scheme for color images,”Pattern Recognition., vol. 39, no. 5, pp. 866–880, May 2006.

[6]. S. J. Shyu, “Image encryption by random grids,” Pattern Recognit., vol.40, no. 3, pp. 1014–1031, 2007.

[7]. S. J. Shyu, “Image encryption by multiple random grids,” Pattern Recognit., vol. 42, no. 7, pp. 1582–1596, Jul. 2009.

[8]. G. Ateniese, C. Blundo, A. De Santis, and D. R. Stinson, "Visual cryptography for general access structures," Inform. Comput., vol. 129, no. 2, pp. 86–106, 1996.
[9]. C. Blundo, S. Cimato, and A. De Santis, "Visual cryptography schemes with optimal pixel expansion," Theor. Comput. Sci., vol. 369, nos. 1–3, pp. 169–182, 2006.
[10]. C. Blundo, P. D'Arco, A. De Santis, and D. R. Stinson, "Contrast optimal threshold visual cryptography schemes," SIAM J. Discrete Math., vol. 16, no. 2, pp. 224–261, 2003.
[11]. C. Blundo, A. De Santis, and D. R. Stinson, "On the contrast in visual cryptography schemes," J. Cryptology, vol. 12, no. 4, pp. 261–289, 1999.
[12]. M. Bose and R. Mukerjee, "Optimal (k, n) visual cryptographic schemes for general k" Designs Codes Cryptography, vol. 55, no. 1, pp. 19–35, 2010.
[13]. S. J. Shyu and K. Chen, "Visual multiple secrets sharing by circle random grids," SIAM J. Imaging Sci., vol. 3, no. 4, pp. 926–953, 2010.
[14]. E. R. Verheul and H. C. A. Van Tilborg, "Constructions and properties of k out of n visual secret sharing schemes," Designs Codes Cryptography, vol. 11, no. 2, pp. 179–196, 1997.
[15]. InKoo Kang, Gonzalo R. Arce, Fellow and Heung-Kyu Lee "Color Extended Visual Cryptography Using Error Diffusion" IEEE Transactions on Image Processing, Vol. 20, No. 1, January 2011
[16]. S. Cimato, R. De Prisco, and A. De Santis, "Optimal colored threshold visual cryptography schemes," Designs Codes Cryptography, vol. 35, no. 3, pp. 311–335, Jun. 2005.
[17]. Y.-C. Hou, "Visual cryptography for color images" Pattern Recognit., vol. 36, no. 7, pp. 1619–1629, 2003.
[18]. N. Askari, H.M. Heys, and C.R. Moloney," Anextended visual cryptography scheme without pixel expansion for halftone images,"26th IEEE Canadian conference of Electrical and Computer Engineering (CCECE), 2013.