Chapter III

Optimal Secret Sharing Schemes for Visual Cryptography

3.1 Preamble

The basic parameters are normally known as the pixel expansion and the relative contrast. These parameters have a great significance in VCS as they are considered as the most critical dimensions used in evaluating the optimality and the effectiveness of the VCS. The optimality is always convinced when the scheme has an ability to minimize the pixel expansion and maximize the contrast simultaneously which is the main problem of binary VC.

This chapter presents two optimal VSS schemes with different access structures for binary valued images. These schemes are designed on the basis of the matrices of the VC to handle the pixel expansion and to get high visual quality of the recovered images. They are proposed to refute the pixel expansion and, at the same time, maximize the contrast, using the codebook and the XOR-ed operation.

Furthermore, the chapter presents the results obtained after implementing the proposed schemes and comparing them with some related schemes previously done in the field of the image sharing in order to prove that these two current proposed schemes are more optimal.

3.2 An Optimal \((n,n)\) Visual Secret Sharing Scheme

This scheme is proposed to be a non-expansible scheme used to eliminate the process of pixel expansion in generating the shared images and creating supreme contrast of the recovered image.
The overall structure of the proposed scheme encodes the secret image into two shares with the same size of the original image as a result of processing two adjacent pixels as one-time input with a view to generate two pixels in each of the two shares based on the designed codebook (as shown in table (3.1)).

3.2.1 The Mathematical Model

Let $P = \{p_1, p_2, \ldots, p_n\}$ be $N$ participants and let $S$ the subset of $P$, which can be determined as $2^P$. Let the qualified set $\Gamma_{\text{Qual}} \subseteq S$ and the forbidden set $\Gamma_{\text{Forb}} \subseteq S$ in such that $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \phi$.

In the proposed scheme, the number of generated shares is two and the number of the participants is also two. So,

$$P = \{p_1, p_2\}, \ 2^P = 4,$$
$$S = \{p_1, p_2, (p_1, p_2)\},$$
$$\Gamma_{\text{Qual}} = \{(p_1, p_2)\}, \ \Gamma_{\text{Forb}} = \{p_1, p_2\}, \ \text{and}$$
$$\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \phi.$$

To recover the secret image $\text{sec}_\text{img}$, it should be recovered through using the following expression:

$$\text{sec}_\text{img} = \sum_{i=1}^{n} p_i \quad (3.1)$$

Where $n$, denotes the required number (which are two in this scheme) of participants/shares to recover the secret image.

3.2.2 The Basis Matrices and Codebook Design

Figure (3.1) shows the basis matrices used to design the codebook in this proposed scheme.
Where $S0$, $S1$ are the basis matrices and $C0$, $C1$ refer to all the basis matrices obtained by permuting the columns of $S0$ and $S1$, respectively.

$C0= \{\text{all the matrices gained by random column-permutation from } S0\}$,

$C1= \{\text{all the matrices gained by random column-permutation from } S1\}$.

From $C0$ and $C1$ matrices, two vectors $V0$ and $V1$ are produced respectively as shown in figure (3.1) which determine the features of staked image.

As it is observed in figure (3.1), the two vectors are produced by using OR-ed operation and based on the colors of each pair of the adjacent pixels in the secret image.

Here, the design of the codebook is based on the above matrices in which the two neighboring pixels are taken in turn. Depending on the colors of each two adjacent pixels, the codebook (as shown in table (3.1)) shows the required color of the pixels for generating two shares.
Table (3.1): Codebook of the proposed A (2, 2) VSS scheme.

<table>
<thead>
<tr>
<th>Adjacent pixels</th>
<th>Share1 (S1)</th>
<th>Share2 (S2)</th>
<th>ORed pixels</th>
<th>XORed pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><img src="image1" alt="Share1" /></td>
<td><img src="image2" alt="Share2" /></td>
<td><img src="image3" alt="ORed pixels" /></td>
<td><img src="image4" alt="XORed pixels" /></td>
</tr>
<tr>
<td><img src="image5" alt="Adjacent pixels" /></td>
<td><img src="image6" alt="Share1" /></td>
<td><img src="image7" alt="Share2" /></td>
<td><img src="image8" alt="ORed pixels" /></td>
<td><img src="image9" alt="XORed pixels" /></td>
</tr>
<tr>
<td><img src="image10" alt="Adjacent pixels" /></td>
<td><img src="image11" alt="Share1" /></td>
<td><img src="image12" alt="Share2" /></td>
<td><img src="image13" alt="ORed pixels" /></td>
<td><img src="image14" alt="XORed pixels" /></td>
</tr>
<tr>
<td><img src="image15" alt="Adjacent pixels" /></td>
<td><img src="image16" alt="Share1" /></td>
<td><img src="image17" alt="Share2" /></td>
<td><img src="image18" alt="ORed pixels" /></td>
<td><img src="image19" alt="XORed pixels" /></td>
</tr>
</tbody>
</table>
3.2.3 The Proposed Algorithm

The necessary steps and graphical representation (as shown in figure (3.2)) to implement the proposed scheme are planned as follows:

| The Algorithm
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
</tr>
<tr>
<td><strong>Output</strong></td>
</tr>
</tbody>
</table>

### Encoding Stage Begin

**Step1.** As one-time input, take two adjacent pixels \(P1\) and \(P2\) from the secret image \(SI\).

**Step2.** Determine the color of \(P1 \& P2\), which will be one of the following possibilities:

- \(A)\) Black & Black
- \(B)\) White & White
- \(C)\) Black & White
- \(D)\) White & Black

**Step3.** Randomly allocate two pixels to each shares \(S1\) & \(S2\) in order to generate two shares with same size of the \(SI\) using the codebook (shown as table (1))

**Step4.** Repeat steps 1 to 3 for all pixels of \(SI\).

### End

### Decoding Stage Begin

**Step1.** Collect two shares images \(S1\) & \(S2\).

**Step2.** Superimpose \(S1\) & \(S2\) by performing bitwise OR operation or bitwise XOR operation.

### End
3.2.4 Experimental Results and Performance Analysis

The simulation results of the proposed (2,2)-VCS, performance evaluation through some general principles such as pixel expansion, contrast, security analysis and computational cost were discussed in details. Further, the comparison of the proposed scheme with the basic VCS, i.e., Naor and Shamir’s scheme are presented in this section in order to show the optimality and efficiency of the proposed scheme.

3.2.4.1 Experimental Results

In proving the optimality of the ‘An optimal (2, 2) VSS Scheme’, some experiments were conducted on different binary images along with applying different bitwise operations of decoding stage.

The first experiment was conducted to implement Naor and Shamir’s scheme in order to find out the drawbacks of this scheme. The results of this experiment show that...
the drawbacks of this scheme are the pixel expansion and the poor contrast of the reconstructed image.

For the purpose of comparing the proposed scheme with Naor and Shamir’s, the Solar System Symbol Earth image of the size of $225 \times 225$ as the secret image of the second experiment is taken for applying the two compared schemes as shown in figure (3.3(a)) and figure (3.4(a)).

As one-time input, Naor and Shamir’s scheme takes one pixel from the secret image, then, encodes it into two sub pixels in each share (share1 & share2) that leads to generating two expansible shares as it is observed in figure (3.3(b & c)).

In the proposed scheme, on the other hand, two adjacent pixels are taken as one-time input, then, encoded into only two sub pixels in each of the generated share (share1 & share2) having the same size of the original image as it is noticed in figure (3.4(b & c)).

![Figure 3.3](image)

Figure (3.3): Simulation results of Naor and Shamir’s scheme: a) Secret binary image, b) First share, c) Second share, d) Recovered image.

As shown in figure (3.4 (b, c & d)), the proposed scheme is non-expansible since it has abolished the need of pixel expansion. Thereby the shared images and the reconstructed image still have the same size of the original image and the aspect ratio is unchanged.
Development of Secret Sharing Schemes for Visual Cryptography

**Figure (3.4):** Simulation results of the proposed scheme: (a) secret binary image, (b) First share, (c) Second share, (d) Recovered image by performing bitwise OR operation.

To clarify the difference between using the bitwise OR operation and bitwise XOR operation, the third experiment was simulated to text image of the size of $256 \times 256$ through performing bitwise XOR operation for the decoding process. Figure (3.5(e)) shows the XOR-ed image with higher contrast than that of OR-ed image shown in figure (3.5(d)).
Figure (3.5): Simulation results of the proposed scheme by performing bitwise OR and XOR operations: (a) Secret binary image, (b) First share, (c) Second share, (d) OR-ed recovered image, (e) XOR-ed recovered image.
3.2.4.2 Performance Evaluation through Statistical Analysis and Comparison

In this part, various analyses such as qualitative, statistical, security analysis, and time complexity are discussed in details in order to show the optimality of the proposed VSS scheme over the Naor and Shamir’s scheme and to prove the superiority of XOR operation on OR operation.

3.2.4.2.1 Qualitative Analysis

The important parameters of VC such as pixel expansion, aspect ratio, codebook requirement, and decoding process are discussed in details as follows:

1. *Pixel Expansion and Aspect Ratio (AR)*

Generally, the pixel expansion and the AR have a great significance in the VC in which they are directly related. The AR describes the proportional relationship between the width and the height of an image that can be represented as:

\[
AR = \frac{m}{n} \quad (3.2)
\]

Where \( m \) and \( n \) denote the height and the width of an image, respectively. As it is clearly shown in figure (3.3(d)) of Naor and Shamir’s scheme, the recovered image size is two times as big as the original image. This doubling in size resulted from the pixel expansion (equals 2) that causes a change in the aspect ratio of the recovered image and changes the original image into an ellipse shape. In addition, the recovered image has poor contrast and destroyed resolution.

Table (3.2) shows the comparison between the Naor and Shamir’s scheme and the proposed scheme based on such metrics as AR, pixel expansion, the number of input pixels in turn, and the number of output pixels in turn.
Table (3.2): Comparison results of Naor and Shamir’s scheme and the proposed scheme.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Naor and Shamir’s scheme</th>
<th>The Proposed scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aspect ratio of original image</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Aspect ratio of recovered image</td>
<td>0.5</td>
<td>1</td>
</tr>
<tr>
<td>Pixel expansion</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>No. of input pixels in turn</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>No. of output pixels in turn</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Graphically, the comparison of the results between the proposed scheme and Naor and Shamir’s scheme appears clearly in figure (3.6).

![Graphical representation of the comparison results.](image)

**Figure (3.6):** Graphical representation of the comparison results.

2. **Codebook Requirement**

Indeed, this algorithm is adopted on the codebook which leads to large shared images. Yet, despite the use of the codebook, the generated shares have the same size of
the original secret image. This is due to the processing of the two neighboring pixels in turn as one-time input.

3. Decoding Process

The proposed scheme can be implemented in one of the two processes, i.e., bitwise OR operation or XOR operation, to retrieve the original secret image. As it has been observed in the third experiment, the using of bitwise OR operation for decoding process darkens the recovered images as shown in figure (5(d)). On the other hand, the use of bitwise XOR operation provides a perfect contrast as figure (5(e)) shows.

3.2.4.2.2 Contrast and Statistical Analysis

To highlight the effectiveness of the proposed scheme when using XOR operation for stacking purpose that provide perfect and enhanced contrast, different metrics such as $MSE$, $PSNR$ and $UQI$ have been measured as shown in Table (3.3).

Table (3.3): Comparison of the visual quality by performing OR and XOR operation in the proposed scheme.

<table>
<thead>
<tr>
<th>Metrics</th>
<th>The Proposed scheme using OR operation</th>
<th>The Proposed scheme using XOR operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSE</td>
<td>0.46555</td>
<td>0.0082703</td>
</tr>
<tr>
<td>PSNR</td>
<td>3.3204</td>
<td>20.8248</td>
</tr>
<tr>
<td>UQI</td>
<td>0.0541</td>
<td>0.9673</td>
</tr>
</tbody>
</table>
1. **Mean Square Error (MSE)**

The error amount by which the values of the secret image differ from the degraded image might be measured by the MSE metric which can mathematically be defined as:

\[
MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} (h_{ij} - h'_{ij})^2
\]

(3.3)

Where \(h_{ij}\) and \(h'_{ij}\) denote the pixel value of the original image and the reconstructed image, respectively. Here, it is worth observing that while computing the amount of error, it is found that the lower the MSE is, the more perfect the quality and contrast of the recovered image is.

2. **Peak Signal to Noise Ratio (PSNR)**

For testing the accuracy of the OR-ed and the XOR-ed images, PSNR metric is used to measure the ratio between the maximum power of the signal and the corrupting noise that affects the accuracy of the recovered image’s presentation. This metric is usually measured in the terms of the logarithmic decibels and can be represented mathematically as:

\[
PSNR = 10 \times \log \frac{R^2}{MSE}
\]

(3.4)

For a perfect quality and accuracy of the recovered image, the PSNR value should be as high as possible, and accordingly, unlike the ORed image, the XORed image has better contrast and accuracy as noticed in table (3.3).

Nowadays, due to their performance, MSE and PSNR are still universal metrics that offer valued comparison for image distortion.

3. **Universal Quality Index (UQI)**

Indeed, the VC is based on HVS features, so it is necessary to use perceptually quality metrics. One of these metrics is UQI which provides meaningful comparison in case of visual information like an image. UQI can be mathematically expressed as:
\[
UIQ = \frac{4\sigma_{xy} \overline{xy}}{(\sigma_x^2 + \sigma_y^2)(\overline{x})^2 + (\overline{y})^2}
\] (3.5)

Where,

\[
\overline{x} = \frac{1}{N} \sum_{i=1}^{N} x_i, \quad \overline{y} = \frac{1}{N} \sum_{i=1}^{N} y_i, \quad \sigma_x^2 = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \overline{x})^2,
\]

\[
\sigma_y^2 = \frac{1}{N-1} \sum_{i=1}^{N} (y_i - \overline{y})^2, \quad \sigma_{xy} = \frac{1}{N-1} \sum_{i=1}^{N} (x_i - \overline{x})(y_i - \overline{y}).
\]

\(UQI\) dynamic range is \([-1, 1]\), the perfect result is 1 and the bad result is -1, and the accepted value is the value close to 1. On the contrary, when the \(UQI\) value is close to -1, it is considered as a rejected value.

Finally, it can be said that the proposed scheme is an optimal, especially in case of using the XOR operation, for the reconstructed image is perfect and non-expansible as shown in tables (3.2) & (3.3). Graphically, the optimality of the proposed method can be seen through having a look at figure (3.7).

**Figure (3.7):** Graphical representation of the comparison results for the proposed scheme by performing OR and XOR operation.
3.2.4.2.3 Security Analysis

The proposed scheme satisfies the security condition due to the generated shared images carrying no information about the original secret image as shown in figure (3.4(b & c) and (3.5 (b & c)). In addition, single share has no ability to recover the secret image.

3.2.4.2.4 Computational Cost

The consumed execution time to generate the two shares in the proposed scheme is less than the consumed execution time in *Naor and Shamir’s* scheme as shown in table (3.4). Accordingly, the proposed scheme is an effective scheme due largely to its ability to handle the pixel expansion and contrast simultaneously.

**Table (3.4):** The consumed execution time to generate two shares in the proposed scheme and Naor and Shamir’s scheme.

<table>
<thead>
<tr>
<th>The proposed scheme</th>
<th>Naor and Shamir’s scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.7581 second</td>
<td>3.1329 second</td>
</tr>
</tbody>
</table>

The compared schemes have a runtime of at least $O(n^2)$ for the same length of $n$. Expectedly, the proposed method implementation is significantly faster than the implementation of the *Naor and Shamir’s* scheme. The evidence can graphically be shown in the figure (3.8).
3.3 An Optimal (k,n) Visual Secret Sharing Scheme

The new (k,n)-VC scheme is proposed to refute the pixel expansion based on codebook and the transpose of matrices. In addition, this scheme will offer promising solutions for the security condition, computation complexity, storage requirement, fast network transmission, and reconstructing the secret image accurately with visual pleasing quality.

3.3.1 The Mathematical Model

Let $P = \{p_1, p_2, \ldots, p_n\}$ be $N$ participants and let $S$ the subset of $P$ which can be determined as $2^P$. Let the qualified set $\Gamma_{\text{Qual}} \subseteq S$ and the forbidden set $\Gamma_{\text{Forb}} \subseteq S$ in such that $\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset$.

In the proposed scheme, the number of generated shares is four and the number of the participants is also four. So,
\[ P = \{p_1, p_2, p_3, p_4\}, \quad 2^p = 16, \]
\[ S = \{p_1, p_2, p_3, p_4, (p_1, p_2), (p_1, p_3), (p_1, p_4), (p_2, p_3), (p_2, p_4), (p_3, p_4), (p_1, p_2, p_3), (p_1, p_2, p_4), (p_1, p_3, p_4), (p_2, p_3, p_4), (p_1, p_2, p_3, p_4)\}. \]

To recover the secret image, there are three possible constructions under this scheme which can be represented below with the qualified set \( \Gamma_{\text{Qual}} \subseteq S \) and the forbidden set \( \Gamma_{\text{Forb}} \subseteq S \) of each construction. As the proposed scheme is \((k,n)\) VC and the \( n \) equals four, the \( k \) should satisfy the \( 1 < K \leq 4 \) condition. Denote that, for each of the following constructions the order of shares is not important.

**A. A (2, 4) Construction**

Under this construction, any two participants can superimpose their shares together to recover the original secret image. The qualified set \( \Gamma_{\text{Qual}} \) and the forbidden set \( \Gamma_{\text{Forb}} \) are shown as follows:

\[ \Gamma_{\text{Qual}} = \{(p_1, p_2), (p_1, p_3), (p_1, p_4), (p_2, p_3), (p_2, p_4), (p_3, p_4)\}, \]
\[ \Gamma_{\text{Forb}} = \{p_1, p_2, p_3, p_4, (p_1, p_2), (p_1, p_3), (p_1, p_4), (p_2, p_3), (p_2, p_4), (p_3, p_4), (p_1, p_2, p_3, p_4)\}, \]
\[ \Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset. \]

**B. A (3, 4) Construction**

Under this construction, any three participants can superimpose their shares together to recover the original secret image. The qualified set \( \Gamma_{\text{Qual}} \) and the forbidden set \( \Gamma_{\text{Forb}} \) are shown as follows:

\[ \Gamma_{\text{Qual}} = \{(p_1, p_2, p_3), (p_1, p_2, p_4), (p_1, p_3, p_4), (p_2, p_3, p_4)\}, \]
\[ \Gamma_{\text{Forb}} = \{p_1, p_2, p_3, p_4, (p_1, p_2), (p_1, p_3), (p_1, p_4), (p_2, p_3), (p_2, p_4), (p_3, p_4), (p_1, p_2, p_3, p_4)\}, \]
\[ \Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset. \]

**C. A (4, 4) Construction**

This construction can be considered as \((n, n)\) VC. Here, all the participants should superimpose their shares together to recover the original secret image. The qualified set \( \Gamma_{\text{Qual}} \) and the forbidden set \( \Gamma_{\text{Forb}} \) are shown as follows:
\[ \Gamma_{\text{Quad}} = \{(p_1, p_2, p_3, p_4)\}, \]
\[ \Gamma_{\text{Forb}} = \{p_1, p_2, p_3, p_4, (p_1, p_2), (p_1, p_3), (p_1, p_4), (p_2, p_3), (p_2, p_4), (p_3, p_4), (p_1, p_2, p_3), (p_1, p_2, p_4), (p_1, p_3, p_4), (p_2, p_3, p_4)\}, \]
and
\[ \Gamma_{\text{Quad}} \cap \Gamma_{\text{Forb}} = \emptyset. \]

3.3.2 The Basis Matrices and Codebook Design

Here, the proposed scheme uses the codebook which is designed on a set of matrices of the traditional VC presented as follows:

\[ C_0 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 1 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix} \}. \]

\[ C_1 = \{ \text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \}. \]

Here, matrix \( C_0 \) denotes the matrix for constructing shares for the white pixels and \( C_1 \) for the black ones. Depending on \( C_0 \) and \( C_1 \) matrices, the codebook is designed for the proposed scheme. The basic matrices used in the proposed scheme are as follows:

\[ C_0 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad C_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \]

In this scheme, the transpose of above matrices is used, then by permutation of all columns the codebook can be designed.

\[ C_0^T = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \quad C_1^T = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}. \]

Table (3.5) shows the designed codebook of the proposed scheme in order to encode a binary image and, then, the constructed shared images can be transmitted to different participants.
Table (3.5): The codebook of the proposed (k,n) -VC scheme.

<table>
<thead>
<tr>
<th>Pixel</th>
<th>S1</th>
<th>S2</th>
<th>S3</th>
<th>S4</th>
</tr>
</thead>
<tbody>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>[ ]</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.3.3 The Proposed Algorithm

The necessary steps of the encoding and decoding stages to implement the proposed scheme are planned as follows:

<table>
<thead>
<tr>
<th>The Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input</strong></td>
</tr>
<tr>
<td><strong>Output</strong></td>
</tr>
<tr>
<td><strong>Encoding Stage</strong></td>
</tr>
<tr>
<td><strong>Step 1.</strong> In turn, take one pixel ((P)) from the secret image.</td>
</tr>
<tr>
<td><strong>Step 2.</strong> Determine the color of ((P)) whether:</td>
</tr>
<tr>
<td>a. Black</td>
</tr>
</tbody>
</table>
Step 3. In case if \((P)\) is:

1. Black:
   a. From the four blocks that are peer to the black pixel in the codebook, one block has to be randomly selected (as shown in the table (3.5)).
   b. One row has to be randomly chosen from the selected block and allocate it to vector \(V\).

2. White:
   a. From the four blocks that are peer to the white pixel in the codebook, one block has to be randomly chosen (shown as the table (3.5)).
   b. One row has to be randomly chosen from selected block and allocate it to vector \(V\).

Step 4. \(V= [v_1, v_2, v_3, v_4]\), generates four shares as:

\[
\begin{align*}
\text{share}_1 &= v_1, \\
\text{share}_2 &= v_2, \\
\text{share}_3 &= v_3, \\
\text{share}_4 &= v_4.
\end{align*}
\]

Step 5. Repeat the above steps (1 to 5) until all pixels of the secret image are being shared.

End

<table>
<thead>
<tr>
<th>Decoding Stage</th>
<th>Begin</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1. To retrieve the secret image, superimpose any order of shares using XOR operation for all possible constructions as follows:</td>
<td></td>
</tr>
</tbody>
</table>

\[
\begin{align*}
(2,4): & \text{ share}_1 \oplus \text{share}_2 \text{ or } \text{share}_1 \oplus \text{share}_3 \text{ or } \text{share}_1 \oplus \text{share}_4 \text{ or } \text{share}_2 \oplus \text{share}_3 \text{ or } \text{share}_2 \oplus \text{share}_4 \text{ or } \text{share}_3 \oplus \text{share}_4. \\
(3,4): & \text{ share}_1 \oplus \text{share}_2 \oplus \text{share}_3 \text{ or } \text{share}_1 \oplus \text{share}_2 \oplus \text{share}_4 \text{ or } \text{share}_1 \oplus \text{share}_3 \oplus \text{share}_4 \text{ or } \text{share}_2 \oplus \text{share}_3 \oplus \text{share}_4. \\
(4,4): & \text{share}_1 \oplus \text{share}_2 \oplus \text{share}_3 \oplus \text{share}_4. 
\end{align*}
\]

Where \(\oplus\) indicates the XOR operation.

End
3.3.4 Experimental Results and Performance Analysis

The experimental results and performance evaluation are presented in details in this section in order to show the optimality of the proposed scheme.

3.3.4.1 Experimental Results

The binary text image with size of 256×256 is taken as a secret image as shown in figure (3.9 (a)) to conduct the experiment of the proposed scheme. The codebook is designed based on the transport of basic matrices that are used in the current scheme. In encoding stage, firstly, one pixel is taken as input by raster-scan order. Then each pixel of secret image is successively taken into the codebook of this scheme in order to generate four shares with the same size of the original secret image as shown in figure (3.9 (b), (c), (d), and (e)).

In decoding stage, as mentioned in the structure of the proposed scheme, three possible constructions are possible to recover the secret image. Figure (3.9. (f) and (g)) shows the recovered image through XORing two shares and three shares, separately and respectively. As it can be notice, figure (3.9 (h)) shows the recovered image by superimposing the four shared images by performing XORing operation without distortion.
Development of Secret Sharing Schemes for Visual Cryptography

3.3.4.2 Performance Evaluation through Statistical Analysis and Comparison

In this section, different analyses are conducted to prove the optimality and effectiveness of the proposed scheme. Then, quality of the recovered images of the possible constructions is discussed. Finally, comparison with different related schemes is also presented.

3.3.4.2.1 Qualitative Analysis

The important concepts of VC are adopted in this section to evaluate the validity of the proposed scheme as follows.

1. *Pixel Expansion and Aspect Ratio*

   Obviously, the proposed scheme is a non-expansible scheme since it has refuted the requirement of pixel expansion. Thereby, the shared images and the reconstructed image

![Figure (3.9) Simulation results of the proposed scheme, (a) the secret image, (b),(c),(d), and (e) the shared images, (f) the reconstructed image (share1&2), (g) the reconstructed image (share1,2&3), (h) the reconstructed image (share1,2,3&4).]
still have the same size of the original image and the AR is unchanged as shown in figure (3.9 (b), (c), (d), (e), (f), (g), and (h)).

2. Codebook Requirement

As the fact that the codebook leads to large generated shared images, yet, due to that the codebook of the proposed scheme is designed with help of the transpose of matrices. Therefore, the generated shared images and reconstructed images have the same size of the original secret image.

3. Decoding Process

The proposed scheme is designed to use the bitwise XOR operation for decoding process, i.e., for reconstructing the original secret image. However, the XORing operation permits the complete restoration of secret image [34]. The XOR-based VC was suggested to increase the quality of the reconstructed image and solve the problem of pixel expansion [37].

3.3.4.2.2 Contrast and Statistical Analysis

In the proposed scheme, the secret image is recovered through three constructions, i.e., (2,4), (3,4), and (4,4). The reconstructed image by superimposing two or three shared images together also has a quite good contrast as shown in figure (3.9 (f) and (g)). In addition, in case of reconstructing (4, 4) for the proposed scheme by using XOR operation, the quality of reconstructed image increases and there is no distortion as shown in figure (3.9 (h)). This can be evaluated by $PSNR$ and $UQI$, which are used to measure the visual quality of the recovered image with respect to the original image and to measure the linear correlation between two images, respectively. To calculate the $PSNR$, the $MSE$ should be calculated first.

Fundamentally, while the $MSE$ value should be as low as possible, the PSNR should be higher. A higher $PSNR$ indicates lower variation between the secret image and the reconstructed image with a good visual quality. However, when the PSNR value is equal to $\infty$, it indicates that the scheme provides standard visual quality [61],[57]. The original secret image and the recovered secret image have strong positive linear correlation if $UQI$ is close to +1.
Table (3.6) shows the obtained values of $MSE$, $PSNR$, and $UQI$ between the original image and the recovered image of each possible construction of the proposed scheme.

**Table (3.6):** The MSE, PSNR, and UQI values of the possible constructions of the proposed scheme.

<table>
<thead>
<tr>
<th>The Construction</th>
<th>MSE</th>
<th>PSNR</th>
<th>UQI</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2,4)</td>
<td>0.0482</td>
<td>13.1687</td>
<td>0.16044</td>
</tr>
<tr>
<td>(3,4)</td>
<td>0.2512</td>
<td>6.023</td>
<td>0.10601</td>
</tr>
<tr>
<td>(4,4)</td>
<td>0</td>
<td>$\infty$</td>
<td>1</td>
</tr>
</tbody>
</table>

The values of MSE, PSNR, and UQI of (4, 4) construction of the proposed scheme with the ‘zero’ MSE value, ‘infinite’ PSNR value, and ‘1’ UQI value confirm that the original images have been recovered completely without any distortion.

### 3.3.4.2.3 Security Analysis

The proposed scheme satisfies the security condition due to the generated shared images carrying no information about the original secret image as shown in figure (3.9 (b, c, d, and f)). The $k$ also satisfies the $1 < K \leq 4$ condition.

Recently, many of VSS schemes have been proposed for securing the binary secret image. The current results in comparison with the some previously published schemes are shown in the table (3.7) which shows the optimality and effectiveness of the proposed scheme.

In general, the results shown in tables ((3.2), (3.3), (3.6), & (3.7)) prove that the proposed schemes in this chapter solve the problem of pixel expansion and poor contrast of VC schemes through refuting the pixel expansion and maximizing the contrast of the recovered images simultaneously.
Table (3.7): The results of the proposed scheme in comparison to some published schemes.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Secret image</th>
<th>Pixel expansion</th>
<th>Aspect ratio</th>
<th>Reconstructed image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ito et al.’s scheme [62]</td>
<td>Binary (m×n)</td>
<td>No</td>
<td>Unchanged</td>
<td>Lossy</td>
</tr>
<tr>
<td>Yang’s scheme [63]</td>
<td>Binary (m×n)</td>
<td>No</td>
<td>Unchanged</td>
<td>Lossy</td>
</tr>
<tr>
<td>Yang and Chen’s scheme [64]</td>
<td>Binary (m×n)</td>
<td>Yes</td>
<td>Changed</td>
<td>Lossy</td>
</tr>
<tr>
<td>Yang and Chen’s scheme [65]</td>
<td>Binary (m×n)</td>
<td>Yes</td>
<td>Changed</td>
<td>Lossy</td>
</tr>
<tr>
<td>Pal et al.’s scheme [66]</td>
<td>Binary (m×n)</td>
<td>Yes</td>
<td>Changed</td>
<td>Lossy</td>
</tr>
<tr>
<td>Yang et al.’s scheme [31]</td>
<td>Binary (m×n)</td>
<td>No</td>
<td>Unchanged</td>
<td>Lossy</td>
</tr>
<tr>
<td>Yang et al.’s scheme [32]</td>
<td>Binary (m×n)</td>
<td>No</td>
<td>Unchanged</td>
<td>Lossy</td>
</tr>
<tr>
<td>Lee and Chiu’s scheme [33]</td>
<td>Binary (m×n)</td>
<td>No</td>
<td>Unchanged</td>
<td>Lossy</td>
</tr>
<tr>
<td>Arya k. et al.’s scheme [42]</td>
<td>Binary (m×n)</td>
<td>Yes</td>
<td>Changed</td>
<td>Lossy</td>
</tr>
<tr>
<td>The proposed scheme</td>
<td>Binary (m×n)</td>
<td>No</td>
<td>Unchanged</td>
<td>(2,4) Quite good</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(3,4) Lossy</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(4,4) Lossless</td>
</tr>
</tbody>
</table>

3.4 Chapter Summary

In this chapter, VSS schemes have been designed and implemented for protecting the security of binary valued images. Two schemes for improving the VC are proposed to be optimal schemes in addressing the main problems of VC: pixel expansion and lossy recovery. The first scheme with (n, n) VC access structure is based on the codebook which designed by using the basis matrices of conventional VC. This scheme addresses the
problem of pixel expansion due to processing two pixels in turn and generating two shared images with the same size of the original secret image. Lossy recovery is improved due to performing the XOR operation for secret image recovery process.

The second scheme with \((k, n)\) VC access structure is based on codebook and transpose of matrix concepts. Pixel expansion problem eliminated in this scheme and the shared images have the same size of the original secret image. Three possible constructions under this scheme can be used in order to recover the secret image by applying the XOR operation while superimposing the qualified shares together. The standard contrast is obtained when all shares superimposed together to recover the original secret image.

The experimental results, performance analysis, and comparison results of the proposed schemes with some recent published schemes prove that the current schemes are more optimal. Their advantages can be listed as follows:

1- The proposed schemes are easy to be implemented very fast without consuming much time.
2- The shared images and the recovered images have the same size of the original secret image and this means that the pixel expansion equals one.
3- And accordingly, it saves the storage space of the participants, provides fast transmission via public network, Internet, and other communication channels.
4- The image obtained after stacking the shared images by performing bitwise XOR operation appears accurately with high visual quality.