A Comprehensive Study of Visual Cryptography

Jonathan Weir and WeiQi Yan

Queen's University Belfast, Belfast, BT7 1NN, UK

Abstract. Visual cryptography (VC) is a powerful technique that combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. VC takes a binary image (the secret) and divides it into two or more pieces known as shares. When the shares are printed on transparencies and then superimposed, the secret can be recovered. No computer participation is required, thus demonstrating one of the distinguishing features of VC. VC is a unique technique in the sense that the encrypted message can be decrypted directly by the human visual system (HVS). In this survey, we will summarize the latest developments of visual cryptography since its inception in 1994, introduce the main research topics in this area and outline the current problems and possible solutions. Directions and trends for future VC work shall also be examined along with possible VC applications.

1 Introduction

Visual cryptography is a powerful technique which combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. A binary image can be divided into shares which can be stacked together to approximately recover the original image. A secret sharing scheme enables distribution of a secret amongst n parties, such that only predefined authorized sets will be able to reconstruct the secret. The secret, in terms of visual cryptography can be reconstructed visually by superimposing shares.

Visual cryptography allows the transmission of visual information and many aspects of this area are covered, including its inception to the current techniques being employed and actively researched today. This survey covers the progress of VC, along with the current trends and the various applications for VC.

Having the ability to hide information such as personal details is very desirable. When the data is hidden within separate images (known as shares), it is completely unrecognizable. While the shares are separate, the data is completely incoherent. Each image holds different pieces of the data and when they are brought together, the secret can be recovered easily. They each rely on one another in order to obtain the decrypted information. There should be no way that anyone could decipher the information contained within any of the shares. When the shares are brought together, deciphering is possible when the shares are placed over one another. At this point, the information becomes instantly available. No computational power is required at all in order to decrypt the information. All decryption is performed by the human visual system (HVS). This kind of problem is formally referred to as a secret sharing problem.

Y.Q. Shi (Ed.): Transactions on DHMS V, LNCS 6010, pp. 70–105, 2010.

Secret sharing using visual cryptography is different from typical cryptographic secret sharing. The latter allows each party to keep a portion of the secret and provides a way to know at least part of the secret, while the former strictly prohibits it. Encryption using multiple keys is a possible solution. However this solution requires a large number of keys, therefore the management of such a scheme becomes troublesome, as demonstrated by Shamir.

In 1979, Adi Shamir published an article titled "How to share a secret" [1]. In this article, the following example was used to describe a typical secret sharing problem:

> "Eleven scientists are working on a secret project. They wish to lock up the documents in a cabinet so that the cabinet can be opened if and only if six or more of the scientists are present. What is the smallest number of locks needed? What is the smallest number of keys to the locks each scientist must carry?
>
> ...
>
> The minimal solution uses 462 locks and 252 keys per scientist."

In the paper, Shamir generalized the above problem and formulated the definition of (k, n)-threshold scheme. The definition can be explained as follows: Let D be the secret to be shared among n parties. A (k, n)-threshold scheme is a way to divide D into n pieces $D_1, \cdots, D_n$ that satisfies the conditions:

1. Knowledge of any k or more D_i pieces makes D easily computable;
2. Knowledge of any $k-1$ or fewer D_i pieces leaves D completely undetermined (in the sense that all its possible values are equally likely).

Visual cryptography is a new type of cryptographic scheme that focuses on solving this problem of secret sharing. Visual cryptography uses the idea of hiding secrets within images. These images are encoded into multiple shares and later decoded without any computation. This decoding is as simple as superimposing transparencies, which allows the secret to be recovered.

Visual cryptography is a desirable scheme as it embodies both the idea of perfect secrecy (using a one time pad) and a very simple mechanism for decrypting/decoding the secret. The interesting feature about visual cryptography is that it is perfectly secure. There is a simple analogy from one time padding to visual cryptography. If we consider the current popular cryptographic schemes, which are usually only conditionally secure, we can see that this is the second critical advantage of visual cryptography over other cryptographic schemes.

This survey is organized as follows: Section 2 details the very first form of visual cryptography and elaborates on the current work still being done in this area, specifically the most recent improvements. In general, these schemes primarily deal with binary images and noisy random shares. Extended forms of VC are also presented within this section which attempt to alleviate the suspicion of encryption within the shares. Section 3 concentrates on cheating prevention within VC along with cheating immune VC schemes. These schemes attempt to have some type of authentication or verification method which gives some clue as to the real hidden secret within a given set of shares. Grayscale, halftone and colour halftone images used in conjunction with visual cryptography are set forth in Section 4. Section 5 elaborates on multiple secret sharing, which involves sharing two or more secrets, typically within a set of two shares. Various applications of visual cryptography are analysed in Section 6 and the summary and future work are discussed within Section 7, along with the final conclusion.

2 Traditional Visual Cryptography

2.1 Basic Visual Cryptography

Image sharing is a subset of secret sharing because it acts as a special approach to the general secret sharing problem. The secrets in this case are concealed images. Each secret is treated as a number, this allows a specific encoding scheme supplied for each source of the secrets. Without the problem of inverse conversions, the digits may not be interpreted correctly to represent the true meaning of the secret.

Image sharing defines a scheme which is identical to that of general secret sharing. In (k, n) image sharing, the image that carries the secret is split up into n pieces (known as shares) and the decryption is totally unsuccessful unless at least k pieces are collected and superimposed.

Visual cryptography was originally invented and pioneered by Moni Naor and Adi Shamir in 1994 at the Eurocrypt conference. Visual cryptography is "a new type of cryptographic scheme, which can decode concealed images without any cryptographic computation" [2]. As the name suggests, visual cryptography is related to the human visual system. When the k shares are stacked together, the human eyes do the decryption. This allows anyone to use the system without any knowledge of cryptography and without performing any computations whatsoever. This is another advantage of visual cryptography over the other popular conditionally secure cryptography schemes. The mechanism is very secure and very easily implemented. An electronic secret can be shared directly, alternatively the secrets can be printed out onto transparencies and superimposed, revealing the secret.

Naor and Shamir's initial implementation assumes that the image or message is a collection of black and white pixels, each pixel is handled individually and it should be noted that the white pixel represents the transparent colour. One disadvantage of this is that the decryption process is lossy, the area that suffers due to this is the contrast. Contrast is very important within visual cryptography because it determines the clarity of the recovered secret by the human visual system. The relative difference in Hamming weight between the representation of white and black pixels signify the loss in contrast of the recovered secret. The Hamming weight is explained further at a later stage. Newer schemes that are discussed later deal with grayscale and colour images which attempt to minimize the loss in contrast [3] by using digital halftoning. Halftoning allows a continuous tone image, which may be made up from an infite range of colours or grays to be represented as a binary image. Varying dot sizes and the distance between those dots create an optical illusion. It is this illusion which allows the human eye to blend these dots making the halftone image appear as a continuous tone image. Due to the fact that digital halftoning is a lossy process in itself [4], it is impossible to fully reconstruct the original secret image.

The encryption problem is expressed as a k out of n secret sharing problem. Given the image or message, n transparencies are generated so that the original image (message) is visible if any k of them are stacked together. The image remains hidden if fewer than k transparencies are stacked together.

Each pixel appears within n modified versions (known as shares) per transparency. The shares are a collection of m black and white sub-pixels arranged closely together. The structure can be described as an $n \times m$ Boolean matrix S. The structure of S can be described thus: $S = (s_{ij})_{m \times n}$ where $s_{ij} = 1$ or 0 *i.f.f.* the j^{th} sub-pixel of the i^{th} share is black or white.

The important parameters of the scheme are:

1. m, the number of pixels in a share. This represents the loss in resolution from the original image to the recovered one.
2. α, the relative difference in the weight between the combined shares that come from a white and black pixel in the original image, i.e., the loss in contrast.
3. γ, the size of the collection of C_0 and C_1. C_0 refers to the sub-pixel patterns in the shares for a white pixel and C_1 refers to the sub-pixel patterns in the shares for a black pixel.

The Hamming weight $H(V)$ of the ORed m-vector V is interpreted by the visual system as follows:

A black pixel is interpreted if $H(V) \leq d$ and white if $H(V) < d - \alpha m$ for some fixed threshold $1 \leq d \leq m$ and a relative difference $\alpha > 0$.

The construction of the shares can be clearly illustrated by a 2 out of 2 visual cryptography scheme (commonly known as $(2, 2)$-VCS). The following collections of 2×2 matrices are defined:

$$C_0 = \{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,1\,0\,0 \\ 1\,1\,0\,0 \end{bmatrix}\}$$

$$C_1 = \{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1\,1\,0\,0 \\ 0\,0\,1\,1 \end{bmatrix}\}$$

Due to this pixel expansion, one pixel from the original image gets expanded into four pixels. The shares can be generated in the following manner:

1. If the pixel of the original binary image is white, randomly pick the same pattern of four pixels for both shares.
2. If the pixel of the original image is black, pick a complementary pair of patterns, i.e., the patterns from the same column in Figure 1.

When the transparencies are superimposed and the sub-pixels are correctly aligned, the black pixels in the combined shares are represented by the Boolean OR of the rows in the matrix. The pixels can be arranged in various ways

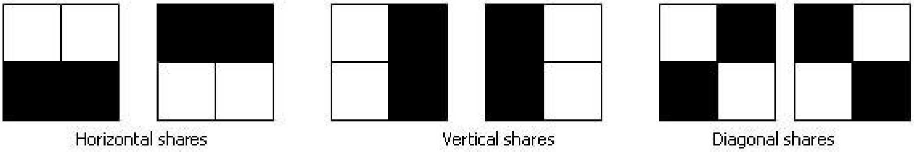
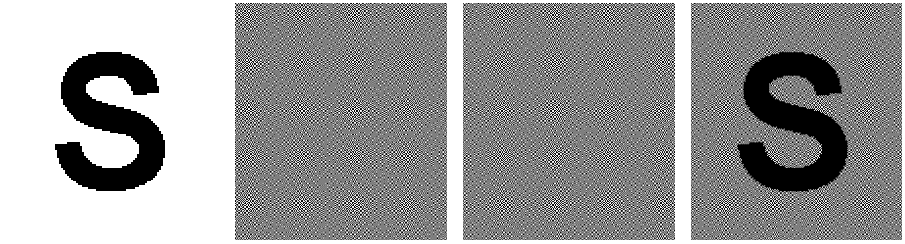


Fig. 1. The various types of pixel patterns used when creating VC shares

within the matrix. Visual representation of the different types of share patterns is present in Figure 1.

Because the individual shares give no clue into whether a specific pixel is black or white it becomes impossible to decrypt the shares, no matter how much computational power is available.

Below in Figure 2, the implementation and results of (2, 2)-VCS basic visual cryptography are shown. It displays the secret image, the two shares that are generated and the recovery of the secret after superimposing share one and share two.



(a) Secret Image (108 × 121) (b) Share 1, S_1 (216 × 242) (c) Share 2, S_2 (216 × 242) (d) Restored image, $S_1 + S_2$ (216 × 242)

Fig. 2. The results of a traditional visual cryptography scheme

2.2 Extended Visual Cryptography

An extended visual cryptography scheme (EVCS) proposed by Ateniese et al. [5] is based on an access structure which contains two types of sets, a qualified access structure Γ_{Qual} and a forbidden access structure Γ_{Forb} in a set of n participants. The technique encodes the participants in that, if any set, which is a member of the qualified access structure, are superimposed, then the secret message is revealed. However, for any set which is a member of the forbidden access structure and has no information on the shared secret, this means no useful information can be gleaned from stacking the participants. The main difference between basic visual cryptography and extended visual cryptography is that a recognizable image can be viewed on each of the shares; once the shares have been superimposed (provided they are part of the qualified access structure), the image on the shares will disappear and the secret message will be visible.

Extended visual cryptography schemes allow the construction of visual secret sharing schemes within which the shares are meaningful as opposed to having random noise on the shares. After the sets of shares are superimposed, this meaningful information disappears and the secret is recovered. This is the basis for the extended form of visual cryptography.

With EVCS, the first n shares need to be images of something like a car, boat or dog, some form of meaningful information. The secret message or image is normally the last to be dealt with $(n + 1)$. This requires a technique that has to take into consideration the colour of the pixel in the secret image we want to obtain, so when the n shares are superimposed, their individual images disappear and the secret image can be seen. In general, this can be denoted by $C_c^{c_1 \cdots c_n}$ with $c, c_1, \cdots, c_n \in \{b, w\}$, the collection of matrices from which we can choose a matrix to determine the shares, given c_i being the colour of the ith innocent image and c being the colour of the secret image. In order to implement this scheme, 2^n pairs of such collections, one for each possible combination of white and black pixels in the n original images need to be generated.

It is assumed that no information is known on the pixel values of the original image that is being hidden. The only thing that is known is that the pixels can be black or white. No probability distribution is known about the pixels. There is no way to tell if a black pixel is more likely to occur than a white pixel. Three conditions must be met when it comes to encrypting the images. Firstly, images that belong to the qualified set access structure, should, when superimposed, reveal the secret image. Secondly, by inspecting the shares, no hint should be available about what secret is hidden within the shares. Finally, the image within the shares should not be altered in anyway, that is, after the n original images have been encoded, they should still be recognizable by the user.

The simplest example is a $(2, 2)$-EVCS problem. The collections $C_c^{c_1,c_2}$ are obtained by permuting the columns of the following matrices:

$$S_w^{ww} = \begin{bmatrix} 1\,0\,0\,1 \\ 1\,0\,0\,0 \end{bmatrix} \quad \mathit{and} \quad S_b^{ww} = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,0 \end{bmatrix} \tag{1}$$

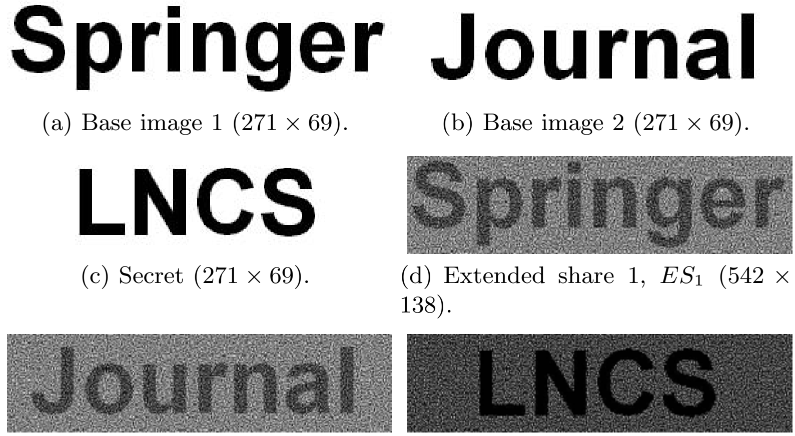
$$S_w^{wb} = \begin{bmatrix} 1\,0\,0\,1 \\ 1\,0\,1\,1 \end{bmatrix} \quad \mathit{and} \quad S_b^{ww} = \begin{bmatrix} 1\,0\,0\,1 \\ 0\,1\,1\,1 \end{bmatrix} \tag{2}$$

$$S_w^{bw} = \begin{bmatrix} 1\,0\,1\,1 \\ 1\,0\,1\,0 \end{bmatrix} \quad \mathit{and} \quad S_b^{bw} = \begin{bmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,0 \end{bmatrix} \tag{3}$$

$$S_w^{bb} = \begin{bmatrix} 1\,0\,1\,1 \\ 1\,0\,1\,1 \end{bmatrix} \quad \mathit{and} \quad S_b^{bb} = \begin{bmatrix} 1\,0\,1\,1 \\ 0\,1\,1\,1 \end{bmatrix} \tag{4}$$

It can also be verified that for a $(2, 2)$-EVCS, the contrast values achieved for both shares and the recovered secret image are all $\frac{1}{4}$.

Figure 3 provides an example of a $(2, 2)$-EVCS. As can be seen from the figure, two meaningful shares are generated from the base images. During this share creation, the secret is encoded between each of the shares. After superimposing



(a) Base image 1 (271 × 69).

(b) Base image 2 (271 × 69).

(c) Secret (271 × 69).

(d) Extended share 1, ES_1 (542 × 138).

(e) Extended share 2, ES_2 (542 × 138).

(f) Recovered secret $ES_1 + ES_2$ (542 × 138).

Fig. 3. The results of an extended visual cryptography scheme

each share, the secret is completely recovered while each shares meaningful information disappears.

In order to use this extended visual cryptography scheme, a general construction needs to be defined. Ateniese et al. [5] have devised a mechanism by which we can generate the shares for the scheme.

A stronger security model for EVCS is one in which the shares associated with a forbidden subset can be inspected by the user, meaning that the secret image will still remain totally hidden even if all n shares are previously known by the user. A systematic approach to fully address a general (k, n) problem was also proposed [6].

For each set of access structures, let $P = \{1, \cdots, n\}$ represent the set of elements called participants, and let 2^P denote the set of all subsets of P. Let $\Gamma_{Qual}/\Gamma_{Forb}$ be the collection of qualified / forbidden sets. The pair is called the access structure of the scheme. Any qualified set can recover the shared image by stacking its participants transparencies, while any forbidden set has no information on the shared image. This extension generalizes the original secret sharing problem by [2]. In [6], the authors propose a new technique to realize (k, n)-VCS, which is better with respect to the pixel expansion than the one proposed by Naor and Shamir. Schemes for improving the contract are discussed later.

Improving the shares quality [7] to that of a photo realistic picture has also been examined within extended visual cryptography. This is achieved using gray subpixels rather than black and white pixels in the form of halftoning.

2.3 Size Invariant Visual Cryptography

One of the first papers to consider image size invariant VC was proposed by Ito et al. [8]. As previously described, traditional visual cryptography schemes employ pixel expansion, although many have worked on how to improve this [9].

Ito's scheme [8] removes the need for this pixel expansion. The scheme uses the traditional (k, n) scheme where m (the number of subpixels in a shared pixel) is equal to one. The structure of this scheme is described by a Boolean n-vector $\mathbf{V} = [v_1, \cdots, v_n]^T$, where v_i represents the colour of the pixel in the i-th shared image. If $v_i = 1$ then the pixel is black, otherwise, if $v_i = 0$ then the pixel is white. To reconstruct the secret, traditional ORing is applied to the pixels in $\mathbf{V}$. The recovered secret can be viewed as the difference of probabilities with which a black pixel in the reconstructed image is generated from a white and black pixel in the secret image. As with traditional visual cryptography, $n \times m$ sets of matrices need to be defined for the scheme:

$$C_0 = \{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 0\,0 \cdots 0 \\ 1 & 0\,0 \cdots 0 \\ \cdots & \\ 1 & 0\,0 \cdots 0 \end{bmatrix}\}$$

$$C_1 = \{\text{all the matrices obtained by permuting the columns of } \begin{bmatrix} 1 & 0\,0 \cdots 0 \\ 0 & 1\,0 \cdots 0 \\ \cdots & \\ 0 & 0\,0 \cdots 1 \end{bmatrix}\}$$

Because this scheme uses no pixel expansion, m is always equal to one and n is based on the type of scheme being used, for example a $(2, 3)$ scheme, $n = 3$. The most important part of any visual secret sharing scheme is the contrast. The lower the contrast, the harder it is to visually recover the secret. The contrast for this scheme is defined as follows: $\beta = |p_0 - p_1|$, where p_0 and p_1 are the probabilities with which a black pixel on the reconstructed image is generated from a white and black pixel on the secret image.

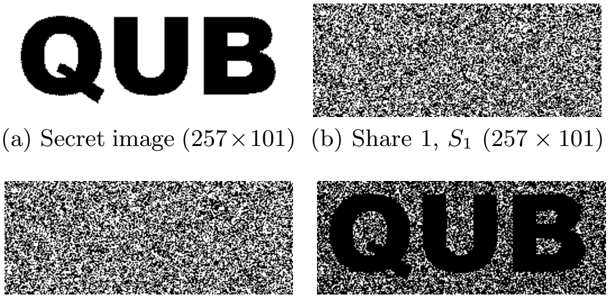
Using the defined sets of matrices C_0 and C_1, and a contrast $\beta = \frac{1}{3}$, $n \times m$ Boolean matrices S^0 and S^1 are chosen at random from C_0 and C_1, respectively:

$$S_0 = \begin{bmatrix} 1\,0\,0 \\ 1\,0\,0 \\ 1\,0\,0 \end{bmatrix}, S_1 = \begin{bmatrix} 1\,0\,0 \\ 0\,1\,0 \\ 0\,0\,1 \end{bmatrix} \tag{5}$$

To share a white pixel, one of the columns in S_0 is chosen and to share a black pixel, one of the columns in S_1 is chosen. This chosen column vector $\mathbf{V} = [v_1, \cdots, v_n]^T$ defines the colour of each pixel in the corresponding shared image. Each v_i is interpreted as black if $v_i = 1$ and as white if $v_i = 0$. Sharing a black pixel for example, one column is chosen at random in S^1, resulting in the following vector:

$$\mathbf{V} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \tag{6}$$

Therefore, the i-th element determines the colour of the pixels in the i-th shared image, thus in this (2,3) example, v_1 is white in the first shared image, v_2 is black in the second shared image and in the third shared image, v_3 is white.



(a) Secret image (257 × 101) (b) Share 1, S_1 (257 × 101)

(c) Share 2, S_2 (257 × 101) (d) Recovered secret, $S_1 + S_2$ (257 × 101)

Fig. 4. Result of a size invariant visual cryptography scheme

This process is repeated for all pixels in the secret image resulting in the final set of shares. Figure 4 provides an example based on the (2,2) scheme.

A probabilistic method to deal with size invariant shares is proposed in [10] in which the frequency of white pixels is used to show the contrast of the recovered image. The scheme is non-expansible and can be easily implemented on the basis of conventional visual secret sharing (VSS) schemes. The term non-expansible means that the sizes of the original image and shadows are the same.

As discussed previously, many schemes presented so far involve pixel expansion. Researchers have examined this area and found it to be a worthwhile research topic [11,12]. This leads on to a related topic within size invariant schemes, namely, aspect ratio.

Aspect ratio invariant secret sharing is presented by Yang and Chen [13]. This aspect ratio invariant secret sharing scheme dramatically reduces the number of extra subpixels needed in order to construct the secret. This results in smaller shares, closer to the size of the original secret while also maintaining the aspect ratio, thus avoiding distortion when reconstructing the secret. Alternatively this problem can be examined from the opposite end, trading overall share size and contrast. A size-adjustable scheme is presented [14] that allows the user to choose an appropriate share size that is practical for the current use of the shares. If quality and contrast matter then the size of the shares will increase, whereas the opposite can happen if these things are not overly important for a user's particular application.

Yang and Chen [15] further progress this research by generalizing the aspect ratio invariant problem. To achieve the same relative position between two square blocks, and to avoid distortion, the re-sampling method in image scaling [16,17] is used.

2.4 Quality Evaluation

From its inception in 1994, VC remains an important research topic. Even this very basic form of VC is still being researched and improved upon. Specific improvements that are worth a mention include the size invariant forms of visual cryptography. More specifically, the schemes which minimize pixel expansion and also increase the overall contrast, which results in very clear secret recovery. The size adjustable scheme discussed above, which allows the user to specify what size of shares to generate is very interesting work. This allows for a user defined tradeoff between quality and portability of shares. This increases the potential for VC once again, rather than being restricted on a specific scheme which only allows for a certain type of quality. Application dependant forms of visual cryptography would be a worthwhile area of further research.

Optimal contrast secret sharing schemes in visual cryptography have been discussed at length because it is an extremely important evaluation metric for any scheme. This is mainly due to how the overall contrast affects the quality of the recovered secret.

Hofmeister et al. [18] present a linear solution to the optimal contrast problem. An approach based on coding theory helps to provide an optimal tradeoff between the contrast and the number of subpixels. Optimal $(2, n)$-schemes are examined in terms of contrast related to the Hamming distance, as well as the subpixel tradeoff required for these optimal schemes. A general scheme for k is also presented which encapsulates a contrast-optimal (k, n)-scheme, where a linear program for calculating the maximum contrast is presented. Solving this linear program results in the optimal achievable contrast in any (k, n)-scheme. Table 1 (taken from Hofmeister) displays some of these calculated optimal contrast solutions.

Table 1. Computed values of a (k, n)-scheme for the optimal contrast solution

$k\backslash n$	2	3	4	5	6	...	10	...	50	...	100
2	1/2	1/3	1/3	3/10	3/10		5/18		25/98		25/99
3		1/4	1/6	1/8	1/10		1/12		13/196		625/9702
4			1/8	1/15	1/18		1/35		1161/65800		425/25608

A possible option for improving the efficiency of VC is to use the XOR operation [19]. This method will not allow traditional stacking of the shares on transparencies but it will improve the overall share quality. The scheme has favourable properties, such as, good resolution and high contrast. It can be applied to colour images as well.

An interesting scheme presented within [20] outlines the procedure for previewing the secret hidden within two shares. The main idea behind this is that if the shares are damaged in some way, recovering the secret using the computationally intensive Lagrange polynomial method [21,22], can turn out to be a waste of time. Therefore, having the ability to check the shares prior to the perfect recover phase is important and can solve a lot of potential problems.

The downside to some of these basic forms of VC is that the shares potentially give away the fact that they are encrypted. Extended VC helps with this, producing meaningful shares which have the same pixel expansion as the original basic VC schemes, but in today's world of high quality imaging, a small minority of users would be dealing with binary images, so most users would not have a use for this in terms of high quality images. However, the use of these efficient basic schemes would provide a secure form of 2D barcodes.

3 Cheating Immune Visual Cryptography

Despite visual cryptography's secure nature, many researchers have experimented with the idea of cheating the system. Methods for cheating the basic VC schemes have been presented, along with techniques used for cheating extended VC schemes [23,24,25].

3.1 Authentication Methods

Prevention of cheating via authentication methods [24] have been proposed which focus on identification between two participants to help prevent any type of cheating taking place. Yang and Laih [25] presented two types of cheating prevention, one type used an online trust authority to perform the verification between the participants. The second type involved changing the VC scheme whereby the stacking of two shares reveals a verification image, however this method requires the addition of extra pixels in the secret.

Another cheating prevention scheme described by Horng et al. [23], whereby if an attacker knows the exact distribution of black and white pixels of each of the shares of honest participants then they will be able to successfully attack and cheat the scheme. Horng's method prevents the attacker from obtaining this distribution.

3.2 Cheat Prevention

Successfully cheating a VCS however, does not require knowledge of the distribution of black and white pixels. Hu and Tzeng [26] where able to present numerous cheating methods, each of which where capable of cheating Horng et al.'s cheating prevention scheme. Hu and Tzeng also present improvements on Yang and Laih's scheme and finally present their own cheating prevention scheme which attempts to minimize the overall additional pixels which may be required. No online trust authority is required and the verification of each image is different and confidential. The contrast is minimally changed and the cheating prevention scheme should apply to any VCS. Hu and Tzeng where also able to prove that both a malicious participant (**MP**), that is $\mathbf{MP} \in P$, and a malicious outsider (**MO**), $\mathbf{MO} \notin P$, can cheat in some circumstances.

The **MP** is able to construct a fake set of shares using his genuine share. After the fake share has been stacked on the genuine share, the fake secret can be viewed. The second cheating method involving an **MO** is capable of cheating the VC scheme without having any knowledge of any genuine shares. The **MO** firstly creates a set of fake shares based on the optimal $(2,2)$-VCS. Next, the fake shares are required to be resized to that of the original genuine shares size.

However, an assumption is to be made on the genuine shares size, namely that these shares where printed onto a standard size of paper, something like A4 or A3. Therefore, shares of those sizes are created, along with fractions of those sizes. Management of this type of scheme would prove to be problematic due to the number of potential shares created in order to have a set of the correct size required to cheat a specific scheme, but once that size is known, cheating is definitely possible as an **MO**.

3.3 A Traceable Model

A traceable model of visual cryptography [27] was also examined which also helps to deal with cheating. It deals with the scenario when a coalition of less than k traitors who stack their shares and publish the result so that other coalitions of the participants can illegally reveal the secret. In the traceable model, it is possible to trace the saboteurs with the aid of special markings. The constructions of traceable schemes for both (k, n) and (n, n) problems were also presented.

3.4 Quality Evaluation

Most notable improvements on cheating immune VC schemes have been presented within [26] which presents examples for traditional and extended schemes. The pixel expansion and contrast reduction are minimal and acceptable due to the overall improvements presented within [26].

The addition of an authentication method, whereby, each participant must verify every other participant is an important improvement. Even with this additional feature, the contrast does not drop significantly enough to rule out this scheme. The drop in contrast is very slight when compared to previous schemes.

Finally, even when some participants collaborate together in order to subvert the system, they cannot succeed. The overall quality and thought that has gone into this scheme is highly impressive and extremely useful.

4 Grayscale, Halftone and Colour Visual Cryptography

A brief introduction to halftoning and error diffusion techniques are given before the main VC schemes which use these technologies are presented. It is important to understand how these technologies work beforehand, as they are frequently used within many visual cryptography schemes.

Halftoning is a print and display technique that trades area for gray-level depth by partitioning an image into small areas in which pixels of different values are purposely arranged to reflect the tone density. There are three main factors that effect these arranged pixels or dot structure, namely, the screen frequency (the number of lines per inch), the dot shape (the shape of the dots as they increase in size from light to dark), and the screen angle (the orientation of lines relative to the positive horizontal axis) [4].

In conjunction, error diffusion techniques coincide with halftone technology. Error diffusion is an adaptive technique that quantizes each pixel according to the input pixel as well as its neighbors. Error diffusion forces total tone content to remain the same and attempts to localize the distribution of tone levels [28]. At each pixel, the errors from its preceding neighbours are added to the original pixel value. This modified value then has a threshold applied to it.

4.1 Grayscale and Halftone Visual Cryptography

This method of secret sharing expands on Naor and Shamir's original findings in the 2-out-of-2 secret sharing scheme. It also takes extended visual cryptography a step further. The halftoning technique that is used can be applied to colour and grayscale images. Halftoning simulates a continuous tone through the use of dots, varying either in size or in spacing [29]. Grayscale halftoning is discussed within this section. Section 4.2 details colour halftone visual cryptography.

Based on the idea of extended visual cryptography, Zhou et al. [30] set about improving these techniques by proposing halftone grayscale images which carry significant visual information. Traditional VC produces random patterns of dots with no visual meaning until the shares are superimposed. This raises the suspicion of data encryption. Halftoning attempts to alleviate this suspicion by having visually pleasing attributes. This means creating halftone shares that carry one piece of information, such as another image, while having the secret hidden until both shares are superimposed. This gives no indication that any encryption has been performed on both shares. This in itself drastically improves the security model for visual cryptography. Along with Zhou, [31,32,33] present novel techniques by which halftone images can be shared with significant visual meaning which have a higher quality than those presented within [34] by employing error diffusion techniques [4]. These error diffusion techniques spread the pixels as homogeneously as possible to achieve the improvements in the shares overall quality.

A halftone scheme [35] was proposed in which the quality of the shares is improved by using contrast enhancement techniques. However the problem with this scheme is that it is not perfectly secure.

By using a space-filling curve ordered dithering technique [36], grayscale images can be converted into an approximate binary image. This allows encryption and decryption of the gray-level images using traditional visual cryptography methods [37].

Further improvements made in this area where achieved by using better error diffusion techniques, the technique proposed in [32] satisfies the following 3 requirements: (i) a secret image should be a natural image, (ii) images that carry a secret image should be a high quality natural images and (iii) computational cost should be low. This technique is based on [38] which satisfies both (ii) and (iii) and in order to satisfy (i), introduces an additional feedback mechanism into the secret image embedding process in order to improve the quality of the visually decoded secret image. Methods described in [35,39] only satisfy part of the three requirements.

The method proposed by Myodo et al. [32] allows natural embedding of grayscale images. The quality of the superimposed image highly depends on its dynamic range and pixel density. The possible pixel density of the superimposed image can be defined as: $max(0, g'_1 + g'_2 - 1) < d_s < min(g'_1, g'_2)$, where g'_1 and g'_2 are pixel values of the dynamic-range-controlled input images and d_s is the pixel density of the superposed image that is estimated with the surrounding pixels. The equation indicates that $g'_1 = g'_2 = 0.5$ gives the widest dynamic range of the superimposed image. Therefore, pixel values of input images should be modified around 0.5 by reducing their dynamic range. Accordingly, each pixel value of a secret image should be restricted between 0 and 0.5. This provides the mechanism for allowing any grayscale natural image to be used as an input.

The next stage is embedding the grayscale secret image. Along with the conventional method of enhancing the images using a feedback mechanism, another feedback mechanism is proposed to the secret image embedding process to enhance the quality of the superimposed image. Outlined below are the details of this method.

The typical error diffusion data hiding process is extended and another new system is also added. The extension involves ANDing the temporary shares within the system. The pixel values of the second share are determined one by one during the embedding process. Therefore, this superimposing operation can only be performed on the processed area of the share. Then the proposed method estimates density of the temporary superimposed image. During this density calculation, a low-pass filter such as a Gaussian filter [17] is used.

In order to make the superimposed result closer to the secret image, the new component is introduced. This new process decides how the current density should be controlled, either made darker or brighter. This is controlled by the distance between the pixel values in the secret and the density. If the density is much lower than the pixel value, then the density becomes brighter in order to achieve the desired embedding of the secret. Overall, this improves the quality of the original grayscale secret image and the most advantageous part of the new mechanism is that no iteration is required in the same way as the method described in [38].

The conventional method described in [38] uses an error diffusion halftoning technique [40] which works as follows: two grayscale images are used for input along with a secret image. Typically, the secret image cannot be used as an input image so a ternary image is used as input in its place. The output images (that carry the secret) are binary images. Firstly, image 1 is taken and an error diffusion process is applied to it (giving share 1). Image 2 then has an image hiding error diffusion process applied. During this image hiding error diffusion process, pixels from image 2 are modulated by corresponding pixels of share 1 and the secret image in order to embed the secret into the resultant share of image 2 (giving share 2). The secret is recovered by superimposing share 1 and share 2.

The previously discussed VC schemes all suffer from pixel expansion in that the shares are larger than the original secret image. Chen et al. [41] present a secret sharing scheme that maps a block in a secret image onto a corresponding equal-sized block in the share image without this pixel expansion. Two techniques which are discussed include histogram width-equalization and histogram depth-equalization. This scheme improves the quality of the reconstructed secret when compared with alternative techniques.

Another scheme proposed by Wang et al. [42] uses only Boolean operations. The contrast is also higher than other probabilistic visual cryptography sharing schemes.

The area of contrast within halftone and grayscale VC is an interesting one because the contrast determines exactly how clear the recovered visual secret is. Cimato et al. [43] developed a visual cryptography scheme with ideal contrast by using a technique known as reversing, which was originally discussed by [44]. Reversing changes black pixels to white pixels and vice-versa. Viet and Kurosawa's scheme allows for perfect restoration of the black pixels but only almost perfect restoration of the white pixels. Cimato et al. provide their results for perfect restoration of both black and white pixels. Each share also contained a smaller amount of information than Viet and Kurosawa's which makes it a more desirable and secure scheme. Yang et al. [45] also looked at reversing and the shortcomings of Viet and Kurosawa's scheme. Their work presented a scheme that allowed perfect contrast reconstruction based on any traditional visual cryptography sharing scheme.

4.2 Colour Visual Cryptography

Applying visual cryptography techniques to colour images is a very important area of research because it allows the use of natural colour images to secure some types of information. Due to the nature of a colour image, this again helps to reduce the risk of alerting someone to the fact that information is hidden within it. It should also allow high quality sharing of these colour images. Colour images are also highly popular and have a wider range of uses when compared to other image types. Many of the techniques presented within this section use halftone technologies on the colour images in order to make them work with visual cryptography. That is why colour visual cryptography is presented within this section.

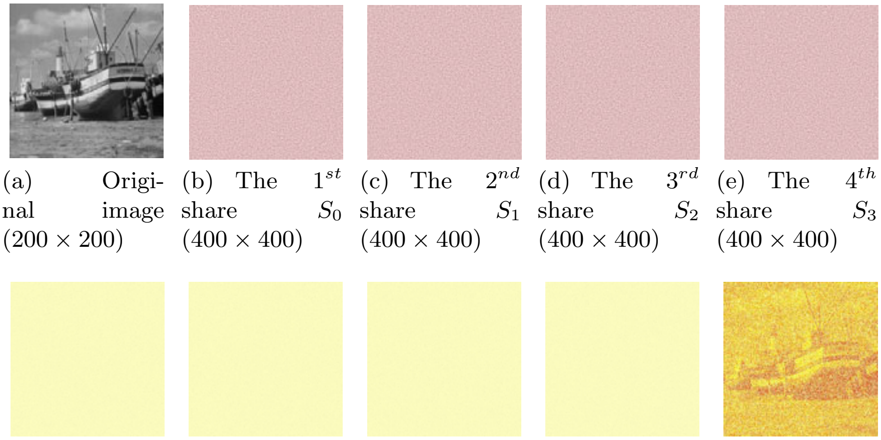
In 1996, Naor and Shamir published a second article on visual cryptography "Visual Cryptography II: Improving the Contrast via the Cover Base" [46]. The new model contains several important changes from their previous work; they use two opaque colours and a completely transparent one.

The first difference is the order in which the transparencies are stacked. There must be an order to correctly recover the secret. Therefore each of the shares needs to be pre-determined and recorded so recovery is possible. The second change is that each participant has c sheets, rather than a single transparency. Each sheet contains red, yellow and transparent pixels. The reconstruction is done by merging the sheets of participant I and participant II, i.e. put the i-th sheet of II on top of the i-th sheet of I and the $(i+1)$-th of I on top of the i-th of II.

The two construction methods are monochromatic construction and bichromatic construction. In the monochromatic construction, each pixel in the original image is mapped into c sub-pixels and each participant holds c sheets. In each of participant I sheets, one of the sub-pixels is red and the remaining $c-1$ sub-pixels are transparent. In each of participant II sheets, one of the sub-pixels is yellow, the other $c-1$ sub-pixels are transparent. The way the sheets of participant I and II are merged is by starting from the sheet number 1 of participant I, then putting sheet number 2 of participant II is put on top of it, then sheet number 2 of participant I on top of that and so on.

The order in which sub-pixels of participant I are coloured red constitutes a permutation π on $\{1, \cdots, c\}$ and the order which the sub-pixels of participant II are coloured yellow constitutes a permutation σ. π and σ are generated as follows: π is chosen uniformly at random from the set of all permutations on c's elements. If the original pixel is yellow, then $\pi = \sigma$, therefore each red sub-pixel of the i-th sheet of participant I will be covered by a yellow sub-pixel of the same position of the i-th sheet of participant II. If the original pixel is red, then $\sigma(i) = \pi(i+1)$ for $1 \leq i \leq c-1$ and $\sigma(c) = \pi(1)$, therefore each yellow sub-pixel of the i-th sheet of participant II will be covered by a red sub-pixel of the same position of the $(i+1)$-th sheet of participant I except the c-th sheet. In practice, the first sheet of participant I is not necessarily stored since it is always covered by other sheets.

Figure 5 shows the results of applying this cover based scheme for a $(2, 2)$-VCS. It is noted that in this example, the original grayscale image is pre-halftoned before it is processed by this scheme.



(a) Original image (200×200) (b) The 1^{st} share S_0 (400×400) (c) The 2^{nd} share S_1 (400×400) (d) The 3^{rd} share S_2 (400×400) (e) The 4^{th} share S_3 (400×400)

(f) The 5^{th} share S_4 (400×400) (g) The 6^{th} share S_5 (400×400) (h) The 7^{th} share S_6 (400×400) (i) The 8^{th} share S_7 (400×400) (j) The stacked image: $S_0, \cdots, S_7$ (400×400)

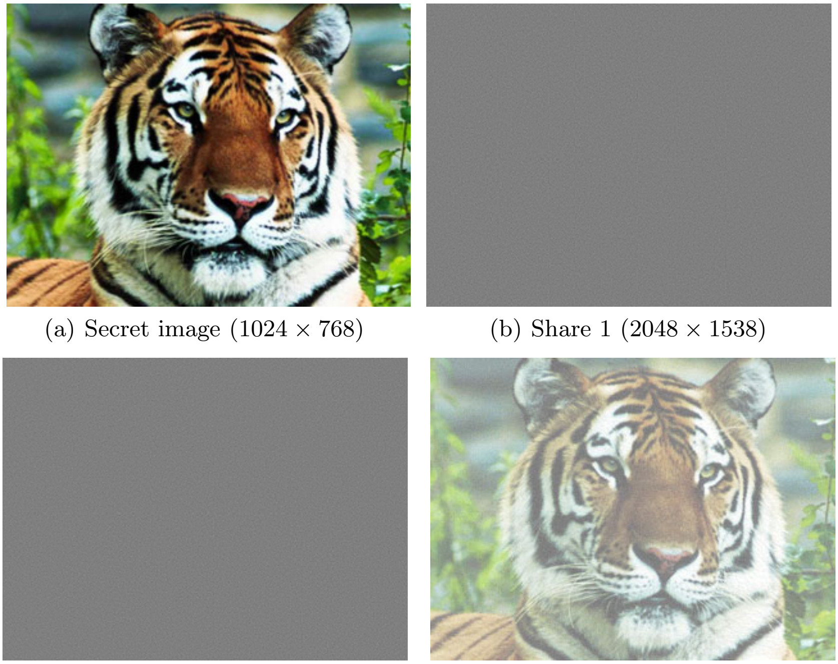
Fig. 5. Result of a monochromatic construction for $(2, 2)$-VCS using a cover base

A very primitive example of colour image sharing appeared in [47]. In this example, each pixel of the colour secret image is expanded to a block of 2 × 2 sub-pixels. Each one of these blocks is filled with red, green, blue and white (transparent) colours respectively. Taking symmetries into account, 24 different possibilities for the combination of two pixels can be obtained. It is claimed that if the sub-pixels are small enough, the human visual system will average out the different possible combinations to 24 different colours. To encrypt a pixel of the coloured image, round the colour value of that pixel to the nearest representable colour. Select a random order for the sub-pixels on the first share and select the ordering on the second share such that the combination produces the required colour.

The advantage of this scheme is that it can represent 24 colours with a resolution reduction of 4, instead of $24^2 = 576$. The disadvantage is that the 24 colours are fixed once the basic set of sub-pixel colours is fixed.

An example of a basic $(2, 2)$ colour visual cryptography scheme can be viewed in Figure 6. Two random colour shares are generated. Simply OR'ing each of them allows for the secret to be recovered. The contrast difference is quite noticeable, however the recovered secrets quality is very impressive.

Another primitive scheme was also presented [48] and extended more recently [49]. Verheul and Van Tilborg's scheme provides a c-colour (k, n)-threshold



(a) Secret image (1024 × 768)

(b) Share 1 (2048 × 1538)

(c) Share 2 (2048 × 1538)

(d) Recovered secret (2048 × 1538)

Fig. 6. Results of a basic colour $(2, 2)$ VC scheme

scheme. This scheme uses the black pixel to superimpose on the result of two colour pixels superimposition, if they give a resultant colour that is not in the original colour palette. This can be achieved by making sure the superimposed colour pixels result in a non-colour palette colour, one of which is changed to a black pixel or by ensuring that one of the colour pixels is changed to black before the superimposing operation [50]. Yang and Laih improve on the pixel expansion aspect of the Verheul and Van Tilborg scheme and their (n, n)-threshold scheme is optimal since they match the following lower bound placed on pixel expansion, formulated in [50]:

$$m \geq \begin{cases} c \cdot 2^{n-1} - 1, & \text{if } n \text{ is even} \\ c \cdot 2^{n-1} - c + 1, & \text{if } n \text{ is odd} \end{cases} \tag{7}$$

Hou et al. [51] proposed a novel approach to share colour images based on halftoning. With this halftone technology, different gray levels can be simulated simply by altering the density of the printed dots. Within bright parts of the image the density is sparse, while in the darker parts of the image, it is dense. This is very helpful in the visual cryptography sense because it is able to transform a grayscale image into a black and white image. This allows for traditional visual cryptography techniques to be applied. Similarly, the colour decomposition method is used for colour images which also allows the proposed scheme to retain all the advantages of traditional visual cryptography, such as no computer participation required for the decryption/recovery of the secret.

Hou himself also provided one of the first colour decomposition techniques to generate visual cryptograms for colour images [52]. Using this colour decomposition, every colour within the image can be decomposed into one of three primary colours: cyan, magenta or yellow. This proposal is similar to traditional visual cryptography with respect to the pixel expansion that occurs. One pixel is expanded into a 2×2 block where two colour pixels are stored along with two transparent (white) pixels.

However, [53] examined the security of Hou's [52] scheme, and while the scheme is secure for a few specific two-colour secret images, the security cannot be guaranteed for many other cases.

An example finite lattice based structure consisting of all 8 colours from the CMYK-RGB colour model has also been proposed [54]. After all the values (each separate colour) have been permuted in each of the 8 lattices, when the 2 shares are generated, the original image will be reproduced when the shares are superimposed.

All the colours within the lattice, $C = \{0, Y, M, C, R, G, B, 1\}$, where 0 represents white and 1 represents black, can be represented within a matrix as follows:

$$\text{White:} \quad \begin{bmatrix} 0 & Y & M & C & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & Y & M & C & 1 \end{bmatrix},$$

$$\text{Yellow:} \quad \begin{bmatrix} Y & 0 & M & C & 1 & 1 & 1 & 1 \\ 0 & Y & 1 & 1 & M & C & 1 & 1 \end{bmatrix},$$

$$
\begin{array}{ll}
\text{Magenta:} & \begin{bmatrix} M & 0 & C & Y & 1 & 1 & 1 & 1 \\ 0 & M & 1 & 1 & M & C & 1 & 1 \end{bmatrix}, \\
\text{Cyan:} & \begin{bmatrix} C & 0 & Y & M & 1 & 1 & 1 & 1 \\ 0 & C & 1 & 1 & Y & M & 1 & 1 \end{bmatrix}, \\
\text{Red:} & \begin{bmatrix} Y & M & C & 0 & 1 & 1 & 1 & 1 \\ M & Y & 1 & 1 & C & 0 & 1 & 1 \end{bmatrix}, \\
\text{Green:} & \begin{bmatrix} C & Y & M & 0 & 1 & 1 & 1 & 1 \\ Y & C & 1 & 1 & M & 0 & 1 & 1 \end{bmatrix}, \\
\text{Blue:} & \begin{bmatrix} M & C & Y & 0 & 1 & 1 & 1 & 1 \\ C & M & 1 & 1 & Y & 0 & 1 & 1 \end{bmatrix}, \\
\text{Black:} & \begin{bmatrix} Y & M & C & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & Y & M & C & 0 \end{bmatrix},
\end{array}
$$

Since, in the above example there are $8 = 4 \times 2$, sub-pixels, the height or width of the image needs to be enlarged by a factor of two before the encryption. Each pixel in the original image is encrypted according to its colour, it is encrypted into an element randomly chosen from one of the lattices. Under such an encryption scheme, the two shares and the reproduced image become $16 = 4 \times 4$ times larger than the original image.

Improving this pixel expansion and also working out the optimal contrast of colour visual cryptography schemes have been investigated [50]. In the paper, they prove that contrast-optimal schemes are available for colour VC and then further go on to prove the optimality with regard to pixel expansion.

A lossless recovery scheme outlined by [55] considers halftoning techniques for the recovery of colour images within visual cryptography. The scheme generates high quality halftone shares which provide lossless recovery of the secrets and reduces the overall noise in the shares without any computational complexity. Their proposed method starts by splitting the colour channels into its constituent parts, cyan (C), magenta (M), and yellow (Y). Each channel has grayscale halftoning applied to it. Error diffusion techniques discussed in [30] are then applied to each halftone channel. A circularly symmetric filter is used along with a Gaussian filter. This provides an adequate structure for the dot placement when constructing the shares.

Lukac and Plataniotis [56] present a scheme based on bit-level operations to provide image encryption for visual cryptography. They argue that the requirements for input restrict the application of VC and the fact that the secret recovery should be done without the use of computation also limits the applicability. Their presented work allows binary, grayscale, and colour images to be used based on their B-bit image sharing scheme. The process takes the input image and breaks it down into its corresponding bit-levels, for example, a grayscale image with 8-bits per pixel is broken down into its corresponding binary bit-levels, from $b = 8$ to $b = 1$ where $b = 1, 2, \cdots, 8$. After the image has been decomposed, traditional VC methods can be applied to each of the binary bit-levels to perform the encryption. An interesting feature of this scheme is that it offers perfect reconstruction of the secret, this is due to its encryption and decryption processes being reciprocal. The performance of this scheme is dependant on the machine, but the results provided in terms of execution time seem acceptable for smaller images. One problem would be the size of the secret to be hidden. The bigger the secret, the longer it will take to encrypt and decrypt. Obviously, this isn't much of a problem with traditional VC methods which cater for instant decryption via stacking the shares. This raises another valid point, the whole idea behind VC is to perform the secret recovery using no computation.

Efficiency within colour visual cryptography [57] is also considered which improves on the work done by [49,58]. The proposed scheme follows Yang and Laih's colour model. The model considers the human visual system's effect on colour combinations out of a set of colour sub-pixels. This means that the set of stacked colour sub-pixels would look like a specific colour in original secret image. As with many other visual cryptography schemes, pixel expansion is an issue. However Shyu's scheme has a pixel expansion of $\lceil log_2 c \rceil$ which is superior to many other colour visual cryptography schemes especially when c, the number of colours in the secret image becomes large. An area for improvement however would be in the examination of the difference between the reconstructed colour pixels and the original secret pixels. Having high quality colour VC shares would further improve on the current schemes examined within this survey, this includes adding a lot of potential for visual authentication and identification.

Chang et al. [59] present a scheme based on smaller shadow images which allows colour image reconstruction when any authorized k shadow images are stacked together using their proposed revealing process. This improves on the following work [60] which presents a scheme that reduces the shadow size by half. Chang et al.'s technique improves on the size of the share in that, as more shares are generated for sharing purposes, the overall size of those shares decreases.

In contrast to colour decomposition, Yang and Chen [61] propose an additive colour mixing scheme based on probabilities. This allows for a fixed pixel expansion and improves on previous colour secret sharing schemes. One problem with this scheme is that the overall contrast is reduced when the secrets are revealed.

In most colour visual cryptography schemes, when the shares are superimposed and the secret is recovered, the colour image gets darker. This is due to the fact that when two pixels of the same colour are superimposed, the resultant pixel gets darker. Cimato et al. [62] examine this colour darkening by proposing a scheme which has to guarantee that the reconstructed secret pixel has the exact same colour as the original. Optimal contrast is also achieved as part of their scheme. This scheme differs from other colour schemes in that it considers only 3 colours when superimposing, black, white, or one pixel of a given colour. This allows for perfect reconstruction of a colour pixel, because no darkening occurs, either by adding a black pixel or by superimposing two colours which are identical, that ultimately results in a final darker colour.

A technique that enables visual cryptography to be used on colour and grayscale images is developed in progressive colour visual cryptography [63]. Many current state of the art visual cryptography techniques lead to the degradation in the quality of the decoded images, which makes it unsuitable for digital media (image, video) sharing and protection. In [63], a series of visual cryptography schemes have been proposed which not only support grayscale and colour images, but also allow high quality images including that of perfect (original) quality to be reconstructed.

The annoying presence of the loss of contrast makes traditional visual cryptography schemes practical only when quality is not an issue which is relatively rare. Therefore, the basic scheme is extended to allow visual cryptography to be directly applied on grayscale and colour images. Image halftoning is employed in order to transform the original image from the grayscale or colour space into the monochrome space which has proved to be quite effective. To further improve the quality, artifacts introduced in the process of halftoning have been reduced by inverse halftoning.

With the use of halftoning and a novel microblock encoding scheme, the technique has a unique flexibility that enables a single encryption of a colour image but enables three types of decryptions on the same ciphertext. The three different types of decryptions enable the recovery of the image of varying qualities. The physical transparency stacking type of decryption enables the recovery of the traditional VC quality image. An enhanced stacking technique enables the decryption into a halftone quality image. A progressive mechanism is established to share colour images at multiple resolutions. Shares are extracted from each resolution layer to construct a hierarchical structure; the images of different resolutions can then be restored by stacking the different shared images together.

The advantage is that this scheme allows for a single encryption, multiple decryptions paradigm. In the scheme, secret images are encrypted / shared once, and later, based on the shares, they can be decrypted / reconstructed in a plurality of ways. Images of different qualities can be extracted, depending on the need for quality as well as the computational resources available. For instance, images with loss of contrast are reconstructed by merely stacking the shares; a simple yet effective bit-wise operation can be applied to restore the halftone image; or images of perfect quality can be restored with the aid of the auxiliary look-up table. Visual cryptography has been extended to allow for multiple resolutions in terms of image quality. Different versions of the original image of different qualities can be reconstructed by selectively merging the shares. Not only this, a spatial multi-resolution scheme has been developed in which images of increasing spatial resolutions can be obtained as more and more shares are employed.

This idea of progressive visual cryptography has recently been extended [64] by generating friendly shares that carry meaningful information and which also allows decryption without any computation at all. Purely stacking the shares reveals the secret. Unlike [63] and [65] which require computation to fully reconstruct the secret, the scheme proposed in [66] has two types of secrets, stacking the transparencies reveals the first, but computation is again required to recover the second-level secret. Fang's scheme is also better than the polynomial sharing method proposed in [67]. The method proposed in [67] is only suitable for digital systems and the computational complexity for encryption and decryption is also a lot higher.

4.3 Quality Evaluation

Grayscale, halftone and colour image techniques for visual cryptography provide an important step for the improvement of VC. The best results are obtained when using error diffusion techniques to spread the pixels as evenly as possible. These results also provide excellent secret recovery because the contrast is high. Using colour images has also improved the potential application for VC, particularly when using computer-specific progressive VC techniques, perfect secret recovery is possible with very high quality colour images and relatively low computational power. However, as discussed, use of computation partially defeats the point of VC.

To measure the quality loss in the meaningful halftone shares, the peak signal-to-noise ratio (PSNR) is used. Firstly the mean squared error must be calculated (Eq. (8)) for all the pixel values in the halftone images. This allows for the PSNR value to be calculated (Eq. (9)).

$$MSE = \frac{1}{nm} \sum_{i=0}^{n-1} \sum_{j=0}^{m-1} \| I(i,j) - K(i,j) \|^2 \tag{8}$$

$$PSNR = 10 \cdot log_{10} \left(\frac{MAX_I^2}{MSE} \right) \tag{9}$$

where I and K are the images with width n and height m. As the share size increases, the visually pleasing attributes improve correspondingly, from an average of 9dB to 12dB, although the overall contrast drops. So a tradeoff must be made in order to obtain good recovered secrets and have suitable quality in the meaningful shares.

5 Multiple Secret Sharing in Visual Cryptography

5.1 Basic Multiple Secret Sharing

The schemes previously discussed deal with sharing just one secret. So the natural extension of that is trying to hide multiple secrets within two shares. Multiple secret sharing has the main advantage of being able to hide more than one secret within a set of shares.

The multiple secret sharing problem was initially examined by Wu and Chen [68]. They concealed two secrets within two sets of shares S_1 and S_2. The first secret is revealed when S_1 and S_2 are superimposed. The second becomes available when S_1 is rotated anti-clockwise 90° and superimposed on S_2. Due to the nature of the angles required for revealing the secrets ($90°, 180°$ or $270°$) and the fact that this scheme can only share, at most, two secrets, it becomes apparent that it is quite limited in its use.

It is also worth noting that another extended form of secret sharing was proposed [69] that is quite similar to the one discussed which involves stacking the transparencies to reveal a different secret each time a new layer is stacked. An improvement on this extended scheme is achieved by reducing the number of subpixels required [70].

Multiple secret sharing was developed further [71] by designing circular shares so that the limitations of the angle ($\theta = 90°, 180°, 270°$) would no longer be an issue. The secrets can be revealed when S_1 is superimposed on S_2 and rotated clockwise by a certain angle between 0° and 360°.

A further extension of this was implemented [72] which defines another scheme to hide two secret images in two shares with arbitrary rotating angles. This scheme rolls the share images into rings to allow easy rotation of the shares and thus does away with the angle limitation of Wu and Chen's scheme. The recovered secrets are also of better quality when compared to [71], this is due to larger difference between the black and white stacked blocks.

More recently [73] a novel secret sharing scheme was proposed that encodes a set of $x \geq 2$ secrets into two circle shares where x is the number of secrets to be shared. This is one of the first set of results presented that is capable of sharing more than two secrets using traditional visual cryptography methods. The algorithms presented can also be extended to work with grayscale images by using halftone techniques. Colour images could also be employed by using colour decomposition [52] or colour composition [57].

One difficulty with this scheme is the pixel expansion. The expansion is twice the number of secrets to be hidden, so the size of the circle shares increases dramatically when many large secrets are hidden. However, the number of secrets that are contained within the shares still remains a secret unless supplementary lines are added to the circle shares to ease the alignment. This is another problem with sharing multiple secrets, especially when dealing with circle shares, knowing the correct alignment points. Knowing how many secrets are actually contained within the shares is also a concern. If the rotation angle is small (meaning many secrets are concealed) and rotation of the shares occurs too quickly, it is possible that all secrets may not be recovered.

Sharing a set of secrets where that set contains more than 2 secrets, using traditional visual cryptography and typical polygonal shapes has also been considered [74]. This scheme presents three joint VC methods for sharing secrets. The first deals with altering the contrast of the shares, which allows multiple secrets to be hidden within a set of shares. This scheme keeps the original aspect ratio of the secrets, but results in darker shares after superimposing has taken place. The revealing share (key share) is also of a smaller size than the share which contains each of the secrets. The second scheme presents a way of using the even and odd scan lines of a share to embed two secrets. This helps with the overall contrast of the white areas of the shares, but also reduces the overall contrast of the recovered secrets. The aspect ratio has also been altered. Finally the multiple joint combination of shares results in two shares which share four secrets. While the aspect ratio remains intact, the overall contrast drops

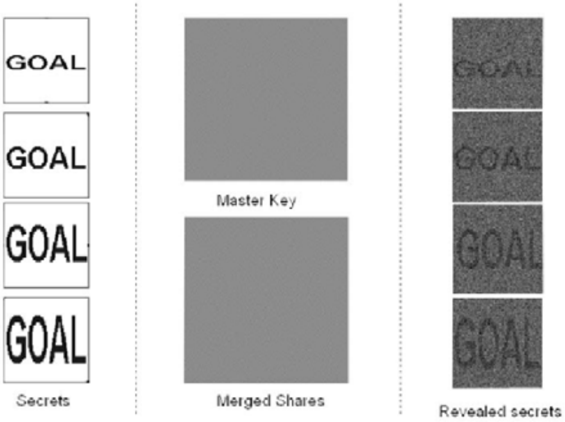


Fig. 7. Joint visual cryptography with multiple secrets, their corresponding shares and the recovered secrets

significantly when more secrets are added. This becomes a problem if many secrets are to be considered. Figure 7 shows this scheme sharing four secrets, the word “GOAL” increases in size as the master key share is moved around.

Another new scheme [75] considers secret sharing for multiple secrets, which is established on a stacking based graph approach to reconstructing the pixels. By stacking the shares at aliquot angles, the secrets can be revealed. Feng et al.'s proposed scheme is formally defined as a 2-out-of-2 m-way extended visual cryptography secret sharing scheme for m secret images, denoted as: $(2, 2)$-m-VSSM. As with many other visual cryptography schemes, this scheme also allows for decryption without the use of computation. Once the shares are positioned at their aliquot angles, the secrets are instantly revealed.

The creation (encryption) of the shares works as follows. Firstly a relationship graph is created between the rows, this is because each row in the scheme is considered independently. For each row, the blocks are collected in the position of the two share images at the required angles $0, \frac{360°}{m}, \frac{360°}{m} \times 2, \cdots, \frac{360°}{m} \times (m-1)$ to form the graph. Every block is related to all the share blocks in the other share image. Therefore, all the share blocks on a row can be separated into sets. These blocks and sets are then combined with the visual patterns developed by Feng et al. [75] and the shares are generated.

Yet another problem with this scheme is the pixel expansion $2m$, where m is the number of secrets to be shared. Again the overall size of the shares increases drastically when more secrets are considered. The contrast of the scheme is also a problem. The previously discussed schemes originated from Wu and Chen, Hsu et al. provide better contrast whereas Feng et al.'s contrast is $\frac{1}{3m}$. This means the more secrets added, the lower the contrast gets, so overall image quality deteriorates.

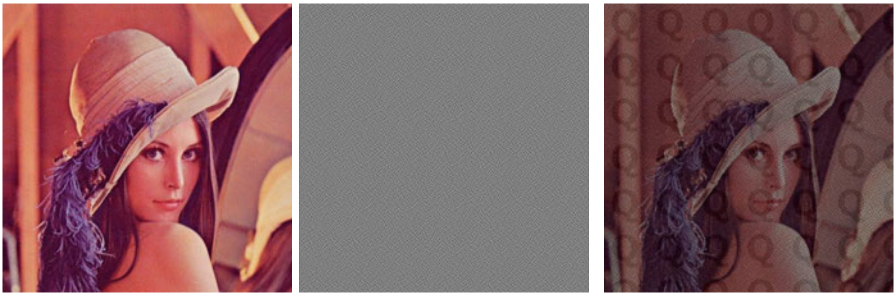
Multiple secret sharing using weighted transparencies is discussed here [76]. Based on an extended style of visual cryptography, stacking qualified subsets of transparencies reveals a different secret at each stacking level. The transparencies with the largest weight determine which images are recovered. The typically advantageous properties of VC are used within this scheme along with a max-weight dominance and a quality-control design to create high quality shares.

Traditional visual cryptography usually leads to inefficiency when shares are electronically stored and transferred. Gnanaguruparan and Kak [77] proposed a way of hiding multiple secret images in one pair of shares thus to improve the efficiency. One share of the large secret image is constructed from the joint shares of the small secret image. This process repeats for even smaller secret images. This recursive hiding scheme utilizes shares in a more efficient way and the efficiency is almost twice as high when compared to traditional visual cryptography schemes.

The efficiency of sharing multiple secrets against sharing a single secret has also been looked at [78]. Checking to see if improvements are even possible are examined along with a proposed scheme that helps to achieve these improvements. A bound is proved to highlight these improvements.

5.2 Colour Multiple Secret Sharing

Using halftone and colour images as a base or cover for multiple secret sharing is an interesting topic. Techniques proposed within [79] allow for a smaller set of shares (which can be unique) to be hidden with these meaningful colour images. Using the idea of a master key is capable of recovering all the secrets which have been generated using the outlined scheme, it is used to cover the halftone or colour image in order to reveal the secrets. The secret shares in this case are embedded within the cover images, this helps to remove suspicion that any encryption has taken place or, that the image has even been altered in any specific noticeable way. Figure 8 illustrates the application of this scheme.



(a) The original colour image containing the merged share.

(b) Secure mask to superimpose.

(c) Secrets revealed after superimposing (b) on (a).

Fig. 8. Merging a share of visual cryptography with a colour image

5.3 Quality Evaluation

Sharing multiple secrets with high quality recovery is very achievable. Depending on the number of secrets a user wishes to hide, this determines the overall size of the shares. The more secrets a user wishes to hide, the larger the resultant shares get. This is one of the shortcomings of multiple secret sharing, the final share size when many large secrets are considered can become unmanageable. Numerous schemes are presented which range from sharing just two secrets to the general case of sharing any number of secrets. Of the schemes presented, circular shares seem to be best in terms of the secrets recovery and contrast. The scheme presented for sharing more than two secrets using standard rectangular shares has issues with contrast while more secrets are added. Using a colour cover image also presents an effective way to share multiple smaller secrets. The difference between the original and the merged shares is not very noticeable to the visual system.

An objective way of testing the actual alteration between the original Lenna image and the Lenna image which contains the merged share is to use the peak signal-to-noise ratio (PSNR) metric to measure this difference.

The PSNR for an $n \times m$ colour image I and its noisy counterpart K is calculated thusly, first, the mean squared error (MSE) must be calculated on each pixel for each of its corresponding RGB channels using Eq. (8). After which, each channel's PSNR value, must be calculated using Eq. (9). The values are then summed and averaged, resulting in the final PSNR value. MAX is the maximum pixel value, 255 in a colour image.

The PSNR between the original image and the image in Figure 8(a) is 21.0715dB, which is an acceptable value of quality loss considering the images secure properties.

Overall, the majority of the multiple secret sharing schemes are successful in effectively hiding two or more secrets with a set of shares. The schemes that roll the secrets into circular shares prove to be the most interesting and effective in terms of sharing many secrets with very high contrast.

6 Visual Cryptography Applications

6.1 Watermarking

Practical uses for visual cryptography come in the form of watermarking. Memon and Wong [80] propose various techniques by which these watermarks can be applied to images. A simple watermark insertion scheme is illustrated [81]. However it is not robust because the watermark is embedded within the least significant bit of the image and could easily be destroyed. A more robust scheme should be able to deal with lossy image compression, filtering, and scanning. The idea of random noise [82] is employed on colour images to make removal of the watermark very difficult. Cryptographic functions such as the MD5 hash [83] have also been employed to improve the security features when it comes to embedding data within images. Similarly [84] also explores the use of watermarks within visual cryptography.

A digital image copyright scheme based on visual cryptography is presented within [85]. It is simple and efficient, both in watermark embedding and retrieval. It is also acceptably robust when the watermarked image is compressed. After compression, the watermark can still be recovered and verified. However, the scheme is not robust in terms of minor modifications to the watermarked image. Accurate recovery is not possible. Another problem is that the watermark could be successfully recovered from an image exhibiting some similarities with the original, even though the image is not the original.

Rather than the random pixel selection scheme proposed within [85] [86] provides a scheme by which specific pixels from the original image are selected. One issue with this non-random scheme is that any changes made on the original, such as defacement of the image, will be reflected in the restored watermark. The watermark is still recognizable but distortions are noticeable. An important part of this scheme, however, is that the watermark itself is invisible. This means that the original image looks exactly the same as the watermarked image. The scheme is robust to minor changes in the image, but those changes are present in the recovered watermark. The key used to recover the watermark depends on the security of the scheme. If a small key is used (8-bits), the scheme will not be as secure as a key of length 128-bits. The watermark also remains hidden until the key is employed to recover it.

A further improvement on Hwang's scheme [85] comes in the form of another VC based watermarking scheme [87]. This improved scheme supports black and white images as well as colour images and is robust against scaling and rotation of the watermarked image. Robust recovery of the watermark is also possible after the image has been defaced. As with the other schemes previously discussed, this scheme is also key dependant. Without the key, no watermark recovery is possible.

One of the most robust ways to hide a secret within natural images is by typically employing visual cryptography based on halftone techniques. The perfect scheme is extremely practical and can reveal secrets without computer participation. Recent state of the art watermarking [88] can hide a watermark in documents which require no specific key in order to retrieve it. Removing the need for a key is quite important because it further increases the security and robustness of the watermarking process.

Hou and Chen [89] implemented an asymmetric watermarking scheme based on visual cryptography. Two shares are generated to hold the watermark. One is embedded into the cover-image and another is kept as a secret key for the watermark extraction. The watermark is extracted using traditional stacking properties of visual cryptography. The watermark is robust in that it is difficult to change or remove and can withstand a number of attacks.

6.2 Moiré Patterns

A potential application for visual cryptography is its use in conjunction with Moiré patterns. Moiré patterns [90] (or fringes) are induced when a revealing layer such as a dot screen or line grating is superimposed on top of a periodically repeating shape. The resulting Moiré pattern is influenced by changing any of the following geometric parameters characterizing the individual grid structures, namely period, orientation, and shape [91,92,93]. Whether a dot screen or a line grating is used, both induce Moiré fringes with the same geometric properties [94].

The revealing layer contains horizontal black lines (line grating), between those lines is transparent white space. When the revealing layer is superimposed, the shapes that appear are the magnified versions of the repeating pattern. This magnifying property [95,96] could be used as a method of locating hidden VC shares within a Moiré pattern.

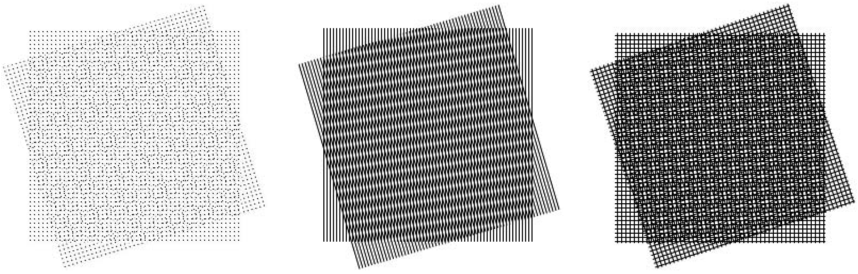
This magnification factor of these patterns can be calculated as follows, let p_b represent the period of shapes in the base layer, the period of the line gratings in the revealing layer is denoted as p_r. In order for the magnification to work, the periods must be sufficiently close. When the revealing layer is superimposed, the repeating pattern in the base layer is stretched along the vertical axis. There is no change in the horizontal axis. This magnification can be represented as p_m [97]. The following equation expresses this magnification along the vertical axis:

$$p_m = -\frac{p_b \cdot p_r}{p_b - p_r} \tag{10}$$

If p_m is negative, this represents a mirrored magnified shape along the vertical axis.

Visual cryptography has been implemented using Moiré patterns. Desmedt and Le [98] provide a scheme by which secrecy and anonymity are both satisfied. Moiré patterns occur when high frequency lattices are combined together to produce low frequency lattice patterns. It is the difference in these high frequencies that give the Moiré patterns. Figure 9 shows an example of these Moiré patterns.

The Moiré cryptography model is as follows: The embedded (secret) image is randomized into two shares, known as pre-shares. Each of these are independent of the original image. XORing these pre-shares will recover the original. Next,



(a) Superimposing two dot screens

(b) Superimposing two line gratings

(c) Superimposing two grids

Fig. 9. Moiré patterns generated with different styles

the hiding algorithm takes the cover image and combines it with each of the pre-shares separately. Its output is the final two shares that are used to reveal the original embedded image. These resulting shares look the same as the input cover image that is used.

There are three different Moiré schemes proposed by Desmedt and Le [98], lattice rotation, lattice smooth rotation, and dot orientation. The problem with lattice rotation is that the boundary between differently-rotated areas in the shares becomes visible. However, this scheme produced very sharp decrypted ciphertext. Lattice smooth rotation fixed the boundary issues but introduced another problem, namely, the artifacts introduced into the shares stand out too much and become visible. The pair settled on the final scheme, dot orientation, as their chosen implementation. The dots from the shares are converted into diamond shape "dots", this makes for a less visible boundary than circular or elliptical dots. The scheme encodes a white pixel by superimposing two squares onto the shares whose dots are oriented at different angles. To encode a black pixel, dot patterns are used that are of the same angle. This produces two different Moiré patterns for the white and black dots. That means this scheme uses the Moiré patterns to recover the secret embedded image, rather than traditional visual cryptography schemes which use the gray level of the squares to recover the secret.

These Moiré patterns could be used in conjunction with hologram technology [99]. This could provide secure solutions for verification of generated holograms.

7 Conclusion and Future Work

7.1 Conclusion

It is apparent that a lot of time and effort have been dedicated to visual secret sharing using visual cryptography. Many of the schemes presented work extremely well and the current state of the art techniques have proven to be very useful for many applications, such as verification and authentication.

The following trends have been identified within visual cryptography:

1. Contrast improvement.
2. Share size improvement.
3. Wider range of suitable image types (binary to colour images).
4. Efficiency of VC schemes.
5. Ability to share multiple secrets.

Essentially the most important part of any VC scheme is the contrast of the recovered secret from a particular set of shares. Ideal schemes provide a high contrast when the secret has been recovered. However, a tradeoff is required in some schemes depending on the size of the shares along with the number of secrets which may be concealed. Especially within extended visual cryptography schemes, contrast is of major importance. Making sure the base images completely disappear and a clear secret is recovered which could be another high quality image is vitally important.

Some schemes present methods which do not work with printed transparencies and these rely on computation in order to recover the secret. In this respect, high quality secret recovery is possible, however it is preferred if the scheme works with printed transparencies. After all, this is the idea behind VC. Conversely, if an application requires digital recovery of the secrets, then perfect recovery can be achieved via the XOR operation.

Improving on the resultant share size has also been a worthwhile research topic. Having shares that are close to the original secret's size is best, because it results in shares that are easier to manage and transmit. Large secrets with even larger shares become cumbersome. However, at times a tradeoff must be made between the size of the shares and the contrast of the recovered secret. The tradeoff between size and the secret recovery must be suitable so that high quality recovery can take place and must also ensure that the shares do not expand into large, unmanageable sizes.

The use of grayscale and colour images has added value to the field of visual cryptography. Reducing the requirements on input image type so that any kind of image can be used to share a secret is very important. The fact that any image can be used to share a secret within visual cryptography shows a great improvement on the very initial work that required an image to be converted to its binary equivalent before any processing could be done on it. However, the application of the scheme depends greatly on the type of images to be input.

Efficiency covers a number of things which have already been discussed, such as contrast and share size. The topic of efficiency also includes how the shares and images have been processed. Numerous methods presented within this survey have improved on prior work and techniques, resulting in schemes that are highly efficient and very simple to implement and use. For the maximum efficiency in recovering the secret, no computer participation should be involved.

The addition of multiple secret sharing has proven to be an interesting area within VC. This further increases the capacity of VC as it allows the same physical amount of data to be sent, ie. two shares, but increases the amount of usable information retrievable at the end.

Overall, this survey has summarized much of the work done in the area of visual cryptography and has also provided a number of ideas for new research within this domain. There are still many topics worth exploring within VC to further expand on its potential in terms of secret sharing, data security, identification, and authentication.

7.2 Future Work

The previously mentioned trends that have emerged within VC require more attention. This allows VC to remain an important research topic. Typically within multiple secret sharing, the alignment points can cause problems. A novel multiple secret sharing scheme that does away with the need for supplementary lines could possibly be grounds for new research.

Future work that would further the progress of visual cryptography would be to examine and create suitable schemes for other image types, such as hatched or line-art based images [100]. The focus being, to apply these techniques in conjunction with modern day image hatching techniques which would allow the extension of VC into the currency domain, potentially making it applicable to a wider range of secure applications, such as within the banking industry.

The use of these types of shares within the secure printing industry should also be considered. For example, creating shares that can be printed using normal print techniques, but when scanned or photocopied, react in an adverse way. This would prevent unauthorized copying of the shares.

Extending the print and scan application of VC [101] may also be considered. Print and scan protection is one possible avenue of research, which would render the shares useless after scanning has taken place. Scanning a share into a computer system and then digitally superimposing its corresponding share could also be considered. This may well prove to be very challenging due to the nature of the scanned shares not being an exact copy and having to work out the borders of the scanned image. Rotation of the resultant scan would also have to be taken into consideration. This would have the potential for secure verification of tickets or other forms of document verification, such as secure barcode scanning.

References

1. Shamir, A.: How to share a secret. Communications of the ACM 22(11), 612–613 (1979)
2. Naor, M., Shamir, A.: Visual cryptography. In: De Santis, A. (ed.) EUROCRYPT 1994. LNCS, vol. 950, pp. 1–12. Springer, Heidelberg (1994)
3. Blundo, C., D'Arco, P., De Santis, A., Stinson, D.R.: Contrast optimal threshold visual cryptography schemes. SIAM Journal on Discrete Mathematics 16(2), 224–261 (2003)
4. Lau, D.L., Arce, G.R.: Modern Digital Halftoning. Marcel Dekker, New York (2000)
5. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended schemes for visual cryptography. Theoretical Computer Science 250, 1–16 (1996)
6. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Visual cryptography for general access structures. Information and Computation 129(2), 86–106 (1996)
7. Yang, C.N., Chen, T.S.: Extended visual secret sharing schemes with high-quality shadow images using gray sub pixels. In: Kamel, M.S., Campilho, A.C. (eds.) ICIAR 2005. LNCS, vol. 3656, pp. 1184–1191. Springer, Heidelberg (2005)
8. Ito, R., Kuwakado, H., Tanaka, H.: Image size invariant visual cryptography. IEICE Transactions E82-A(10), 2172–2177 (1999)
9. Tzeng, W.G., Hu, C.M.: A new approach for visual cryptography. Designs, Codes and Cryptography 27(3), 207–227 (2002)
10. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters 25(4), 481–494 (2004)
11. Yang, C.N., Chen, T.S.: New size-reduced visual secret sharing schemes with half reduction of shadow size. IEICE Transactions 89-A(2), 620–625 (2006)

12. Yang, C.N., Chen, T.S.: Visual secret sharing scheme: Improving the contrast of a recovered image via different pixel expansions. In: Campilho, A., Kamel, M.S. (eds.) ICIAR 2006. LNCS, vol. 4141, pp. 468–479. Springer, Heidelberg (2006)
13. Yang, C.N., Chen, T.S.: Aspect ratio invariant visual secret sharing schemes with minimum pixel expansion. Pattern Recognition Letters 26(2), 193–206 (2005)
14. Yang, C.N., Chen, T.S.: Size-adjustable visual secret sharing schemes. IEICE Transactions 88-A(9), 2471–2474 (2005)
15. Yang, C.N., Chen, T.S.: Reduce shadow size in aspect ratio invariant visual secret sharing schemes using a square block-wise operation. Pattern Recognition 39(7), 1300–1314 (2006)
16. Kim, C.H., Seong, S.M., Lee, J.A., Kim, L.S.: Winscale: an image-scaling algorithm using an area pixel model. IEEE Transactions on Circuits and Systems for Video Technology 13(6), 549–553 (2003)
17. Gonzalez, R.C., Woods, R.E.: Digital Image Processing. Addison-Wesley Longman Publishing Co., Inc., Boston (2001)
18. Hofmeister, T., Krause, M., Simon, H.U.: Contrast-optimal k out of n secret sharing schemes in visual cryptography. Theoretical Computer Science 240(2), 471–485 (2000)
19. Tuyls, P., Hollmann, H.D.L., van Lint, J.H., Tolhuizen, L.M.G.M.: XOR-based visual cryptography schemes. Designs, Codes and Cryptography 37(1), 169–186 (2005)
20. Yang, C.N., Chen, T.S.: An image secret sharing scheme with the capability of previvewing the secret image. In: ICME 2007, pp. 1535–1538 (2007)
21. Thien, C.C., Lin, J.C.: Secret image sharing. Computers & Graphics 26, 765–770 (2002)
22. Wang, R.Z., Su, C.H.: Secret image sharing with smaller shadow images. Pattern Recognition Letters 27(6), 551–555 (2006)
23. Horng, G., Chen, T., Tsai, D.S.: Cheating in visual cryptography. Des. Codes Cryptography 38(2), 219–236 (2006)
24. Naor, M., Pinkas, B.: Visual authentication and identification. In: Kaliski Jr., B.S. (ed.) CRYPTO 1997. LNCS, vol. 1294, pp. 322–336. Springer, Heidelberg (1997)
25. Yang, C., Laih, C.: Some new types of visual secret sharing schemes, vol. III, pp. 260–268 (December 1999)
26. Hu, C.M., Tzeng, W.G.: Cheating prevention in visual cryptography. IEEE Transactions on Image Processing 16(1), 36–45 (2007)
27. Biehl, I., Wetzel, S.: Traceable visual cryptography. In: Han, Y., Quing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 61–71. Springer, Heidelberg (1997)
28. Kang, H.R.: Digital Color Halftoning. In: Society of Photo-Optical Instrumentation Engineers (SPIE), Bellingham, WA, USA (1999)
29. Campbell, A.: The Designer's Lexicon. Chronicle Books, San Francisco (2000)
30. Zhou, Z., Arce, G.R., Crescenzo, G.D.: Halftone visual cryptography. IEEE Transactions on Image Processing 15(8), 2441–2453 (2006)
31. Myodo, E., Sakazawa, S., Takishima, Y.: Visual cryptography based on void-and-cluster halftoning technique. In: ICIP, pp. 97–100 (2006)
32. Myodo, E., Takagi, K., Miyaji, S., Takishima, Y.: Halftone visual cryptography embedding a natural grayscale image based on error diffusion technique. In: ICME, pp. 2114–2117 (2007)
33. Wang, Z., Arce, G.R.: Halftone visual cryptography through error diffusion. In: ICIP, pp. 109–112 (2006)
34. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. Theoretical Computer Science 250(1-2), 143–161 (2001)

35. Nakajima, M., Yamaguchi, Y.: Extended visual cryptography for natural images. In: WSCG, pp. 303–310 (2002)
36. Zhang, Y.: Space-filling curve ordered dither. Computers & Graphics 22(4), 559–563 (1998)
37. Lin, C.C., Tsai, W.H.: Visual cryptography for gray-level images by dithering techniques. Pattern Recognition Letters 24(1-3), 349–358 (2003)
38. Fu, M.S., Au, O.C.: A novel method to embed watermark in different halftone images: data hiding by conjugate error diffusion (dhced). In: ICME 2003, Washington, DC, USA, pp. 609–612. IEEE Computer Society, Los Alamitos (2003)
39. Wu, C.W., Thompson, G.R., Stanich, M.J.: Digital watermarking and steganography via overlays of halftone images. In: SPIE, vol. 5561, pp. 152–163 (2004)
40. Ulichney, R.A.: Digital Halftoning. MIT Press, Cambridge (1987)
41. Chen, Y.F., Chan, Y.K., Huang, C.C., Tsai, M.H., Chu, Y.P.: A multiple-level visual secret-sharing scheme without image size expansion. Information Sciences 177(21), 4696–4710 (2007)
42. Wang, D., Zhang, L., Ma, N., Li, X.: Two secret sharing schemes based on boolean operations. Pattern Recognition 40(10), 2776–2785 (2007)
43. Cimato, S., De Santis, A., Ferrara, A.L., Masucci, B.: Ideal contrast visual cryptography schemes with reversing. Information Processing Letters 93(4), 199–206 (2005)
44. Duong, Q.V., Kurosawa, K.: Almost ideal contrast visual cryptography with reversing. In: Okamoto, T. (ed.) CT-RSA 2004. LNCS, vol. 2964, pp. 353–365. Springer, Heidelberg (2004)
45. Yang, C.N., Wang, C.C., Chen, T.S.: Real perfect contrast visual secret sharing schemes with reversing. In: Zhou, J., Yung, M., Bao, F. (eds.) ACNS 2006. LNCS, vol. 3989, pp. 433–447. Springer, Heidelberg (2006)
46. Naor, M., Shamir, A.: Visual cryptography ii: Improving the contrast via the cover base. In: Lomas, M. (ed.) Security Protocols 1996. LNCS, vol. 1189, pp. 197–202. Springer, Heidelberg (1997)
47. Rijmen, V., Preneel, B.: Efficient color visual encryption for shared colors of benetton. In: EUCRYPTO 1996 (1996)
48. Verheul, E.R., Tilborg, H.C.A.V.: Constructions and properties of k out of n visual secret sharing schemes. Des. Codes Cryptography 11(2), 179–196 (1997)
49. Yang, C.N., Laih, C.S.: New colored visual secret sharing schemes. Designs, Codes and Cryptography 20(3), 325–336 (2000)
50. Cimato, S., De Prisco, R., De Santis, A.: Optimal colored threshold visual cryptography schemes. Designs, Codes and Cryptography 35(3), 311–335 (2005)
51. Hou, Y.C., Chang, C.Y., Tu, S.F.: Visual cryptography for color images based on halftone technology. Image, Acoustic, Speech and Signal Processing, Part 2 (2001)
52. Hou, Y.C.: Visual cryptography for color images. Pattern Recognition 36, 1619–1629 (2003)
53. Leung, B.W., Ng, F.Y., Wong, D.S.: On the security of a visual cryptography scheme for color images. Pattern Recognition (August 2008)
54. Koga, H., Yamamoto, H.: Proposal of a lattice-based visual secret sharing scheme for color and grey-scale images. IEICE Transactions Fundamentals E81-A(6), 1262–1269 (1998)
55. Krishna Prakash, N., Govindaraju, S.: Visual secret sharing schemes for color images using halftoning. Proceedings of Computational Intelligence and Multimedia Applications 3, 174–178 (2007)

56. Lukac, R., Plataniotis, K.N.: Bit-level based secret sharing for image encryption. Pattern Recognition 38(5), 767–772 (2005)
57. Shyu, S.J.: Efficient visual secret sharing scheme for color images. Pattern Recognition 39(5), 866–880 (2006)
58. Blundo, C., De Bonis, A., De Santis, A.: Improved schemes for visual cryptography. Designs, Codes and Cryptography 24(3), 255–278 (2001)
59. Chang, C.C., Lin, C.C., Lin, C.H., Chen, Y.H.: A novel secret image sharing scheme in color images using small shadow images. Information Sciences 178(11), 2433–2447 (2008)
60. Yang, C.N., Chen, T.S.: New size-reduced visual secret sharing schemes with half reduction of shadow size. In: Gervasi, O., Gavrilova, M.L., Kumar, V., Laganá, A., Lee, H.P., Mun, Y., Taniar, D., Tan, C.J.K. (eds.) ICCSA 2005. LNCS, vol. 3480, pp. 19–28. Springer, Heidelberg (2005)
61. Yang, C.N., Chen, T.S.: Colored visual cryptography scheme based on additive color mixing. Pattern Recognition 41(10), 3114–3129 (2008)
62. Cimato, S., De Prisco, R., De Santis, A.: Colored visual cryptography without color darkening. Theoretical Computer Science 374(1-3), 261–276 (2007)
63. Jin, D., Yan, W.Q., Kankanhalli, M.S.: Progressive color visual cryptography. SPIE Journal of Electronic Imaging 14(3) (2005)
64. Fang, W.P.: Friendly progressive visual secret sharing. Pattern Recognition 41(4), 1410–1414 (2008)
65. Chen, S.K., Lin, J.C.: Fault-tolerant and progressive transmission of images. Pattern Recognition 38(12), 2466–2471 (2005)
66. Fang, W.P., Lin, J.C.: Visual cryptography with extra ability of hiding confidential data. Journal of Electronic Imaging 15(2), 023020 (2006)
67. Thien, C.C., Lin, J.C.: An image-sharing method with user-friendly shadow images. IEEE Transactions on Circuits and Systems for Video Technology 13(12), 1161–1169 (2003)
68. Wu, C., Chen, L.: A study on visual cryptography. Master's thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C. (1998)
69. Katoh, T., Imai, H.: An extended construction method for visual secret sharing schemes. IEICE Transactions J79-A(8), 1344–1351 (1996)
70. Yang, C.N., Chen, T.S.: Extended visual secret sharing schemes: Improving the shadow image quality. IJPRAI 21(5), 879–898 (2007)
71. Wu, H.C., Chang, C.C.: Sharing visual multi-secrets using circle shares. Computer Standards & Interfaces 28, 123–135 (2005)
72. Hsu, H.C., Chen, T.S., Lin, Y.H.: The ringed shadow image technology of visual cryptography by applying diverse rotating angles to hide the secret sharing. Networking, Sensing and Control 2, 996–1001 (2004)
73. Shyu, S.J., Huang, S.Y., Lee, Y.K., Wang, R.Z., Chen, K.: Sharing multiple secrets in visual cryptography. Pattern Recognition 40(12), 3633–3651 (2007)
74. Weir, J., Yan, W.Q.: Sharing multiple secrets using visual cryptography. In: IEEE ISCAS 2009, Taiwan (2009)
75. Feng, J.B., Wu, H.C., Tsai, C.S., Chang, Y.F., Chu, Y.P.: Visual secret sharing for multiple secrets. Pattern Recognition 41(12), 3572–3581 (2008)
76. Chen, S.K.: A visual cryptography based system for sharing multiple secret images. In: ISCGAV 2007: Proceedings of the 7th WSEAS International Conference on Signal Processing, Computational Geometry & Artificial Vision, Stevens Point, Wisconsin, USA, World Scientific and Engineering Academy and Society (WSEAS), pp. 117–122 (2007)

77. Gnanaguruparan, M., Kak, S.: Recursive hiding of secrets in visual cryptography. Cryptologia 26(1), 68–76 (2002)
78. Crescenzo, G.D.: Sharing one secret vs. sharing many secrets. Theoretical Computer Science 295(1-3), 123–140 (2003)
79. Weir, J., Yan, W., Crookes, D.: Secure mask for color image hidding. In: Communications and Networking in China, ChinaCom 2008, August 2008, pp. 1304–1307 (2008)
80. Memon, N., Wong, P.W.: Protecting digital media content. Communications of the ACM 41(7), 35–43 (1998)
81. van Schyndel, R.G., Tirkel, A.Z., Osborne, C.F.: A digital watermark. In: ICIP(2), pp. 86–90 (1994)
82. Braudaway, G.W., Magerlein, K.A., Mintzer, F.: Protecting publicly available images with a visible image watermark. In: van Renesse, R.L. (ed.) Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, March 1996. Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, vol. 2659, pp. 126–133 (1996)
83. Wong, P.W.: A watermark for image integrity and ownership verification. In: PICS, IS&T - The Society for Imaging Science and Technology, pp. 374–379 (1998)
84. Luo, H., Pan, J.S., Lu, Z.M.: Hiding multiple watermarks in transparencies of visual cryptography. Intelligent Information Hiding and Multimedia Signal Processing 1, 303–306 (2007)
85. Hwang, R.J.: A digital image copyright protection scheme based on visual cryptography. Tamkang Journal of Science and Engineering 3(2), 97–106 (2000)
86. Hassan, M.A., Khalili, M.A.: Self watermarking based on visual cryptography. Proceedings of World Academy of Science, Engineering and Technology 8, 159–162 (2005)
87. Sleit, A., Abusitta, A.: A visual cryptography based watermark technology for individual and group images. Systemics, Cybernetics And Informatics 5(2), 24–32
88. Chuang, S.C., Huang, C.H., Wu, J.L.: Unseen visible watermarking. In: ICIP(3), pp. 261–264. IEEE, Los Alamitos (2007)
89. Hou, Y.C., Chen, P.M.: An asymmetric watermarking scheme based on visual cryptography. In: WCCC-ICSP 5th International Conference on Signal Processing Proceedings, vol. 2, pp. 992–995 (2000)
90. Hersch, R.D., Chosson, S.: Band moiré images. In: ACM SIGGRAPH 2004, pp. 239–247. ACM, New York (2004)
91. Knotts, M.E., Hemphill, R.G.: Selected papers on optical moiré and applications. Optics & Photonics News, 53–55 (August 1996)
92. Kafri, O., Glatt, I.: The physics of Moire metrology. Wiley, New York (1990)
93. Indebetouw, G., Czarnek, R.: Selected papers on optical moiré and applications. SPIE Milestones Series, vol. MS64 (1992)
94. Amidror, I.: The Theory of the Moiré Phenomenon. Kluwer, Dordrecht (2000)
95. Hutley, M., Stevens, R.: Optical inspection of arrays and periodic structures using moire magnification. In: Searching for Information: Artificial Intelligence and Information Retrieval Approaches (Ref. No. 1999/199), IEE Two-day Seminar, pp. 8/1–8/5 (1999)
96. Kamal, H., Völkel, R., Alda, J.: Properties of moir[e-acute] magnifiers. Optical Engineering 37(11), 3007–3014 (1998)

97. Gabrielyan, E.: Shape moiré patterns (March 2007), `http://switzernet.com/people/emin-gabrielyan/070320-shape-moire/`
98. Desmedt, Y., Le, T.V.: Moiré cryptography. In: ACM Conference on Computer and Communications Security, pp. 116–124 (2000)
99. Liu, S., Zhang, X., Lai, H.: Artistic effect and application of moireé patterns in security holograms. Applied Optics 34(22), 4700–4702 (1995)
100. Praun, E., Hoppe, H., Webb, M., Finkelstein, A.: Real-time hatching. In: ACM SIGGRAPH 2001, pp. 579–584. ACM, New York (2001)
101. Yan, W.Q., Jin, D., Kankanhalli, M.S.: Visual cryptography for print and scan applications. In: Proceedings of International Symposium on Circuits and Systems, Vancouver, Canada, May 2004, pp. 572–575 (2004)