Smart Computing Review

A Novel XOR-based Visual Secret Sharing Scheme with Random Grid

Ram Sekher Pati[1] and Amitava Nag[2]

[1] Dept. of CSE, Academy of Technology / West Bengal, Adisaptagram 712148, India / ramsekher.pati@aot.edu.in

[2] Dept. of IT, Academy of Technology / West Bengal, Adisaptagram 712148, India / amitava.nag@aot.edu.in

*Corresponding Author: Ram Sekher Pati

Received July 20, 2015; Revised August 21, 2015; Accepted September 27, 2015; Published October 31, 2015

Abstract: The basic concept of secret image sharing is to encrypt a secret image into a number of meaningless share images. Except for all the images, no information should leak out from any of the share images. The original secret image is printed onto transparencies, and stacking these transparencies directly reveals the original image. The advantage lies in the fact that no computational cost is encountered, and only the human visual system is required to decode the secret image. The visual secret sharing scheme is to encrypt a secret image into a set of share images to increase the encryption capacity. However, the schemes available use a codebook, and used pixel expansion to encrypt secret images into share images. In general, pixel expansion of twice the original order is seen. It is neither practical nor the best solution when secret images are more in number. This paper proposes a novel visual secret sharing scheme that can share a binary secret image on two share images with no codebook requirement. The experimental result reveals that the proposed approach has high contrast and also has an excellent recovery quality of the secret image. The recovered secret image type is lossless.

Keywords: Human Visual System, Pixel Expansion, Random Grid, Visual Secret Sharing

Introduction

In the present scenario, effective and secure protection of sensitive information is a prime concern. Medical sciences and military systems need more secure channels to share their data. The reliability of a data transport mechanism is of utmost importance. To repair such vulnerabilities, an encryption technique known as Visual Cryptography (VC) is implemented.

VC is a method of encrypting a secret image into a set of covered or random images that may or may not mean anything. It simply uses human eyes to recover the secret, avoiding the computational cost generated by decoding the message using

DOI: 10.6029/smartcr.2015.05.004

computers or any other complex mechanism or device. Military or defense and medical sciences provide the hotspots for implementation of different visual secret sharing (VSS) schemes.

A VC scheme eliminates the complex computation problem during decryption, since the secret images reveal the original image when stacked one on top of the other. This property has the lowest possible computation load requirement. The traditional process of visual cryptography is shown in the figure below.

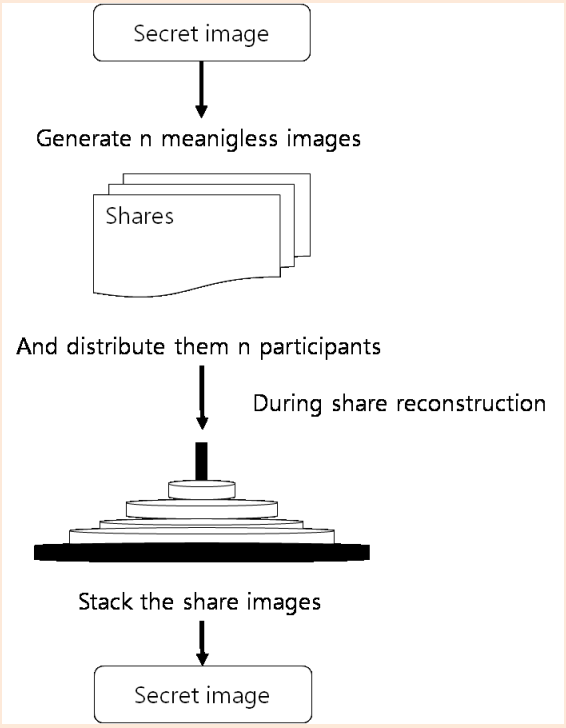

Figure 1. A generalized VSS scheme

Related Works

In 1994, Naor and Shamir [1] proposed a (k, k) threshold VSS scheme for the first time. This was known as a (k, k)-VSS scheme. Here a secret image is shared in k share images, and all k share images are required to retrieve the original secret image.

According to pixel transparency, a black pixel does not allow light to pass through and a white pixel acts like transparent glass. Different stacking processes yield different results. Hence, visual colors generated from the stacked blocks are distinguished by their relative differences.

VSS schemes have been formulated to secure visual information like images and video. A VSS scheme was first formulated by Moni Naor and Adi Shamir in 1994. They can be considered the forefathers of this security scheme. They took a secret image and decomposed the image into n shares. These n shares were distributed to n participants. All the participants were required to generate the original secret image during the overlapping process. But during the decryption process, the secret image could be revealed by directly stacking the share images. The recovered secret image could thereafter be recognized by the human visual system without any additional computational devices. This VSS scheme was very convenient for revealing the secret image, as it could be done without any computational devices.

Later, a threshold VSS scheme called the (k, n)-threshold scheme was developed. It required at least k ($2 \leq k \leq n$) share images to get the perfect stacking result. Any single share image or less than k share images that were stacked together could not reveal the shared secret, even when using computational devices.

Keeping the threshold scheme parallel, a new scheme came out which used general access structures. In the (k, n) model, any k shares will decode the secret image, which reduces the security level. To overcome this issue, the basic model is extended to general access structures by G. Ateniese, C. Blundo, A. De Santis and D. R. Stinson [2], where an access structure is a specification of all qualified and forbidden subsets of 'n' shares. Any subset of 'k' or more qualified shares can decrypt the secret image, but no information can be obtained by stacking a lesser number of qualified shares or by stacking disqualified shares. So, visual cryptography for a general access structure improves the security of the system.

BlundoC. Blundo, P. D'Arco, A.D. Santis, D. Stinson [3] constructed the optimal (2, n) VCS from BIBD while studying the optimal contrast of threshold VCSs. To resolve the pixel expansion problem and the reliability of the basis matrices, Ito et al. [4] and Yang et al. [5] propose probabilistic VCS. Shift-tolerant VCSs were proposed by F. Liu, C. Wu, X. Lin [6] and D. Wang, L. Dong, X. Li [7], where shares are not required to be aligned exactly in decoding stage. To detect fake shares during the decoding stage, G. Horng, T. Chen, D. Tsai [8], Hu and Tzeng[9] and Y. Chen, G. Horng, D. Tsai [10] proposed a cheating prevention VCS. The equivalence between two different definitions of VCS is shown by T. Guo, F. Liu, C. Wu [11].Construction of region-incrementing VCSs was done by R. Wang[12], C. Yang, H. Shih, C. Wu, L. Harn [13] and Shyu[14], where secret information is revealed gradually, region by region. The multi-pixel encryption model discovered by T. Guo, F. Liu, C. Wu, [15] shows different properties of VCS. A visual quality of size-invariant VCS was done by F. Liu, T. Guo, C. Wu, and L. Qian [16]. Improvement in the contrast of Chen and Tsao's[17] threshold VCS was done by T. Guo, F. Liu, C. Wu [18] using random grids.

The random grid technique can encrypt one binary image into two shadows, called random cipher grids, without expanding the number of pixels necessary and without designing a codebook. O. Kafri and E. Keren[19] proposed this technique first, where each image pixel can be represented as either transparent (white) or opaque (black), and the choice between them is made randomly. Therefore, each shadow image has an average light transmission that equals half (1/2). The transparent pixel lets the light through, while the opaque pixel stops it.

A new random grid-based VSS with edge enhancement was proposed by Tzung-Her Chen and Yao-Sheng Lee [20]. They consider a secret binary image of size w×h pixels. The secret image S is encoded into two random grids, r1 and r2, where there was no pixel expansion. The scheme integrated the process of an RG-based VSS algorithm and Robert's Cross operator. During decryption, the two r1 and r2 grids were stacked to disclose the original secret information that was easily discernible to the human eyes. One distinction in this process is that the edges become darker than other portions.

Random grid VCS provides the following advantages:

(i) Pixel expansion of (n, n)-VCS is 2^{n-1} is solved, as there is no need of extra pixels.

(ii) Codebook provides more complexity to a VCS which is not a matter of concern here, as no codebook is being used.

T. Chen and K. Tsao [21] used friendly RG-based VCS where the shares generated were meaningful. Their scheme included no codebook. The security of such VCS requires transmission of light from a pixel of a shared image to be equal to a fixed value whether it is a white pixel or a black pixel.

The security of RG based VCS requires light being transmitted from a pixel to be of a certain value regardless from a white pixel or from a black pixel. Now the paper approaches to XOR-based scheme where P. Tuyls, H. D. L. Hollmann, J. H. Van Lint, and L. Tolhuizen [22] gave formal conditions for XOR based VCS. From the paper about property analysis of XOR based VC by Ching-Nung Yang and Dao-Shun Wang [23], a conclusion that XOR is better than OR during computation of pixels, can be drawn. XOR based computed images are of higher quality and the shares generated are also meaningless which keeps the attacker at bay.

The proposed scheme

A random grid is a two dimensional array of pixels that are either transparent or opaque. Each pixel in a random grid is produced in a totally random way. In this scheme a binary image is selected which is later treated by two random grids I_2 and I_4 to generate I_3 and I_5 as unrecognizable images using Boolean XOR operation. Now two shares S_1 and S_2 are generated in such a way that I_2 and I_4 are inherited in S_1 and I_3 and I_5 are inherited in S_2. This overall results into the formation of two share images S_1 and S_2. Figs. 2 and 3 show the complete process of the proposed scheme.

■ Proposed algorithm

Input: A secret binary image I_1 with m×n pixels where $1 \leq m \leq 255$ and $1 \leq n \leq 255$.

Output: Two shares S_1 and S_2.

Step 1: Generate 1st random grid I_2, of size m×n limits, which is same as the original image, where $I_2(i,j) \in_r \{0,1\}$ $\in_r$ denotes random selection of 0 and 1.

Step 2: Perform XOR operation between I_2 and I_1 to generate I_3.

Step 3: Distribute a pixel of I_2 and I_3, conjoined together to form first grid pixel of share S_1 and S_2.

Step 4: Generate 2nd random grid $I_4$of size m×n limits, which is the same as the original image where $I_2(i,j) \in_r \{0,1\}$.

Step 5: Perform XOR operations between I_1 and I_4 to construct a new generated image $I_5$and between I_1 and I_2 to construct new generated image I_3.

Step 6: Distribute a pixel of I_2I_4 and I_3I_5 to construct the grid pixels of shares S_1 and S_2 and continue until all the pixels have been sorted out (as shown in Fig. 3).

Step 7: Output (S_1, S_2).

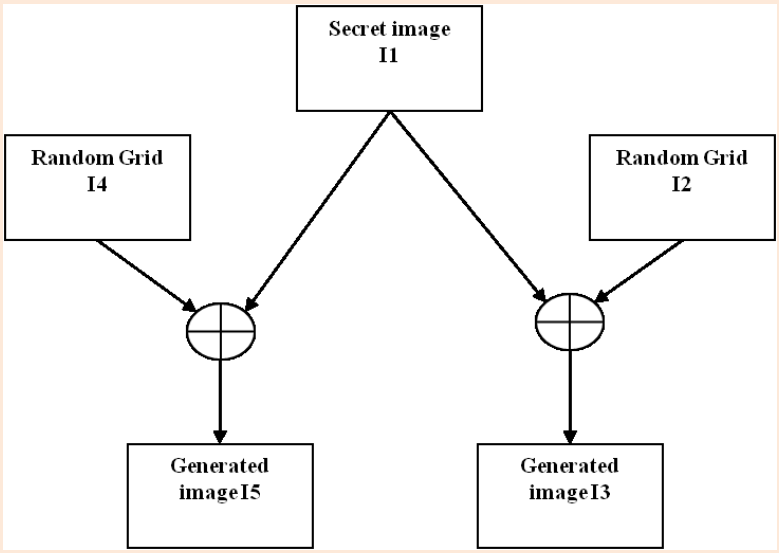

Figure 2. The encoding process for (2, 2)-VCS using proposed scheme

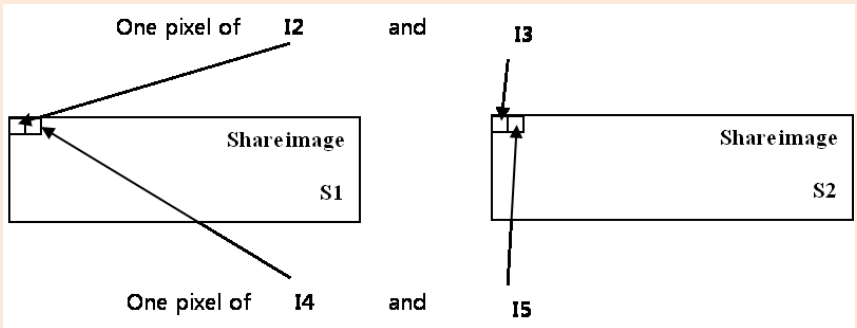

Figure 3. Step 6 of the algorithm is demonstrated below

■ Illustration of the proposed scheme

Let secret image, $\mathbf{I_1} = \begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}$

Generated 1st random grid, $\mathbf{I_2} = \begin{matrix} 1 & 1 \\ 0 & 0 \end{matrix}$

Compute $\mathbf{I_1} = I_2 \oplus I_3 = \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix}$

Generated 2nd random grid, $\mathbf{I_4} = \begin{matrix} 1 & 0 \\ 1 & 1 \end{matrix}$

Compute, $\mathbf{I_1} = I_4 \oplus I_5 = \begin{matrix} 1 & 1 \\ 1 & 1 \end{matrix}$

Two random shares generated $\mathbf{S_1} = \begin{matrix} 1 & 11 & 0 \\ 0 & 10 & 1 \end{matrix}$, $\mathbf{S_2} = \begin{matrix} 1 & 10 & 1 \\ 0 & 10 & 1 \end{matrix}$

Reconstructed secret image, $\mathbf{S_1} \oplus \mathbf{S_2} = \begin{matrix} 0 & 01 & 1 \\ 0 & 00 & 0 \end{matrix}$

Here it is seen that the original image I_1 is enlarged to twice its original size during the decryption phase. If the two consecutive columns (i.e. the odd-even column) do not possess the same values, the secret image will be considered to be tampered with.

■ Experimental Results

The experiment was performed on a 256× 256 binary image (Lena). The given algorithm was fed onto the image to generate two random shares. The two random shares do not disclose any information of the secret image when taken one at a time. As stated, Fig.4 (a) is the original Lena image of size 256×256. Fig.4 (b) demonstrates the first share image, which is to be shared with the first participant, and Fig.4(c) is the second share image delivered to the second participant. The two participants meet and place their individual shares one on top of the other to get the original secret image in an enlarged format as shown in Fig.4 (d). If any share is misplaced, the original secret image cannot be reconstructed as the Boolean XOR values will not generate the exact results.

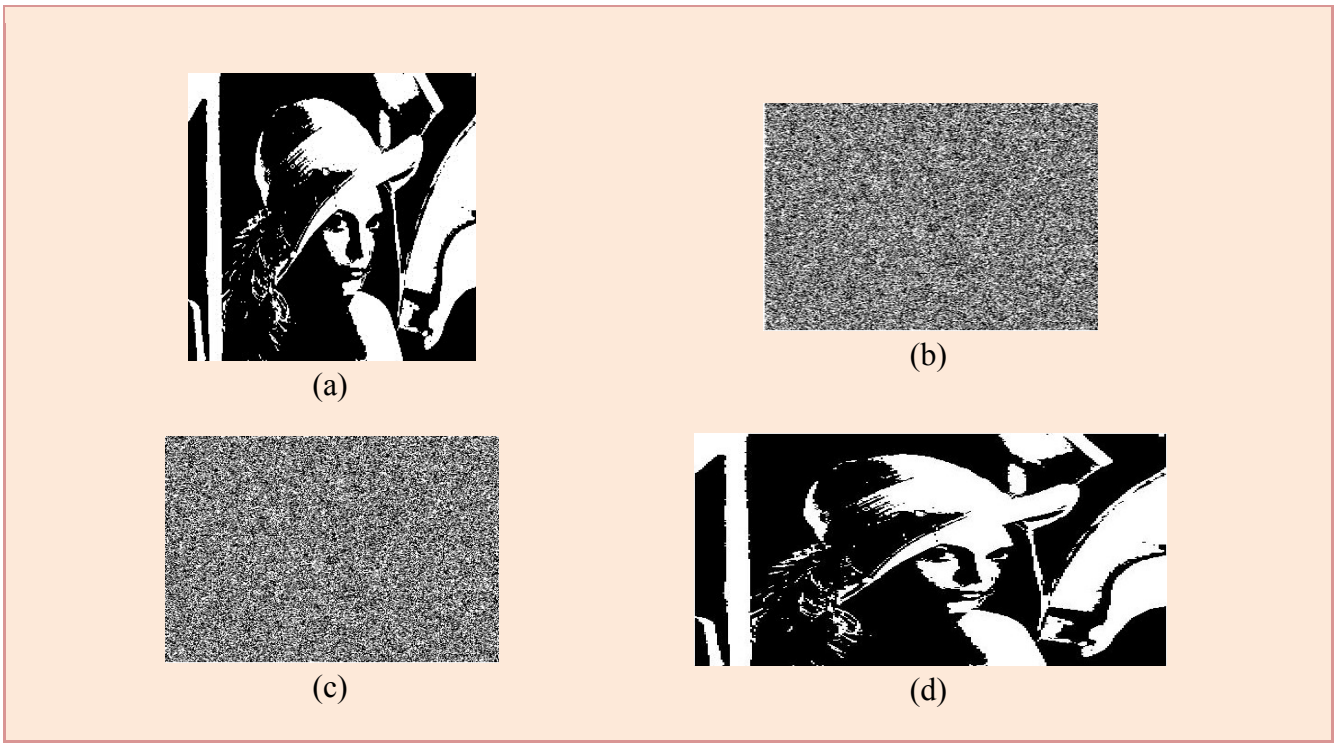

Figure 4. : (a) Secret image I_1 of Lena (b) Share S_1 (c) Share S_2 (d) reconstructed image

■ Discussions on the Proposed Scheme

When compared to conventional cryptography and watermarking techniques, the decryption of this scheme requires no computation. It is especially suitable for harsh conditions where power availability is nil (e.g. a war field). Moreover, this scheme requires no codebook or any cover images. Shares generated will never attract attackers, as they seem to be meaningless. Cover images in corrupted forms mainly attract intruders. This algorithm generates a high-quality visual of the decoded image using a Boolean XOR technique. The maximum number of different visual cryptography schemes use Boolean OR operations for decoding, which result in the degraded image quality of the reconstructed image. Here, the reconstructed image is of high quality, as the contrast of the image is very high.

Different RG schemes use an OR operation, which faces the following problems:

(i) The contrast of the reconstructed image is measured in terms of average light transmission, which decreases exponentially with an increase in the number of cipher grids.
(ii) The decryption process requires perfect alignment of stacking of the cipher grids.

The proposed scheme has eliminated the two disadvantages mentioned above, as the contrast is visually seen to be very high and the decryption process uses a Boolean XOR operation. Moreover, one cannot get a high contrast with zero pixel expansion in the reconstructed secret image at the same time. Since the proposed scheme used only XOR calculations, the computational load of the proposed scheme is relatively low. The computational complexity of Boolean XOR calculation is

O(n), where n is the number of secret images being shared. The XOR calculations take little time. Therefore, output performance shows that the proposed scheme achieves good sharing and recovery phase.

This section presents a comparison of the proposed scheme with other secret image sharing schemes based on codebook design, pixel expansion, share type, and the reconstructed image. The reconstructed image type shows that the recovered secret images are visually identifiable and are losslessly recovered. Pixel expansion shows that the pixels in secret images are excess of the share images. Codebook design defines a particular rule to be followed while embedding the pixels in the shared image. Share type defines the actual format of the share, which is being generated. The recovered secret image is derived from stacking operations. Losslessly recovered secret images can only be generated by stacking the share images which is actually a Boolean XOR operation. Sharing capacity gives a theoretical comparison of the generated share images with secret images. A high sharing capacity yields a better output. Without including any compression techniques, the sharing capacity is restricted within the range of 1.

The experimental results show that the proposed scheme generates a good computational complexity and a high sharing capacity of n/n. The lossless recovery shows that the proposed scheme is good for sharing highly secure images. Comparisons among the proposed scheme and related methods are listed in Table 1. In Table 1, the major advantages of the proposed scheme are (1) shares are meaningless content and (2) lossless recovery. Moreover, requirement of a code book and high pixel expansion are not allowed.

Table 1. Comparison of features among proposed algorithm and related methods

Scheme	Share type	Reconstructed image	Codebook design	Pixel expansion
Naor and Shamir[1]	Meaningless	Lossy	No	1:4
Kafri and Keren[19]	Meaningless	Lossy	No	1:1
Chen and Tsao 1) Threshold[24] 2) User friendly[25]	 Meaningless Meaningful	 Lossy Lossy	 No No	 1:1 1:1
Wu and Sun[26]	Meaningful	Lossy	No	1:1
Guo, Liu and Wu[27]	Meaningless	Lossy	No	1:1
Proposed scheme.	Meaningless	Lossless	No	1:2

Conclusion

The XOR-based visual cryptography scheme uses XOR operations to decode the secret, which is nothing but stacking of the shares being generated. The proposed scheme has higher contrast compared to OR-based visual cryptography. The reconstructed image is lossless and the difficulty of aligning the cipher grids has been removed. Neither of the two share images has leaked any information of the secret image. The future scope of this proposed scheme lies in the direction of developing a scheme where multiple secret shares and no pixel expansion exist side by side.

References

[1] M. Naor, Adi Shamir, "Visual cryptography," In *Proceedings of Advances in Cryptology*, *EUROCRYPT 94, Lecture Notes in Computer Science*, (950): pp. 1-12, 1995.

[2] G. Ateniese, C. Blundo, A. DeSantis, D. R. Stinson, "Visual cryptography for general access structures," *Proc.ICAL96,Springer*, Berlin, pp.416-428, 1996. Article (CrossRef Link)

[3] C. Blundo, P. D'Arco, A.D. Santis, D. Stinson, "Contrast optimal threshold visual cryptography schemes," *SIAM Journal on Discrete Mathematics* 16 (2), pp. 224–261, 2003. Article (CrossRef Link)

[4] R. Ito, H. Kuwakado, H. Tanaka, "Image size invariant visual cryptography," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Science E82-A (10)*, pp. 2172–2177, 1999.

[5] C. Yang, "New visual secret sharing schemes using probabilistic method," *Pattern Recognition Letters 25*, pp. 481–494, 2004. Article (CrossRef Link)

[6] F. Liu, C. Wu, X. Lin, "The alignment problem of visual cryptography schemes", *Designs, Codes and Cryptography* 50, pp. 215–227, 2009. Article (CrossRef Link)

[7] D. Wang, L. Dong, X. Li, "Towards shift tolerant visual secret sharing schemes," *IEEE Transactions on Information Forensics and Security 6* (2), pp. 323–337, 2011. Article (CrossRef Link)

[8] G. Horng, T. Chen, D. Tsai, "Cheating in visual cryptography", *Designs, Codes and Cryptography* 38, pp. 219–236, 2006. Article (CrossRef Link)

[9] C. Hu, W. Tzeng, "Cheating prevention in visual cryptography", *IEEE Transactions on Image Processing* 16 (1), pp. 36–45, 2007. Article (CrossRef Link)

[10] Y. Chen, G. Horng, D. Tsai, Comment on "cheating prevention in visual cryptography", *IEEE Transactions on Image Processing 21* (7), pp. 3319–3323, 2012. Article (CrossRef Link)

[11] T. Guo, F. Liu, C. Wu, "Multi-pixel encryption visual cryptography", in: *Inscrypt 2011*, *Lecture Notes in Computer Science*, vol. 7537, pp. 86–92, 2012. Article (CrossRef Link)

[12] R. Wang, "Region incrementing visual cryptography,"*IEEE Signal Processing Letters* 16 (8), pp. 659–662, 2009. Article (CrossRef Link)

[13] C. Yang, H. Shih, C. Wu, L. Harn, "k out of n region incrementing scheme in visual cryptography", *IEEETransactions on Circuits and Systems for Video Technology* 22 (6), pp. 779–810, 2012.

[14] S. Shyu, "Efficient construction for region incrementing visual cryptography,"*IEEE Transactions on Circuits and Systems for Video Technology 22* (5), pp. 769–777, 2012. Article (CrossRef Link)

[15] T. Guo, F. Liu, C. Wu, "Multi-pixel encryption visual cryptography", in: *Inscrypt 2011*, *Lecture Notes in Computer Science,* vol. 7537, pp. 86–92, 2012. Article (CrossRef Link)

[16] F. Liu, T. Guo, C. Wu, L. Qian, "Improving the visual quality of size invariant visual cryptography scheme,"*Journal of Visual Communication and Image Representation* 23, pp. 331–342, 2012. Article (CrossRef Link)

[17] T. Chen, K. Tsao, "Threshold visual secret sharing by random grids,"*Journal of Systems and Software* 84, pp. 1197–1208, 2011. Article (CrossRef Link)

[18] T. Guo, F. Liu, C. Wu. "Threshold visual secret sharing by random grids with improved contrast."*Journal of Systems and Software*, in press. Article (CrossRef Link)

[19] O. Kafri, E. Keren, "Encryption of pictures and shapes by random grids", *Optics Letters* 12 (6), pp. 377–379, 1987. Article (CrossRef Link)

[20] Tzung-Her CHEN, Yao-Sheng LEE "A New Random-grid-based Visual Secret Sharing by Edge Enhancement"*Journal of Computational Information Systems* 8: 4, pp. 1507–1513, 2012.

[21] T. Chen, K. Tsao, "User-friendly random-grid-based visual secret sharing,"*IEEE Transactions on Circuits and Systems for Video Technology,* 21 (11), pp. 1693–1703, 2011. Article (CrossRef Link)

[22] P. Tuyls, H. D. L. Hollmann, J. H. Van Lint, L. Tolhuizen, "XOR-based visual cryptography schemes," *Designs Codes Cryptography*, vol. 37, no.1, pp. 169–186, 2005. Article (CrossRef Link)

[23] C.-N. Yang, D.-S. Wang, "Property Analysis of XOR-Based Visual Cryptography," *IEEE transactions on circuits and systems for video technology*, vol. 24, no. 2, pp. 189-197, 2014. Article (CrossRef Link)

[24] T. Chen, K. Tsao, "Threshold visual secret sharing by random grids," *Journal of Systems and Software*, vol. 84, pp. 1197–1208, 2011. Article (CrossRef Link)

[25] T. Chen, K. Tsao, "User-friendly random-grid-based visual secret sharing," *IEEE Transactions Circuits System Video Technology*, vol. 21, no. 11, pp.1693–1703, Nov. 2011. Article (CrossRef Link)

[26] X.Wu, W. Sun, "Random grid-based visual secret sharing for general access structures with cheat-preventing ability," *Journal of Systems and Software,* vol. 85, no. 5, pp. 1119–1134, 2011. Article (CrossRef Link)

[27] T. Guo, F. Liu, C.K. Wu, "k out of k extended visual cryptography scheme by random grids"*Signal Processing 94*, pp. 90–101, 2014. Article (CrossRef Link)

Ram Sekher Pati received his B. Tech. degree in computer science and engineering from West Bengal University of Technology, West Bengal, India, in 2014. He is currently pursuing his M. Tech. from the Academy of Technology at West Bengal University of Technology, West Bengal, India. His research interests include cryptography and information security.

Amitava Nag is working as an Assistant Professor and Head of the IT Department, Academy of Technology, West Bengal, India, and is a member of the ACM and IEEE. He is one of the authors of the books Data Structures and Algorithms Using C, Numerical Methods and Programming, Basic Computation And Principles Of Computer Programming, Operating System, and contributes articles to CSI Communications. Amitava Nag received his M. Tech. degree from the University of Calcutta and recently submitted his Ph.D. thesis at the Dept. of Engineering & Technological Studies, University of Kalyani. His areas of interest include Image Processing, Information Security, Cloud Computing, and Data Mining.