About a visual secret sharing scheme

RUXANDRA-FLORENTINA OLIMID
Faculty of Mathematics and Computer Science
University of Bucharest
ROMANIA
E-mails: ruxandra.olimid@fmi.unibuc.ro

Abstract: The paper presents a VSS (Visual Secret Sharing Scheme) for sharing black-and-white secret images, providing perfect recovery of the initial picture when all participants cooperate and full secrecy for at most 2 cooperating participants. The construction of the scheme is based on the idea that the shares are represented by colored images constructed by using a random choice of pixel color, except some mandatory but easy to achieve constraints. One other advantage of the scheme is its simplicity exposure.

Key-Words: secret sharing, visual secret sharing, visual cryptography

1 Introduction

Visual secret sharing schemes (VSS) were first introduced by Naor and Shamir in 1994. A secret scheme permits the “splitting” of a secret between n participants. Each participant receives one share through a secure channel. The secret can be reconstructed only by authorized groups of users, by putting together their private shares. Unauthorized groups of users should not be able to reveal the secret or significant information about it.

In the case of VSS the secret, and therefore the shared components, consist of images, each image being considered a matrix of pixels. From their first introduction in [3], multiple ways of constructing VSS have been created for each class of images: black-and-white, gray-scale or colored.

Despite the multitude of existing VSS for each category of images, usually a secret image corresponding to one class is divided into components belonging to the same class. However, Ito, Kuwakado and Tanaka introduced a way to share a black-and-white secret image into colored images components. For more information, the reader is invited to refer to [2].

The paper will exemplify and analyze a scheme based on the same idea of using colored shares for black-and-white images. The scheme will provide no secret information for a coalition of less then 3 out of n participants.

2 The VSS Scheme

2.1 RGB Model

The RGB model is a model in which Red (R), Green (G) and Blue (B) are mixed together, each one with its own intensity, in order to reproduce the whole color spectrum. RGB is an additive color model in the sense that white results by adding red, green and blue together at maximum intensity. Adding any other color to white it remains white. Black is considered to be the absence of any color (Figure 1).

The presented scheme uses just the primary colors for the shares. Because in the composed image each pixel is obtained by adding the corresponding pixels of the components, the reconstructed image will be colored in cyan, magenta, yellow and white.

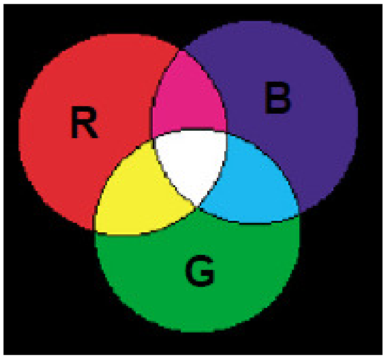


Figure 1

2.2 Scheme Presentation

The secret image consists of only black and white pixels, while the shared components will contain only red (R), green (G) or blue (B) pixels. To each pixel of the secret image will correspond exactly one pixel of each share.

A white pixel of the secret image can be compose by adding together colored pixels of components if among the added pixels exist at least one red pixel, one green pixel and one blue pixel.

In order to complete the sharing of a black-and-white picture, the black pixel must be somehow coded. To achieve that, every pixel different from white from the resulting picture will be considered to be black.

More precisely, the VSS can be presented as follows:

- <u>Computing shares</u>

a) The pixels of the secret shares are randomly choose from {R, G, B} so that:

a1) if the pixel of the secret image is white, then there must exist a component with the corresponding pixel R, another component with the corresponding pixel G and a third component, different from the previous two, with the corresponding pixel B;

a2) if the pixel of the secret image is black, then all the corresponding pixels of the shares are randomly chose from {R, G}, from {R, B} or from {G, B} so that there exist at least 2 pixels of different colors.

b) Previous step is repeated for each pixel of the secret image;

- <u>Components sharing</u>

Shares previously computed are securely transmitted, one to each participant.

- <u>Secret reconstruction</u>

a) k users try to reconstruct the secret by overlapping their correspondent shares (the shares are added together, pixel by pixel);

b) Each colored computed pixel in the resulting image is transformed into a black pixel. White pixels remain unchanged.

As a remark, a1 condition assures that all white pixels from the initial image are correct reconstructed when all participants cooperate. Similarly, a2 condition ensures that a black pixel can never be reconstructed into a white pixel.

Black pixel coding is not always the same, but differs between the 3 possible variants (R and G, R and B, G and B) in order to keep a similar repartition of R, G, and B into the shares. This is important because otherwise, a participant could benefit of some secret information from its only share.

It is important to notice that the components of the participants must be kept colored, and not converted to black-and-white. Otherwise the addition model will not work anymore.

A significant difference from Ito, Kuwakado and Tanaka scheme is that the pixels color in the components are randomly chosen from R, G and B. The usage of randomness eliminates the need of the fixed matrices, idea inherited from Naor-Shamir.

Another add-on to the presented scheme is the conversion of the recreated image from color to black and white. This way, the contrast of the reconstructed image grows, getting the picture closer to the original one.

Figure 2 exemplifies the shares generation and the reconstruction in the case of a 2x2-pixel white image and a black 2x2-pixel black image for n=5 participants. It can be observed that the black pixel does not always use the same couple of colors.

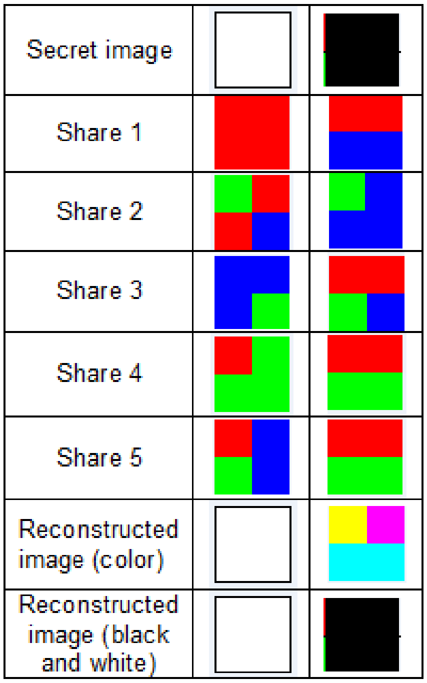

Secret image
Share 1
Share 2
Share 3
Share 4
Share 5
Reconstructed image (color)
Reconstructed image (black and white)

Figure 2

3 Scheme Analysis

3.1. Parameters

As it derive from the scheme definition, in order to represent a white pixel, at least 3 shares are needed (one R pixel, one G pixel and one B pixel, each one belonging to a component). So, the scheme can be used only for 3 or more participants.

3.2. Efficiency

Each participant is required to store one image of the same size of the shared image. Therefore, the scheme can be considered efficient.

3.3. Information revealing

The scheme secrecy analysis is done under the general accepted assumption that the entity that computes the shares is trustable and the distribution of shares to participants is perfectly secure.

The goal is to identify the quantity of information revealed to k participants by putting their shares together.

- k=1

One participant cannot find any information about the secret image by using only its component. This is because its image is composed from randomly chosen R, G or B pixels, which can lead to either white or black pixels by the overlapping of another component;

- k=2

Two participants putting their shares in common will lead to a totally black image. This is because in order to obtain a white pixel at least 3 components are needed.

- 2<k<n

More than 2 participants can obtain additional information about the secret image by adding their shares.

A white pixel obtained in their reconstructed image definitely corresponds to a white pixel in the secret image. That is because the secret image is reconstructed by adding together all the components and no matter what the other component's pixel colors are, added with white will remain unchanged.

But, they cannot find any information about the pixels in the secret image that corresponds to black pixels in the reconstructed image. This is due to the fact that a black pixel corresponds to adding pixels of only 2 types (R and G, R and B or G and B) and there can exist another component that has the corresponding pixel of the different color (B, G or R).

By growing the number k of complotting participants, the probability to compose a correct white pixel becomes higher (the probability to meet a R, G and B pixels on 3 different shares on the same position increases).

Therefore, the scheme is monotone.

- k=n

If all the participants add their components together, the result will be exactly the secret image. The proof is clear from the construction.

So, the scheme is perfectly secure for less then 3 participants putting together their shares and it leads to a perfect reconstruction of the secret image if all participants cooperate. For all other possible associations of participants, the reconstructed image quality depends of the randomly chosen colors of pixels. The information revealed to k > 2 participants is high (fact supported also by experiment), revealing important information about the image.

3.4. Random generator

One random choice should be taken for each black pixel of the secret image in order to establish the selected pair of colors and one random decision should be taken for the color of each pixel of each share.

The generation of random numbers can be sometimes tricky and difficult to implement. However, this is not the case because the selections must be done in a narrow range and the quality of the random generator could be not very high.

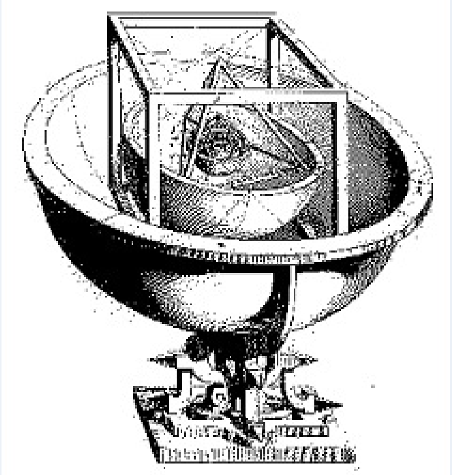


Figure 3

4 Implementation and results

The previous presented scheme was implemented in Python, using Python Imaging Library (PIL) [4].

For exemplifying, the picture from Figure 3 and n = 4 participants are given as input. The result components are listed below, to a smaller scale:

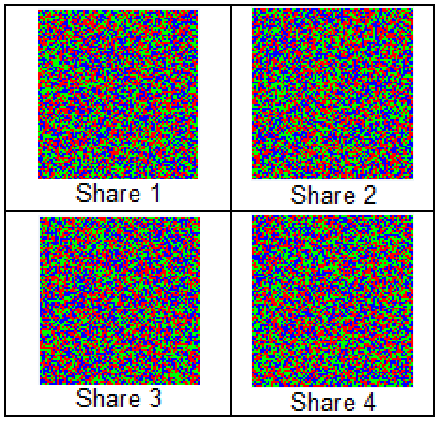


Figure 4

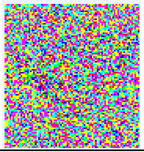
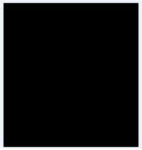
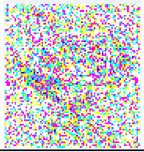
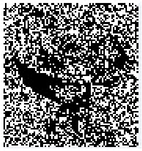
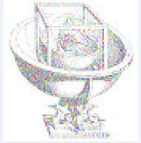
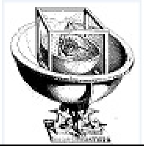
No of hares used (k)	Color computed secret	Black and white computed secret
2		
3		
4		

Figure 5

An example for a possible reconstruction for k = 2 and 3, as well as the computation using all shares is given in Figure 5.

The components and reconstructed image

were rescaled at pasting to the present paper for a proper editing. The scheme restores the image at its original size.

It can easily be seen that the practical implementation supports the theory presented in the previous section:

- 1 participant doesn't benefit of any information regarding the secret image from its only share;
- 2 shares combined together are providing a totally black image;
- 3 participants can reconstruct an image quite closed to the original one;
- 4 participants obtain the exact secret image.

The images obtained directly by adding participant's secret components, before the conversion to black and white are also printed in order to highlight the importance of the final black and white conversion.

5 Conclusions

The presented visual secret scheme allows splitting a secret image into n secret components relying on a random choose of colored pixels, satisfying some easily achieve constraints. The scheme reveals no information for 1 or 2 associated participants, but provides information to 3 or more than 3 coupling participants. Adding the conversion to black and white image at the end of the reconstruction phase has effect on raising the quality of the obtained image. Therefore, when all participants cooperate, the exact secret image is recovered.

References:

[1] Y.C.Hou, Visual Cryptography for Color Images, http://ma1.eiius.es/miembros/valvarez/proyectos/viscryptcolor.pdf

[2] R.Ito, H.Kuwakado, H.Tanaka, Image size Invariant Visual Cryptography, citeseer.ist.psu.edu/353362.html

[3] M.Naor, A.Shamir, Visual Cryptography, http://www.cs.ncuu.edu.tw/~raylin/UndergraduateCourse/ContemporaryCryptography/Spring2009/VisualCrypto.pdf

[4] Python Imaging Lybrary (PIL), http://www.pythonware.com/products/pil/