Development of Secret Sharing Schemes for Visual Cryptography

Chapter II

Literature Review

2.1 Preamble

A comprehensive review of the related literature and research works presented from different perspectives in the area of VC is provided in this chapter. Generally, the basic scheme of VC was suggested by Noar and Shamir in 1994. It was applied for binary valued images. However, it suffered from some problems such as pixel expansion and lossy recovery. Therefore, many researchers have suggested some schemes to address such problems. Yet, not all the previous schemes have concentrated on binary valued images; every scheme concentrated on a specific type of images while others concentrated on more than one type.

The review of the related works is categorized based on the image formats under which different aspects of VC are discussed. Here, three categorizes related with the current study are presented as follows:

2.2 Binary Visual Cryptography

This type of VSS is concerned with some previous schemes of VSS that concentrated on binary valued images and addressed the problem of pixel expansion and lossy recovery.

Due to the use of pixel expansion, two types of VCS can be raised: the Deterministic VCS (DVCS) and the Probabilistic VCS (PVCS). The secret pixel can be represented by one and \( m \) subpixels in DVCS and PVCS respectively. Yang et al. [31] proposed a \((k, n)\)-PVCS on the basis of the \((k, n)\)-DVCS construction. In addition, it has another construction; it could be created by extending the \((k, k)\)-PVCS. Furthermore, the most attractive merit of this scheme is the pixel expansion problem has refuted. Nevertheless, the visual quality of
the retrieved image is destroyed because of performing OR operation for the reconstruction process.

Furthermore, so as to address the subpixels management, an Aspect Ratio Invariant VCSs (ARIVCSs) were proposed. The mechanism of some developed ARIVCSs be dependent on the addition of dummy subpixels to the shared images. In order to reducing the dummy subpixels number, ARIVCSs used a mapping pattern. However, the designing of a mapping pattern was a huge challenge of these methods. To face this challenge, an easy scheme has proposed by Yang et al. [32] to construct ARIVCS with the use of image filtering and resizing. It used a (Gaussian Low Pass Filter (LPF) with parameters- a 3×3 square matrix) to convert a binary image into gray level image. Halftoning function is applied as an image resizer with the VCS which can be indicated as \( R(\cdot) \rightarrow H(\cdot) \rightarrow V(\cdot) \) for the gray level image. Here, for the binary image, the halftoning function has to be modified as \( F(\cdot) \rightarrow R(\cdot) \rightarrow H(\cdot) \rightarrow V(\cdot) \). The filtering function \( F(\cdot) \) is used to convert a binary image into a gray level one. Moreover, the construction of this scheme is \((k, n)\)-ARIVCS with pixel expansion \((m)\). Subsequently, \((k, n)\)-VCS is applied to gain \(n\) shared images with size about \(x\sqrt{m} \times y\sqrt{m}\). This is to say that this scheme is expansible. Furthermore, it can be extended to another scheme called Arbitrary-Size VCS (ASVCS). Under the extended scheme, the shared images can be obtained with any size with keeping the AR unchanged. Here, it is to conclude that the ASVCS enjoying the same feature of the PVCS, i.e. the shared images and the reconstructed image have the same size of the original image. However, the contrast of the recovered image in the both schemes should be improved.

Recently, Lee and Chiu [33] proposed a systematic approach called Size Invariant VCS (SIVCS) to address the problems of VC. It is based on the PVCS and its contribution is to eliminate the using of codebook design. Since the use of codebook design leads to pixel expansion and make the display quality of retrieved images uncontrollable. Instead, it designed a set of column vectors in order to encode secret pixels. This is to say that the general construction of this approach is different from the PVCS construction which relies on the existing basic matrices of VCS whereas the SIVCS construction relies on \(n\)-tuple
Boolean column vectors. In other words, this approach has to rely on the following definition:

“The n-tuple Boolean column vector \( S = [s_j]^T \) with \( 1 \leq j \leq n \), is defined as an encoding pattern for each original pixel, where \( s_j = 0(1) \) indicates that the pixel is encoded as a white(black) shared pixel in share \( j \)”.

In spite of the fact that this approach solves the problems of pixel expansion and easy and low in complexity, the contrast of the recovered images is still uncontrollable.

With respect to the decryption process in VCS, the superimposing process can be done by using OR operation. Therefore, the traditional VCS can also be raised to as OR-based VCS (OVCS). However, the monotone property of OR operation destroys the display quality of recovered images in OVCS. Accordingly, XOR-based VCSs (XVCSs) have been proposed [34], [35] so as to enhance the visual quality by allowing participants to apply XOR operation for stacking purpose.

Yang and Wang [36] investigated the relation between OVCS and XVCS by providing a theoretical prove that the basic matrices of OVCS can be used in XVCS with \((k, n)\) general access structure. In other words, they provided a theoretical analysis to prove that the basic matrices in \((k, n)\)-OVCS also satisfy the security and contrast conditions of \((k, n)\)-XVCS. Meantime, the XOR operation enhanced the contrast to be \(2^{(k-1)}\) times. The following example supports their theoretical analysis.

Example: consider Tuyls et al.’s XVCS in [34], the \((4, 5)\)-XVCS with the following basis matrices:

\[
B_1 = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1
\end{pmatrix}
\]

\[
B_2 = \begin{pmatrix}
0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\
0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1
\end{pmatrix}
\]
Once XORing any four shares, every secret pixel is 4 blacks and 4 whites. This is to say that nothing can be seen. Furthermore, when all five shares XORed together, the original secret image is recovered again. That is because the secret black pixel is 8 and the secret white pixel is 8. Thus,

\[ \alpha_{\text{XOR}} = \frac{H(\text{XOR}(B_1|5))-H(\text{XOR}(B_0|5))}{M} = \frac{8-0}{8} = 1. \]

In this case, the original secret image is perfectly retrieved. However, the contrast of (4, 5)-XVCS is \( \alpha_{\text{XOR}} = \frac{8}{15} \). Let the (4, 5)-XVCS depending on OR operation, the contrast is \( \alpha_{\text{OR}} = \frac{1}{15} \). Thus, it is to observe that the OR operation degrades the recovered image.

Accordingly, XVCS is a suitable solution for poor image quality and alignment problems in VC system. Nevertheless, Ou et al. [37], mentioned that such defects remain to be continuing challenges on existing XVCS which can be represented in pixel expansion and meaningless shares. To fix these challenges, they introduced a XVCS with meaningful shares. Under this scheme, three algorithms were introduced. The basic algorithm was presented for improving the image quality, meantime refuting the pixel expansion by generating a \( 2^n \times n \) matrix \( M_n \) which was used for constructing (n, n)-XVCS. Under the following rules, \( M_n \) matrix is generated:

\[ M_n(i, 1:n) = de2bi(i - 1, n). \]

Here, the function \( de2bi(i - 1, n) \) converts a decimal \( i-1 \) into a row vector of \( n \)-bit, e.g., \( de2bi(2, 4) = [0,0,1,0] \), and \( de2bi(3, 5) = [0,0,0,1,1] \). Two sub-matrices with size of \( 2^{n-1} \times n \) are generated from the matrix \( M_n, M^n_{\text{odd}} \) and \( M^n_{\text{even}} \), respectively. In the second algorithm, a (n, n)-XVCS is constructed by using \( M_n, M^n_{\text{odd}} \) and \( M^n_{\text{even}} \) in such that \( M^n_{\text{odd}} \cup M^n_{\text{even}} = M_n \) and \( M^n_{\text{odd}} \cap M^n_{\text{even}} = \emptyset \). For each pixel in a binary secret image, either \( M^n_{\text{odd}} \) or \( M^n_{\text{even}} \) is adopted to construct two shares \( R_1 \) and \( R_2 \). Obviously, XOR operation is applied to recover the original secret image. Furthermore, in the third algorithm including the first and second algorithms, a cover image is used to produce (n, n)-XVCS with meaningful shares. However, this scheme has the advantages of no pixel expansion and the superior visual quality. According to the researcher’s point of view, in the previous VC schemes that concentrate on binary valued images, there is no a dire need to produce
meaningful shares due to the fact that VCS is unconditional secure and offers unbreakable encryption if a random-liked share includes truly random pixels.

In tracing to improvement of VCS, the concept of Random Grid (RG) is used to the pixel expansion avoidance as well as codebook designing. RG-based VCS received researchers’ attention. For binary secret image encryption based on RG, every secret image is reconstructed into two noise-like RG (shared images) with the similar size of the original one. Here, the decoding process pursues similar procedures occurred in conventional VCS.

_Kafri and Keren_ [38] are considered as the initiators of VSS scheme based on RG. In 1987, they suggested three distinct schemes for binary images. The idea of one of the suggested methods is to generate two random grids $R1$ and $R2$. Firstly, $R1$ is generated randomly with values belonging to $[0, 1]$. Secondly, on the basis of the value of each pixel $P$ in the secret image, the $R2$ can be generated under the following rules [39]:

\[
\begin{align*}
\text{if } & p(i,j) == 0 \\
R2(i,j) &= R1(i,j) \\
\text{else } & \\
R2(i,j) &= \neg R1(i,j)
\end{align*}
\]

Finally, two encoded grids $R1$ and $R2$ are generated with a similar size of the secret image. This is to say that this algorithm solves the pixel expansion problem faced in the conventional method of _Naor and Shamir_. In addition, RG-based VCS does not bolster $(k, n)$ threshold. To address this downside, _Chen and Tsao_ [40] presented $(k, n)$-VCS based on RG and Boolean operations.

It is significant that the merits of RG-based VCS involve no pixel expansion, improved contrast, and so on. Besides, the constraint of RG-based OVCS is that the background becomes darker. In other words, the OVCS cannot acquire whiteness when more shares are superimposed together since the monotone property of OR operation degrades the display quality of the recovered image. In spite of the fact that the XVCS is an alternative approach to fix the issue of RG-based OVCS and to obtain a better image quality, it is futile when a device having XOR operation is not available [41].
In contrast, VCS with multiple decryption has the merits of both OVCS and XVCS as it very well may be performed in extensive applications. X. Yan et al. [41] have proposed a VC scheme that integrates both RG-based OVCS and XVCS together to perform both OR and XOR operations at the decryption side. Under this scheme, two algorithms have been adopted: shared images construction and recovering of secret. In the first algorithm, conventional RG-based (2, 2)-VCS has been applied repeatedly \(k-1\) times. In addition, to make all shares equally important to each other, the generated \(n\) temporary bits are arbitrarily rearranged for corresponding \(n\) shared images bits. The second algorithm is designed to retrieve the secret image by applying OR or XOR operation. However, the visual quality should be improved especially when less than \(n\) shares superimposed together.

Arya k. et al. [42] have proposed a (2,2) VC scheme to enhance the quality of binary image by using the Simple Block Replacement (SBR) technique as a post processing stage. This scheme has focused on improving the visual quality of the retrieved image. At the same time, it neglects the pixel expansion problem. As being observed in this scheme, the pixel expansion \((m)\) is equivalent to 4 as used in the traditional VC in case of two-out-of-two scheme (4 subpixels). The differences between this scheme and two-out-of-two VC scheme (4 subpixels) can be presented as follows:

- In traditional VC, every white pixel is replaced by 2×2 block of both black and white pixels, whereas in this scheme, it is replaced by 2×2 block of only white pixels when the shares is stacked.
- Every black pixel is replaced by 2×2 block of only black pixels whereas in this scheme, it is replaced by 2×2 block of both black pixels and white ones.

For the decryption process, OR operation is used. In this scheme, after the secret image is recovered, the post processing stage is required to enhance the quality of the recovered image. Thus, SBR approach is used to convert the reconstructed image into fully blocks of black pixels and white ones. However, this scheme enhances the contrast of the retrieved image to be satisfied, but it has such drawbacks which can be represented in pixel expansion and computation cost which is because of the utilization of the post processing stage.
In the light of what has been discussed above, it is clear that there are diverse types of VC which can be described as follows:

- **DVCS**
  
The mechanism of DVCS relies on representing a secret pixel with \( m \) subpixels in the shared images. Due to that, the DVCSs are expansible. Furthermore, they suffer from the problem of lossy recovery.

- **PVCS**
  
  This type represents a secret pixel with only one pixel to be shared into \( n \) shared images. Thus, PVCSs are non-expansible. Due to using the OR operation for recovering purpose, the display quality of the retrieved images is degraded.

- **ARIVCS**
  
  ARIVCS deals with subpixels management to make an AR invariant. The main idea behind ARIVCS is that it relies on adding dummy pixels to the shared images. Thus, this type keeps the AR unchanged and make the recovering process of the original images occur with losing no information.

- **ASVCS**
  
  ASVCS is an extended type of ARIVCS, having the same features of PVCS. ASVCSs are non-expansible and they have a poor contrast drawback.

- **SIVCS**
  
  As a matter of fact, using codebook for shares generation creates two critical problems: pixel expansion and lossy recovery. This type, therefore, depends on \( n \)-tuple Boolean column vectors instead of using a codebook design. However, by eliminating the use of codebook design, the shared images are gained with the similar size of the original one. Nevertheless, SIVCSs face the problem of poor contrast.
- **OVCS**

OVCS refers to the schemes which perform the OR operation in the decryption process. Obviously, the recovered images are degraded because of the monotone property of OR operation.

- **XVCS**

XVCS is considered as an enhanced type of OVCS since it performs XOR operation rather than OR operation at the decryption process. The XOR operation allows complete recovering of secret image and increases the quality of the reconstructed image. Thus, XVCSs can recover the secret image with a quiet good visual quality.

- **RG-based VCS**

In this type, a secret image is shared into two noise-like RG with a similar size of the secret image. Decryption process can be done by applying OR or XOR operation. However, under this type, there is no pixel expansion and the contrast is related to the operation used at the decryption side.

2.3 **Halftone Visual Cryptography**

This category is concerned with HVC schemes that concentrated on halftoned images obtained by halftoning techniques. Halftoning is a technique of converting a gray-level image into a binary valued one. In general, HVC scheme refers to the method that embed the secret image into halftoned meaningful shares of the cover image. Meaningful shares are critically significant; if the effectiveness of shares management is increased, the suspicion of encrypted secret image is decreased. This is on the contrary to the conventional VC, under which the constructed shares are meaningless as they do not convey any visual information, which might affect the shares management. In other words, the suspicion of secret image encoding and the shares management affection might be gained when the shares carry noise-like information instead of meaningful information.

In general, HVC is considered one of the hiding information techniques such as a steganography technique. Yet, there are some differences. HVC scheme is used to embed a secret image into halftone shares with meaningful information of the cover images. Steganography is used to embed not only images but any secret message through different
It provides only one copy of a secret information, and this means that there is no way to retrieve it after being destroyed. HVC is, however, preferred as it is possible to have more than one copy of secret information.

Recently and before the advent of HVC, as one of the VC schemes, Extended Visual Cryptography (EVC) has introduced by Ateniese et al. to construct meaningful shares rather than noise-like shares through embedding the secret information into the visual information of the cover shares [43]. Unfortunately, the image quality of shares is low. Hence, to address this flaw, embedded EVC as one of the VC schemes has been proposed to generate meaningful shares with good enough quality. Liu et al. [44] have proposed embedded EVC scheme based on the special design of the dithering matrix by ‘y’ emending the SIPs into meaningful cover shares. Due to using dithering matrix, the shares might be carrying slight grid patterns. However, this scheme has failed to produce a high visual quality of shares since that the cover shares are darkened before halftoning process. To get hold of a better quality of shares with conveying visual information, HVC was presented by Zhou et al. [45] so as to embed secret image into shares on the basis of dithering.

Before reviewing the existing research works done by other researchers in the different perspectives on HVC, the principle idea of HVC can be illustrated through the simplest two-out-of-two HVC threshold scheme as appeared in figure (2.1).

2.3.1 Two-out-of-two HVC Scheme

In this scheme [45], the gray level image $GI$ is halftoned by ED filter to gain halftoned image $I$. The halftoned image $I$ is allocated to participant ‘1’ and the complementary image $I'$ is gained by reversing the halftoned image $I$; all black/white pixels in $I$ are reversed into white/black pixels in $I'$, and then, it is allocated into participant ‘2’ as observed in figure (2.1). Secret pixel $P$ must be encoded into a $Q1 \times Q2$ halftone cell in each of the two shares, and to do this, only two pixels ought to be altered as the SIPs in each halftone cell. These two SIPs must also be in the similar positions in the two shares as pixels $A$ and $B$ in figure (2.1). If $P$ is white, a matrix $M$ is arbitrary chosen from the collection of matrices $C_0$ of traditional VC. If $P$ is black, it is arbitrary chosen from $C_1$. The
SIPs in the $i^{th}$ share is replaced by the two subpixels in the $i^{th}$ row of the chosen matrix as observed in figure (2.1).

![Diagram](image)

**Figure (2.1):** Construction of a two-out-of-two HVC scheme with cell size is $Q = 4$ [45].

Since $C_0$ and $C_1$ are the collections of basic matrices in traditional VC, these pixels which carry the encoded secret are called modified pixels whereas the other pixels in the halftone cell which have not been modified are referred to as the ordinary pixels. It can also be found that if $P$ is white, one out of $Q_1Q_2$ pixels in the reconstructed halftone cell, which is obtained by superimposing the two encoded halftone cells, is white while all other
pixels are black and if \( P \) is black, all pixels in the reconstructed halftone cell are black. Thus, the contrast condition is satisfied and the secret pixel can be visually decoded with contrast \( (1/Q_1 Q_2) \).

However, proposing a HVC scheme by Zhou et al. [45] has provided a better visual quality than the EVC does. Yet, it is computationally expensive due to the fact that it inserts the SIPs into pre-existing uncoded halftone shares. Furthermore, in using this scheme, a pair of complementary shares is required to prevent the share visual information shown in the decoded image. That is to say that some participants may store more than one share, which may lead to increasing the suspicion of secret image encoding and the bandwidth.

Furthermore, Wang et al. [46] have proposed HVC method to improve the image quality of the halftone shares and completely remove the cross interference of the share images on the reconstructed image. This method has an ability to concurrently halftone grayscale images and encode the secret information into the halftone images instead of modifying halftone images to encode secret information. Generally, in this proposed method, the pixels that carry the secret image information are predetermined before the generation of halftone shares. These pixels are, then, naturally embedded into the halftone shares when the grayscale images are halftoned. In this method, the ED is utilized as the halftoning algorithm to generate halftone shares since it is able to generate a visually pleasing halftoned image with a simple computation. As the location of the SIPs is determined by using the image feature of the key complementary pair, the location of the SIPs on other shares are randomly distributed, and this results in producing a poor visual quality.

To address this limitation, Devi [47] proposed a global optimization approach across all halftone shares. Based on the void and cluster algorithm, the optimization method jointly rearranges the pixels of the \( n \) shares in order to obtain better overall visual quality of the \( n \) shares. Without the loss of generality, the shares 1 and 2 are assumed as the key complementary pair among the \( n \) halftone shares. Then, the visual quality optimization can be performed on the \( 3^{rd}, 4^{th}, ..., n^{th} \) shares successively.
Moreover, Alex and Anbarasi [48] applied various techniques of ED such as classical fixed, edge enhancement, green noise, and block ED to improve the image quality of the halftone shares. The quality of the halftone shares is enhanced by using Floyd-Steinberg and Jarvis ED filters.

In order to avoid the distortion and enhance the visual quality of halftone shares, X. Yan et al. [49] proposed a HVC scheme with minimum and homogeneously distributed Auxiliary Black Pixels (ABPs). This scheme is designed on the basis of conventional VCS and the binary secret image is encoded into the halftone shares. The access structure of this scheme is a (k,n), through embedding prefixed in parallel and maximally separating SIPs into meaningful shares in the halftoning process of the cover images by ED. Nevertheless, while it provides a good visual quality, the problem of share’s cross interference still unsolved. Unlike the schemes discussed above, the HVC scheme proposed by Kumar et al. [50] is based on EVC using ED filters for halftoning purpose. The secret and cover images are both in a gray-level form. In this scheme, the pixel expansion is three times as big as the secret image, which leads to consuming storage and difficult handling issues.

In the light of the schemes reviewed, it is apparent that the poor visual quality, large pixel expansion, and the interfering of the recovered image with shared images or cross interference from the shared images are as yet the primary issues debated in the HVC.

2.4 Gray level and Colored Visual Cryptography

Recently, many VCSs have been proposed to deal with gray level and color images. The application of the VC schemes to gray level and color images is very vital area of research due to their high popularity and the extensive range uses while contrasted with different kinds of image. Some of those proposed schemes applied to gray level and colored images are reviewed as follows:

Lukac and Plataniotis [51] proposed a B-bit secret sharing scheme to be utilized to both gray-level and color images. This scheme is implemented by decomposing a secret gray-level image into 8 bit-planes where every bit-plane is processed as a binary image. At that point, each binary image is encrypted into two shared images using the concept of traditional VC. After that, by combining the binary shared images, two gray-level shared images are obtained. Finally, the original secret image is retrieved when the two gray-level
shared images are decomposed into 8 bit-planes, respectively. Here, the secret image can be retrieved without degradation, but the shared images are expanded and this is an indication of the problem of pixel expansion.

Shyu [52] proposed a VSS method to deal with binary, gray-level, and color images based on the RG concept suggested by Kafri and Keren [38]. In the first stage of this scheme, random images with values fitting to [0, 1] are generated. Then, two random images with the similar size of the original one are obtained. This method refutes the pixel expansion whereas the recovered image is destroyed.

Moreover, a progressive VC scheme was proposed by Fang [22]. This scheme encodes an expanded secret and a cover image into $n$ meaningful shared images. By superimposing only two shared images, the recovered image is destroyed. Otherwise; in case of stacking all shared images, the recovered images can be obtained without degradation. Whatever, the pixel expansion problem is as yet unaddressed.

In addition, Chen and Tsao [53] proposed two RG algorithms. Under these methods, the secret image is recovered clearly when only more shared images are superimposed together.

Mishra and Gupta [54] proposed a (2,2) ProbVSS scheme using the threshold concept. Under this scheme, two algorithms have been designed and applied on such kind of images like binary, gray level, and color images. In these designed algorithms, the authors experimentally set the threshold value $T$ to be equal to 128 in case of gray level images. The shares generation phase is based on generating a random share with values belonging to [0,256], and second share is generated according to the following rules:

$$
\text{if } P(i,j) \leq T \\
S2(i,j) = S1(i,j)
\text{ else } \\
S2(i,j) = S1(i,j) \oplus I(i,j)
$$

(2.2)

Where $P$ denotes the pixel value of the original image, and $S2$, $S2$, and $I$ indicate the first share, second share, and original image respectively, and $\oplus$ indicates the XOR.
operation. The difference between these algorithms is in the reconstruction phase. The former requires XOR operation whereas the latter requires OR operation.

Since the pixel expansion is removed in this scheme, the retrieved image is not exactly the same as the original one in terms of contrast. As a matter of fact, using the threshold is useful to remove unimportant pixel information, but it affects the resolution of the revealed image. To improve the security of the VC, some methods have merged between the VC and the cryptography concepts.

For instance, *Yadar and Ojha* [55] proposed a scheme on the basis of Caser Cipher algorithm and the concept of RG for gray-level images. In this method, the constructed shares have a similar size of the original image and the retrieved image is lossless.

Moreover, *Shetty and Abraham* [56] proposed a VC scheme and applied it to both binary and color images. It is executed in four phases. In the first phase, the traditional VC concept is used to generate two shares from the secret image after being converted to binary-valued image. In the second phase, the public key generation of RSA algorithm is performed to generate a key and, by applying the RSA encryption procedure, the generated key is used to encrypt the generated shares in the first phase. In the third phase, the RSA encryption procedure is used to decrypt the encrypted shares of phase two. Finally, the final generated shares of the third phase are XOR-ed together so as to recover the secret image. Here, the generated shares and the recovered image have a similar size of the original one. Yet, the retrieved image is lossy and the use of the RSA algorithm leads to time consumption.

To ensure a confidentiality of image transmission, *Shankar & Eswaran* [57] have proposed a (2, 2) VC scheme with a combination of AES algorithm. This combined scheme is designed to secure color images that can be transmitted over a public channel. Four stages are involved in this scheme. First stage is to create three separated matrices (Rᵢ, Gᵢ, Bᵢ) from the original image in order to generate two shares (R₁ R₂, G₁ G₂, B₁ B₂), respectively, from every separated matrix by dividing every value by 2. Thereafter, XOR operation is applied between a key matrix which is randomly generated with values belonging to [0, 255] and every generated share in order to have six generated shares (Rs₁ Rs₂, Gs₁ Gs₂, Bs₁ Bs₂). Finally, in this stage, two shares (share₁ & share₂) are generated by combine (Rs₁,
Gs₁, Bs₁) and (Rs₂, Gs₂, Bs₂), respectively. In the second stage, the generated shares of first stage are being encrypted by applying AES algorithm as final shares. Regarding recovering the original image, shares decryption in the third stage is performed by using the correct secret key and the reverse processes of the stage two. Sequentially, perform the fourth stage which is the reverse of first stage processes. Whatevsoever, AES algorithm requires more processing and more key rounds. Also, each round in the AES algorithm needs round key from the key expansion algorithm. On the whole, when the size of images increases, the time of applying this scheme also increases.

Furthermore, Shankar & Eswaran [58] have proposed an Elliptic Curve Cryptography (ECC) based VSS scheme in order to be applied on RGB images. In their scheme, the RGB image pixels are extracted to be represented as R, G, and B matrices with the similar size of the original one. Then, n shares are being created from the extracted pixels depending on the user’s need. Based on the required number of shares, basic matrices should be constructed. Thereafter, the created shares are divided into blocks to be double encrypted by using ECC. Here, it should be noted that a random key is generated on the basis of the block size of the secret image which usually can be 4×4 or 8×8. By implementing the reverse processes, the original image is recovered. Regardless that this scheme is secured, it requires additional verification of the public key to be performed. Otherwise, the quality of the retrieved image has to be enhanced. In addition, it is more complex and more difficult to be implemented since it is ECC-based VSS scheme.

Here, it is worth noting that the classical Hill Cipher algorithm is not used with VSS. It is only Chen [59] who uses a linear equation Hill Cipher to construct two sub-images in his VSS method proposed for gray-level images. In this method, the RG concept is utilized to the two sub-images to generate the final shared images. To retrieve the original image, the reverse process is applied with the invers Hill Cipher. Here, the recovered image is lossless. Yet, one of the problems faced in using classical Hill Cipher in Chen [59] method is that the invers of matrix may not exist due to which decryption will not be possible [60].

Approximately, the schemes discussed above have various problems such as pixel expansion, image distortion, time and storage consumption, and weak security.
2.5 Chapter Summery

In this chapter, the previous studies on VC have been presented and categorized into three categories. While the first category (binary VC) has dealt with VCSs that concentrated on binary images, the second (HVC) and third (gray level and colored VC) have dealt with halftoned images, gray level and color images, respectively. In addition, different aspects such as pixel expansion, contrast, storage and transmission bandwidth, and security have been discussed in order to find out the problems which can be listed below:

1. Based on the related works on binary VC, it is noted that the pixel expansion leads to increase the storage and transmission bandwidth. Moreover, the relevance between the pixel expansion and the contrast is clearly important in determining the optimality of VCSs, where the pixel expansion is used, the poor contrast is. Hence, there is a dire need to design an optimal VCS with an ability to minimize/refute the pixel expansion and maximize the contrast simultaneously.

2. According to the previous studies presented under the second category, some issues such as large pixel expansion, interference of secret image on shared images, interference of shared images on recovered image, and poor visual quality should be given more concern.

3. The brief related works of gray level and colored VC show the necessity for developing an effective scheme to improve the problems mentioned before and create a balance between security, time and storage cost, and performance.

Moreover, the use of classical Hill Cipher algorithm in VC to provide a more security gives rise to some important problems such as:

- The non-invertible key matrix is the main demerit of Hill Cipher due to which the encrypted share cannot be decrypted.
- The linear feature of Hill Cipher can make it succumb to Known-plaintext-attack.
Due to using only one key, Hill Cipher is weak against the brute-force attack and the secret can be revealed when the key is hacked.

Therefore, the security of the classical Hill Cipher should be improved by addressing the problem of non-invertible key matrix and preventing any hacker to obtain any secret information by producing a new key procedure as it is difficult to be predicated and exposed to the hackers.

To sum up, the VC problems and issues mentioned before may create some difficulties for different applications of VC. Owing to these difficulties, the overall potential for the VC practical applications will be reduced. Therefore, the present study aims at providing optimal and secured schemes to increase the uses of VC in wider applications.