IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 26, No. 1, February, 2021, pp. 135-142
Journal homepage: http://iieta.org/journals/isi

A Novel Image Encryption Using Parity Based Visual Cryptography

Kanusu Srinivasa Rao[1*], Mandapati Sridhar[2]

[1] Dept. of Computer Science and Engineering, Acharya Nagarjuna University, Guntur 522510, India
[2] Dept. of Compute Applications, R.V.R. & J.C College of Engineering, Guntur 522019, India

Corresponding Author Email: kanususrinivas@yogivemanauniversity.ac.in

https://doi.org/10.18280/isi.260115

Received: 13 November 2020
Accepted: 29 January 2021

Keywords:
pixel expansion, parity, bit slicing, XOR operation

ABSTRACT

The current era is mainly focused on secured data transmission and every organization takes preventive measures to protect network's private data. Among different techniques visual cryptography is a prominent one that that encrypts the visual information and decrypts secret using mechanical operations without any computation, but each share need pixel expansion. In the current work, we propose an Image encryption technique using (n, n) Visual cryptography based on simple operations without pixel expansion. The proposed novel technique gives an image encryption using visual cryptography based on Least significant bit (LSB) technique in spatial domain and parity mechanism using Exclusive-OR(XOR) operation. developed for encrypting grey scale image. Image encryption and decryption uses simple Boolean operations. The technique provides better quality of shares and recovers without any loss.

1. INTRODUCTION

In the current generation people are contemporary and moving towards e-commerce, the field of computers and electronics with rapid speed [1]. This is made possible with digitalization of data and rapid growth in internet applications. Because of this rapid growth, expansion of the network bandwidth has increased enormously thus allowing to flow large amount of data that includes images, audio, videos. All transactions made by these applications uses internet which is considered as primary medium throughout the world. As this medium is not secure there is every possible of data duplication and tampering of data. In these circumstances securing data is very important at both the ends. There are wide ranges of security techniques available that are used in communication systems to make it secure and reliable over the network [2, 3].

In protecting the sensitive data [3] that travels through non secure network, cryptography is a systematic approach that is being used from the past few decades. This approach transforms the original data into other unrecognizable form as shown in Figure 1. This is a scientific approach that has extended and striking history [4]. In providing security this science has developed into a crucial element of modern generation [5].

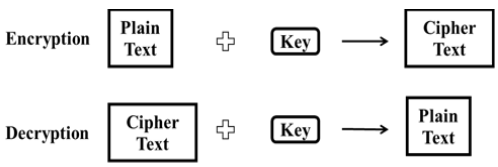


Figure 1. Framework of cryptography

In developed secured systems cryptography not only provides security to the sensitive data but also provides user authentication and message integrity. But the algorithms that are developed from cryptography require more computational capabilities to perform encryption and decryption. Along with computational processing time, these algorithms are also responsible for different types of new security attacks.

Besides cryptography there is another form that hides confidential data of any form inside image and is referred as steganography. This method of image hiding is broadly divided into two categories. The first category is frequency domain [6] that has less data hiding capacity and is more complicated in processing. The second category is spatial domain [7, 8] that has huge data hiding capacity and is less complicated than frequency domain. The well-known approach in spatial domain is the least significant bit method that is more prominent. This is very simple to use and sensitive scheme. This approach straightforwardly hides the secret data in least significant bit of cover image pixel to generate stego image. But the stego image that is generated by using least significant bit approach is of poor quality when the range of LSB used for hiding data is greater than or equal to 4.

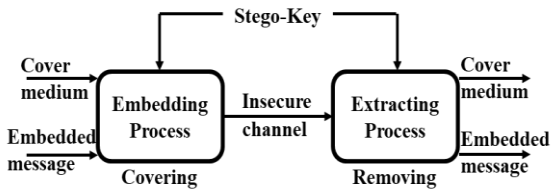


Figure 2. Framework of steganography

In 1994 Naor & Shamir first proposed the new cryptographic technique referred as Visual Cryptography [9]. The idea behind this scheme is secret sharing of data. This presents more confidentiality to data with less computation. By using this technique visual information like text, pictures

can be encrypted by combining the notations of exact ciphers and cryptographic secret sharing with that of raster graphics. Decryption process is a mechanical aspect where no computational effort is needed and it is nearly impractical to get back the secret data from encrypted images. To get back the original form both transparent images and layers are essential to disclose the data and are carried out by human visual system. Here Figure 2 represents Framework of steganography.

In process of providing security unlike cryptography and steganography, two different transparent images are used in visual cryptography. In these two images one image holds random pixels and the other image holds the secret data. While encrypting, the secret image is divided into different shares and they are hidden in shares of separate image which becomes completely impossible to identify the secret data. It is confusing and very difficult to understand the data until the shares are separate. When the shares are brought together and placed one over the other recovering the hidden data is possible. Original image is achieved by heaping all n shares. Secret sharing helps in distributing different shares between n different people, so that only authorized people can be capable of recovering the secret data. The uniqueness of visual cryptography than other hiding methods and benefits over them is that, visual cryptography requires very little computational methods. This can be directly seen while handling the decryption process, where the hidden data can be recovered by stacking operation and simply by human vision.

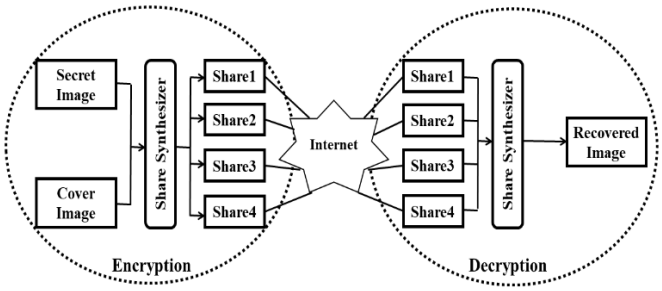


Figure 3. Framework of visual cryptography

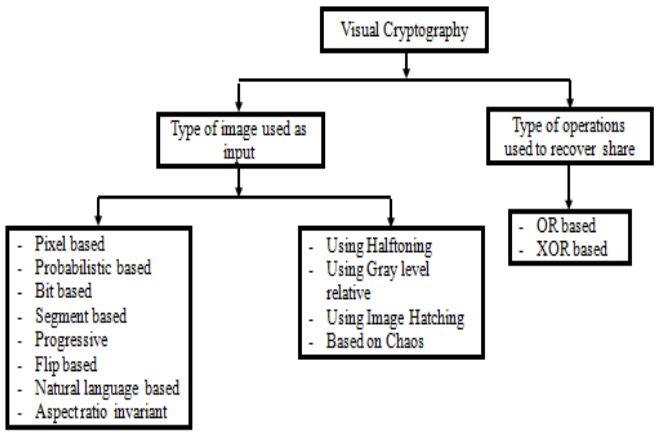


Figure 4. Classification of visual cryptography

Sharing of image is subset of secret sharing. This is because it acts as a non-regular method to the common secret sharing pitfall. Secret data in this form are hidden images. Generally secret is denoted as a number. This permits an exact encrypting system provided for individual source of secrets. Without the problem of inverse conversions, the digits cannot be understood exactly to characterize the correct meaning of the secret. Sharing of image describes a system that is similar to regular secret sharing. In (k, n) sharing of image, the image that conveys the secret message is divided into n parts known as shares. The reverse decryption process is completely ineffective unless at least k pieces are collected and superimposed. The Classification of visual cryptography is shown in Figure 4. This classification is made on the basis of image that we give in the form of input (like binary image, grayscale and color image) and logical operations that are used during the recovery of the share. Figure 3 represents Framework of Visual Cryptography. And Figure 4 describes Classification of visual cryptography sharing.

Ateniese et al. [10] proposed an extended visual cryptgraphic scheme that is based on access struture. This structure contains two types of sets. The first one is qualified access structure and the second one is forbidden access structure in aset of n participants. Extended visual cryptography is different visual cryptography that the recognizable image can be seen on every share, once the shares are superimposed. This is only possible when all parts have qualified access structure. The other difference is that the image on the share will vanish and secret message will be visible. In extended visual cryptography first n shares need to be images with meaningful information. The mesage to be secured is generally the last with $(n + 1)$.To use extended visual cryptography method, a common construction is to be defined. Ateniese et al. [10] developed a system that can generate shasres for the scheme.

In developing a new visual cryptography scheme for gray scale image the present work is organized in the following pattern. Section 2 analyzes the over all work in the field of visual cryptography. Section 3 expalin the theme of the work. Section 4 illustrates the proposed method develpoed. Section 5 elaboratly discuessed the results of the work and proposed visual cryptography scheme. Section 6 concludes the work with features and performance.

2. LITERATURE SURVEY

Shamir [11] in 1979 initially proposed the concept of secret sharing by using shares. This method is intended to encrypt sensible data set into n shares. After dividing them into n shares then they are distributed to n users. In decryption process k number of shares or additional shares are used to recover the sensible data. Noar and shamir [9, 12] in 1995 were the first authors to propose the concept of visual cryptography. But the concept proposed by them are fit for only binary images. The main drawback of this concept is that noisy shares are derived, that might be apprehensive to hackers. Chang and Lee [13] in 1993 and Sun and Shieh [14] in 1994 with the concept of Noar and Shamir studied different correlated methods. But the study carried was confined to digital text form of data and are not useful for multimedia data sets. Verheul and Van Tilborg, [15] in 1997, Blundo et al., [16] in 2000 and Lin and Tsai, [16] in 2003 tried to extend the visual cryptography system to gray-level images and then to color images. But they could not succeed because of problem arousing suspicion.

Tuyls et al. [17] used *XOR* operation and developed a system that shares data securely by using binary images. Yi et al. [18] proposed a method using color image that has no expansion in pixel. Chao et al. [19] developed a method that extends (n, n)

method to (k, n). This extension is made by using shadows assignment matrix. Singh et al. [20] developed a method by using random matrices. These matrices are used as key for sharing secret data.

Chen and Lin [21] worked on Fault tolerant system that securely transmits images. This method is based on several threshold which controls quality of the revealed secret image. Wu et al. [22] developed a method by using visual cryptography that shares two secret images in two different shares. Feng et al. [23] proposed a visual cryptographic method that hides multiple secret images. These multiple images that needs to be protected will be divided into two shares. Shyu et al. [24] developed visual cryptographic scheme on multiple secret sharing. This system encrypts secrets that are set of $n \geq 2$ into two circle where n secrets are stacked one by one for the first share. The second share is rotated with n dissimilar angles.

Hwang [25] developed a visual cryptographic system that improves the visual effect of generated shares. Adhikari and Bose [26] developed a method that used Latin squares in providing security for sensitive data. Liu et al. [27], developed visual cryptographic step construction method based on optimum pixel expansion. Wang and Hsu [28] proposed a method that adds tag to the shares generate from images. Lin and Chung [29] developed a method that dynamically modifies the quantity of shares and gives new shares without troubling the original shares. Verheul and Van Tilborg [14] introduced arcs in developing a system for colored images in visual cryptography. Wang et al. [30] used simple Boolean operations in developing secret shares.

Adelson [31] in 1990, Bender et al. [32] in 1996, Wu and Tsai [33] in 1998, Hsu and Wu [34] in 1999, Kundur and Hatzinakos [35] in 1999 developed different methods to hide sensible data. The study by these authors mainly focused on generating shares that are free from noise. In enhancing this protection mechanism, data hiding procedures to share the data securely has been adopted. Lin and Delp [36] in 1999 studied on false share data and concentrated on capacity of authentication. They identified that secret sharing of sensitive data can be by using fragile watermarks. They developed the scheme of fragile watermark that embed data in an image. If any attempt is made to hack watermarked image, it will be demolished.

Yang and Laih [37] in 2000 developed a visual secret sharing system for coloured images. In this system length ofthe block derived are effective that previously developed blocks. Share derived in this method are of no meaning and is intended for exchanging a single secret. Mizuhanakajima and Yasushi [38] in 2002 proposed an extended visual cryptographic method that specially used for natural images. This method as an alternative creates meaningful share rather than random shares. Because of these shares noise is avoided and difficulties with noise images are easily handled. Lin and Tsai [16] in 2003 used indecisive technique for grey images. This technique used is good for changing from binary level image to grey level image.

Hou and Tu [39] in 2005 developed a system for chromatic images. In the developed system multi pixel encoding technique is used to secure sensitive data. Zhizhou, Gonzalo R. arce and Giovanni Di Crescendo [40] in 2006 developed a system by using halftone visual cryptography. This method uses dots to simulate adjoining tone images that might differ either in size or in space. Authors for encoding sensitive image in binary form used void and cluster algorithm. Once they are encoded n Halftone shares are generated that holds important visual information. Sozan Abdullah [41] in 2010 developed a visual cryptographic scheme that works on colour images that takes four images and gives three images as output. This scheme hides sensitive data in images that divides secret image into multiple layers. Each layer that is divided holds some sensitive data. To decrypt the original data, layers are to be arranged in order and revealed by human vision without any specific operations or computation.

Liao and Huang [42] in 2011 worked on multiple watermarking schemes by using visual cryptography and Integer wavelet transform. These schemes are applied on Gray scale images. Sharma [43] in 2012 worked on visual cryptography and error filters in halftone cryptography. In removing the doubt in eve dropper's halftone visual cryptography an extended technique of visual cryptography embeds random shares in high quality grayscale image. In this work sensitive data is visually translated by overlaying a qualified subset of transparencies. This work also describes several error diffusions filters that are used to improve the image quality.

Wangein [44] in 2013 worked on securing biometric databases. In this method, shares that are from secret image are secured and digitally transmitted. These are used only for one time. Pandey and Shukla [45] in 2014 worked on compressed random shares. This scheme transforms the secret image into printable transparent sheets and then they are distributed to authorized users. While decrypting, the transparent sheets are stacked to recover the image. Ritesh et al. [46] in 2015 worked onasymmetric cover image encryption. The method developed embeds random shares into a meaningful cover share. Rakhude and Gedam [47] in 2016 developed a new visual cryptographic method to secure both text and multimedia. Here in this process images are divided shares that are encoded images and then the shares are distributed to authorized users.

Besides the above mentioned visual cryptography techniques proposed by various authors, few more techniques were also developed, in which the decryption is not just by mechanical operation like stacking of the shares; Wherein decryption is implemented using simple boolean operations like *XOR*. Tuyls at el. [17] developed a threshold visual secret sharing associated with simple *XOR* (modulo two addition) operations. Wang et al. [30] has worked on probabilistic $(2, n)$ scheme for binary images and a deterministic $(n.n)$ scheme for grayscale images. The decryption is completly based on simple boolean operations.

Dong et al. [4] has developed a *XOR* based $(2, n)$ secret sharing scheme with multiple shares held by each participant. The decryption is based on simple and precise boolean operations.

Liu et al. [48] in 2017 developed an that reconstructs secret image losslessly by using simple oerations like addition.

Bhat et al. [49] in 2019 developed a key management system that uses third party to generate shares and distrbute to participants in the group. It also generates share extra share for itself to communicate with the participants. This helps in regeneraition and redistribution of
shares. It gives perfect contrast and security.

Guttikonda and Mundukur [50] in 2020 proposed a method that provides security for multimedia data which is stored in cloud centers. Two different mehods are used to generate meaningless audio shares. These generated shares are less in dimension when compared to the original share. This work focus on reducing the dimensions of shares.

Yadav [51] in 2020 developed a system that converts fake and modified shares into original shares that has very good accuracy. This helps to identify fake shares that are intended to cheat users.

3. CONTRIBUTION

The method proposed in this paper is towards construction of encryption technique for gray scale images. It is a novel technique for image encryption based on visual cryptography. The proposed method is an application of visual cryptography. The (n, n) secret sharing technique is adopted in encryption process. Each secret image is divided into four shares in encryption process. Shares are generated based on bit slicing technique and further processed using parity *(XOR)* mechanism. Unlike visual cryptography, in the decryption it uses simple mathematical operations and extraction steps to reconstruct the secret image from all shares.

4. PROPOSED METHOD

In the proposed model, an effort is made to transmit the gray scale image securely using a novel encryption based on visual cryptography technique. The technique used in this method is (n, n) secret sharing scheme. Firstly, the secret image is encrypted by splitting it into number of shares using bit slicing technique [1]. Each pixel of the secret image is processed and its bits are distributed inorder to produce four shares. Each pixel of the secret image consists of 8 bits and its representation is given in Figure 5.

B_1	B_2	B_3	B_4	B_5	B_6	B_7	B_8
MSB							*LSB*

Figure 5. Representation of pixel - gray scale image

4.1 Encryption

The 8-bits of pixel are paired into 4 groups and each group is merged with its corresponding cover image pixel, and it is further processed through a parity based mechanism to produce four shares. On the other side, upon receiving all four shares, the original secret image can be reconstructed by using the parity *(XOR)* and extraction mechanism. It is not possible to reconstruct the original secret image without any one of those four shares.

Algorithm – Encryption of pixel of secret image

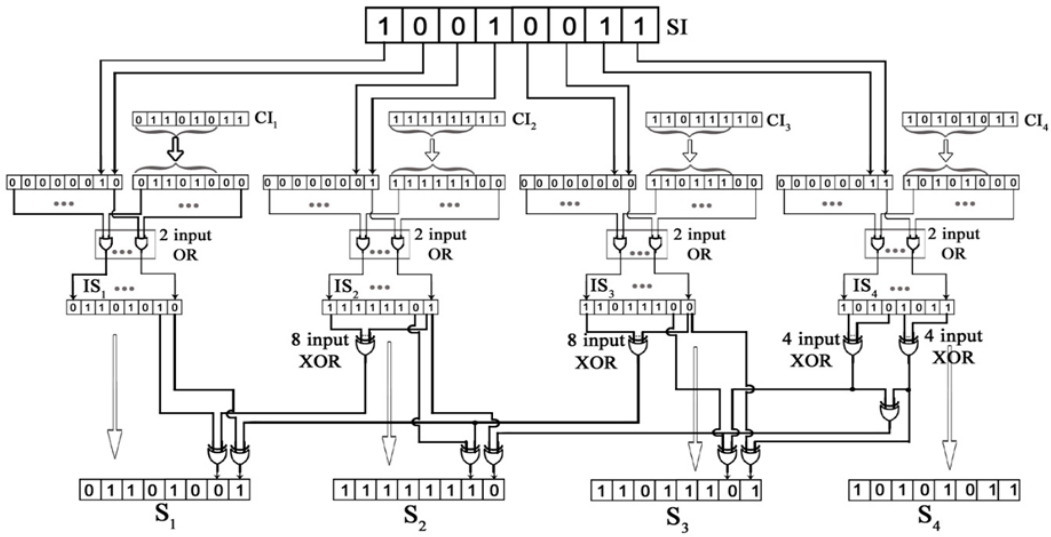
Input: SecretImage[ ][ ]
// input Secret image of size M×N
CoverImage1[ ][ ], CoverImage2[ ][ ],
CoverImage3[ ][ ], CoverImage4[ ][ ]
// cover images of size M×N for four shares
M, N // M rows and N columns of the input images
SI_pixel[ ] // secret image pixel array of 8 bit size
CI1_pixel[ ], CI2_pixel[ ], CI3_pixel[ ], CI4_pixel[ ]
// cover image pixel array of size 8 bits

Output: Share1[ ][ ], Share2[ ][ ], Share3[ ][ ], Share4[ ][ ]
// Shares
Algorithm:
1)for i = 0 to M-1 repeat
2) for j = 0 to N-1 repeat
// for each pixel of SecretImage repeat the steps from 3 to 24
3) SI_pixel[ ] = binary(SecretImage[i][j])
4) CI1_pixel[ ] =binary(CoverImage1 [i][j])
5) CI2_pixel[ ] =binary(CoverImage2 [i][j])
6) CI3_pixel[ ] =binary(CoverImage3 [i][j])
7) CI4_pixel[ ] =binary(CoverImage4 [i][j])
// binary representation of the pixel of the secret image in 8-bit form
8) CI1_pixel[6] = SI_pixel[0];
CI1_pixel[7] = SI_pixel[1];
9) CI2_pixel[6] = SI_pixel[2];
CI2_pixel[7] = SI_pixel[3];
10)CI3_pixel[6] = SI_pixel[4];
CI3_pixel[7] = SI_pixel[5];
11) CI4_pixel[6] = SI_pixel[6];
CI4_pixel[7] = SI_pixel[7];
// merging with cover image
12) for k = 0 to 7
13)CI1_pixel[6]=CI1_pixel[6]*XOR*CI2_pixel[k];
14) CI1_pixel[7]=CI1_pixel[7]*XOR*CI3_pixel[k];
// parity computation for share1
15)for k = 0 to 7
16) CI2_pixel[6]=CI2_pixel[6]*XOR*CI3_pixel[k];
17) CI2_pixel[7]=CI2_pixel[7]*XOR*CI4_pixel[k];
// parity computation for share 2
18) for k = 0 to 3
19)CI3_pixel[6]=CI3_pixel[6]*XOR*CI4_pixel[k];
20) CI3_pixel[7]=CI3_pixel[7]*XOR*CI4_pixel[k+4];
// parity computation for share 3
21) Share1[i][j] = binaryTodecimal(CI1[ ]);
22) Share2[i][j] = binaryTodecimal(CI2[ ]);
23) Share3[i][j] = binaryTodecimal(CI3[ ]);
24) Share4[i][j] = binaryTodecimal(CI4[ ]);

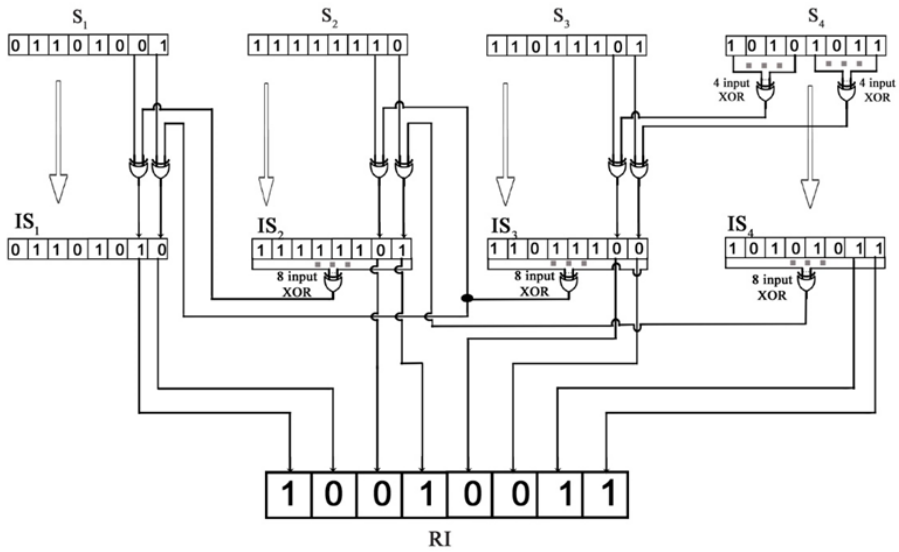
Three steps are involved in encrypting a pixel of the secret image: 1. Bit slicing, 2. Merging with cover image, 3. Finally share generation using Parity mechanism. In step 1 and 2 [52-54], the first two most significant bits (MSB) B_1 and $B_2$of the pixel are merged with its corresponding cover image pixel to produce intermediate share for Share$_1$. Similarly, the bits B_3 and B_4; B_5 and B_6; and B_7 and B_8 are processed to produce the intermediate share for Share$_2$, Share$_3$ and Share$_4$ respectively.

In step 3, the two LSB bits B_7 and B_8 of each intermediate shares are processed with other intermediate shares though parity mechanism inorder to produce the respective bits $B_7$and B_8 of the final share. For Share$_1$, bit B_7 is computed from bit B_7 of its corresponding intermediate share and all bits of intermediate Share$_2$, i.e., it is computed by *XORing*B_7 of intermediate Share$_1$ and all bits of intermediate Share$_2$. Similarly, bit B_8 is computed from bit B_8 of its corresponding intermediate share and all bits of intermediate Share$_3$.

For Share$_2$, bit B_7 is computed from bit B_7 of its corresponding intermediate share and all bits of intermediate Share$_3$.Similarly, bit B_8 is computed from bit B_8 of its corresponding intermediate share and all bits of intermediate Share$_4$. Now for Share$_3$, bit B_7 is computed from bit B_7 of its corresponding intermediate share and first four MSB bits of intermediate Share$_4$.Similarly, bit B_8 is computed from bit $B_8$of its corresponding intermediate share and four LSB bits of intermediate Share$_4$. Share$_4$ is just copied from the intermediate Share$_4$.



SI- Secret Image
CI_1- Cover Image$_1$, CI_2- Cover Image$_2$, CI_3- Cover Image$_3$, CI_4- Cover Image$_4$
IS_1 – Intermediate Share$_1$, IS_2 – Intermediate Share$_2$, IS_3 – Intermediate Share$_3$, IS_4 – Intermediate Share$_4$
S_1- Share$_1$, S_2- Share$_2$, S_3- Share$_3$, S_4- Share$_4$
(a)



S_1- Share$_1$, S_2- Share$_2$, S_3- Share$_3$, S_4- Share$_4$
IS_1 – Intermediate Share$_1$, IS_2 – Intermediate Share$_2$,
IS_3 – Intermediate Share$_3$, IS4 – Intermediate Share$_4$
RI- Reconstructed Image
(b)

Figure 6. An example of Encryption and Decryption of a Pixel using proposed method (a) Encryption of the pixel (147 gray value/ intensity), (b) Decryption of the pixel

4.2 Decryption

Similarly, in decryption two steps are involved to reconstruct the pixel of original secret image from all its shares: 1) construction of intermediate shares from the shares using parity *(XOR)* mechanism, 2) extraction of secret image from the intermediate shares.

In the first step, it begins with construction of intermediate Share$_4$ from Share$_4$ where Share$_4$ is just copied to intermediate Share$_4$. Now intermediate Share$_3$ is constructed from intermediate Share$_4$ and Share$_3$, wherein the bit B_7 of intermediate Share$_3$ is computed from *XORing* of B_7 of Share$_3$ and first four MSB bits of intermediate Share$_4$.Similarly, bit B_8 of intermediate Share$_3$ is computed from *XORing* of B_8 of Share$_3$ and four LSB bits of intermediate Share$_4$. Intermediate Share$_2$ is now constructed from intermediate Share$_3$, intermediate Share$_4$ and Share$_2$, wherein bitB_7 of intermediate Share$_2$ is computed from *XORing* of B_7 of Share$_2$ and all eight bits of intermediate Share$_3$. Similarly, bit B_8 of intermediate Share$_2$ is computed from *XORing* of B_8 of Share$_2$ and all eight bits of intermediate Share$_4$. Finally in step 1, the intermediate Share$_1$ is constructed from intermediate Share$_2$, intermediate Share$_3$ and Share$_1$, where the bit B_7 of intermediate Share$_2$ is computed from *XORing*ofB_7 of Share$_1$and all eight bits of intermediate Share$_2$, then bit B_8 of intermediate Share$_1$ is computed from *XORing* of B_8 of Share$_1$ and all eight bits of intermediate Share$_3$.

In step 2, pixel of secret image is reconstructed from last

two LSB bits (B_7 and B_8) of all four intermediate shares respectively from intermediate Share$_1$ to intermediate Share$_4$.

4.3 Example

In encryption as input secret image is taken at a pixel level and same process is repeated for every pixel of the secret image. As mentioned in section 4.1, encrypting a pixel of the secret image through bit slicing and merging with its corresponding cover image pixels is demonstrated with an example. Let's consider a pixel at some i^{th} row and j^{th} column for encryption and decryption, and consider the pixel intensity value of Secret image is 147, cover image$_1$ is 107, cover image$_2$ is 255, cover image$_3$ is 222 and cover image$_4$ is 171. The binary representation of the pixels is considered throughout the encryption and decryption process. The encryption of secret image pixel is given in Figure 6(a) and reconstruction of a pixel of the secret is given in Figure 6(b). After encryption corresponding pixel in the share$_1$, share$_2$, share$_3$ and share$_4$ becomes 105, 254, 221 and 171 respectively. These pixels are almost close to the pixels of its respective cover images. The change in pixel value is very little, which a human eye cannot perceive difference in the intensity. Therefore, after encryption of the entire secret image, final four shares of secret image look like its corresponding four cover images only.

4.4 Security

Each pixel of original image is shared into four shares which are completely covered by a cover image. The Pixels of secret image are distributed and merged with cover images through traditional LSB based water marking technique. Since, intermediate Share$_1$ consists of two MSB bits of secret image pixel, it is more prone to attack and from which secret image can easily be recovered. Similarly, some traces of the secret image are visible in intermediate share$_2$ and intermediate share$_3$. Intermediate Share$_4$ is constituted with last two LSB bits, therefore no traces of secret image are found. In step 3, parity mechanism will provide additional security on intermediate share$_1$ to intermediate share$_3$ through *XOR* operation over multiple shares. The order of shares must be followed during decryption process for reconstruction of the secret image. Decryption of the secret is possible only when all shares are arranged in correct sequence. The security is mainly depending on order of the shares and size of the input image. For n shares, without knowing the order one has to try all possible $n!$ combinations. The size of the input image reflects on the complexity of encryption and decryption.

5. RESULT AND DISCUSSION

The secret image encryption and decryption is implemented using the proposed method and its experimental results are presented in Figure 7. The secret image Figure 7(a) of 512 × 512 Image size with 72 resolution, is divided into four shares which are covered by four Cover Images given in Figure 7(b)-(e) respectively. The final four shares of secret image are given in Figure 7(f)-(i). Figure 7(J) is recovered secret image from the received four shares in decryption process. The experimental results presented in Figure 7 are showing that all final shares have same look as its corresponding cover images and also, the decrypted secret image is lossless and has same quality of the input secret image.

The features and performance of proposed method is compared with other similar techniques with respect to secret sharing mechanism. The comparison is presented in Table 1.

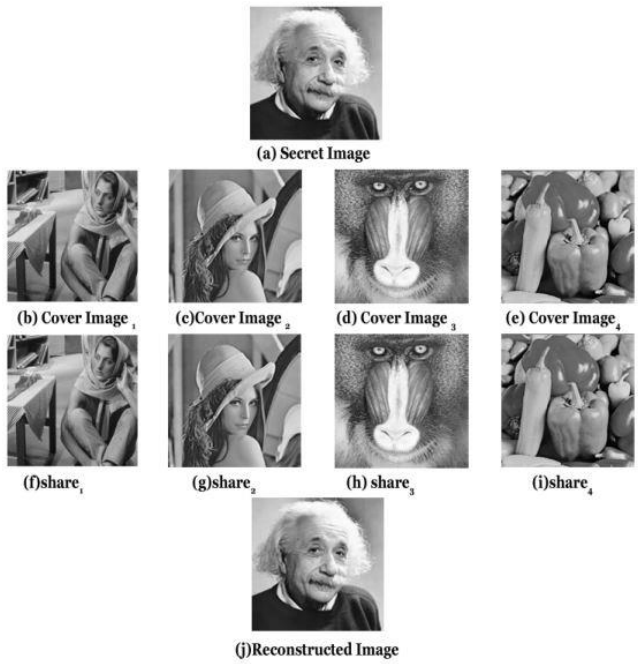


Figure 7. (a) Secret Image, (b) to (e) Cover Images 1 to 4, (f) to (i) Share Images 1 to 4, (j) Recovered Image

Table 1. Features and performance comparison of XOR based secret sharing techniques

Scheme	Image type	Scheme type	Contrast	Pixel Expansion	No. of shares held by each	Boolean Operations used in decryption
Tuyls [2]	Binary	(k,n) k<n and k is odd	<<1	Yes	1	XOR
Wang [3]	Binary	$(2,n)$	1/2	No	1	XOR, AND
	Gray scale/color	(n,n)	1			
Dong [4]	Gray scale	$(2,n)$	1	No	>>1	XOR, OR
Proposed	Gray Scale	(n,n)	1	No	1	XOR

6. CONCLUSION

A technique for gray scale image encryption using visual cryptography has been proposed in this work. A novel (n,n) secret sharing technique using LSB technique in spatial domain and parity mechanism has been developed and used

for image encryption. The decryption has been implemented using simple and precise Boolean computations. The proposed technique has been implemented and explored with an example. The experimental results of image encryption and decryption using proposed (n, n)secret sharing approach are presented and it is shown that the reconstructed secret image in the decryption is lossless and maintaining the same quality of the original secret image. The features and performance of proposed technique has been compared with the existing similar secret sharing techniques.

REFERENCES

[1] Reddaiah, B. (2016). A Study on Pairing Functions for Cryptography. International Journal of Computer Applications, 975: 8887.

[2] Jeyanthi, N., Iyengar, N.C.S.N. (2012). An entropy based approach to detect and distinguish DDoS attacks from flash crowds in VoIP networks. IJ Network Security, 14(5): 257-269.

[3] Jeyanthi, N., Thandeeswaran, R., Vinithra, J. (2014). RQA based approach to detect and prevent DDoS attacks in VoIP networks. Cybernetics and Information Technologies, 14(1): 11-24. https://doi.org/10.2478/cait-2014-0002

[4] Khan, D. (1976). The Code Breackers, Macmillan Publishing Company. New Yark, WWW.SimonandSchuster.con.

[5] Tanenbaum, A.S., Bos, H. (2015). Modern operating systems. Pearson.

[6] Chang, C.C., Chiang, C.L., Hsiao, J.Y. (2005). A DCT-domain system for hiding fractal compressed images. 19th International Conference on Advanced Information Networking and Applications (AINA'05), Volume 1 (AINA papers), Taipei, Taiwan, pp. 83-86. https://doi.org/10.1109/AINA.2005.17

[7] Wu, D.C., Tsai, W.H. (2000). Spatial-domain image hiding using image differencing. IEE Proceedings-Vision, Image and Signal Processing, 147(1): 29-37. https://doi.org/10.1049/ip-vis:20000104

[8] Thien, C.C., Lin, J.C. (2003). A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function. Pattern recognition, 36(12): 2875-2881. https://doi.org/10.1016/S0031-3203(03)00221-8

[9] Naor, M., Shamir, A. (1994). Visual cryptography. Workshop on the Theory and Application of Cryptographic Techniques, 1-12. https://doi.org/10.1007/BFb0053419

[10] Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R. (1995). Extended schemes for visual cryptography. Theoretical Computer Science.

[11] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11): 612-613. https://doi.org/10.1145/359168.359176

[12] Chang, C.C., Lee, H.C. (1993). A new generalized group-oriented cryptoscheme without trusted centers. IEEE journal on Selected Areas in Communications, 11(5): 725-729. https://doi.org/10.1109/49.223873

[13] Sun, H.M., Shieh, S.P. (1994). Construction of dynamic threshold schemes. Electronics Letters, 30(24): 2023-2025.

[14] Verheul, E.R., Van Tilborg, H.C. (1997). Constructions and properties of k out of n visual secret sharing schemes. Designs, Codes and Cryptography, 11(2): 179-196. https://doi.org/10.1023/A:1008280705142

[15] Blundo, C., De Santis, A., Naor, M. (2000). Visual cryptography for grey level images. Information Processing Letters, 75(6): 255-259. https://doi.org/10.1016/S0020-0190(00)00108-3

[16] Lin, C.C., Tsai, W.H. (2003). Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters, 24(1-3): 349-358. https://doi.org/10.1016/S0167-8655(02)00259-3

[17] Tuyls, P., Hollmann, H.D., Van Lint, J.H., Tolhuizen, L.M.G.M. (2005). XOR-based visual cryptography schemes. Designs, Codes and Cryptography, 37(1): 169-186. https://doi.org/10.1007/s10623-004-3816-4

[18] Yi, F., Wang, D., Luo, P., Dai, Y. (2007). Two new color (n, n)- secret sharing schemes. Journal on Communications, 28(5): 30-35.

[19] Chao, K.Y., Lin, J.C. (2009). Secret image sharing: A Boolean-operations-based approach combining benefits of polynomial-based and fast approaches. International Journal of Pattern Recognition and Artificial Intelligence, 23(2): 263-285. https://doi.org/10.1142/S0218001409007090

[20] Singh, J.P., Nag, A., Bhattacharjee, T. (2011). Random matrices based image secret sharing. International Journal of Advanced Research in Computer Science, 2(4): 104-108.

[21] Chen, S.K., Lin, J.C. (2005). Fault-tolerant and progressive transmission of images. Pattern recognition, 38(12): 2466-2471. https://doi.org/10.1016/j.patcog.2005.04.002

[22] Wu, C.C., Chen, L.H. (1998). A Study on Visual Cryptography. Master Thesis, Institute of Computer and Information Sciences, National Chiao Tung University, Taiwan, R.O.C.

[23] Feng, J.B., Wu, H.C., Tsai, C.S., Chang, Y.F., Chu, Y.P. (2008). Visual secret sharing for multiple secrets. Pattern Recognition, 41(12): 3572-3581. https://doi.org/10.1016/j.patcog.2008.05.031

[24] Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z., Chen, K. (2007). Sharing multiple secrets in visual cryptography. Pattern Recognition, 40(12): 3633-3651. https://doi.org/10.1016/j.patcog.2007.03.012

[25] Hwang, R., Chang, C. (1998). Some secret sharing schemes and their applications. Ph. D. dissertation of the Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan.

[26] Adhikari, A., Bose, M. (2004). A new visual cryptographic scheme using Latin squares. IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences, 87(5): 1198-1202.

[27] Liu, F., Wu, C., Lin, X. (2009). Step construction of visual cryptography schemes. IEEE Transactions on Information Forensics and Security, 5(1): 27-38. https://doi.org/10.1109/TIFS.2009.2037660

[28] Wang, R.Z., Hsu, S.F. (2011). Tagged visual cryptography. IEEE Signal Processing Letters, 18(11): 627-630. https://doi.org/10.1109/LSP.2011.2166543

[29] Lin, S.J., Chung, W.H. (2011). A probabilistic model of (t, n) visual cryptography scheme with dynamic group. IEEE Transactions on Information Forensics and

Security, 7(1): 197-207. https://doi.org/10.1109/TIFS.2011.2167229
[30] Wang, D., Zhang, L., Ma, N., Li, X. (2007). Two secret sharing schemes based on Boolean operations. Pattern Recognition, 40(10): 2776-2785. https://doi.org/10.1016/j.patcog.2006.11.018
[31] Adelson, E.H. (1990). U.S. Patent No. 4,939,515. Washington, DC: U.S. Patent and Trademark Office.
[32] Bender, W., Gruhl, D., Morimoto, N., Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3-4): 313-336. https://doi.org/10.1147/sj.353.0313
[33] Wu, D.C., Tsai, W.H. (1998). Data hiding in images via multiple-based number conversion and lossy compression. IEEE Transactions on Consumer Electronics, 44(4): 1406-1412. https://doi.org/10.1109/30.735844
[34] Hsu, C.T., Wu, J.L. (1999). Hidden digital watermarks in images. IEEE Transactions on Image Processing, 8(1): 58-68. https://doi.org/10.1109/83.736686
[35] Kundur, D., Hatzinakos, D. (1999). Digital watermarking for telltale tamper proofing and authentication. Proceedings of the IEEE, 87(7): 1167-1180. https://doi.org/10.1109/5.771070
[36] Lin, E.T., Delp, E.J. (1999). A review of fragile image watermarks. Proceedings of the Multimedia and Security Workshop (ACM Multimedia'99) Multimedia Contents, 1: 25-29.
[37] Yang, C.N., Laih, C.S. (2000). New colored visual secret sharing schemes. Designs, Codes and Cryptography, 20(3): 325-336. https://doi.org/10.1023/A:1008382327051
[38] Nakajima, M., Yamaguchi, Y. (2002). Extended visual cryptography for natural images. Journal of WSCG. v10 i2. 303310.
[39] Hou, Y.C., Tu, S.F. (2005). A visual cryptographic technique for chromatic images using multi-pixel encoding method. Journal of Research and Practice in Information Technology, 37(2): 179-191.
[40] Zhou, Z., Arce, G.R., Di Crescenzo, G. (2006). Halftone visual cryptography. IEEE Transactions on Image Processing, 15(8): 2441-2453. https://doi.org/10.1109/TIP.2006.875249
[41] Abdulla, S. (2010). New visual cryptography algorithm for colored image. arXiv preprint arXiv:1004.4445.
[42] Liao, H.W., Huang, H.W. (2011). A multiple watermarking scheme for gray-level images using visual cryptography and integer wavelet transform. Journal of Computers, 22(1): 18-36.
[43] Sharma, A. (2012). Performance of error filters in halftone visual cryptography. International Journal on Cryptography and Information Security (IJCIS), 2(3): 143-159. https://doi.org/10.5121/ijcis.2012.2313
[44] Wange, S. (2013). A visual cryptography to secure biometric database. International Journal of Advanced Research in Computer Science and Software Engineering, 3(11).
[45] Pande, L.N., Shukla, N. (2013). Visual cryptography schemes using compressed random shares. International Journal of Advance Research in Computer Science and Management Studies, 1(4): 62-66.
[46] Yelane, R.D., Nitiket. N., Chilke, M.B.J. (2015). Security approach by using visual cryptographic technique. International Journal of Advanced Research in Computer Science and Software Engineering, 5(1).
[47] Rakhunde, S.M., Gedam, M. (2016). Survey on visual cryptography: Techniques, advantages and applications. National Conference on Recent Trends in Computer Science and Information Technology (NCRTCSIT-2016).
[48] Liu, X., Wang, S., Sang, J., Zhang, W. (2018). A novel lossless recovery algorithm for basic matrix-based vss. Multimedia Tools and Applications, 77(13): 16461-16476. https://doi.org/10.1007/s11042-017-5215-7
[49] Bhat, M.N., Buradagunta, S., Rani, K.U. (2019). A novel approach to key management using visual cryptography. Ingénierie des Systèmes d'Information, 24(6): 627-632. https://doi.org/10.18280/isi.240610
[50] Guttikonda, P., Mundukur, N.B. (2020). Secret Sharing with Reduced Share Size and Data Integrity. Ingénierie des Systèmes d'Information, 25(2): 227-237. https://doi.org/10.18280/isi.250210
[51] Yadav, M. (2020). Cheating Prevention and Detection Technique in Visual Secret Sharing. Ingénierie des Systèmes d'Information, 25(4): 453-460. https://doi.org/org/10.18280/isi.250407
[52] Peda, G.A., Lakshman Narayana, V. (2017). Protected strength approach for image steganography. Signal Processing, 34(3-4): 175.
[53] Dong, L., Wang, D., Ku, M., Dai, Y. (2010). (2, n) secret image sharing scheme with ideal contrast. 2010 International Conference on Computational Intelligence and Security, Nanning, China, pp. 421-424. https://doi.org/10.1109/CIS.2010.97
[54] Rao, K.S., Sridhar, M. (2018). A lossless secret image sharing scheme based on bit sharing visual cryptography. 2018 International Conference on Recent Innovations in Electrical, Electronics & Communication Engineering (ICRIEECE), Bhubaneswar, India, pp. 1417-1420. https://doi.org/10.1109/ICRIEECE44171.2018.9009306