Sharing Multiple Secrets Using Visual Cryptography

Jonathan Weir
Queen’s University Belfast
Belfast BT7 1NN UK
Email: jweir07@qub.ac.uk

WeiQi Yan
Queen’s University Belfast
Belfast BT7 1NN UK
Email: w.yan@qub.ac.uk

Abstract — Visual cryptography provides a very powerful technique by which one secret can be distributed into two or more pieces known as shares. When the shares on transparencies are superimposed exactly together the original secret can be discovered without computer participation. In this paper, we take multiple secrets into consideration, and generate a master key for all the secrets; correspondingly, we share each secret using the master key and obtain multiple shares. We merge these shares into a combined share, we adjust the master key and generate a new key, the secrets are revealed when the key is superimposed on the combined share in different locations using the proposed scheme. We provide the corresponding results in this paper.

I. INTRODUCTION

Visual cryptography (VC) [1] is a powerful technique that combines the notions of perfect ciphers and secret sharing in cryptography with that of raster graphics. A binary image can be divided into shares that can be stacked together to approximately recover the original image. Visual cryptography is a unique technique in the sense that the encrypted messages can be decrypted directly by the human visual system. The distinguishing characteristic of VC is the ability to restore secrets without the use of computation.

The initial implementation assumes that the image or message is a collection of black and white pixels, each pixel is handled individually. The encryption technique 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.

Originally, visual cryptography shares binary images; later on, researchers introduced halftone and color halftone mechanisms to visual cryptography [2], to share color and grayscale images [3]. This paper will focus on how to share multiple secrets using visual cryptography rather than considering only one secret.

Fig. 1 illustrates the flowchart of our proposal. We merge two secrets into shares using the master key, we combine the two shares to form a new share $S_1$, correspondingly, we modify the master key and generate a key share, $S_2$. The new share ($S_1$) and the key share ($S_2$) are employed to recover the secrets by shifting the key share ($S_2$) to various positions on $S_1$.

For disjoint sharing, this scheme involves two secrets and one key. The secrets are encrypted using the same master key and placed next to each other, either vertically, horizontally or diagonally. When the key is superimposed the first secret becomes revealed. The same is true for the second secret. The key has to be shifted by the images width or height in order to reveal the next secret. Any number of shares can be encrypted using the same key.

The joint sharing scheme works in a similar way. Shares are generated using the master key, these shares will be merged by inserting different rows of the shares into the scanning lines of the combined share in the spatial domain. When the key share is superimposed on the combined share, the first secret becomes visible, when the key is shifted down slightly, the second secret is revealed.

The remaining sections of this paper will be organized as follows: Section II outlines the related work based on visual cryptography and in particular how the shares should be generated. In Section III, our contributions to visual cryptography are outlined and the results discussed in Section IV. The final conclusions are detailed in Section V.

II. RELATED WORK

In visual cryptography, 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. 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 operation of the rows in the matrix. The pixels can be arranged in various ways within the matrix. 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.
Zhou et al. [4] along with [5], [6] and [7], present novel techniques by which halftone images can be shared with significant visual meaning which have a higher quality than the images presented in [8] by employing error diffusion techniques [9]. However, these schemes are still constrained in that only one secret can be hidden within the halftone shares.

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.

This problem was previously considered by Wu and Chen [10]. They concealed two secrets with 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 $90^\circ$ and superimposed on $S_2$. Due to the nature of the angles required for revealing the secrets ($90^\circ$, $180^\circ$ or $270^\circ$) and the fact that this scheme can only share, at most, two secrets, it becomes apparent that it is quite limited in its use.

Multiple secret sharing was developed further [11] by designing circular shares so that the limitations of the angle ($\theta = 90^\circ$, $180^\circ$, $270^\circ$) 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 $0^\circ$ and $360^\circ$.

A further extension of this was implemented in [12] 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 Chang’s scheme.

More recently, another novel multi-secret sharing scheme [13] 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. 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 [3] or colour composition [14].

Finally, the aspect ratio of the shares becomes an issue. It isn’t possible to share images using this technique without distorting the aspect ratio. We attempt to rectify this issue within this paper.

III. OUR CONTRIBUTIONS

Our contribution in this paper is to deal with joint sets of shares. The aim of the research is to merge the existing shares of Visual Cryptography together (jointly) and use one master key to decrypt them.

The master key is a randomly generated image using the patterns of visual cryptography. It is generated using a random one-time pad, this allows it to be unconditionally secure [15] when combined with a truly random pad. This means that even if an adversary knows how to generate the master key or the disjoint/joint shares they will have no clues as to how they can reconstruct the hidden secrets. After the master key is generated using the random one-time pad, the pad is discarded, leaving no evidence as to how the disjoint/joint shares or master key where generated.

A. Disjointly Dynamic Visual Cryptography

The idea behind a disjoint combination of shares is to share separate images with the same master key and then arrange the shares into one image horizontally, vertically or diagonally. When the key is superimposed on the combined image, the secret will become available. If the shares are arranged horizontally, shifting the key in the horizontal direction will reveal all the secrets. Instead of generating two shares in the traditional visual cryptography, one share is combined from various shares using the master key. Disjointly dynamic visual cryptography has the ability to compose any size of shares.

B. Jointly Dynamic Visual Cryptography

The idea of a joint sharing scheme allows a user to generate two shares based on the original visual cryptography scheme, like the disjoint example plus the secure key. Outlined below are three different techniques used to accomplish this.

1) Contrast Based Joint combination of Shares: Contrast based joint combination of shares is built on the idea that we can create multiple shares and one master key. Overlapping the shares to give one final share and by superimposing the key, the first share is revealed. Shifting the key horizontally or vertically will reveal the other secrets.

Given the first secret and the master key, we write the pixels from the corresponding patterns of black pixels of the secret onto a blank image as a combined share using visual cryptography. For the second secret, we write the similar pixels on the blank region of the combined share. For the remaining regions on the combined share, we fill them up using the sharing patterns of white pixels. Mathematically, we can express this scheme by the following equations:

\[
b_{w,0} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \] (1)

\[
b_{w,1} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix} \] (2)

\[
b_{w,2} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \] (3)

where $b_{s_1,s_2} \in \{0,1\}$ is the pixel value of the share by given the pixel $s_1$ of secret 1 and $s_2$ of secret 2 with the pixel $c \in \{0,1\}$ of the cover image [16].

One solution to this problem can be implemented during the encryption process on each of the shares before they are overlapped. The process involves creating the first half of a share, $S_1$, with a darker (3/4) contrast to its upper half and creating the lower half of the other share, $S_2$, with a darker contrast, so when $S_1$ and $S_2$ are overlapped to generate the final share, it appears to be of a single contrast and does not give away any information about how many layers it could be made up from.

The disadvantage of this scheme is that it cannot share the secrets which have been made up fully of black pixels since
the second secret will have no room to be inserted in the rest space. To deal with this scheme, we propose the following scanning lines based even-odd joint combination of shares.

2) Even-Odd Joint Combination of Shares: Given two secrets with the same size, we can share them via two shares using a randomly generated master key. The two shares can be merged by filling the first share to the even rows of the combined image and the second share to the odd rows. The combined share will be twice the size of the secrets. Therefore, the master key has to be adjusted to generate a new key, the key will be employed to restore the secrets.

Even-odd joint combination can generate any size of share. The difference between even-odd joint combination and the disjoint combination of shares is that the key is of the same size as the share with the two hidden secrets. This helps to increase the capacity and security of the scheme as it gives away no indication to the amount of secrets hidden, based on the key size.

In dynamic joint sharing, each pixel from secret one is converted to its $2 \times 2$ array and then placed into the group of four pixels in the final share. The same process is repeated for all other pixels in secret one. The same is done for the other three secrets, but they are offset by a certain amount. The same process is done when creating the key share from the master key, but the ordering is reversed. If it wasn’t reversed then simply superimposing the key would reveal all four secrets at once. As such, we have to shift the key by four pixels (two pixels up or down, two pixels right or left) in each case to reveal the hidden secret.

IV. RESULTS

We developed and designed a web based system using python which can be used globally at any time. The results from this system are presented within this section.

A. Disjointly Dynamic Visual Cryptography

Given two secrets of the same size, the shares will be generated from them using the same master key. When the shares are lined up in vertical, horizontal or diagonal direction respectively, the key is able to decrypt each of the shares when it is superimposed. Fig. 3 is an example of disjoint image sharing, Fig. 3(a) and (b) are original images, Fig. 3(c) is the combined share, Fig. 3(d) is the master key, Fig.3(e) and (f) are the recovered secrets.

B. Jointly Dynamic Visual Cryptography

Given two secrets, a master key and the corresponding shares will be generated. The shares will be merged to one image spatially. The challenge is to merge two shares that intersect. When the master key is superimposed on different positions of the merged shares, the secret images should appear. One of our results with multiple secrets is shown in Fig.4, from left to right, the figures are master key, combined share, recovered secret 1 and recovered secret 2. When the key is superimposed, secret 1 appears; when the key is shifted down to the bottom, secret 2 is revealed.

In order to merge multiple shares together, we extend the size of the merging shares and insert one share into odd scan lines and another into even scan lines shown in Fig.5(a). Correspondingly, the master key has to be extended. One of our results with multiple secret sharing is shown in Fig.5(b).
Based on the four secrets (black bars), we generate a master key and a combined share using the proposed scheme. When the master key is moved to different positions on the combined share, we can recover multiple secrets. The same is true for Fig. 5(c) which also illustrates the secret recovery using the word GOAL which increases in size as the master key is moved around the merged share. We insert all the recovered images into a GIF file to get an animated illustration of the process.

V. CONCLUSIONS

From the previous visual cryptography schemes proposed and demonstrated within this paper, it is possible to see that being able to hide secrets within images can prove to be highly advantageous. The most interesting results are gained when using a key that is the same size as the final share which may contain a number of different images. This makes it harder to determine whether the shares have actually been encrypted with just one hidden secret or with a large number of secrets.

Our future work will focus on multiple secret sharing using color images by hiding secrets within the color image without specifically altering the image in any noticeable way.

REFERENCES