International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 2, May 2014, PP 171-177

Improved Visual Cryptographic Scheme Using Average Filter and Additional Pixel Patterns

Shyla M.G

PG Student, Department of Computer Science
and Engineering
Adichunchanagiri Institute of Technology
Chikmagalur, Karnataka
shyla.mg.15@gmail.com

Gowramma B.H

PG Student, Department of Computer Science
and Engineering
Adichunchanagiri Institute of Technology
Chikmagalur, Karnataka
gow.paru@gmail.com

Vivekananda

Assatante Professor, Department of Computer Science and Engineering
Adichunchanagiri Institute of Technology
Chikmagalur, Karnataka
vivek.dream@gmail.com

Abstract: *Visual cryptography (VC) is a kind of secret image sharing scheme that uses the human visual system to perform the decryption computations. Contrast is one of the most important parameter in visual cryptography schemes. Usually, the reconstructed secret image will be darker than the original secret image. Additional pixel patterns are used to improve the contrast of the reconstructed secret images. The proposed scheme applies filterto reduce the noise and to improve the contrast in the reconstructed secret images.*

Keywords: *Visual cryptography, visual secret sharing, additional matrix, filter*

1. Introduction

Visual cryptography is a cryptographic technique, which allows visual information to be encrypted in such a way that decryption becomes a mechanical operation, does not require any computational complexity.

Digital information and data are transmitted more often over the Internet now than ever before. The availability and efficiency of global computer networks for the communication of digital information and data have accelerated the popularity of digital media. There is a great need to handle information in a secure and reliable way. In such situations, secret sharing is of great relevance.

The basic idea of secret sharing is to divide the information into pieces, so that qualified subsets of these pieces (shares) can be used to recover the secret. Intruders need to get access to several shares to retrieve the information and also to destroy the information. Secret sharing is very essential whenever secret information needs to be kept collectively by a group of participants in such a way that only a qualified subgroup is able to reconstruct the secret. Secret sharing is also useful if the owner of the secret does not trust any single person [1].

Visual cryptography (VC) implements secret sharing for images. Too much loss of contrast causes problems in the reconstruction of the original image.

Filters transform pixel intensity values to reveal certain image characteristics like improves contrast, removes noise and detection of known patterns.

This paper describes additional pixel patterns for white pixels to enhance contrast and application of filter to reduce noise and improve contrast in the reconstructed secret images.

2. Literature Survey

Much work has been done in visual cryptography schemes. In visual cryptography [2], they proposed a new type of cryptographic scheme, which can decode concealed images without any cryptographic computations. The scheme is perfectly secure and very easy to implement. This is similar to a one time pad in the sense that each page of cipher text is decrypted with a different transparency. The drawback of this proposal was a loss in contrast: a black pixel is translated in the reconstruction into a black region, but a white pixel is translated into a grey region (half black and half white).

Thomas Monoth and Babu Anto P [3], they proposed a visual cryptography scheme to encode a black and white image into the same size shares as the secret image. In addition, an improved method for the generation of shares is proposed using additional matrix. Visual cryptography method for encrypting printed texts, handwritten notes, and pictures are done in a perfectly secure way, and decoding these data with the human visual system. The contrast is the most important parameter in visual cryptography. Usually, the reconstructed secret image will be darker than the background of the original secret image. It achieves better contrast and reduces the noise in the reconstructed secret image without adding any computational complexity. In this technique the number of white pixels in the reconstructed secret image can be improve 50% or more. This method increases the number of white pixels and thus the contrast of the decrypted image compare to the conventional VCS.

3. Visual Cryptographic Schemes

Visual cryptography, proposed by Naor and Shamir [4], is one of the cryptographic methods to share secret images. A visual cryptography for a set P of n participants is a method to encode a secret image (SI) into n shadow images called shares, where each participant in P receives one share. Certain qualified subsets of participants can visually recover the SI, but other, forbidden sets of participants have no information on the SI.

The VCS describes the way in which an image is encrypted and decrypted. There are different types of visual cryptography schemes [5][6]. For example, there is the k-out- of-n scheme that says n shares will be produced to encrypt an image, and k shares must be stacked to decrypt the image. If the number of shares stacked is less than k, the original image is not revealed. The other schemes are 2-out-of- n and n-out-of-n VCS. In the 2-out -of-n scheme n shares will be produced to encrypt an image, and any two shares must be stacked to decrypt the image. In the n-out-of-n scheme, n shares will be produced to encrypt an image, and n shares must be stacked to decrypt the image. If the number of shares stacked is less than n, the original image is not revealed. Increasing the number of shares or participants will automatically increase the level of security of the encrypted message.

3.1. The Model

Let $P = \{1, 2,. . . , n\}$ be a set of elements called participants and let 2^P denote the collection of all subsets of P. Let $\Gamma_Q \subseteq 2^P$ and $\Gamma_F \subseteq 2^P$, where $\Gamma_Q \cap \Gamma_F = \theta$ .The members of Γ_Q are called qualified sets and members of Γ_F are called forbidden sets. The pair (Γ_Q, Γ_F) is called the access structure of the scheme [7].

Define Γ_O to consist of all minimal qualified sets: $\Gamma_O = \{A \in \Gamma_Q : A^| \notin \Gamma_Q \text{ for all } A^| \subset A\}$

The message (secret data) consists of a collection of black and white pixels. Each pixel appears in n version called shares, one for each transparency. Each share is a collection of m black and white sub pixels. The resulting structure can be described by an n x m Boolean matrix $S = [s_{ij}]$, where, $s_{ij} = 0$ the jth sub pixel in the ith share is black.

$s_{ij} = 1$ the jth sub pixel in the ith share is white.

Let (Γ_Q, Γ_F) be an access structure on a set of n participants. A $(\Gamma_Q, \Gamma_F, \alpha)$- VCS with the relative difference α and set of thresholds $1 \leq d \leq m$ is realized using the two n x m basis matrices S^0 and S^1 if the following two conditions hold:

(1). If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_Q$, then the "or" V of rows $i_1, i_2, \ldots\ldots i_p$ of S^0 satisfies $H(V) \leq d - \alpha * m$; whereas, for S^1 it results that $H(V) \geq d$.

(2). If $X = \{ i_1, i_2, \ldots\ldots i_p \} \in \Gamma_F$, then the two p x m matrices obtained by restricting S^0 and S^1 to rows $i_1, i_2, \ldots\ldots i_p$ are identical up to a column permutation.

The first condition is called contrast and the second condition is called security. The contrast should be as large as possible and at least one sub pixel over the m sub pixels, that is $\alpha \geq 1/m$. The second condition is called security; it implies that by inspecting the shares of nonqualified subsets of participants one cannot identify whether the shared pixel is white or black. The collections C_0 and C_1 are obtained by permuting the columns of the basis matrices S^0 and S^1 in all possible ways. The important parameters of the scheme are:

- m, the number of subpixels in a share. This represents the loss in resolution from the original image to the shared one. The m should be as small as possible. The m is computed using the equation: $m = 2^{n-1}$ (1)
- α, the relative difference. It determines how well the original image is recognizable. This represents the loss in contrast. The α should be as large as possible. The relative difference α is calculated using the equation:

$$\alpha = | n_b - n_w | / m \qquad (2)$$

where n_b and n_w are the number of black subpixels which are generated from a black and white pixels in the original image, respectively.

- r, the size of the collections C_0 and C_1. The r is computed using the equation:

$$r = 2^{n-1}\,! \qquad (3)$$

- β, the contrast. The value β is to be as large as possible. The minimum contrast that is required to ensure that the black and white areas will be distinguishable is $\beta \geq 1$. The contrast β is computed using the equation: $\beta = \alpha * m$. (4)

4. EXISTING METHOD

4.1. 2-out-of-2 VCS with 4-Subpixel Layout with Additional Pixel Patterns

The basic idea of 2-out-of-2 visual cryptography with4-subpixel is to replace each pixel in the original image with the randomly selected column matrix from the collection matrix. Let us, consider a binary secret image S containing exactly m pixels. The dealer creates two shares (binary images), S_1 and S_2, consisting of exactly two pixels for each pixel in the secret image as shown in Table 1. If the pixel in S is black, the dealer randomly chooses one row from the six rows of Table 1. Similarly, if the pixel in S is white, the dealer randomly chooses one row from the six rows of Table1.

In this method, new pixel patterns are used to improve the contrast of reconstructed secret image. By using the new pixel patterns for the white pixels, the contrast of the reconstructed secret image is improved. The method is based on papers [8][9].

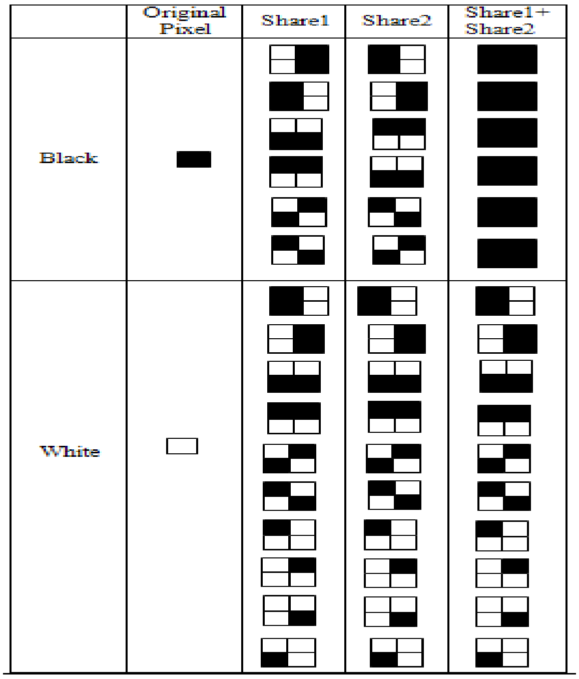
The new pixel patterns for the method are shown on Table 1. In the case of white pixel patterns, more pixel patterns are included in the Table 1 (new pixel patterns in the last four rows of the white pixels). By increasing the pixel patterns for white pixels, the contrast of the reconstructed image can be improved without adding any computational complexity. In this method, we use one additional basis matrix to represent new pixel patterns. We call the additional basis matrix AS^0. The basis matrix AS^0 is used to share white pixels in the secret data. AS^0 can be defined by n x m Boolean matrix, where n is the number of shares and m is the pixel expansion ($m = 2^{n-1}$). The matrix $AS^0 = [as_{ij}]$, where, as_{ij} = 0 the jth subpixel in the i^{th} share is black.

$as_{ij} = 1$ the jth subpixel in the i^{th} share is white.

The additional matrix AS^0 can be designed according to the following condition.

$as_{ij}^0 = 1$, $1 \le i \le n$ and $j \le 1$,
$as_{ij}^0 = 0$, $1 \le i \le n$ and $2 \le j \le 2^{n-1}$

Table1. *The Pixel Patterns for 2-Out-of-2 VCS with 4-Subpixel Layout*



	Original Pixel	Share1	Share2	Share1+ Share2
Black				
White				

For the 2-out-of-2 VCS with four sub pixels, the basis matrices for above pixel pattern S^0, AS^0 and S^1, are represented as follows:

$$S^0 = \begin{bmatrix} 1010 \\ 1010 \end{bmatrix} \quad AS^0 = \begin{bmatrix} 1000 \\ 1000 \end{bmatrix} \quad S^1 = \begin{bmatrix} 1001 \\ 0110 \end{bmatrix}$$

There are two collections of matrices, C_0 for encoding white pixels and C_1 for encoding black pixels. The collection of matrices C_0 is obtained by permuting the columns of S^0 plus permuting the columns of AS^0 and the collection of matrices C_1 is obtained by permuting the columns of S^1. The matrices C_0 and C_1 can be designed as:

C_0 = {Matrices obtained by permuting columns of $\begin{bmatrix} 1010 \\ 1010 \end{bmatrix}$

+ Matrices obtained by permuting the columns of $\begin{bmatrix} 1000 \\ 1000 \end{bmatrix}$ }

C_1 = {Matrices obtained by permuting the columns of $\begin{bmatrix} 1001 \\ 0110 \end{bmatrix}$ }

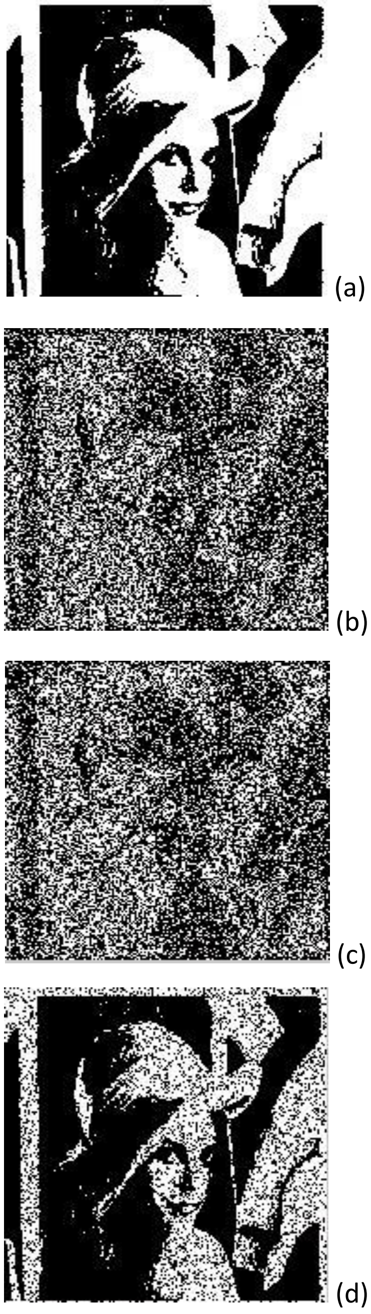


Fig1. *A 2-out-of-2 VCS using additional pixel patterns (a) the original image, (b) the first share S_1, (c) the second share S_2, and (d) superimposed S_1 and S_2.*

The α and β of the reconstructed secret data in this method are computed as α and β of the basis matrices S^0 and S^1 plus α and β of AS^0 using the equations (2) and (4).

Then, $\alpha = 3/4$ and $\beta = 3$.

We have noted that the additional matrix (AS^0) does not satisfy the security conditions of the traditional VCS. But this does not affect the final security of the proposed VCS; because it employs random basis column pixel expansion for sharing black and white pixels.

The details of pixels in the secret image, and the reconstructed image for figure 1 are shown in

Table 2. *The Details of the Pixels of the Secret Image and Reconstructed Image of Figure1*

Image	No. of Black Pixels	No. of White Pixels	No. of False Black Pixels	No. of False White Pixels
Secret Image	17270	14234	0	0
Reconstructed Secret Image	20859	10645	0	3589

The PSNR value of the original image and the reconstructed secret image is shown in table 3.

Table3. *PSNR Value of the Secret Image and Reconstructed Image of Figure 1*

Image	PSNR Value
Secret Image Reconstructed Secret Image	9.4339

5. Proposed Method

In the proposed method an averaging filter is applied to the two share images generated by the additional pixel patterns method to reduce the noise in the reconstructed secret images and also to improve the contrast of the reconstructed secret images.

The details of pixels in the secret image, and the reconstructed image for figure 2 are shown in Table 4. The PSNR value of the original image and the reconstructed secret image is shown in table 5.

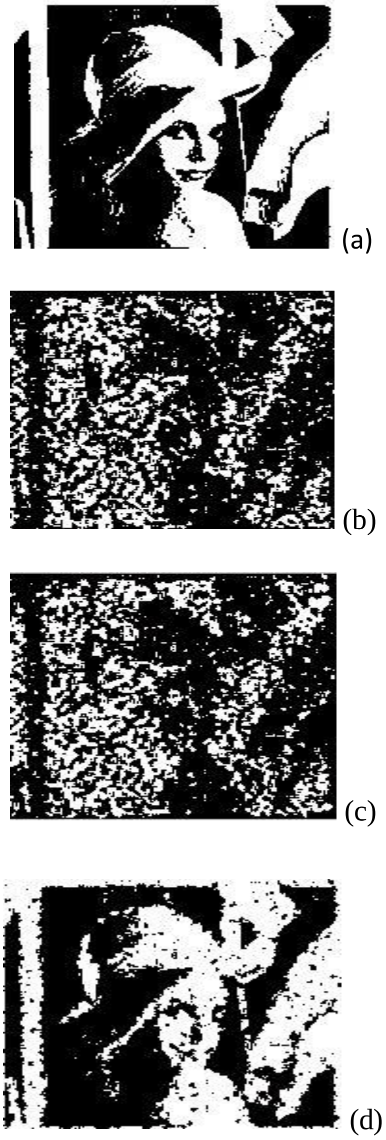


Fig2. *A 2-out-of-2 VCS using average filter (a) The original image (b) applying filter to the share1 image of figure1, (c) applying filter to the share2 image of figure1, (d) superimposition of filter applied share images.*

Table4. *The Details of the Pixels of the Secret Image and Reconstructed Image of Figure2*

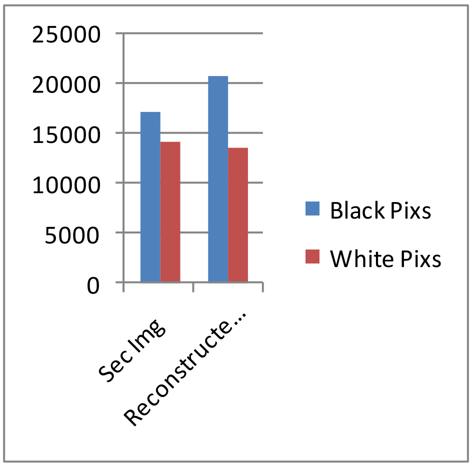
Image	No. of Black Pixels	No. of White Pixels	No. of False Black Pixels	No. of False White Pixels
Secret Image	17270	14234	0	0
Reconstructed Secret Image	16990	14514	1582	1302

Table5. *PSNR Value of the Secret Image and Reconstructed Image of Figure 2*

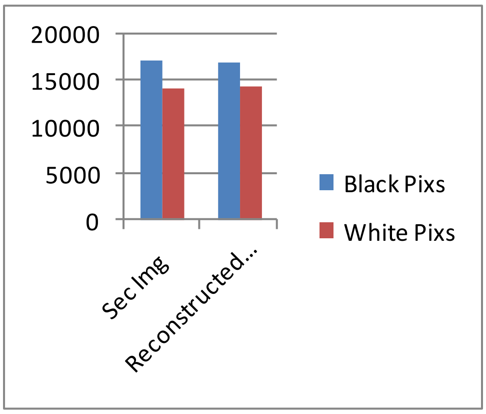
Image	PSNR Value
Secret Image Reconstructed Secret Image	10.2400

6. Analysis of Experimental Results

When we analyze Table 1 and Table 3, we see that the reconstructed image has more white pixels in Table 3 than in Table 1. The number of white pixels in the reconstructed image has been increased.



Graph1. *Graphical Representation of Pixels of the Secret Image and Reconstructed Image of Figure 1*



Graph2. *Graphical Representation of Pixels of the Secret Image and Reconstructed Image of Figure 2*

Also, by analyzing the table2 and table4, we see that the PSNR value of the proposed method is larger than the existing method. Also, comparing the reconstructed images in Figure 1d and Figure 2g, we can see that proposed method achieves better contrast and also reduces the noise in the reconstructed secret image.

The graphical representation of the existing method and the proposed method are shown in graph1 and graph2 respectively. By comparing both the graphs we can see that number of white pixels in graph2 is larger than in graph1. This means that by applying average filter to the share images we can improve the contrast of the reconstructed secret image.

7. Conclusion and Future Work

This paper describes a 2-out-of-2 VCS with 4-subpixel layout with additional pixel patterns scheme has no pixel expansion and has better contrast. By applying filter to the share images we can reduce the noise and to improve the contrast in the reconstructed images. Future work will is to further reducing the noise, increasing security and edge construction in reconstructed secret images.

References

[1] Josef Pieprzyk, Thomas Hardjono and Jennifer Sberry, Fundamentals of Computer Security. Springer, 2003.

[2] M. Naor and A. Shamir, “Visual Cryptography”, Advances in Cryptology-Eurocrypt’94, LNCS 950: 1-12, 1995.

[3] Thomas Monoth and Babu Anto P, “Optimal contrast in ‘3 out of 3’ Visual Secret Sharing Scheme Using Additional Matrices”, Pro.International Conferences on Emerging.

[4] Tzung-Her Chen, Kai-Hsiang Tsao, “Visual secret sharing by random grids revisited”, Pattern Recognition: 42 (2009) 2203-2217.

[5] Jen-Bang Feng, Hsien-Chu Wu, Chwei-Shyong Tsai, Ya-Fen Chang, Yen-Ping Chu, “Visual secret sharing for multiple secrets”, Pattern Recognition 41(2008) 3572 – 3581.

[6] G.R. Bakley, “Safeguarding Cryptographic Keys”, Proc. AFIPS National Computer Conference, 48: 313-317, 1979.

[7] Thomas Monoth & Babu Anto P. “Recursive Visual Cryptography Using Random Basis Column Pixel Expansion”, Proc. IEEE International Conference on Information Technology(ICIT), 2007, pp. 41-43.

[8] Thomas Monoth and Babu Anto P, "Improved contrast in '3 out of 3' Visual Secret Sharing Scheme using Additional Matrix", Pro.International Conferences on Managing Next Generation Software Applications (MNGSA 2008), Coimbatore, Tamil Nadu, India. pp.1109 – 1115, 2008.

[9] Thomas Monoth, Babu Anto P, "Contrast-Enhanced Visual Cryptography Schemes Based on "Additional Pixel Patterns". International Conference on Cyber worlds 978-0-7695-4215-7/10, IEEE, 2010.Trends in Computing (ICETiC 2009), Madurai, Tamil Nadu, India. pp.47-50, 2009.

AUTHOR'S BIOGRAPHY

Shyla M G, is currently Pursuing 4th Semester, Master of Technology in Computer Science and Engineering at AIT, Chickmagalur. She has completed her Bachelor of Engineering from Adichunchanagiri Institute of Technology, Chikmagalur. She had published a paper. Her areas of interests include image processing and Information Security.

Gowramma B H, is currently Pursuing 4th Semester, Master of Technology in Computer Science and Engineering at AIT, Chickmagalur. She has completed her Bachelor of Engineering from PES Institute of Technology, Shivamogga. She had published a paper. Her areas of interests include image processing and Information Security.

Vivekananda, presently working as assistant professor in the Department of Computer Science and Engineering, Adichunchanagiri Institute of Technology, Chikmagalur, Karnataka, India. He obtained his Master of Technology degree from SJCE Mysoor under Visveswaraya Technological University, Belgaum. He had 9 years of teaching experience. His research interests include Image Stegonography, Visual Cryptography, and Language Processing.