4.1. Introduction

Security is one of the key parameter in visual cryptography schemes. Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than \( k \) shares collected. This chapter presents a novel method for security-enhanced visual cryptography scheme called recursive visual cryptography scheme. In this method, the secret image is encoded into shares and subshares in a recursive manner. By using recursion, the security and reliability of the visual cryptography scheme can be greatly improved.

Hybrid approach for encryption and decryption techniques is also presented in this chapter to improve the security of data based on matrix ciphers and visual cryptography schemes. This technique provides a very secure way to encrypt and decrypt secret data. In this method, the secret data is first encoded by using matrix cipher and then by visual cryptography. This will increase the level of security of the encrypted data.
4.2. Recursive Visual Cryptography Scheme\textsuperscript{1,2}

4.2.1 The Model

Let \( P = \{p_1, p_2, \ldots, p_n\} \) be \( n \) participants and let \( 2^P \) denote the subsets of \( P \). Let \( \Gamma_{\text{Qual}} \subseteq 2^P \) and \( \Gamma_{\text{Forb}} \subseteq 2^P \) such that \( \Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset \). In the first phase of the encryption process, \( \Gamma_{\text{Qual}} \) are referred to as \textit{qualified sets} and \( \Gamma_{\text{Forb}} \) as \textit{forbidden sets}.

In the second phase of encryption, let \( p_i = \{p_{i1}, p_{i2}, \ldots, p_{in}\} \), for \( i = 1 \) to \( n \). Then the \textit{qualified sets} \( \Gamma_{\text{Qual}_i} \subseteq 2^{p_i} \) and \textit{forbidden sets} \( \Gamma_{\text{Forb}_i} \subseteq 2^{p_i} \) such that \( \Gamma_{\text{Qual}_i} \cap \Gamma_{\text{Forb}_i} = \emptyset \). This process can be repeated up to the desired security and contrast. The value of \( n \) can be different at each phase or depends on the number of shares/participants required at each phase.

In the decryption process, SI can be reconstructed as follows:

In the first phase,

\[ \text{SI} = \sum_{i=1}^{k} p_i \]

where \( k \) is the number of participants/shares required to reconstruct the SI. The value of \( k \) is different for different VCS. In this, each of the participants (for example, \( p_i \)) is reconstructed as


\[ p_i = \sum_{j=1}^{k} p_{ij} \quad 1 \leq j \leq n \]

4.2.2 The Tree Structure for RVCS

The recursive visual cryptography model can be represented by a tree structure.

**Figure 4.1** Tree representation of recursive visual cryptography model
4.2.3 The Construction of Recursive Visual Cryptography Scheme

In order to demonstrate that the recursive visual cryptography scheme (RVCS) is feasible, some experiments were conducted using 2-out-of-2 VCS with two levels of encryptions. The secret image (SI) is encoded into two shares at first level by using 2-out-of-2 VCS. In the second level, each share is further encoded into two shares by using 2-out-of-2 VCS. This encryption process can be represented by a tree as shown below.

![Tree representation for 2-out-of-2 VCS with recursion using two levels of encryption](image)

**Figure 4.2** Tree representation for 2-out-of-2 VCS with recursion using two levels of encryption

From Figure 4.2, SI is encoded into two shares $S_1$ and $S_2$. Then from the first level of encryption the share $S_1$ is further encoded into two shares $S_{11}$ and $S_{12}$ and the share $S_2$ into $S_{21}$ and $S_{22}$. In the decryption process, the SI is reconstructed by stacking shares in different ways. That is:
Here, there are four different ways to reconstruct the SI by using visual cryptography scheme with recursion. But the existing visual cryptography scheme can recreate secret image in only one way. Therefore, RVCS provides greater security and reliability than existing VCS.

4.2.4 Experimental Results

The experiments were conducted using 2-out-of-2 VCS with two levels of encryptions. Figure 4.3 and 4.4 show RVCS applied to two different images:
Figure 4.3 The 2-out-of-2 VCS with recursion for the image SI1: (a) SI1, (b) S1, (c) S2, (d) S11, (e) S12, (f) S21, (g) S22, (h) S1 + S2 (i) S1+S21+S22 (j) S2+S11+S12 (k) S11+S12+S21+S22 (l) S1 ⊕ S21 ⊕ S22 (m) S11 ⊕ S12 ⊕ S21 ⊕ S22
Figure 4.4  The 2-out-of-2 VCS with recursion for the image SI2:
(a) SI2, (b) S1, (c) S2, (d) S11,(e) S12, (f) S21,(g) S22, (h) S1 + S2  (i) S1+S21+S22 (j) S2+S11+ S12 (k) S11+S12 + S21+S22 (l) S1⊕S21⊕S22 (m) S11⊕S12⊕S21⊕S22

Table 4.1 The details of the pixels in SI1 for the 2-out-of-2 RVCS

<table>
<thead>
<tr>
<th>Image</th>
<th>No. of Columns</th>
<th>No. of Rows</th>
<th>No. of Black Pixels</th>
<th>No. of White Pixels</th>
<th>Total Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI</td>
<td>250</td>
<td>100</td>
<td>7510</td>
<td>17490</td>
<td>25000</td>
</tr>
<tr>
<td>S1 + S2</td>
<td>250</td>
<td>100</td>
<td>16371</td>
<td>8629</td>
<td>25000</td>
</tr>
<tr>
<td>S1 + S21+S22</td>
<td>250</td>
<td>100</td>
<td>20657</td>
<td>4343</td>
<td>25000</td>
</tr>
<tr>
<td>S2 + S11+ S12</td>
<td>250</td>
<td>100</td>
<td>20660</td>
<td>4340</td>
<td>25000</td>
</tr>
<tr>
<td>S11 + S12 + S21 + S22</td>
<td>250</td>
<td>100</td>
<td>22762</td>
<td>2238</td>
<td>25000</td>
</tr>
</tbody>
</table>

Table 4.2 The details of the pixels in SI2 for the 2-out-of-2 RVCS

<table>
<thead>
<tr>
<th>Image</th>
<th>No. of Columns</th>
<th>No. of Rows</th>
<th>No. of Black Pixels</th>
<th>No. of White Pixels</th>
<th>Total Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI</td>
<td>200</td>
<td>200</td>
<td>16665</td>
<td>23335</td>
<td>40000</td>
</tr>
<tr>
<td>S1 + S2</td>
<td>200</td>
<td>200</td>
<td>28273</td>
<td>11727</td>
<td>40000</td>
</tr>
<tr>
<td>S1 + S21+S22</td>
<td>200</td>
<td>200</td>
<td>34188</td>
<td>5812</td>
<td>40000</td>
</tr>
<tr>
<td>S2 + S11+ S12</td>
<td>200</td>
<td>200</td>
<td>34177</td>
<td>5823</td>
<td>40000</td>
</tr>
<tr>
<td>S11 + S12 + S21 + S22</td>
<td>200</td>
<td>200</td>
<td>37162</td>
<td>2838</td>
<td>40000</td>
</tr>
</tbody>
</table>
4.2.5 Analysis of Experimental Results

Analyse the security in RVCS by comparing it with Naor & Shamir VCS. By using different levels of encryptions the security and reliability has been greatly improved. By using different levels of encryption, the cryptanalysis becomes very complex or even impossible.

The details of the pixels in the two different secret images and the reconstructed images obtained by stacking the shares in different ways are shown in Table 4.1 and 4.2. The contrast of the RVCS is analyzed with the help of graphs. That is

![Graphical representation of pixel details of SI1 based on RVCS](image)

**Figure 4.5** The graphical representation of pixel details of SI1 based on RVCS
From the graphs, one can see that the number of white pixels is reduced considerably in the reconstructed image by stacking three shares \((S_1+S_{21}+S_{22} \text{ or } S_2+S_{11}+S_{12})\) compared to stacking two shares \((S_1+S_2)\) in both images. Similarly, in the second level also white pixels are reduced in the reconstructed image by stacking four shares \((S_{11}+S_{12}+S_{21}+S_{22})\) compared to stacking three shares \((S_1+S_{21}+S_{22} \text{ or } S_2+S_{11}+S_{12})\). When the number of shares stacked is increased, this will reduce the contrast. In order to minimize the contrast loss in recursive visual cryptography scheme, use...
ABM method. RVCS based on XOR operation can get back a perfect secret image.

4.3 Recursive Visual Cryptography Schemes with ABM

This section presents RVCS with ABM method which enhances the contrast of RVCS.

The ABM is used for the generation of shares at each phase. By using ABM and recursion together, the security can be improved and contrast can be equivalent to Noar & Shamir scheme. The construction and implementation of ABM is explained in Chapter 3 (subsection 3.2).

4.3.1 Experimental Results

The experiments were conducted using 2-out-of-2 VCS with two levels of encryptions with recursion and ABM. Figures 4.7 and 4.8 show RVCS with ABM applied to two different images.
Figure 4.7 The 2-out-of-2 RVCS with ABM of SI₁: (a) SI₁, (b) S₁, (c)S₂, (d)S₁1, (e)S₁2, (f) S₂₁, (g) S₂₂, (h)S₁ + S₂, (i) S₁ + S₂₁ + S₂₂, (j) S₂ + S₁₁ + S₁₂, (k) S₁₁ + S₁₂ + S₂₁ + S₂₂
Figure 4.8 The 2-out-of-2 RVCS with ABM of SL2: (a) S1, (b) S2, (c) S2, (d) S11, (e) S12, (f) S21, (g) S22, (h) S1 + S2, (i) S1 + S21 + S22, (j) S2 + S11 + S12, (k) S11 + S12 + S21 + S22
Table 4.3 The details of the pixels in SI for the 2-out-of-2 RVCS with ABM

<table>
<thead>
<tr>
<th>Image</th>
<th>No. of Columns</th>
<th>No. of Rows</th>
<th>No. of Black Pixels</th>
<th>No. of White Pixels</th>
<th>Total Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI</td>
<td>250</td>
<td>100</td>
<td>7510</td>
<td>17490</td>
<td>25000</td>
</tr>
<tr>
<td>$S_1 + S_2$</td>
<td>250</td>
<td>100</td>
<td>13760</td>
<td>11240</td>
<td>25000</td>
</tr>
<tr>
<td>$S_1 + S_2 + S_21 + S_22$</td>
<td>250</td>
<td>100</td>
<td>17844</td>
<td>7156</td>
<td>25000</td>
</tr>
<tr>
<td>$S_2 + S_1 + S_12$</td>
<td>250</td>
<td>100</td>
<td>17766</td>
<td>7234</td>
<td>25000</td>
</tr>
<tr>
<td>$S_11 + S_12 + S_21 + S_22$</td>
<td>250</td>
<td>100</td>
<td>20388</td>
<td>4612</td>
<td>25000</td>
</tr>
</tbody>
</table>

Table 4.4 The details of the pixels in SI for the 2-out-of-2 RVCS with ABM

<table>
<thead>
<tr>
<th>Image</th>
<th>No. of Columns</th>
<th>No. of Rows</th>
<th>No. of Black Pixels</th>
<th>No. of White Pixels</th>
<th>Total Pixels</th>
</tr>
</thead>
<tbody>
<tr>
<td>SI</td>
<td>200</td>
<td>200</td>
<td>16665</td>
<td>23335</td>
<td>40000</td>
</tr>
<tr>
<td>$S_1 + S_2$</td>
<td>200</td>
<td>200</td>
<td>25079</td>
<td>14921</td>
<td>40000</td>
</tr>
<tr>
<td>$S_1 + S_21 + S_22$</td>
<td>200</td>
<td>200</td>
<td>30396</td>
<td>9604</td>
<td>40000</td>
</tr>
<tr>
<td>$S_2 + S_11 + S_12$</td>
<td>200</td>
<td>200</td>
<td>30513</td>
<td>9487</td>
<td>40000</td>
</tr>
<tr>
<td>$S_11 + S_12 + S_21 + S_22$</td>
<td>200</td>
<td>200</td>
<td>33873</td>
<td>6127</td>
<td>40000</td>
</tr>
</tbody>
</table>

4.3.2 Analysis of Experimental Results

For the analysis of experimental results, first analyze the contrast of RVCS with ABM by comparing it with RVCS, using graphs.
Figure 4.9 The graphical representation of pixel details of SI₁ in RVCS with ABM

Figure 4.10 The graphical representation of pixel details of SI₂ in RVCS with ABM
From the graphs (Figures 4.9 and 4.10), we can see that the number of white pixels is increased in the reconstructed images in RVCS with ABM in various ways compared with RVCS. Therefore, one can see that RVCS with ABM achieves better contrast than RVCS.

Next, analyse the reconstructed images in RVCS and RVCS with ABM.

**Table 4.5** The comparison of reconstructed images between RVCS and RVCS with ABM

<table>
<thead>
<tr>
<th>Shares Superimposed</th>
<th>RVCS</th>
<th>RVCS with ABM</th>
</tr>
</thead>
<tbody>
<tr>
<td>S1 + S2</td>
<td><img src="image" alt="RVCS S1 + S2" /></td>
<td><img src="image" alt="RVCS with ABM S1 + S2" /></td>
</tr>
<tr>
<td>S1 + S2 + S3</td>
<td><img src="image" alt="RVCS S1 + S2 + S3" /></td>
<td><img src="image" alt="RVCS with ABM S1 + S2 + S3" /></td>
</tr>
</tbody>
</table>
$S_2 + S_{11} + S_{12}$

$S_{11} + S_{12} + S_{21} + S_{22}$
By comparing the reconstructed images in the Table 4.5, we see that RVCS with ABM achieves better and clearer image than RVCS. From this, we can conclude that the RVCS with ABM method provides same contrast and better security than Naor and Shamir VCS.

4.4 Security Analysis of Different VCS

Let us assume that the binary secret image consists of $m \times n$ bits. In the case of $k$-out-of-$n$ VCS, each share consists of $mn$ bits. Thus, there are $2^{mn}$ possible combinations. If an intruder takes one microsecond to generate and check one combination, then it takes $(k-1) \cdot 2^{mn} \cdot 10^{-6}$ seconds to break the secret for a $k$-out-of-$n$ VCS, where $m$ and $n$ are the number of rows and columns of the secret image.

Consider the binary secret image consisting of 50 bits (5x10). In the case of $3$-out-of-$4$ VCS, each share consists of 50 bits. Thus there are $2^{50}$ possible combinations. If an intruder takes one microsecond to generate and check one combination, then it will take $2 \cdot 2^{50} \cdot 10^{-6}$ seconds
~ 35 years to reconstruct the secret image. By using recursion, the security of the visual cryptography scheme can be greatly improved.

### 4.5 Hybrid Approach for Information Security

The data encryption and decryption based on matrix ciphers and visual cryptography provides two levels of security. Most available cryptographic systems are fully or partially scalable, in the sense that one can choose different security levels. Scalability is usually achieved by allowing variable key sizes or by allowing different number of iterations, or rounds. A higher level of security is achieved with larger key sizes or larger number of rounds. Consequently, an algorithm becomes more complex and slower. But the new technique presented here is less complex and fast compared to other cryptosystems. When matrix ciphers are combined with visual cryptography scheme, the resulting cipher can be very hard to crack or even impossible. The next two sections explain these processes in detail with examples.

#### 4.5.1 Matrix Ciphers and Visual Cryptography

In this model, the matrix cipher maps blocks of $n$ characters from plaintext $P$ to the ciphertext $C$. The $P$ is a column vector of numbers corresponding to a block of plaintext letters of length $m$, $B$ is a column

---

vector of length $m$ and $A$ is the enciphering square matrix of order $m$. Then the transformation is

$$AP + B \equiv C \pmod{n}$$

where $n$ is the number of symbols used.

Then to decipher the ciphertext use the inverse transformation

$$P \equiv A^{-1}(C - B) \pmod{n}$$

### 4.5.2 Experimental Results

For the experiment, here the ordinary letters of the alphabets are used; so $n = 26$. Let the enciphering matrix $A$ be taken as

$$
\begin{bmatrix}
5 & 17 \\
4 & 15 \\
\end{bmatrix}
$$

Let the shift vector $B$ be

$$
\begin{bmatrix}
5 \\
2 \\
\end{bmatrix}
$$

Let the message to be encrypted be ICMCM, which is split into blocks of size two to get

IC MC MX

and, if necessary, pad with X’s (or random letters, if desired). This corresponds to the number pairs

8 2, 12 2, 12 23
To encipher the plaintext IC, use the vector $P$ as

\[
\begin{bmatrix}
8 \\
2
\end{bmatrix}
\]

and go through the transformation $AP + B \equiv C \pmod{26}$.

\[
\begin{bmatrix}
5 & 17 \\
4 & 15
\end{bmatrix}
\begin{bmatrix}
8 \\
2
\end{bmatrix}
+ \begin{bmatrix}
5 \\
2
\end{bmatrix}
\equiv \begin{bmatrix}
1 \\
12
\end{bmatrix} \pmod{26}
\]

The number pair 1, 12 corresponds to the letter pair BM, which is the cipher text of IC. Next encipher the pair MC

\[
\begin{bmatrix}
5 & 17 \\
4 & 15
\end{bmatrix}
\begin{bmatrix}
12 \\
2
\end{bmatrix}
+ \begin{bmatrix}
5 \\
2
\end{bmatrix}
\equiv \begin{bmatrix}
21 \\
2
\end{bmatrix} \pmod{26}
\]

This yields the ciphertext VC. Finally, encipher the pair MX

\[
\begin{bmatrix}
5 & 17 \\
4 & 15
\end{bmatrix}
\begin{bmatrix}
12 \\
23
\end{bmatrix}
+ \begin{bmatrix}
5 \\
2
\end{bmatrix}
\equiv \begin{bmatrix}
14 \\
5
\end{bmatrix} \pmod{26}
\]

to get the ciphertext OF. So the message (ciphertext) becomes BMVCOF.

This encrypted message is again encoded by using visual cryptography. In VC all documents are considered as images. Before encrypting, the message is converted into image format. That is

BMVCOF

Figure 4.11 Secret data
Chapter-4

Here use 2-out-of-2 VCS. The original image is split into two separate images called shares. The shares are such that no information from the original image is revealed to the viewer. Thus the two shares are

![Figure 4.12 Share 1](image1)
![Figure 4.13 Share 2](image2)

The two shares are sent to participants via secure channels.

In the decryption process, first the combiner (the trusted part/authenticated receiver) combines the two shares (i.e., just stack the shares) sent by the trusted party to get the secret data. The reconstructed secret data is:

![BMVC0F](image3)

Figure 4.14 Decrypted data (Share1 + Share 2)

Then to decipher the ciphertext use the inverse transformation

\[ P \equiv A^t (C - B) \pmod{26} \]

The letter pair IC is got back through

\[
\begin{bmatrix}
17 & 5 \\
18 & 23
\end{bmatrix}
\begin{bmatrix}
1 - 5 \\
12 - 2
\end{bmatrix}
\equiv
\begin{bmatrix}
8 \\
2
\end{bmatrix}
\pmod{26}
\]
Similarly the pair MC through
\[
\begin{bmatrix}
17 & 5 \\
18 & 23
\end{bmatrix}
\begin{bmatrix}
21 - 5 \\
2 - 2
\end{bmatrix}
\equiv
\begin{bmatrix}
12 \\
2
\end{bmatrix}
\pmod{26}
\]
And the pair MX through
\[
\begin{bmatrix}
17 & 5 \\
18 & 23
\end{bmatrix}
\begin{bmatrix}
14 - 5 \\
5 - 2
\end{bmatrix}
\equiv
\begin{bmatrix}
12 \\
23
\end{bmatrix}
\pmod{26}
\]
Where the pairs 8 2, 12 2, 12 23 correspond to the letter pairs IC, MC, MX, which is the plaintext.

4.6 The VCS with Indispensable Participants

In VCS with Indispensable Participants (IP) scheme, any one or more participants/shares are identified as indispensable participants for \(k\)-out-of-\(n\) VCS. The reconstruction of SI is impossible without IP. The model for VCS with IP is discussed below.

4.6.1 The Model

Let \(P = \{p_1, p_2, \ldots, p_n\}\) be a set of elements called participants, and let \(2^P\) denote all the subsets of \(P\). Let \(\Gamma_{\text{Qual}} \subseteq 2^P\) and \(\Gamma_{\text{Forb}} \subseteq 2^P\), where \(\Gamma_{\text{Qual}} \cap \Gamma_{\text{Forb}} = \emptyset\). Here take \(\Gamma_{\text{Qual}}\) as qualified sets and \(\Gamma_{\text{Forb}}\) as forbidden sets.

\(p_i \in P\) is an indispensable participant if the qualified set becomes,

\[\Gamma_{\text{Qual}} = \{A \subseteq 2^P : p_i \in A\}\]
If there are two indispensable participants, then

\[ \Gamma_{Qual} = \{ A \subseteq 2^p : \{p_i, p_j\} \in A, \ i \neq j \} \]

In general, \( k\)-out-of-\( n\) VCS with indispensable participants,

\[ \Gamma_{Qual} = \{ A \subseteq 2^p : \{p_1, p_2, \ldots, p_r\} \in A, \ 1 \leq r \leq k \} \]

4.7 Conclusion

This chapter presented a new method for security-enhanced secret image sharing method with simple examples. In Noar & Shamir scheme only one type and one level of VCS is used for the encoding and decoding of the SI, but in VCS with recursion different VCS and more than one level of encoding and decoding can be used. Therefore the security and reliability are enhanced. Contrast-enhanced recursive visual cryptography schemes with ABM is presented here. The RVCS with ABM provides almost the same contrast but better security compared to Naor and Shamir VCS. This chapter has also presented a hybrid cryptographic technique based on matrix ciphers and visual cryptography. These methods are less complex and fast compared to other cryptosystems and are very hard to crack. This approach can easily be extended to \( k\)-out-of-\( n\) VCS too. Indispensable Participants model also has been discussed here.