New Constructions for Thin Line Problem in Visual Cryptography

MAGED WAFY
Helwan University
Department of Information Technology
Computer Sciences Faculty, Ain Helwan, Egypt
w_h82@hotmail.com

Abstract: Visual cryptography schemes (VCSs) are techniques that divide a secret image into n shares. Stacking exactly n shares reveals the secret image. One VCS technique is the deterministic VCS (D-VCS), which suffers from the pixel expansion issue. This problem has been solved by probabilistic size invariant VCS (P-SIVCS); however, the visual quality of the revealed secret image produced by P-SIVCS is low. In D-VCS, a thin line is converted to a thick line and pixel expansion problem while it may not be visible in the revealed secret image created by P-SIVCS. In this paper, two new constructions are introduced for resolving the thin line problem with well visible quality and non expansion pixel by using image manipulation, D-VCS, a mixture of D-VCS and P-SIVCS.

Key–Words: Visual cryptography; Thin line problem; Pixel expansion,

1 Introduction

Ensuring the security of information has become a necessity, because trade, as well as other fields, rely on the transmission of information across networks. Thus, data encryption has become a major research issue.

Encryption is a secure means of protecting valuable information. All the encryption types, except for visual cryptography, require computation and/or hardware for the decryption operation.

In visual cryptography, the secret image (SI) is split into n shares and no information can be gained from any one share or a stack of k shares, when $k < n$. However, stacking exactly n shares reveals the SI.

Decryption in a visual cryptography scheme (VCS) relies only on a human visual system. Naor and Shamir [1] developed a deterministic VCS technique, D-VCS, that satisfies two conditions, security and contrast. The security condition guarantees that a cryptanalyst cannot acquire information from a number of shares k that is smaller than the number of required shares n, $k < n$. The contrast condition guarantees the visibility of the SI. The major issue in D-VCS is the pixel expansion problem: the size of the revealed secret image (RSI) and the shares is at least double that of the SI; however, the visual quality of the RSI is good. In contrast, Yang [2] adopted a probabilistic size invariant VCS (P-SIVCS), a non expansion technique that produces RSIs having a poor visual quality.

Subsequently, Hou and Tu [4] showed that not only the contrast affects the visual quality of the RSI but also the variance. Therefore, Hou and Tu [4] introduced multi pixel size invariant VCS (ME-SIVCS), which takes both the contrast and variance into account, and thus, the visual image quality achieved using ME-SIVCS is better than that using P-SIVCS.

An SI may include fine details, such as a map and shapes represented by a thin line. If P-SIVCS is employed for such an SI, the RSI is unclear, and it is hard to realize a thin line when the visual quality is poor. This problem was first called the thin line problem (TLP-1) in [5] [6]. ME-SIVCS generated another two issues: TLP-2, where some vertical lines are missing in the RSI, and TLP-3, where thin vertical lines become thick in the RSI. More details are given in section 3.

Feng et al. [5] adopted two new constructions, Construction 3, which suffers from TLP-3, and Construction 1 [5], which does not suffer from any of the three problems, TLP-1, TLP-2, and TLP-3. However, Construction 1 satisfies only a weak version of the traditional security condition. A second issue, is that, because of the nature of Construction 1, the visibility of parts of its resulting images is poor as compared with those of D-VCS, i.e., it suffers partially from TLP-1.

In this paper, two new constructions are introduced. Construction 1 avoids the three problems, TLP-1, TLP-2, and TLP-3, but suffers partially from TLP-4 if SI has a thickness of horizontal lines equals 1 pixel. Construction 2 avoids the three problems, TLP-1, TLP-2, and TLP-3. Construction 2 suffers only partially from TLP-1.

The rest of this paper is organized as follows. In the following section, the traditional definitions of D-VCS, P-SIVCS, ME-SIVCS are given, and the background for the TLP. The proposed two new constructions are introduced in section 3. In section 4 the experimental results for the two constructions are also examined. In section 5, some concluding remarks are presented.

2 Background and Definitions

2.1 Notations

Let C^t be a collection of S_i^t, where S_i^t represents $n \times m$ Boolean matrices, $t \in \{0, 1\}$, and $1 \leq i \leq g^t$, where $g^t = |C^t|$ is the cardinality of C^t. Consider $s_{i,k}^t$ is **any** $k \times m$ submatrix of a matrix $S_i^t \in C^t$, where $2 \leq k \leq n$. $V_{i,k}^t$ defines the OR vector for $s_{i,k}^t$ and $H(V_{i,k}^t)$ is the Hamming weight for the vector $V_{i,k}^t$. Let $x \in \lambda_k^t$, $\lambda_k^t = \{H(V_{i,k}^t) : 1 \leq i \leq g^t$, for any k out of $n\}$. Denote x^0, x^1

$$x^0 = \max_{x \in \lambda^0} x,\ x^1 = \min_{x \in \lambda^1} x, .$$

The average and variance of the darkness level are denoted by μ^t and σ^t, respectively:

$$\mu^t = \frac{\sum_{x \in \lambda_k^t} x}{|\lambda_k^t|},\ \sigma^t = \frac{\sum_{x \in \lambda_k^t} (x - \mu^t)^2}{|\lambda_k^t|}. \quad (1)$$

2.2 D-SEVCS (k, n) (Ateniese et al. [7])

Two collections of C^0 and C^1 constitute the **D**eterministic **S**cale **E**xpansion **V**isual **C**ryptography **S**cheme (D-SEVCS) if they satisfy the contrast and security conditions:

Contrast: $x^0 < x^1 \leq m$.

Security: For any $j_1 < j_2 < ... < j_d$ in $\{1, 2, ..., n\}$, $d < k$ the two collections B^t of submatrices $s_{i,d}^t$ obtained by restricting each $s_{i,k}^t \in C^t$ to rows $j_1, j_2, ..., j_d$ are indistinguishable in the sense that they contain the same matrices with the same frequencies.

The steps of the encryption of an SI are as follows.

- Convert the SI to a binary image, say, SIB.
- Select a pixel from SIB. If the pixel is black (white), randomly select a matrix $S_i^1(S_i^0) \in C^1(C^0)$, and subsequently, distribute n rows for n shares, where every row has m elements representing the size of the pixel expansion.

Stacking a sufficient number of shares $k \leq n$ yields the RSI, which is the simplest decryption method among all the types of cryptography. The size of the shares and the RSI is m times the size of the SI. This is called the pixel expansion problem. Good visual quality of D-SEVCS was at expense of pixel expansion. In this paper we are not highlight methods such as random gird [8, 9], turning and flipping [10], and visual cryptograms [9, 11] because these methods have poor visual quality approximately as **P**robability **S**ize **I**nvariant VCS (P-SIVCS). Yang [2] adopted P-SIVCS to resolve the issues of pixel expansion at expense of poor visual quality. Also Yang [12] and Yan [3] discussed the relation between P-SIVCS and random gird.

2.3 P-SIVCS(k, n)

Without loss of generality, let $n = k = 2$. Two collections, C^0 and C^1, of the matrices 2×1,

$$C^0 = \left\{ \begin{bmatrix} 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1 \\ 1 \end{bmatrix} \right\}, C^1 = \left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

form P-SIVCS if they satisfy the contrast and security conditions:

Contrast: Denote $P_{i,k}^t$ as the probability that $V_{i,k}^t$ is 1 for any i, then $P_{i,k}^0 < P_{i,k}^1$.

Security: For any $j_1 < j_2 < ... < j_d$ in $\{1, 2, ..., n\}$, $d < k$, the two probabilities $P_{i,d}^0$ and $P_{i,d}^1$ for the two collections C^t, $t = 0, 1$, are equal.

The P-SIVCS algorithm designed by Yang results in an RSI having an unclear visual quality (see Figure 2(a)). Therefore, Hou and Tu [4, 13] introduced the following construction, the image visibility of which is good.

Definition 1. (ME-SIVCS-1) (k, n, m). Let m be a block size of pixels and b the number of black pixels in m. $N(b)$ represents the number of blocks that have been encrypted, and every block has b black pixels. To encrypt a block L having m pixels

- (A) $N(b) = 0, b = 1, 2..., m$.
- (B) If $N(b)\ mod\ m < b$, then select randomly a matrix S_i^1, distribute n rows of S_i^1 on n shares.
- (C) Else, encrypt the block L by a matrix S_i^0 is selected randomly, distribute n rows of S_i^0 on n shares.
- (D) $N(b) = N(b) + 1$.
- (E) Encrypt a new block.

Example 1. To simplify the above definition, consider $m = 2$; then, the block may have $b = 0,\ 1,$ or 2. When both pixels are black, i.e., $b = 2$, then the inequality in step B is satisfied $((N(b)\ mod\ 2) = (0\ or\ 1) < 2)$, which guarantees that the block of two black pixels is encrypted by a matrix from C^1. When $b = 0$, this means that two pixels are white and the inequality in step B will never be satisfied ($N(b)\ mod\ 2 \nless 0$), which guarantees that the block of two white pixels is encrypted from C^0. Finally, when $b = 1$, i.e., one pixel is white and the other is black, the inequality in step B becomes $((N(b)\ mod\ 2) = (0\ or\ 1)) < 1$, which means that the first block having $b = 1$ is encrypted using a matrix from C^1, and then, the second block having $b = 1$ is encrypted via a matrix from C^0. If the total number of blocks that have $b = 1$ is n_b, then $\frac{n_b}{2}$ is encrypted by a matrix from C^1 and $\frac{n_b}{2}$ is encrypted by a matrix from C^0.

In ME-SIVCS-1 some vertical thin lines were removed see Figure3(b) and Figure 5(c). To recover this problem Feng et al. [5] introduced the following construction ME-SIVCS-2.

Definition 2. (k, n, m) ME-SIVCS-2. Divide the SI into q blocks, and define $D(M[b])$ as a function generating a random number between 0 and $M[b] - 1$, where b is the number of black pixels in the block that have already been encrypted. To encrypt a block from q blocks, the following steps are followed.

- (A) $N[b] = b,\ b = 1, 2..., m.$
- (B) $M[b]) = m,\ b = 1, 2, ..., m.$
- (C) If $D(M[b]) < N[b]$, then select randomly a matrix S_i^1, and subsequently, distribute n rows of S_i^1 on n shares.
- (D) $D[M] = D[M] - 1$
- (E) $N[b] = N[b] - 1$
- (F) Else, encrypt the block by select randomly a matrix S_i^0, distribute n rows of S_i^0 on n shares.
- (G) $D[M] = D[M] - 1.$
- (H) If $D[b] = 0\ then\ N[b] = b,\ D[b] = m$
- (I) Encrypt a new block.

Feng et al. introduced Construction 4 in [5], which satisfies a weak version of the conventional security condition. In this study, we restricted ourselves to only the conventional security condition.

2.4 Measurements of the RSI quality

Average contrast $\bar{\alpha}$ was introduced in [2, 4, 14, 15] as an appropriate measure of quality for the RSI in P-SIVCS, instead of the traditional definition of contrast α in D-SEVCS:

$$\alpha = \frac{x^1 - x^0}{m},\ \bar{\alpha} = \mu^1 - \mu^0,$$

$$\bar{\alpha_p}(\text{for P-SIVCS}) = P^1_{1,k} - P^0_{1,k}.$$

In fact, the average contrast in P-SIVCS, ME-SIVCS-1, and ME-SIVCS-2 is equal to the corresponding contrast in D-SEVCS. However, the visual quality of the RSI, as shown in Figure 3(a-c), is not the same. Hou and Tu [4] and Feng [5] showed that the variance should be used together with the average contrast to evaluate the visual quality.

Variance. The general definition of variance was given in equation (1). The variance for P-SIVCS is $\sigma_p = \frac{bx^1(m-x^1)+(m-b)(m-x^0)x^0}{m^2}$, and that for both ME-SIVCS-1 and ME-SIVCS-2 is $\sigma_{ME} = \frac{b(m-b)}{m^2}(x^1 - x^0)^2$ (see [5]). Simply, without loss of generality, for $m = 2,\ b = 0, 1, 2,\ \sigma_{ME} \leq \sigma_p$. Therefore, the visual quality produced by both ME-SIVCS-1 and ME-SIVCS-2 is better than that produced by P-SIVCS.

2.5 Review of the current thin line methods

Fine images have valuable information, such as edges and corner points, that can be utilized to detect and identify essential features. Both edges and corner points are formed from lines, and therefore, lines are frequently essential in image processing, image analysis, feature detection and identification, and many applications. Thus, lines constitute valuable information in a map or architectural plan. VCS can be an excellent approach for transforming vital information such as lines. However, the visual quality of the RSI of P-SIVCS is poor in the case of a fine image, and it is hard to see a thin line. This problem was called TLP-1 in [5] (see Figure3(a)). ME-SIVCS-1 can resolve TLP-1 (see Figure3(b)). In Figure3(b) and Figure5(c), some vertical lines have been removed, which represents the problem called TLP-2 in [5].

TLP-2 problem as the result of step "B" in Definition 1 and step "C" in Definition 2, two pixels, one of which is black and the other white, are encrypted only from C^1 or C^0, respectively. If the thin line (only one pixel in thickness) is white and the second neighbor pixel is black, they may both be encrypted as black, and thus, the white pixel that represents the thin line is removed.

Another problem in ME-SIVCS-1, vertical lines have become thicker, a problem that Feng et al. [5] called TLP-3. Subsequently, Feng et al. [5] adopted ME-SIVCS-2. ME-SIVCS-2 suffers from TLP-3 and partially from TLP-2 (see Figure3(c) and Figure5(d)).

3 The Proposed Constructions

In this section, the proposed constructions are introduced. In the first construction, the unsharp mask will be utilized. Therefore, analysis of the unsharp mask has adopted (in the next section) to study the impact of the unsharp mask on SI.

3.1 Unsharp mask

Contrast play an important role in improving the quality of RSI. For this reason, we apply the unsharp mask for SI in the two new constructions to improve the contrast in SI, accordingly the contrast in RSI will be enhanced. Unsharp mask increases the edge contrast and local contrast in SI. The kernel of unsharp mask equals a Dirac delta function minus Gaussian blur kernel we refer the reader to [16].

The question can raise: Is the unsharp mask can change the details of SI? The answer can be in three points, visually (see Figure1 and Figure2), explanation of how the unsharp mask works and the ratio of white pixels turned to black or vice versa (see table 1).

The unsharp mask is high pass filter, that sharper the fine details in image (edges, corner points and thin line). Simply, the white edges in lena's hair Figure 1(b) sharper than in Figure 1(a) and the written word on plane's tail ("F16") became clearer in Figure 1(h) than Figure 1 (g).
In the table 1 Let $w2b$ ($b2w$) be the number of pixels that are converted from white (black) in SI (see left column in Figure 1) to black (white) in SI after applying the unsharp mask (see right column in Figure 1), $b2w$. The size of images in Figure1 is $512 \times 512 = 262144$, R_{w2b} =w2b/262144 and R_{b2w} =b2w/262144. In table 1, the total ratio of change in an image Figure 1 between $0.04 - 0.16$ which is tiny change that improves the fine details at the same time does not change the contents of the SI.

Another example, in Figure 2 shows the impact of unsharp mask to improve the visual quality of RSI. Figure2(a-b) represents P-SIVCS, ME-SIVCS-1 and ME-SIVCS-2 respectively, without applying the unsharp mask for SI. In the Figure 2 (d-f) the unsharp mask was applied to SI, and then, the methods P-SIVCS, ME-SIVCS-1 and ME-SIVCS-2 were applied on SI respectively.

Construction 1. This construction can be classified as D-SEVCS; it is summarized in the following steps.

1. SI of size $x \times y$ to be reduced to size $x \times \frac{y}{2}$ (Figure 3(d) and (e)).

2. Use a cubic interpolation to smooth the SI after reduction.

3. Use the unsharp mask, to sharpen the line that may have become thicker in the interpolation step.

4. Apply the conventional D-SEVCS of Naor and Shamir [1] that require pixel expansion $m = 1 \times 2$, then the size of two shares and RSI is $x \times (\frac{y}{2} \times 2) = x \times y$.

Steps 1-3 were applied before using of D-SEVCS. Therefore no require to prove that construction 1 satisfy security condition.

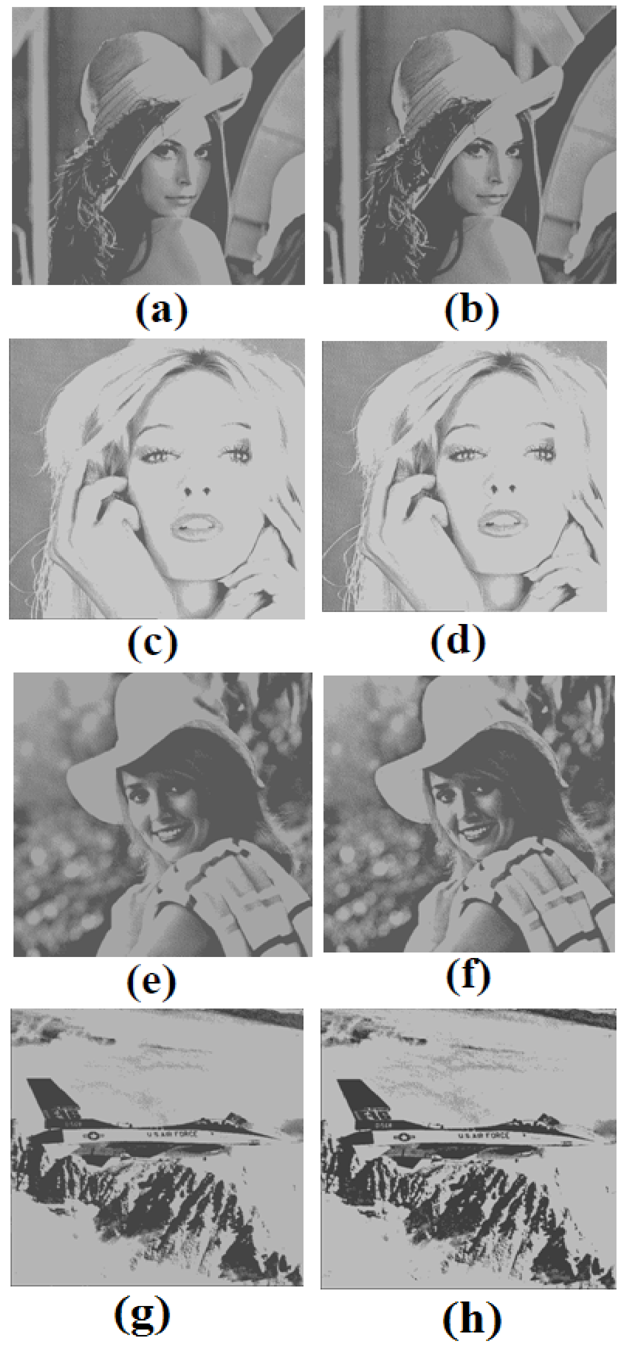

Figure 1: The impact of the unsharp mask. The left column represents the SI, and in the right column, the unsharp mask was applied to the SI in the first column.

Table 1: The impact of the unsharp mask.

Figure	$w2b$	R_{w2b}	$b2w$	R_{b2w}	$Total$
Figure 1(a)	17299	0.06	26762	0.1	0.16
Figure 1(c)	16773	0.06	14850	0.05	0.11
Figure 1(g)	21593	0.08	16769	0.06	0.14
Figure 1(e)	6166	0.02	5771	0.02	0.04

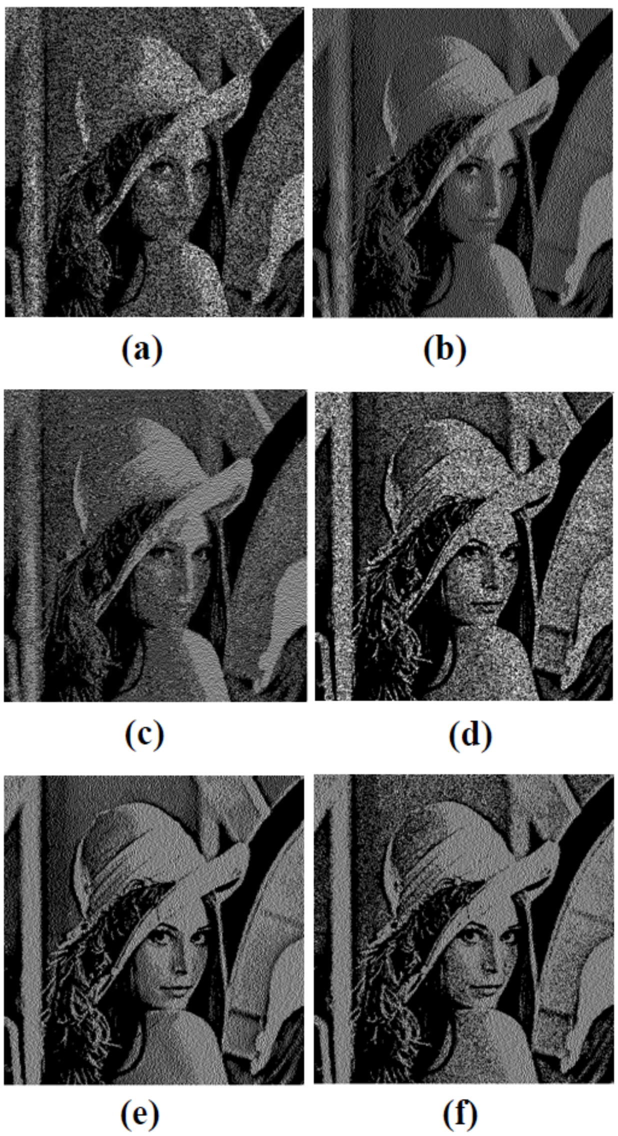

Figure 2: Comparison between applying the unsharp mask for SI (the second row) before using methods P-SVICS, ME-SIVCS-1, ME-SIVCS-2 and using methods without applying the unsharp mask (the first row): **(a)** P-SVICS , **(b)** ME-SIVCS-1, **(c)** ME-SIVCS-2, **(d)**-**(f)** are P-SVICS , ME-SIVCS-1, and ME-SIVCS-2, respectively, after the unsharp mask was applied on SI.

The visual quality in Figure 3(f) is better than that in both Figure 3(b-c), which shows the result of ME-SIVCS-1, and Figure 3(c), which shows the result of ME-SIVCS-2, the variance of Construction 1 is $\leq$ the variance for ME-SIVCS-1 or ME-SIVCS-2 see table 2. In addition, TLP-1, TLP-2, and TLP-3 are avoided in Construction 1 and the vertical lines are straight and not partially removed, as in ME-SIVCS-2 in Figure 3(c). However, the horizontal lines in Construction 1

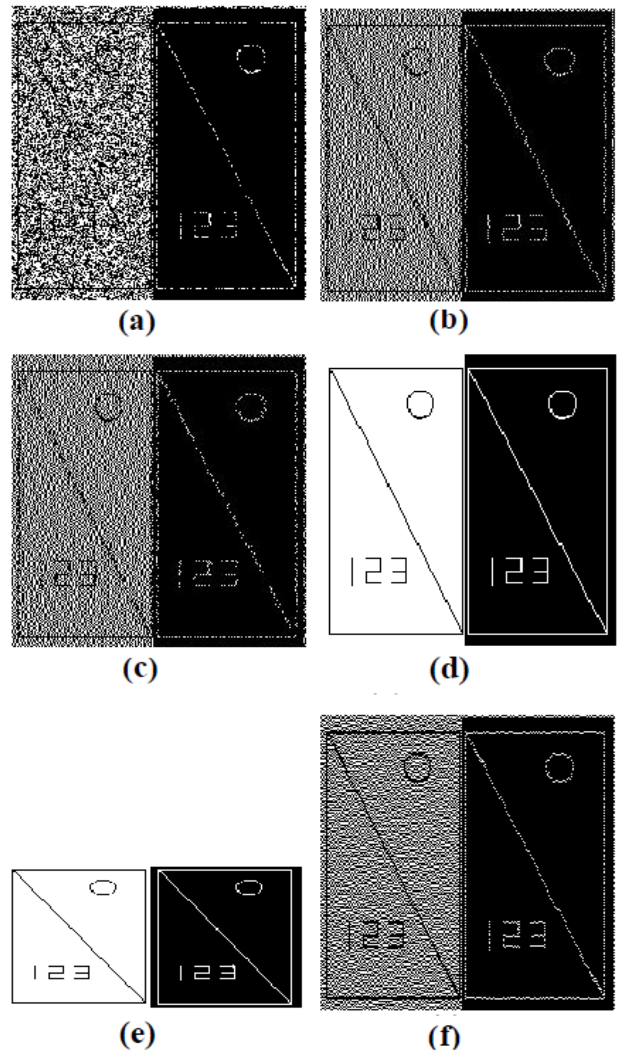

Figure 3: Comparison of all previous techniques and our first construction technique: **(a)** P-SVICS, **(b)** ME-SIVCS-1, **(c)** ME-SIVCS-2, **(d)** the secret image (SI) with size 209×208, **(e)** the resized image with size 209×104, **(f)** our Construction 1.

became thicker, which means that if the thickness of the horizontal line is one pixel in the SI, it is converted to two pixels in the RSI. In this paper, we call this type of thin line problem the fourth type thin line problem (TLP-4).

TLP-4 can exist in Construction 1 only when a horizontal line having a thickness of 1 pixel exists. However, if the thickness of a horizontal line is 2 pixels in the SI, it is converted to 1 pixel in the reduction step of the SI, i.e., the line has a thickness of 1 pixel in the reduced image. Thereafter, in the encryption step, the line returns to a thickness of 2 pixels. Thus, TLP-4 occurs when the thickness of a line in the SI is only 1 pixel. In Figure 4, the line having a thickness of 8 pixels in Figure 4(a) becomes one having a thickness of only 4 pixels in Figure4(b), and then, after using Construction 1, the line returns to a thickness of 8 pixels in Figure4(c). Similarly, the line having a thickness of 4 pixels becomes a line consisting of 2 pixels Figure4(b), and then one consisting of only 4 pixels in Figure4(c). The thin line having a thickness of 1 pixel became thicker (2 pixels). Apparently, Construction 1 does not increase the thickness of a line, if its thickness > 1, and some lines may become thinner.

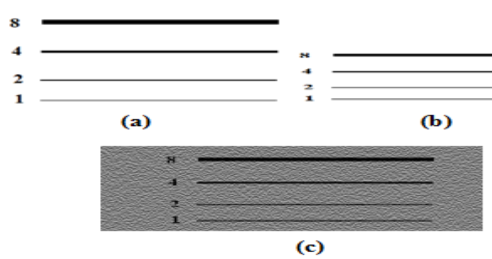

Figure 4: Effect of Construction 1 on the line thickness. **(a)** The secret image (SI) of size 415×190: the top line has a thickness of 8 pixels, the second line a thickness of 4 pixels, the third line a thickness of 2 pixels, and the last line a thickness of 1 pixel, **(b)** Reduced image of size 415×95, **(c)** Construction 1.

Another example illustrates that construction 1 has not issues TLP-1 to TLP-4 in case, thickness of the horizontal lines >1 pixel. In the Figure 5(a), the thickness of horizontal lines is 2 pixels. In this case, construction 1 not suffers from TLP-4, the thickness of horizontal lines in RSI is 2 pixels, see Figure5(f).

The Construction 1 has only one problem occurs while horizontal lines of thickness one pixel. There is no need to prove security condition for Construction 1. Because the steps 1-3 are pre-processing operations on SI, then the conventional D-SEVCS (that satisfied security condition) of Naor and Shamir [1] is applied.

Construction 2. There are several algorithms mixed between D-SEVCS and P-SIVCS (see [5] and [17], pp. 138) that suffer from TLP-1 or/and TLP-3. Feng [5] introduced three methods (pp.334-335), however, Feng mentioned that three algorithms are not suitable for the thin problem, and then Feng [5] introduced ME-SIVCS-1 and ME-SIVCS-2 (both were explained above).

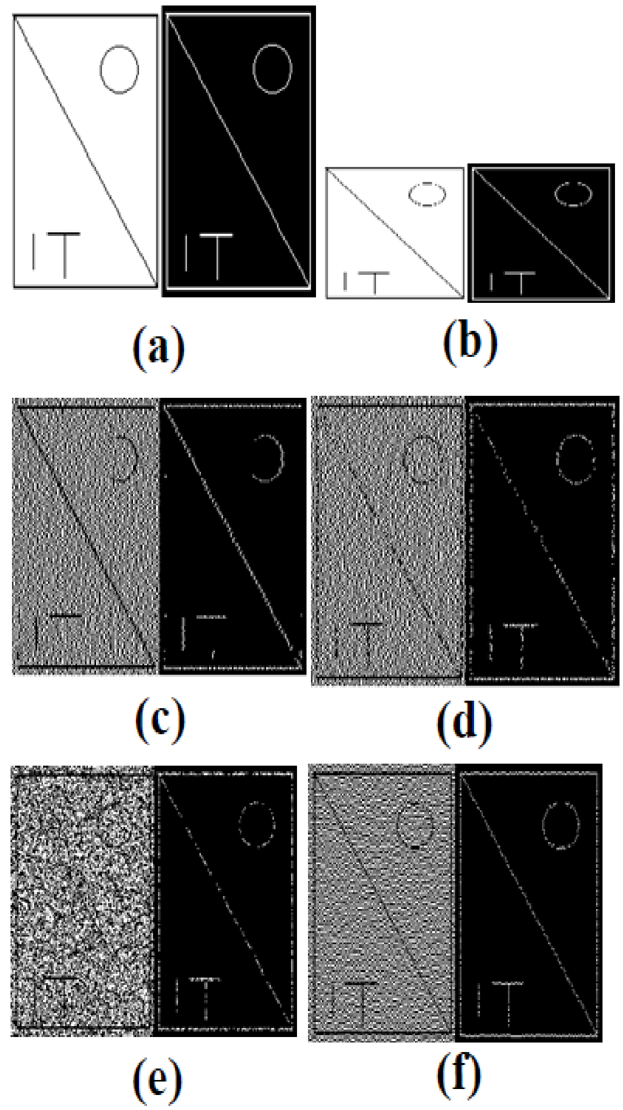

Figure 5: Comparison of all techniques, whereas the horizontal lines of thickness 2 pixels: **(a)** the secret image (SI) with size 256×202, **(b)** the resized image with size 256×102, **(c)** ME-SIVCS-1, **(d)** ME-SIVCS-2, **(e)** P-SVICS, **(f)** our Construction 1.

The second construction (has not been introduced in any published paper so far) encrypts a vertical block of three pixels (⊟). $b = 0, 1, 2, 3$ represents the number of black pixels in this block. The construction is a mixture of D-SEVCS and P-SIVCS. The construction can be divided into two steps.

Step – I: Every block of 3 pixels in SI is converted to a block of 3 pixels in the converted secret image (CSI). Three techniques are used.

Construction 2(a). A block has one black (white) pixel. This black (white) pixel may be the upper pixel (), middle pixel (), or lower pixel (). Convert these three cases to a block that has only one black (white) pixel in the lower position. In other words, for $b = 1$ the situations for the block of 3 pixels are (, , and). Convert these three situations to the block () in the CSI. For $b = 2$, convert (, , and) to ().

Construction 2(b). This technique (construction 2(b)) is similar to construction 2(a), but the black (white) pixel is in the upper position of the new block in CSI. In other words, convert (, , and) to (), and (, , and) to ().

Construction 2(c). In this technique, the black (white) pixel is the middle pixel of the block in the CSI. In other words, convert (, , and) to (), and (, , and) to ().

In the above construction 2(a-c), the block, $b = 0, 3$ (and) remains unchanged. The construction 2(a-c) is summarized in Figure6.

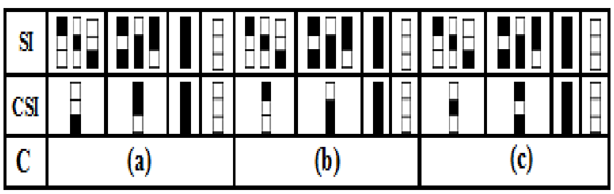

Figure 6: Construction 2(a-c): The top row represents the blocks in the secret image (SI) that are converted into blocks in the converted secret image (CSI) (second row from top). Construction 2(C) (a-c).

Step – II: For simplicity, in this step, only Construction 2(a) will be introduced; the other techniques are similar. CSI for Construction 2(a) has the upper pixel and middle pixel are both white or both pixels are black, third pixel is white or black. To encrypt the block of three pixels, if the upper and middle are white (black) randomly permute the columns of the matrix $S^0 = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$ ($S^1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$), and distribute two subpixels to each share. The third pixel (lower pixel) will be encrypted according to P-SIVCS. Then the share matrices collections W, W_b, B_w, and B are as follows.

$$W = \left\{ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix} \right\}$$

$$W_b = \left\{ \begin{bmatrix} 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix} \right\}$$

$$B_w = \left\{ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \right\}$$

$$B = \left\{ \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \right\}$$

To encrypt a block in the CSI, for $b = 0, 1, 2$, and 3, select a matrix randomly from W, W_b, B_w, and B, respectively. Distribute a first row for a share and a second row for the other share.

Construction 2(a-c) are shown in the images of Figures 7-9(d-f) respectively.

Theorem 3. *Construction 2(a-c) satisfy the security condition.*

Proof. The proof is for Construction 2(a); Construction 2(b-c) can be proved similarly.

Let λ^w be the set of all submatrices in W. According for the definition of security condition in section 2.2, it is enough to prove $\lambda^w = \lambda^{w_b} = \lambda^{B_w} = \lambda^B$.

$\lambda^w = \{[1\ 0\ 1], [1\ 0\ 1], [0\ 1\ 1], [0\ 1\ 1], [1\ 0\ 0], [1\ 0\ 0], [0\ 1\ 0], [0\ 1\ 0]\} = \lambda^{w_b} = \lambda^{B_w} = \lambda^B$. All the sets are equal, and then, Construction 2(a) satisfies the security condition.

□

4 Experimental results and Discussion

Figures 7-9 (b), (c), (d), (e), and (f) represent ME-SIVCS-2, Construction 1, Construction 2(a-c), respectively, and Figures 7-8 (g) and (h) are P-SIVCS and VCRG respectively. The best visual quality is seen in Figure 7(c), which shows our Construction 1, and the second best visual quality is seen in Figure 7(d), which shows more details than Figure 7(b). The visual quality of Figure 7(d)-(e) is better than that of Figure 7(f), in spite of their variance being equal (see Table 2). The reason for this is spatial variance. In Construction 2(a-b) , two attached pixels are encrypted together and one pixel is encrypted alone. Conversely, in construction 2(c), two pixels that are not attached, the upper and the lower pixel, are encrypted together while the middle pixel that separates them is encrypted alone. Therefore, the visual quality can be effected by spatial variance, where in Construction 2(a-b) the spatial variance is less than in Construction 2(c).

Let s_1, s_2, and s_3 (w_1, w_2, and w_3) be the number of blocks that have only one black (white) pixel in the upper, middle, and lower position in the block, respectively (see table 3). In construction 2(a), if $b = 1$ in a block, the black pixel is moved to the lower position in the block. In contrast, in Construction 2(b) the black pixel is moved to the upper position in the block.

A question can raise: Can step I in construction 2 change details in SI dramatically? The answer approximately no, The change is slight. Numerically,

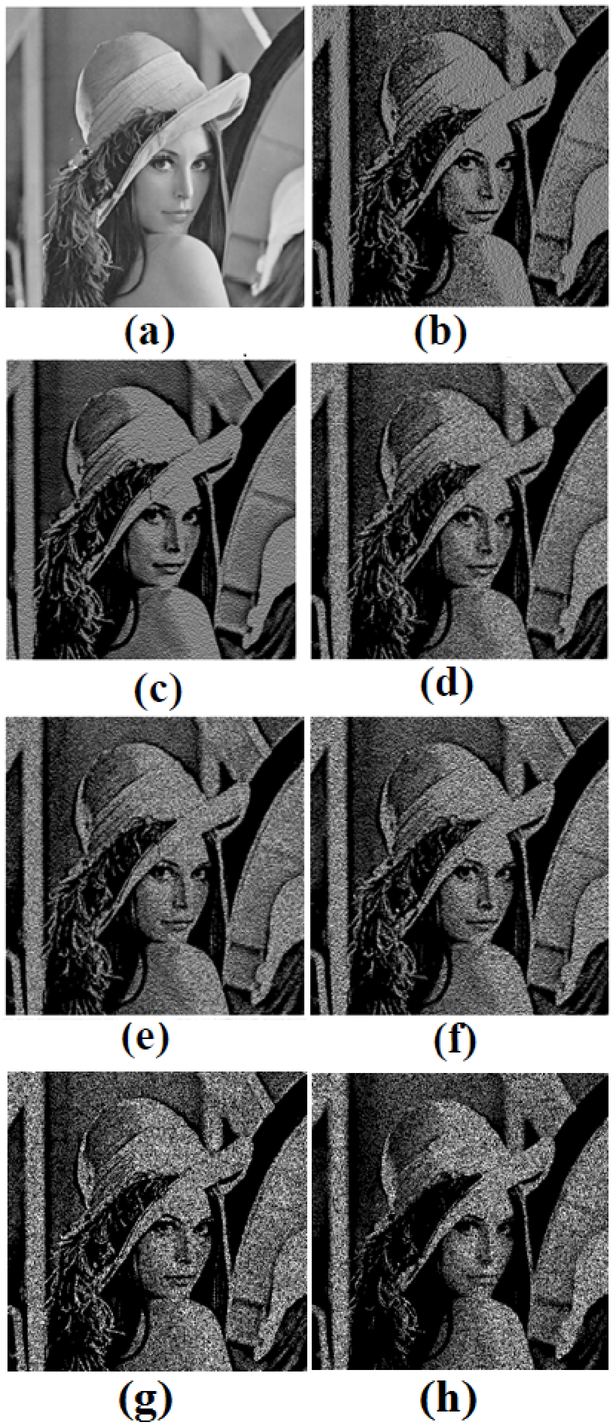

Figure 7: Comparison of all methods: **(a)** SI, **(b)** ME-SIVCS-2, **(c)**our Construction 1, **(d)-(f)** represent Construction 2(a-c), respectively,**(g)** P-SIVCS, **(h)** VCRG.

if the Construction 2(a), Construction 2(c), and Construction 2(b) will be employed for Figures7, 8, and9, then 0.06%, 0.009% and 0.01% of pixels in SI will be move one pixel or two pixels respectively. The distortion 0.009-0.06% may be preferable compared with the disadvantages of other methods. Visually, in Fig.

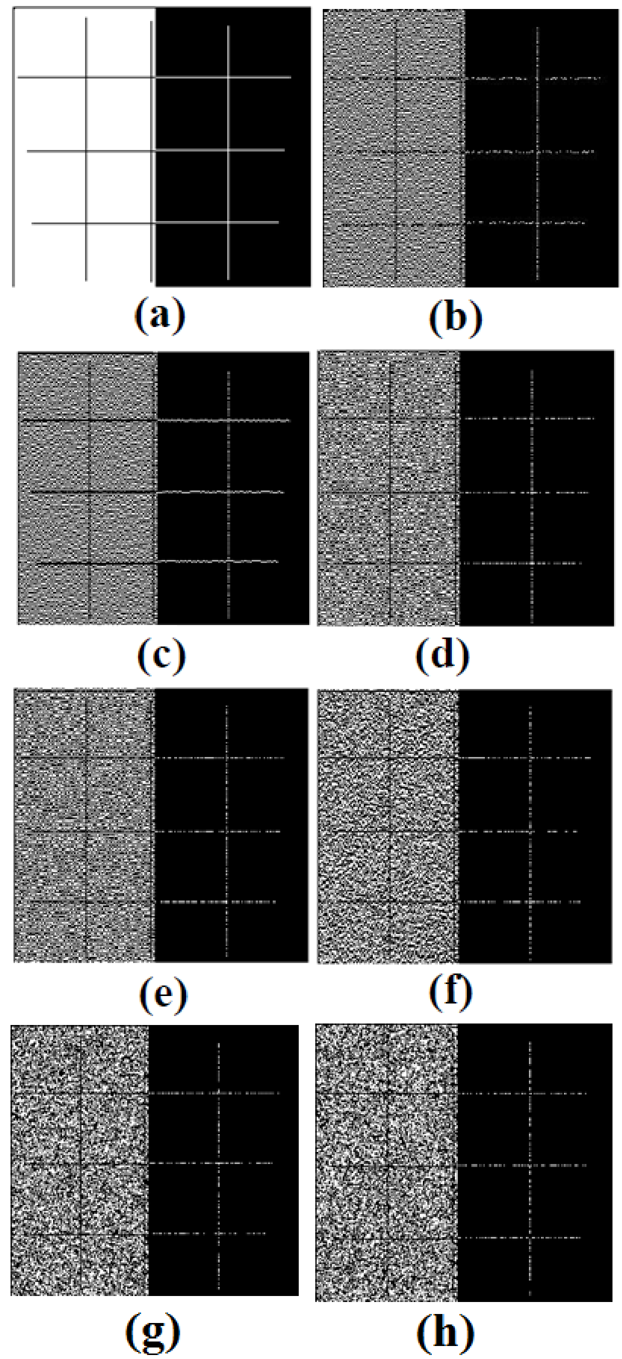

Figure 8: Comparison of all methods: **(a)** SI, **(b)** ME-SIVCS-2 ,**(c)** our Construction 1, **(d)-(f)** represent Construction 2(a-c), respectively, **(g)** P-SIVCS, **(h)** VCRG.

7-8(d-f) nearly no effect of step I on SI and Figure9(e-f) show a slight change in the circle in the half black background.

The results shown in Figures (7-9)(d) are slightly better than those in Figures (7-9)(e). Since $s_1 < s_3$, the distortion that is generated when moving a black pixel in Construction 2(a) is less than that produced by Construction 2(b).

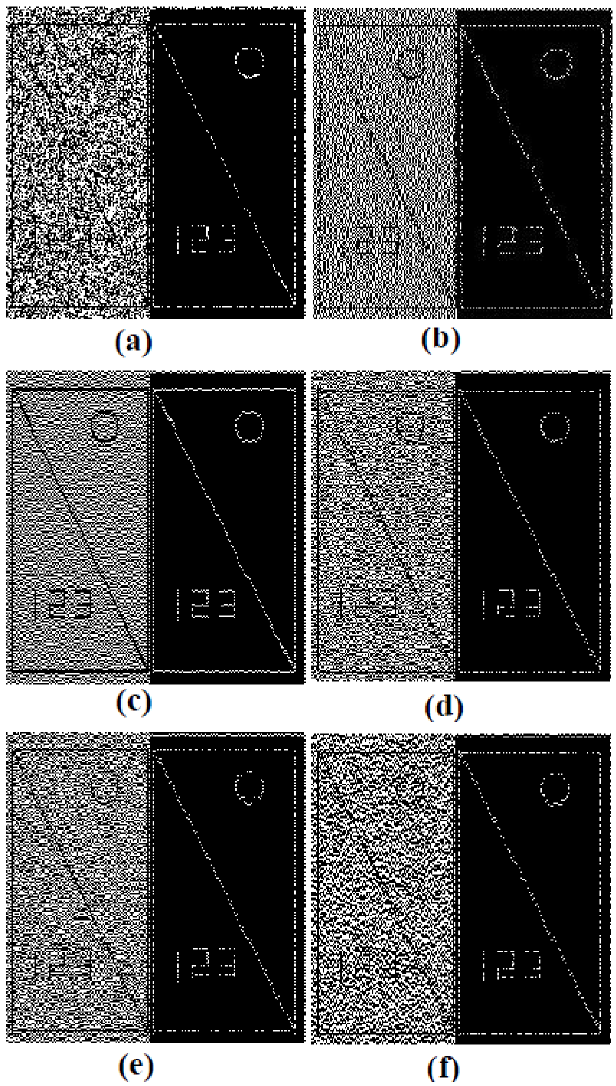

Figure 9: Comparison of all methods: **(a)** P-SIVCS,, **(b)** ME-SIVCS-2 **(c)** our Construction 1, **(d)-(f)** represent Construction 2(a-c), respectively.

An analysis of the SI properties can help determine the best method of encryption. Apparently, if the SI is simple (see Figure 8), then the best method is one of the sub-construction 2(a-c) that does not suffer from TLP-1 to TLP-4. For a SI such as that in Figure 7, the best construction for encryption is Construction 1 and the second best is Construction 2(a). However, an SI that has several horizontal, vertical, shapes, numbers and characters, and lines of varying thinness, such as that in Figure 9, is critical. In this case, we have to scarify by accepting TLP-4 in quality or accepting one of the problems partially. If the thinness of a horizontal line is not essential or horizontal lines have thickness > 1, then the best method is Construction 1. If the partially poor visual quality

Table 2: Comparison of our constructions and other constructions based on variance and thin line problems

Method	Block Size	Variance=$\sigma_{m,b}$	Thin Line Problems.
P-SIVCS	2	$\sigma_{2,0} = 0.5,\ \sigma_{2,1} = 0.25,$ $\sigma_{2,2} = 0$	TLP-1
ME-SIVCS-2	2	$\sigma_{2,0} = 0,\ \sigma_{2,1} = 0.25,$ $\sigma_{2,2} = 0$	TLP-3 & partially TLP-2
Construction 1	2	$\sigma_{2,0} = 0,\ \sigma_{2,1} = 0,$ $\sigma_{2,2} = 0$	partially TLP-4
Construction 2(a)	3	$\sigma_{3,0} = 0.25,\ \sigma_{3,1} = 0,$ $\sigma_{3,2} = 0.25,\ \sigma_{3,3} = 0$	partially TLP-1
Construction 2(b)	3	$\sigma_{3,0} = 0.25,\ \sigma_{3,1} = 0,$ $\sigma_{3,2} = 0.25,\ \sigma_{3,3} = 0$	partially TLP-1
Construction 2(c)	3	$\sigma_{3,0} = 0.25,\ \sigma_{3,1} = 0,$ $\sigma_{3,2} = 0.25,\ \sigma_{3,3} = 0$	partially TLP-1

Table 3: Analysis of s_1, s_2, s_3 and w_1, w_2, w_3.

Figure	s_1	s_2	s_3	w_1	w_2	w_3	Comparison
Figure 7	4639	5051	4662	3895	4240	3806	$s_1 < s_3, w_1 > w_3$
Figure 8	120	106	217	108	103	114	$s_1 < s_3, w_1 < w_3$
Figure 9	194	96	235	203	101	132	$s_1 < s_3, w_1 > w_3$

in the white background area is not important, then P-SIVCS or Construction 2(a-b) depend on $s_1 < s_3$ or $s_1 > s_3$, respectively.

5 Conclusion

The thin line problem is critical in the encryption of an SI that has a map, characters, or shapes. In this paper, two constructions were adopted. In the first construction (Construction 1), TLP-1 to TLP-3 were avoided, and the construction suffers partially from TLP-4 only when the SI has a horizontal line of the thickness of 1 pixel. However, when all the horizontal lines have a thickness of more than 1 pixel, the construction does not suffer from TLP-4. The second construction includes three sub-constructions, a-c. Construction 2(a) and Construction 2(b) suffer partially from TLP-1. Researchers mentioned there might be no perfect solution for the thin line problem in secret image [5]. Finally, in the thin line problem, the analysis of the SI properties is essential for finding the best construction for encryption. Future work will extend the above two constructions in color and gray images. Also, utilize the meaningful images in Thin line Problem.

References:

[1] M. Naor, A. Shamir, Visual Cryptography. De Santis, A. (ed.) EUROCRYPT, LNCS, 950, 1994, pp. 1–12.

[2] C. N. Yang, New Visual Secret Sharing Schemes Using Probabilistic Method, *Pattern Recogn. Lett.*, 25, 2004, pp. 481–494.

[3] X. Yan, S. Wang, X. Niu, C. N. Yang, Generalized Random Grids-Based Threshold Visual Cryptography with Meaningful Shares, *Signal Processing*, 109, 2015, pp. 317-333.

[4] C. Y. Hou, S. F. Tu, A Visual Cryptographyic Technique for Chromatic Images Using Multi-Pixel Encoding Method, *J. of Res. and Prac. in Info. Technol.*, 37(2), 2005, pp. 179–191.

[5] L. Feng, G. Teng, W. ChuanKun, Q. Lina, Improving the Visual Quality of Size Invariant Visual Cryptography Scheme, *J Vis. Commun. Image R.*, 23, 2012, pp. 331–342.

[6] L. Feng, G. Teng, C. Wu, C. N. Yang, Flexible Visual Cryptography Scheme and Its Application, *Trans. on Data Hid. and Multi. Sec.*, 8363, 2014, pp. 110-130.

[7] G. Ateniese, C. Blundo, A. De Santis, D. R. Stinson, Extended Schemes for Visual Cryptography, *Theor. Comput. Sci.*, 250, 1996, pp. 1–16.

[8] S. J. Shyu, Image Encryption by Random Grids, *Pattern Recogn.*, 40, 2007, pp. 1014–1031.

[9] S. J. Shyu, Visual Cryptograms of Random Grids for Threshold Access Structures, *Theor. Comput. Sci.*, 565, 2015, pp. 30-49.

[10] S. J. Shyu, K. Chen, Visual Multiple Secret Sharing Based Upon Turning and Flipping, *Info. Sci.*, 181, 2011, pp. 3246–3266.

[11] S. J. Shyu, Visual Cryptograms of Random Grids for General Access Structures, *IEEE Trans. Circuits Syst. Video Technol.*, 23(3), 2013, pp. 414–424.

[12] C. N. Yang, C. C. Wua, D. S. Wang, A Discussion on the Relationship Between Probabilistic Visual Cryptography and Random Grid, *Info. Sci.*, 278, 2014, pp. 141–173.

[13] C. Y. Hou, S. F. Tu, Visual Cryptography Techniques for Color Images Without Pixel Expansion, *J Info. Technol. Soc.*, 1, 2004, pp. 95–110.

[14] S. Cimato, R. De Prisco, D. De Santis, Colored Visual Cryptography Without Color Darkening, *Theor. Comput. Sci.*, 374, 2007, pp. 261–276.

[15] R. Ito, H. Kuwakado, H. Tanaka, Image Size Invariant Visual Cryptography, *IEICE Trans. on Fund. of Elec., Comm. and Comput. Sci.*, E82-A(10), 1999, pp. 2172–2177.

[16] T. Luft, C. Colditz, O. Deussen, Image Enhancement by Unsharp Masking the Depth Buffer, *Proc. of ACM SIGGRAPH*, 25(3), 2006, pp. 1206–1213.

[17] S. Cimato, C. N. Yang, Visual Cryptography and Secret Image Sharing, Taylor & Francis group, 2012.