

Security-Enhanced Visual Cryptography Schemes With Recursion

Debashis Sanki¹, Dr. Nisarg Gandhewar²

¹ Research Scholar, Department of Computer Science and Engineering, Dr. A.P.J Abdul Kalam University, Indore, M.P.

² Research Guide, Department of Computer Science and Engineering, Dr. A. P. J. Abdul Kalam University, Indore, M.P.

Abstract:

Security is one of the key parameters 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 article 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.

Keywords: Visual, Cryptography, Recursion, Security.

INTRODUCTION

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 [1].

RECURSIVE VISUAL CRYPTOGRAPHY SCHEME

The Model

Let $P = \{p_1, p_2, \dots, p_n\}$ 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, Γ_{Qual} are referred to as qualified sets and Γ_{Forb} as forbidden sets.

In the second phase of encryption, let $p_{\text{Researcher}} = \{ p_{i1}, p_{i2}, \dots, p_{in} \}$, for $i= 1$ to n . Then the qualified sets $\Gamma_{\text{QualResearcher}} \subseteq 2^{p_{\text{Researcher}}}$ and forbidden sets $\Gamma_{\text{ForbResearcher}} \subseteq 2^{p_{\text{Researcher}}}$ such that $\Gamma_{\text{QualResearcher}} \cap \Gamma_{\text{ForbResearcher}} = \emptyset$. 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 [2].

In the decryption process, SRESEARCHER can be reconstructed as follows:In the first phase,

$$SI = \sum_{i=1}^k p_i$$

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, $p_{\text{Researcher}}$) is reconstructed as

$$p_i = \sum_{j=1}^k p_j \quad 1 \leq i \leq n$$

The Tree Structure for RVCS

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

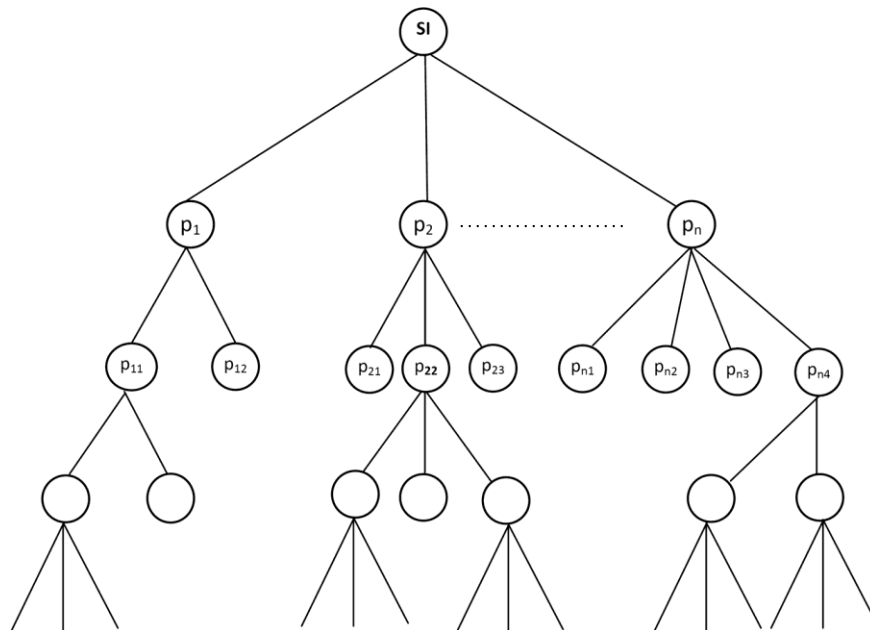


Figure 1 Tree representation of recursive visual cryptography model

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 [3].

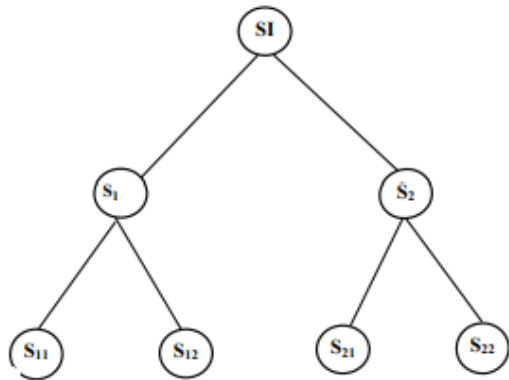


Figure 2 Tree representations for 2-out-of-2 VCS with recursion using two levels of encryption

From Figure 4.2, SRESEARCHER 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 SRESEARCHER is reconstructed by stacking shares in different ways. That is:

$$\text{SRESEARCHER} = S_1 + S_2$$

$$\text{SRESEARCHER} = S_1 + S_{21} + S_{22} \quad \text{SRESEARCHER} = S_2 + S_{11} + S_{12}$$

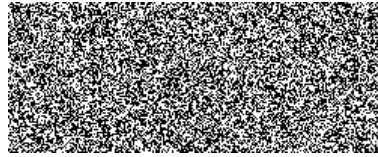
$$\text{SRESEARCHER} = S_{11} + S_{12} + S_{21} + S_{22}$$

Here, there are four different ways to reconstruct the SRESEARCHER 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].

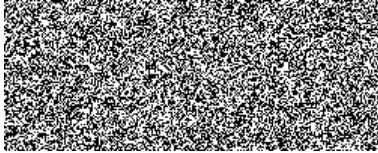
Experimental Results

The experiments were conducted using 2-out-of-2 VCS with two levels of encryptions. Figure 3 and 4 show RVCS applied to two different images:

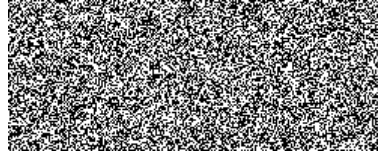
DEBASHIS



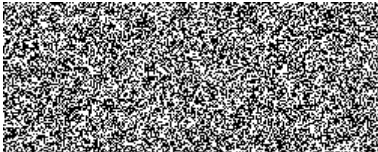
(a)



(b)



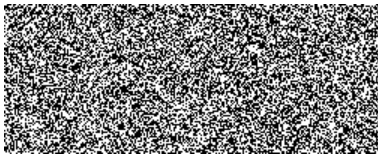
(c)



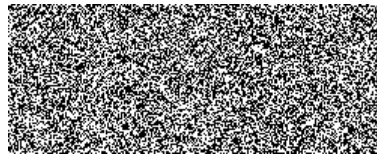
(d)



(e)



(f)



(g)



(h)



(i)



(j)



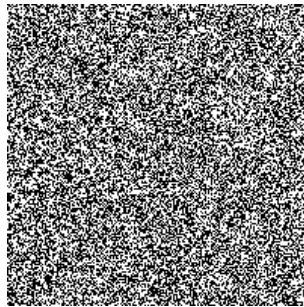
(k)



(l)

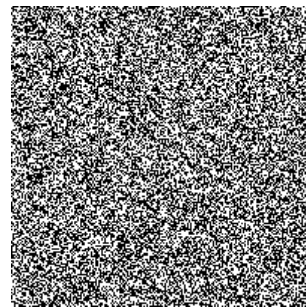
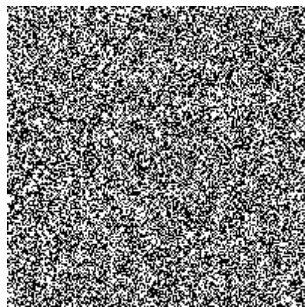
(m)

Figure 3. The 2-out-of-2 VCS with recursion for the image SI_1 : (a) SI_1 , (b) S_1 , (c) S_2 , (d) S_{11} , (e) S_{12} , (f) S_{21} , (g) S_{22} , (h) $S_1 + S_2$ (i) $S_1 + S_{21} + S_{22}$ (j) $S_2 + S_{11} + S_{12}$ (k) $S_{11} + S_{12} + S_{21} + S_{22}$ (l) $S_1 \oplus S_{21} \oplus S_{22}$ (m) $S_{11} \oplus S_{12} \oplus S_{21} \oplus S_{22}$



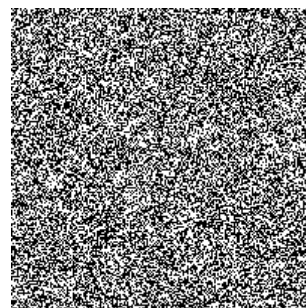
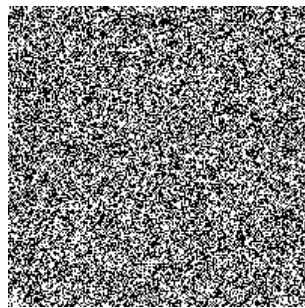
(a)

(b)



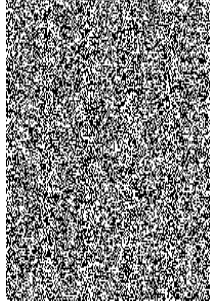
(c)

(d)

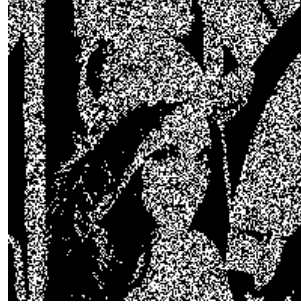


(e)

(f)



(g)



(h)



(i)



(j)



(k)



(l)



(m)

Figure 4. The 2-out-of-2 VCS with recursion for the image SI_2 : (a) SI_2 , (b) S_1 , (c) S_2 , (d) S_{11} , (e) S_{12} , (f) S_{21} , (g) S_{22} , (h) $S_1 + S_2$ (i) $S_1 + S_{21} + S_{22}$ (j) $S_2 + S_{11} + S_{12}$ (k) $S_{11} + S_{12} + S_{21} + S_{22}$ (l) $S_1 \oplus S_{21} \oplus S_{22}$ (m) $S_{11} \oplus S_{12} \oplus S_{21} \oplus S_{22}$

Table 1. The details of the pixels in SI_1 for the 2-out-of-2 RVCS

| Image | No. of Columns | No. of Rows | No. of Black Pixels | No. of White Pixels | Total Pixels |
|-------------------------------------|----------------|-------------|---------------------|---------------------|--------------|
| SI | 250 | 100 | 7510 | 17490 | 25000 |
| $S_1 + S_2$ | 250 | 100 | 16371 | 8629 | 25000 |
| $S_1 + S_{21} + S_{22}$ | 250 | 100 | 20657 | 4343 | 25000 |
| $S_2 + S_{11} + S_{12}$ | 250 | 100 | 20660 | 4340 | 25000 |
| $S_{11} + S_{12} + S_{21} + S_{22}$ | 250 | 100 | 22762 | 2238 | 25000 |

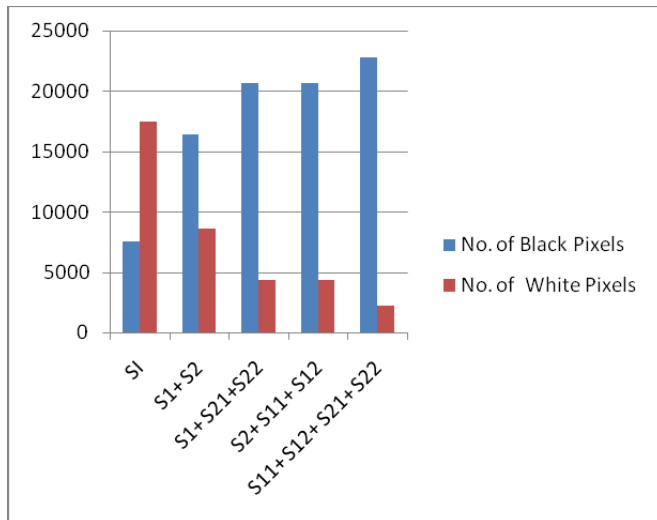
Table 2. The details of the pixels in SI_2 for the 2-out-of-2 RVCS

| Image | No. of Columns | No. of Rows | No. of Black Pixels | No. of White Pixels | Total Pixels |
|-------------------------------------|----------------|-------------|---------------------|---------------------|--------------|
| SI | 200 | 200 | 16665 | 23335 | 40000 |
| $S_1 + S_2$ | 200 | 200 | 28273 | 11727 | 40000 |
| $S_1 + S_{21} + S_{22}$ | 200 | 200 | 34188 | 5812 | 40000 |
| $S_2 + S_{11} + S_{12}$ | 200 | 200 | 34177 | 5823 | 40000 |
| $S_{11} + S_{12} + S_{21} + S_{22}$ | 200 | 200 | 37162 | 2838 | 40000 |

- Analysis of Experimental Results

Analyse the security in RVCS by comparing it with Naor & Shamir VCS. By using different level of encryptions the security and reliability has been greatly improved. By using different levels of encryption, the cryptanalysis becomes very complex or even impossible [5].

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

Figure 5 The graphical representation of pixel details of SI_1 basedon RVCS

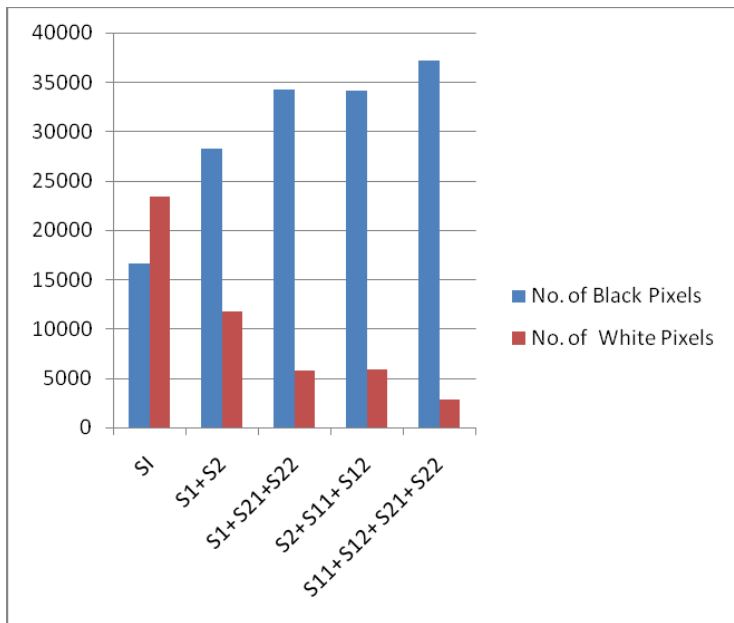


Figure 6 The graphical representation of pixel details of SI_2 basedon RVCS

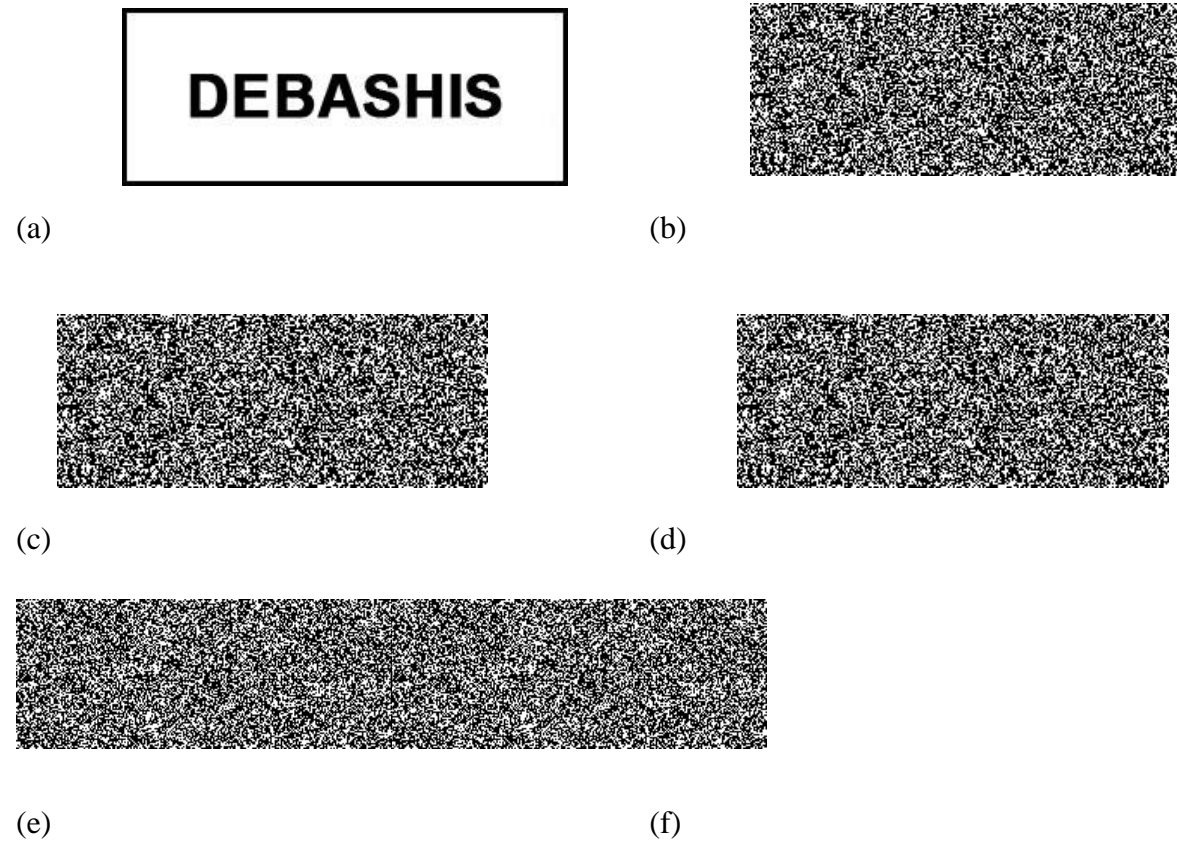
From the graphs, one can see that the number of white pixels is reduced considerably in the reconstructed image by stacking three shares ($S_1+S_{21}+S_{22}$ or $S_2+S_{11}+S_{12}$) compared to stacking two shares (S_1+S_2) in both images. Similarly, in the second level also white pixels are reduced in the reconstructed image by stacking four shares ($S_{11}+S_{12}+S_{21}+S_{22}$) compared to stacking three shares ($S_1+S_{21}+S_{22}$ 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 [6].

Recursive Visual Cryptography Schemes with ABM

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

Experimental Results

The experiments were conducted using 2-out-of-2 VCS with two levels of encryptions with recursion and ABM. Figures 7 and 8 show RVCS with ABM applied to two different images.



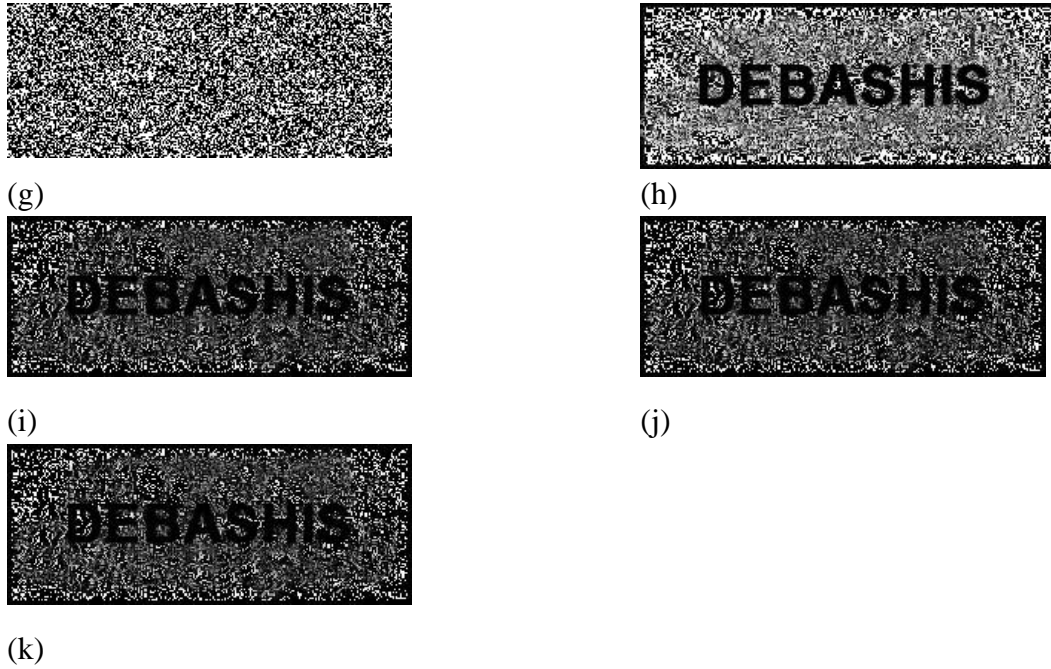
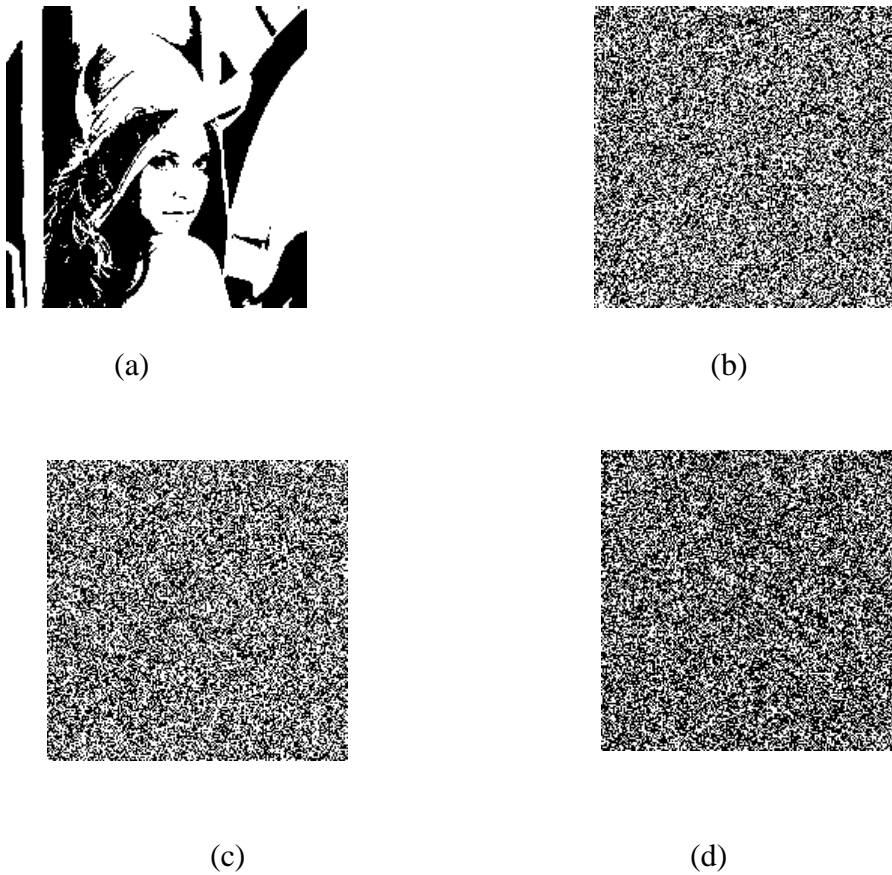


Figure 7 The 2-out-of-2 RVCS with ABM of SI_1 : (a) SI_1 , (b) S_1 , (c) S_2 , (d) S_{11} , (e) S_{12} , (f) S_{21} , (g) S_{22} , (h) $S_1 + S_2$ (i) $S_1 + S_{21} + S_{22}$ (j) $S_2 + S_{11} + S_{12}$ (k) $S_{11} + S_{12} + S_{21} + S_{22}$



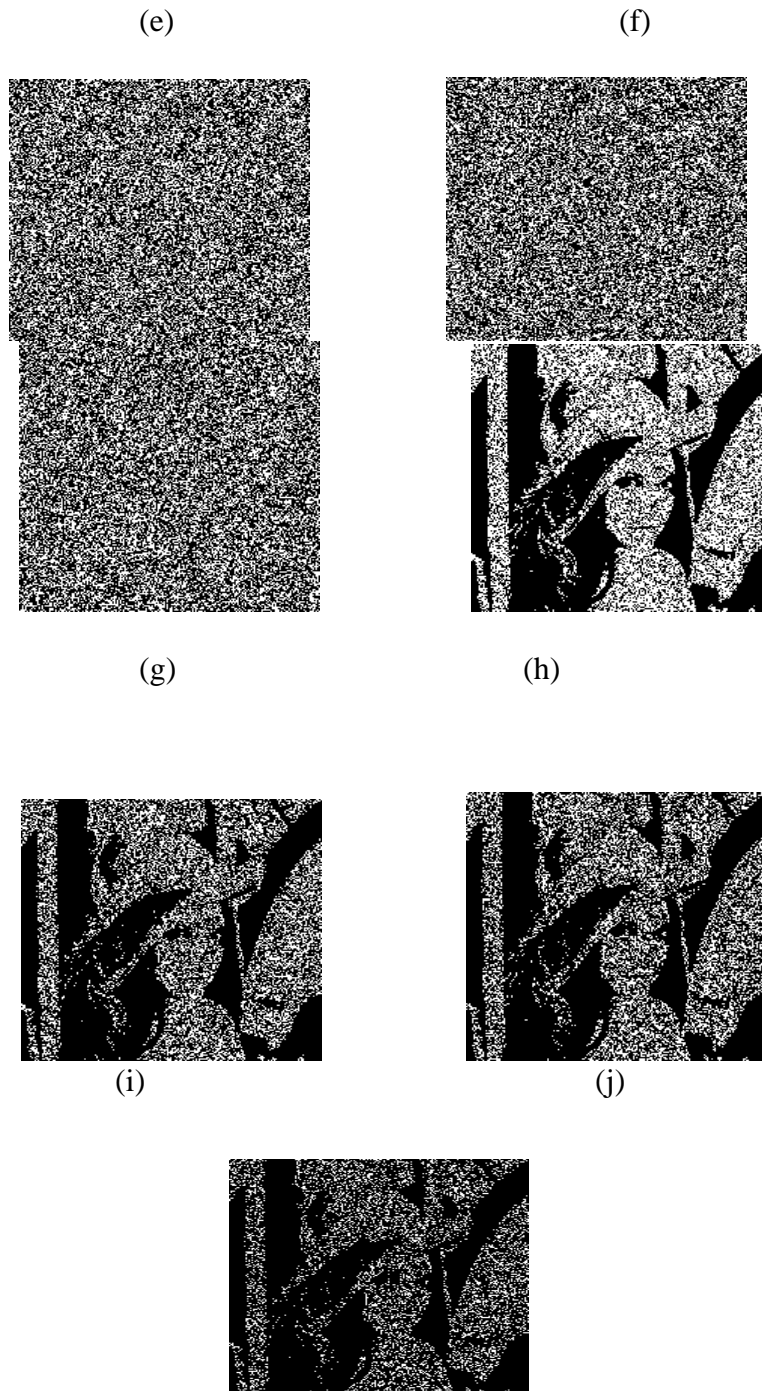


Figure 8 The 2-out-of-2 RVCS with ABM of SI_2 : (a) SI_2 , (b) S_1 , (c) S_2 , (d) S_{11} , (e) S_{12} , (f) S_{21} , (g) S_{22} , (h) $S_1 + S_2$ (i) $S_1 + S_{21} + S_{22}$ (j) $S_2 + S_{11} + S_{12}$ (k) $S_{11} + S_{12} + S_{21} + S_{22}$

Table 3 The details of the pixels in SI_1 for the 2-out-of-2 RVCS with ABM

| Image | No. of Columns | No. of Rows | No. of Black Pixels | No. of White Pixels | Total Pixels |
|-------------------------------------|----------------|-------------|---------------------|---------------------|--------------|
| SI | 250 | 100 | 7510 | 17490 | 25000 |
| $S_1 + S_2$ | 250 | 100 | 13760 | 11240 | 25000 |
| $S_1 + S_{21} + S_{22}$ | 250 | 100 | 17844 | 7156 | 25000 |
| $S_2 + S_{11} + S_{12}$ | 250 | 100 | 17766 | 7234 | 25000 |
| $S_{11} + S_{12} + S_{21} + S_{22}$ | 250 | 100 | 20388 | 4612 | 25000 |

Table 4. The details of the pixels in SI_2 for the 2-out-of-2 RVCS with ABM

| Image | No. of Columns | No. of Rows | No. of Black Pixels | No. of White Pixels | Total Pixels |
|-------------------------------------|----------------|-------------|---------------------|---------------------|--------------|
| SI | 200 | 200 | 16665 | 23335 | 40000 |
| $S_1 + S_2$ | 200 | 200 | 25079 | 14921 | 40000 |
| $S_1 + S_{21} + S_{22}$ | 200 | 200 | 30396 | 9604 | 40000 |
| $S_2 + S_{11} + S_{12}$ | 200 | 200 | 30513 | 9487 | 40000 |
| $S_{11} + S_{12} + S_{21} + S_{22}$ | 200 | 200 | 33873 | 6127 | 40000 |

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.

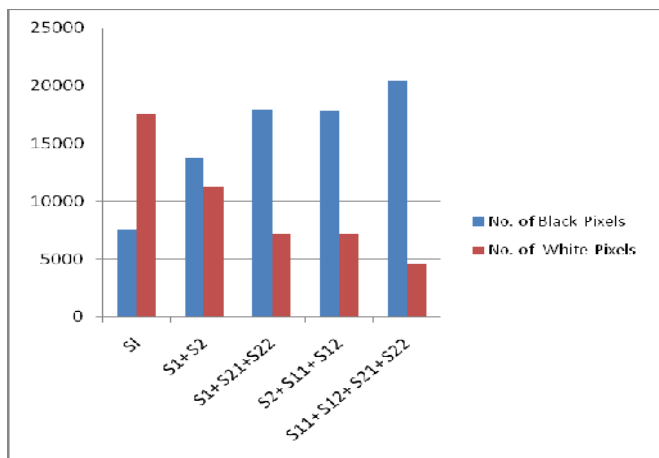


Figure 9 The graphical representation of pixel details of SI_1 in RVCS with ABM

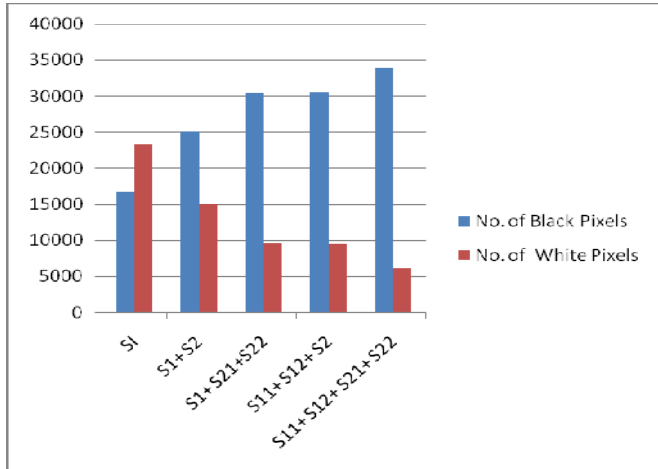

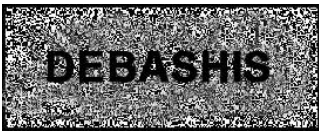




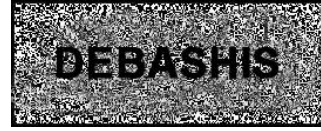
Figure 10 The graphical representation of pixel details of SI_2 inRVCS with ABM

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 [7]

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

Table 5 The comparison of reconstructed images between RVCS and RVCS with ABM

| Shares | RVCS | RVCS with ABM |
|--------------|---|--|
| Superimposed |  |  |
| S_1+S_2 |  |  |



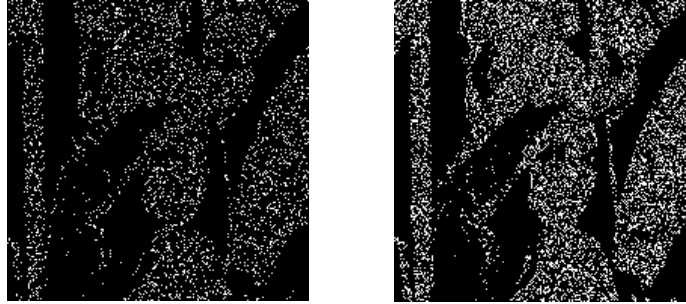
$$S_1 + S_{21} + S_{22}$$



$$S_2 + S_{11} + S_{12}$$



$$S_{11} + S_{12} + S_{21} + S_{22}$$



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 [8].

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 [9].

Then to decipher the ciphertext use the inverse transformation

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

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 $AP + B \equiv C \pmod{26}$.

$$\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} 12 \\ 2 \end{bmatrix} + \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 21 \\ 2 \end{bmatrix} \pmod{26}$$

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

$$\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} 12 \\ 2 \end{bmatrix} + \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 21 \\ 2 \end{bmatrix} \pmod{26}$$

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

$$\begin{bmatrix} 5 & 17 \\ 4 & 15 \end{bmatrix} \begin{bmatrix} 12 \\ 23 \end{bmatrix} + \begin{bmatrix} 5 \\ 2 \end{bmatrix} = \begin{bmatrix} 14 \\ 5 \end{bmatrix} \pmod{26}$$

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

Secret data

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 [10]



Share 1



Share 2

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:



Decrypted data (Share1+ Share 2)

Then to decipher the ciphertext use the inverse transformation

$$P \equiv A^{-1}(C - B) \pmod{26}$$

The letter pair IC is got back through

$$\begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \begin{bmatrix} 1 - 5 \\ 12 - 2 \end{bmatrix} = \begin{bmatrix} 8 \\ 2 \end{bmatrix} \pmod{26}$$

Similarly the pair MC through

And the pair MX through

$$\begin{bmatrix} 17 & 5 \\ 18 & 23 \end{bmatrix} \begin{bmatrix} 14 - 5 \\ 5 - 2 \end{bmatrix} = \begin{bmatrix} 12 \\ 23 \end{bmatrix} \pmod{26}$$

Where the pairs 8 2, 12 2, 12 23 correspond to the letter pairs IC, MC, MX, which is the plaintext.

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 SRESEARCHER is impossible without IP. The model for VCS with IP is discussed below [11].
 The Model

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

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

$$\Gamma_{Qual} = \{ A \subseteq 2^P : p_i \in A \}$$

If there are two indispensable participants, then

$$\Gamma_{\text{Qual}} = \{ A \subseteq 2^P : \{p_{\text{Researcher}}, p_j\} \in A, i \neq j\}$$

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

$$\Gamma_{\text{Qual}} = \{ A \subseteq 2^P : \{p_1, p_2, \dots, p_r\} \in A, 1 \leq r \leq k\}$$

CONCLUSION:

Here presented a new method for security-enhanced secret image sharing method with simple examples [12]. In researcher 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 [13]. Therefore, the security and reliability are enhanced. Contrast-enhanced recursive visual cryptography schemes with ABM are 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.

REFERENCES:

1. Cimato, S, De Prisco, R & De Santis, A 2006, 'Probabilistic visual cryptography schemes', The Computer Journal, vol.49, no.1, pp.97-107.
2. Cimato, S, De Prisco, R & De Santis, A 2007, 'Colored visual cryptography without color darkening', Theoretical Computer Science, vol.374, no.1, pp.261-276.
3. Cimato, S, De Santis, A, Ferrara, AL & Masucci, B 2005, 'Ideal contrast visual cryptography schemes with reversing', Information Processing Letters, vol.93, no.4, pp.199-206.
4. De Bonis, A & De Santis, A 2004, 'Randomness in secret sharing and visual cryptography schemes', Theoretical Computer Science, vol.314, no.3, pp.351-374.
5. De Prisco, R & De Santis, A 2014, 'On the relation of random grid and deterministic visual cryptography', IEEE Transactions on Information Forensics and Security, vol.9, no.4, pp.653-665.
6. Droste, S 1996, 'New results on visual cryptography', in Annual International Cryptology Conference, pp.401-415.
7. Eisen, PA & Stinson, DR 2002, 'Threshold visual cryptography schemes with specified whiteness levels of reconstructed pixels', Designs, Codes and Cryptography, vol.25, no.1, pp.15-61.

8. Fang, W-P & Lin, J-C 2006, 'Visual cryptography with extra ability of hiding confidential data', Journal of Electronic imaging, vol.15, no.2, pp.023020-023020-023027.
9. Floyd, RW 1976, 'An adaptive algorithm for spatial gray-scale', in Proc.Soc. Inf. Disp. , vol.17, pp.75-77.
10. Gnanaguruparan, M & Kak, S 2002, 'Recursive hiding of secrets in visual cryptography', Cryptologia, vol.26, no.1, pp.68-76.
11. Hawkes, L, Yasinsac, A & Cline, C 2000, 'An application of visual cryptography to financial documents', Florida State University, Florida, pp.1-7.
12. Hofmeister, T, Krause, M & Simon, HU 2000, 'Contrast-optimal k out of n secret sharing schemes in visual cryptography', Theoretical Computer Science, vol.240, no.2, pp.471-485.
13. Horng, G, Chen, T & Tsai, D-S 2006, 'Cheating in visual cryptography', Designs, Codes and Cryptography, vol.38, no.2, pp.219-236.