Feature and Future of Visual Cryptography Based Schemes

Dhiraj Pandey[1], Anil Kumar[2], and Yudhvir Singh[3]

[1] JSS Noida
[2] CSE Deptt.,
Manipal University Jaipur
[3] MDU Rohtak
University Instt.of Engg.&Technology
{dhip2,dahiyaanil}@yahoo.co.in, yudhvirsingh@rediffmail.com

Abstract. Visual cryptography (VC) is a useful technique that combines the notions of perfect ciphers and secret sharing in cryptography. 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. There are various measures on which performance of visual cryptography scheme depends, such as pixel expansion, contrast, security, accuracy, computational complexity, share generated is meaningful or meaningless, type of secret images (either binary or color) and number of secret images(either single or multiple) encrypted by the scheme. In this paper, we will summarize the developments of visual cryptography since its birth in 1994, introduce the main research topics in this area where researchers have been contributing and outline the application of these schemes.

Keywords: Visual cryptography scheme (VCS), pixel expansion, contrast, security, accuracy, computational complexity.

1 Introduction

With the rapid advancement of network technology, most of the information is transmitted over the Internet conveniently. Various confidential data such as military maps and commercial secrets are transmitted over the Internet. While using secret images, security issues should be taken into consideration because hackers may utilize weak link over communication network to steal information that they want. To deal with the security problems of secret images, various image secret sharing schemes have been developed. Visual cryptography was introduced first in 1994 Naor and Shamir [1]. Visual cryptography is a cryptographic technique which allows visual information (e.g. printed text, handwritten notes and pictures) to be encrypted in such a way that the decryption can be performed by the human visual system, without the aid of computers. Visual cryptography scheme eliminates complex computation problem in decryption process, and the secret images can be restored by stacking operation. This property makes visual cryptography especially useful for the low computation load requirement.

K. Singh, A.K. Awasthi, and R. Mishra (Eds.): QSHINE 2013, LNICST 115, pp. 816–830, 2013.

This paper covers the progress of VC, along with the current trends and the various applications for VC. When the data is hidden within separate images (known as shares), it is completely unrecognizable. While the shares are separate, the data is completely unrelated. Each image holds random images and when they are brought together, the secret can be recovered easily. They each depend on one another in order to obtain the original image.

This paper is organized as follows: Section 2 elaborates on the work being done in this area, specifically the most recent improvements. In general, these schemes primarily deal with binary images and noisy random shares. Extended VC is also presented within this section. Section 3 discuss on cheating prevention within VC along with cheating immune VC schemes. These schemes attempt to have some type of authentication or verification method. Grayscale, halftone and color halftone images used with visual cryptography are presented 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 analyzed in Section 6 along with performance analysis in section 7 and the summary is discussed within Section 8, 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. 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 pioneered by Moni Naor and Adi Shamir in 1994 at the Eurocrypt conference [2]. 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.

Naor and Shamir's initial implementation assumes that the image is a collection of black and white pixels. One disadvantage of this is that the decryption process is lossy; in terms of 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. Newer schemes that are discussed later deal with grayscale and color images which attempt to minimize the loss in contrast [3] by using digital halftoning. 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 Hamming weight $H(V)$ of the ORed m-vector V is interpreted by the visual system as follows: A black pixel is interpreted if $H(V) <= d$ and white if $H(V) <$d-αm for some fixed threshold 1<=d<=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:

$C0$ = all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$

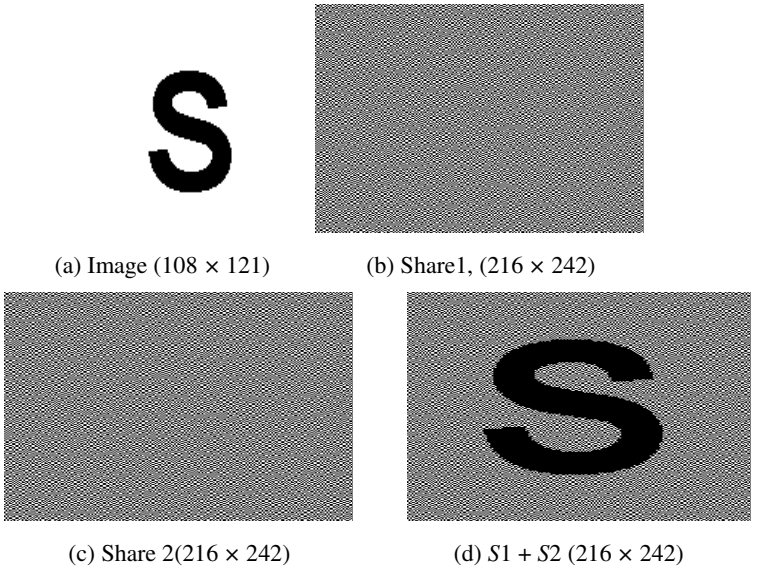
$C1$ = all the matrices obtained by permuting the columns of $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

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.

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.

Below in Figure 1, 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) Image (108 × 121) (b) Share1, (216 × 242)

(c) Share 2(216 × 242) (d) $S1 + S2$ (216 × 242)

Fig. 1. The results of a traditional visual cryptography scheme

2.2 Extended Visual Cryptography

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 the image on the shares will disappear and the secret message will be visible. This is the basis for the extended form of visual cryptography. An extended scheme proposed by Ateniese et al. [5] is based on an access structure which contains two types of sets. 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.

In EVCS, the first n shares need to be images of something like a car, boat or, some form of meaningful information. The secret message is normally the $(n + 1)$ th message. This requires a technique that has to take into consideration the color 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.

Three conditions must be satisfied for 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.

2.3 Size Invariant Visual Cryptography

Image size invariant VC was proposed by Ito et al. [6]. Traditional visual cryptography schemes employ pixel expansion, although many researchers have worked on how to improve problem of pixel expansion [7]. Ito's scheme [6] removes the need for this pixel expansion. The scheme uses the traditional (k, n) scheme where m is equal to one. 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. The most important part of any VC scheme is the contrast. The lower the contrast of the recovered secret, the harder it is to visually recover the secret. The contrast for this scheme is defined as follows: $\beta = |p0 - p1|$, where $p0$ and $p1$ are the probabilities with which a black pixel on the reconstructed image is generated from a white and black pixel on the secret image. Another method to deal with size invariant shares is proposed in [8] in which the frequency of white pixels is used to show the contrast of the recovered image. The scheme is non-expansible. Many researchers have examined size invariant schemes [9,10]. Aspect ratio is a related topic within size invariant schemes. Yang and Chen [11] has presented aspect ratio invariant secret sharing. Aspect ratio invariant secret sharing scheme reduces the number of extra sub pixels needed. A size-adjustable scheme is presented by Yang et al. [12] that allow choosing an appropriate share size. If quality and contrast matter then the size of the shares will increase, for a user's particular application.

2.4 Integrated Review of Basic Schemes

VC remains an important research topic from its inception in 1994. 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. 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. An approach based on coding theory helps to provide an optimal tradeoff between the contrast and the number of sub pixels. Optimal (2, *n*)-schemes are examined in terms of contrast related to the Hamming distance, as well as the sub pixels tradeoff required for these optimal schemes. A possible option for improving the efficiency of VC is to use the XOR operation [13]. This method will not allow traditional stacking of the shares on transparencies but it will improve the overall share quality. The scheme has favorable properties, such as, good resolution and high contrast. It can be applied to color images as well. 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.

3 Cheating Immune Visual Cryptography

The cheating process could cause damage to victims because they will accept a forged image different from the actual secret image as authentic. Many researchers have experimented with the idea of cheating the system and suggested solution for its prevention also. Methods for cheating the basic VC schemes have been presented, along with techniques used for cheating extended VC schemes [14,15,16].

3.1 Authentication Methods

Prevention of cheating via authentication methods [16] has been proposed which focus on identification between two participants to help prevent any type of cheating taking place. Yang and Laih [16] 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 logo; however this method requires the addition of extra pixels in the secret. Another cheating prevention scheme is described by Horng et al. [14]. 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. Method which prevents the attacker from obtaining this distribution can be useful to prevent cheating.

3.2 Cheat Prevention

Hu and Tzeng [17] were able to present numerous cheating methods, each of which where capable of cheating Horng et al.'s cheating prevention scheme. They also present improvements on Yang 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 MP $\in P$, and a malicious outsider (MO), MO $/\in P$, 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.

3.3 A Traceable Model

A traceable model of visual cryptography [18] 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 [17] which present examples for traditional and extended schemes. The pixel expansion and contrast reduction are minimal and acceptable due to the overall improvements presented within [17]. The addition of an authentication method, whereby, each participant must verify every other participant is an important improvement. The drop in contrast is very slight when compared to previous schemes. The overall quality that has gone into this scheme is highly impressive and extremely useful.

4 Grayscale, Halftone and Colour Visual Cryptography

It is important to understand how halftoning technologies work, 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. 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 [19]. 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 is an extension 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.

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. [20] set about improving these techniques by proposing halftone grayscale images which carry significant visual information. This in itself drastically improves the security model for visual cryptography. Along with Zhou, [21,22,23] present novel techniques by which halftone images can be shared with significant visual meaning which have a higher quality than those presented within [24] by employing error diffusion techniques . These error diffusion techniques spread the pixels as homogeneously as possible to achieve the improvements in the shares overall quality. A halftone scheme [25] 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.

The method proposed by Myodo et al. [22] 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: $max(0, g`_1+g`_2-1) < ds < min(g`_1, g`_2)$, where $g`_1$ and $g`_2$ are pixel values of the dynamic-range-controlled input images and ds 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 conventional method described in [26] uses an error diffusion halftoning technique [27] 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. [28] 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. [29] 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. [30] developed a visual cryptography scheme with ideal contrast by using a technique known as reversing, which was originally discussed by [31]. 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. [32] 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. In 1996, Naor and Shamir published a second article on visual cryptography "Visual Cryptography II: Improving the Contrast via the Cover Base" [33]. 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.

Efficiency within colour visual cryptography is also considered which improves on the work done by [34]. 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 $log2c$ 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.

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.

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.

This idea of progressive visual cryptography has recently been extended [35] 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.

4.3 Evaluation of Grayscale and Color Schemes

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. 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. 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

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 problems was initially examined by Wu and Chen [36]. They concealed two secrets within two sets of shares $S1$ and $S2$. The first secret is revealed when $S1$ and $S2$ are superimposed. The second becomes available when $S1$ is rotated anti-clockwise 90° and superimposed on $S2$. 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 [37] 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 [38]. Multiple secret sharing was developed further [39] 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 $S1$ is superimposed on $S2$ and rotated clockwise by a certain angle between 0° and 360°. A further extension of this was implemented [40] 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 [39], this is due to larger difference between the black and white stacked blocks. More recently [41] 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. 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.

5.2 Quality Evaluation of Sharing Multiple Secrets

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.

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

Visual cryptography applications range from banking industry, satellite imaging to commercial application for preserving collected biometric data.

Practical uses for visual cryptography come in the form of watermarking. Memon and Wong [42] propose various techniques by which these watermarks can be applied to images. Similarly [43] also explores the use of watermarks within visual cryptography. A digital image copyright scheme based on visual cryptography is presented within [44]. It is simple and efficient, both in watermark embedding and retrieval. It is also acceptably robust when the watermarked image is compressed. 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. VC potentially making it applicable to a wider range of secure applications, such as within the banking industry.

7 Performance Analysis

Various parameters are recommended by researchers to evaluate the performance of visual cryptography scheme. Naor and Shamir [1] suggested two main parameters, pixel expansion m and contrast. Pixel expansion m refers to the number of subpixels in the generated shares that represents a pixel of the original input image. It represents the loss in resolution from the original picture to the shared one.Security is satisfied if each share reveals no information of the original image and the original image cannot be reconstructed if there are fewer than k shares collected. Accuracy is considered to be the quality of the reconstructed secret image and evaluated by peak signal-to-noise ratio (PSNR) measure. Computational complexity concerns the total number of operators

required both to generate the set of n shares and to restructure the original secret image .Jen-Bang Feng et al[9] suggested that VCS should support multiple secret to work efficiently. If scheme support only one secret to share at a time to share multiple secret images numerous share have to be generated, transmitted and maintained.

Table 1. Comparison of Visual Cryptography Schemes on the Basis of Number of Secret Images, Pixel Expansion, Image format, Type of Share Generated

Sr. No.	Authors	Year	No. of Secret Images	Pixel Expansion	Image Format	Type of Share generated
1	Naor and Shamir	1995	1	4	Binary	Random
2	Wu and chen	1998	2	4	Binary	Random
3	Hsu et al.	2004	2	4	Binary	Random
4	Wu and cheng	2005	2	4	Binary	Meaningful
5	Chin-chen chang	2005	1	4	Binary	Random
6	Liguo fang	2006	1	2	Binary	Random
7	s. j. shyu	2007	n>=2	2n	Binary	Random
8	w.p.fung	2007	2	9	Binary	Random
9	Jen bang	2008	n>=2	3n	Binary	Random
10	Mustafa Ulutas	2008	2	4	Binary	Random
11	Tzung-Her Chen et al.	2008	2	1	Binary	Random
12	Chen et al.	2008	n(n>=2)	4	Binary, gray, color	Random
13	Zhengxin Fu	2009	4	9	Binary	Random
14	Jonathan Weir et al.	2009	n	4	Binary	Random
15	Xiao-qing Tan	2009	1	1	Binary	Random
16	Verheul Tilborg	1997	1	C*3	Color	Random
17	Yang & Liah	2000	1	C*2	Color	Radom
18	Chin Chen Chang et al.	2002	1	9	Gray	Meaningful
19	Haibo Zhang et al.	2008	1	1	Gray	Random
20	Jonathan Weir	2011	1	4	Binary, gray, color	Hatched

As shown in the Table 1 only few visual cryptography schemes achieve minimum pixel expansion. Less overhead for storage and transmission is required to share multiple secrets while using the scheme [7,9]. Meaningful shares [4, 18] can be helpful to avoid attacks by hacker. Scheme supporting color images and gray [16, 17, 18, 19] are useful in the multimedia environment.

8 Conclusion and Further Direction

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. 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 paper 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.

Overall, this paper has summarized much of the work done in the area of visual cryptography. 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.

The previously mentioned trends that have emerged within VC require more attention. This allows VC to remain an important research topic. 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. Scanning a share into a computer system and then digitally superimposing its corresponding share could also be considered.

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 (1995)
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. Ito, R., Kuwakado, H., Tanaka, H.: Image size invariant visual cryptography. EICE Transactions E82-A(10), 2172–2177 (1999)
7. Tzeng, W.G., Hu, C.M.: A new approach for visual cryptography. Designs, Codes and Cryptography 27(3), 207–227 (2002)
8. Yang, C.N.: New visual secret sharing schemes using probabilistic method. Pattern Recognition Letters 25(4), 481–494 (2004)
9. 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)
10. 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)
11. 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)
12. Yang, C.N., Chen, T.S.: Size-adjustable visual secret sharing schemes. IEICE Transactions 88-A(9), 2471–2474 (2005)
13. 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)
14. Horng, G., Chen, T., Tsai, D.S.: Cheating in visual cryptography. Des. Codes Cryptography 38(2), 219–236 (2006)

15. 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)
16. Yang, C., Laih, C.: Some new types of visual secret sharing schemes, vol. III, pp. 260–268 (December 1999)
17. Hu, C.M., Tzeng, W.G.: Cheating prevention in visual cryptography. IEEE Transactions on Image Processing 16(1), 36–45 (2007)
18. Biehl, I., Wetzel, S.: Traceable visual cryptography. In: Han, Y., Quing, S. (eds.) ICICS 1997. LNCS, vol. 1334, pp. 61–71. Springer, Heidelberg (1997)
19. Kang, H.R.: Digital Color Halftoning. In: Society of Photo-Optical Instrumentation Engineers (SPIE), Bellingham, WA, USA (1999)
20. Zhou, Z., Arce, G.R., Crescenzo, G.D.: Halftone visual cryptography. IEEE Transactions on Image Processing 15(8), 2441–2453 (2006)
21. Myodo, E., Sakazawa, S., Takishima, Y.: Visual cryptography based on void-and cluster halftoning technique. In: ICIP, pp. 97–100 (2006)
22. 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)
23. Wang, Z., Arce, G.R.: Halftone visual cryptography through error diffusion. In: ICIP, pp. 109–112 (2006)
24. Ateniese, G., Blundo, C., De Santis, A., Stinson, D.R.: Extended capabilities for visual cryptography. Theoretical Computer Science 250(1-2), 143–161 (2001); 102 Weir, J., Yan, W.
25. Nakajima, M., Yamaguchi, Y.: Extended visual cryptography for natural images. In: WSCG, pp. 303–310 (2002)
26. 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)
27. Ulichney, R.A.: Digital Halftoning. MIT Press, Cambridge (1987)
28. 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)
29. Wang, D., Zhang, L., Ma, N., Li, X.: Two secret sharing schemes based on Boolean operations. Pattern Recognition 40(10), 2776–2785 (2007)
30. 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)
31. Viet, D.Q., 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)
32. 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)
33. Naor, M., Shamir, A.: Visual cryptography ii: Improving the contrast via the cover base. In: Crispo, B. (ed.) Security Protocols 1996. LNCS, vol. 1189, pp. 197–202. Springer, Heidelberg (1997)
34. Yang, C.N., Laih, C.S.: New colored visual secret sharing schemes. Designs, Codes and Cryptography 20(3), 325–336 (2000)
35. Fang, W.P.: Friendly progressive visual secret sharing. Pattern Recognition 41(4), 1410–1414 (2008)

36. 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)
37. Katoh, T., Imai, H.: An extended construction method for visual secret sharing schemes. IEICE Transactions J79-A(8), 1344–1351 (1996)
38. Yang, C.N., Chen, T.S.: Extended visual secret sharing schemes: Improving the shadow image quality. IJPRAI 21(5), 879–898 (2007)
39. Wu, H.C., Chang, C.C.: Sharing visual multi-secrets using circle shares. Computer Standards & Interfaces 28, 123–135 (2005)
40. 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)
41. 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)
42. Memon, N., Wong, P.W.: Protecting digital media content. Communications of the ACM 41(7), 35–43 (1998)
43. 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)
44. Hwang, R.J.: A digital image copyright protection scheme based on visual cryptography. Tamkang Journal of Science and Engineering 3(2), 97–106 (2000)
45. 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)
46. Sleit, A., Abusitta, A.: A visual cryptography based watermark technology for individual and group images. Systemics, Cybernetics and Informatics 5(2), 24–32
47. Chuang, S.C., Huang, C.H., Wu, J.L.: Unseen visible watermarking. In: ICIP(3), pp. 261–264. IEEE, Los Alamitos (2007)
48. 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)
49. Praun, E., Hoppe, H., Webb, M., Finkelstein, A.: Real-time hatching. In: ACM SIGGRAPH 2001, pp. 579–584. ACM, New York (2001)
50. 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, pp. 572–575 (May 2004)