Visual Cryptography - Supporting Documentation

Sparsh Gupta, Mark Belanger, Sidney Taylor

December 12, 2023

Intro to Visual Cryptography

Visual cryptography is an encryption technique that decomposes images into multiple noisy and individually meaningless images, called shares. It is a unique form of encryption as it relies solely on human vision to decrypt and understand the information as images without complex mathematics needed to process the decrypted message. The most common type of visual cryptography was developed by Moni Naor and Adi Shamir in 1994, and will be the focus of the rest of our exploration.

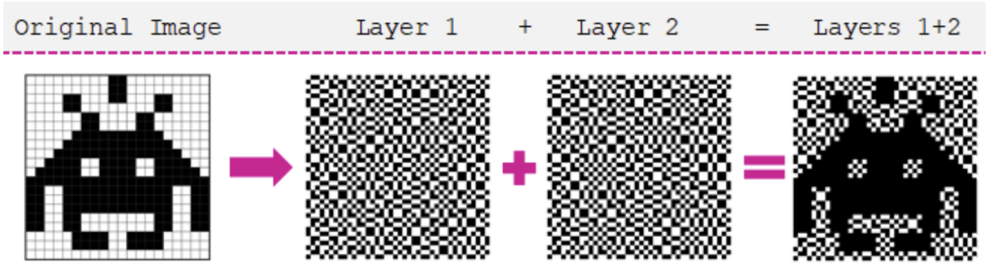


Figure 1: Base level diagram outlining the idea of visual cryptography.

The approach is commonly described as the “secret sharing problem”.

In particular, this approach consists of superimposing the shares to recover the secret image. Naor and Shamir extended this basic idea to a k out of n secret sharing problem ((k,n) scheme), where n is the number of shares and k is the minimum number of shares required to recover the secret image.

For example, this means that in a “3 out of 7” visual cryptography scheme, the secret image would be divided into 8 shares, Any 3 or more shares overlayed should provide the the original secret image, and any less than 3 shares overlayed should result in no information about the secret image being discernible.

This approach is one of the most reliable for many reasons, one of these being its robustness. As long as the number of shares required for reconstruction is kept secret. It also has a high degree of independence, as having less than k shares gives 0 information about the secret image and whatever information may be encoded.

Shamir's Visual Secret Sharing Scheme

The scheme's broad idea is that we have an image with black-and-white pixels, and this image is broken up into n shares such that the image can only be decrypted if k or more shares are stacked together, otherwise stays encrypted.

The original problem involves generalizing k=2 and n=2.

This scheme (Shamir's VC scheme) can also be generalized as a k out of n secret sharing problem.

Each share is made up of m black and white sub-pixels and these shares can also represented as a $n \times m$ matrix (let us call it S) consisting of only binary values. So, white pixels have a value of 0 and black pixels have a value of 1.

Each individual sub-pixel in a share can be represented as $(s_{i,j})_{m \times n}$ such that j denotes the sub-pixel-position and i refers to the share.

$(s_{i,j})_{m \times n} = 1$ if the j-th sub-pixel in the i-th share is black or $(s_{i,j})_{m \times n} = 0$ if the j-th sub-pixel in the i-th share is white.

For the (2,2) Shamir's VC scheme, we can obtain matrices C_0 and C_1 depending upon the permutations of shares and pixels for the sub-pixel shares for a white pixel and a black pixel respectively. Let us understand it deeply below.

If we look at Fig.[2], we can see that the first share, when converted into a vector would have the values [0 0 1 1]. The second share in the same figure also has the same vector value [0 0 1 1]. Now, when we overlay these 2 shares, we can obtain a share for a white pixel, and therefore obtain the matrix for this particular share which is $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$. Now, we can permute the columns in this matrix to obtain other matrices that would also work for a white sub-pixel pattern, and therefore this set of matrices would be C_0.

If we look at Fig.[3], we can see that the first share, when converted into a vector would have the values [0 0 1 1]. The second share in the same figure also has the same vector value [1 1 0 0]. Now, when we overlay these 2 shares, we can obtain a share for a black pixel, and therefore obtain the

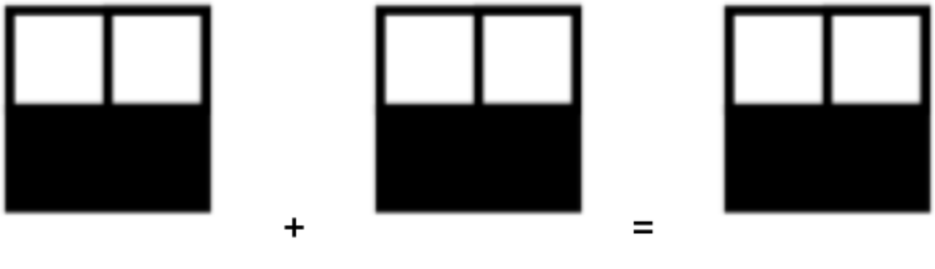


Figure 2: White pixel (C_0) example

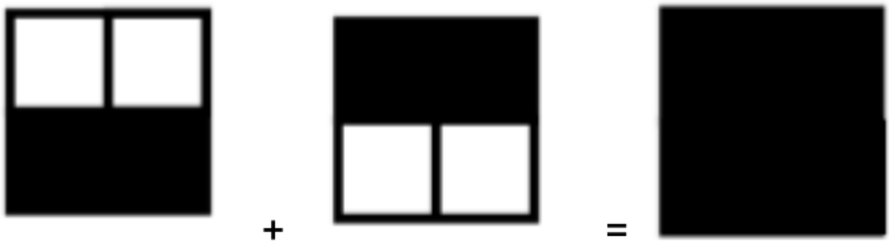


Figure 3: Black pixel (C_1) example

matrix for this particular share which is $\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$. Now, we can permute the columns in this matrix to obtain other matrices that would also work for a black sub-pixel pattern, and therefore this set of matrices would be C_1.

This scheme therefore results in a pixel expansion such that a single white or black pixel can be represented using 4 sub-pixels.

Furthermore, there are three parameters in this scheme:

1. m is the number of pixels in each share.
2. α is the relative weight difference of a white pixel and a black pixel between the original image and the decrypted image (i.e. the combined shares). For a k out of n scheme, this is calculated by using $\alpha = \frac{1}{2^{k-1}}$ where k is the number of shares required to decrypt the image. Therefore, for Shamir's (2, 2) scheme, this is 1/2.
3. γ represents the size of the collection of matrices C_0 and C_1.

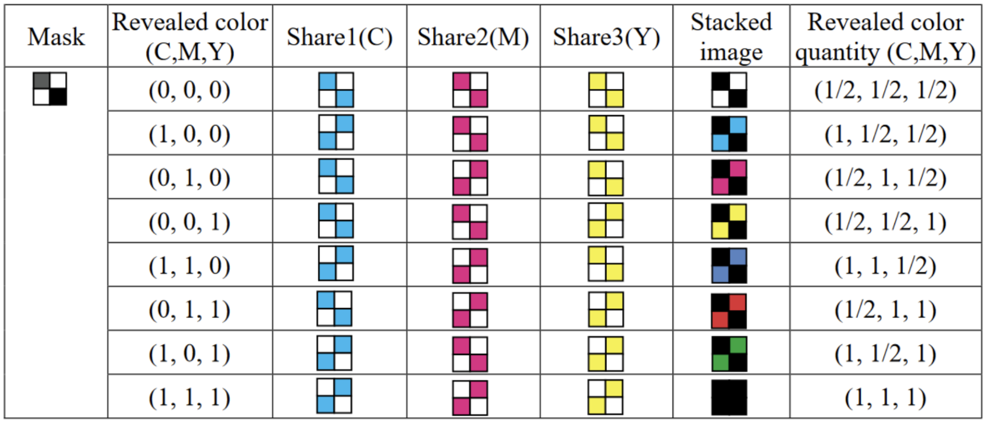
Once we obtain the overlayed image, it is basically an OR operation of each m vector V in the matrix. The Hamming weight of these vectors can be denoted by $H(V)$. Now, to determine if we have a black pixel pixel or a white pixel, we perform this simple computation. So, if $H(V) \leq d$, then it is interpreted as a black pixel, and if $H(V) \leq d - \alpha m$, then it is interpreted as a white pixel. Here, d is some fixed threshold such that $1 \leq d \leq m$ and relative difference $\alpha > 0$.

Visual Cryptography for Color Images

An image message is disassembled into cyan, magenta, and yellow (CMY) pixel weights, where varying combinations of these weights generate different colors. The potential colors include white, cyan, magenta, yellow, blue, red, green, and black. Notably, white is considered transparent, and the overlay of all three CMY components results in black. The pixel expansion involves breaking down each pixel into 2x2 sub-pixels, with two remaining black and the other two determined by the desired color. Four shares are created for cyan, magenta, yellow, and black, respectively. Fig.[4]

The algorithm is applied to each pixel, starting with randomly assigning two sub-pixels for the black mask. The positions of the cyan sub-pixels are then determined based on the location of the black sub-pixels, where two are cyan, and two are white/transparent. If the cyan weight is 1, the pixel is shown and should not be covered by the black sub-pixels; conversely, if the cyan weight is 0, the pixel should be covered. This process is repeated for magenta and yellow, resulting in the final composition of the image.

Figure 4 shows the possible colors that this scheme can create. For example, red requires magenta and yellow to be mixed and overlayed to output red. If cyan is present the resulting color would not be red so the cyan must be colored. In this example, the black subpixel group selected for a pixel has the 2 left subpixels black and 2 right subpixels white/transparent. Since magenta and yellow, the colored portions of their respective subpixel groups will be selected so that they correspond with the white/transparent. Cyan however cannot be present so the colored part of the cyan subpixel group must correspond to the black part of the black shares subpixel group. This means that magenta and yellow will be shown but cyan will not



Mask	Revealed color (C,M,Y)	Share1(C)	Share2(M)	Share3(Y)	Stacked image	Revealed color quantity (C,M,Y)
	(0, 0, 0)					(1/2, 1/2, 1/2)
	(1, 0, 0)					(1, 1/2, 1/2)
	(0, 1, 0)					(1/2, 1, 1/2)
	(0, 0, 1)					(1/2, 1/2, 1)
	(1, 1, 0)					(1, 1, 1/2)
	(0, 1, 1)					(1/2, 1, 1)
	(1, 0, 1)					(1, 1/2, 1)
	(1, 1, 1)					(1, 1, 1)

Figure 4: Color VC scheme

Bibliography

[1] Shamir Visual Cryptography: https://www.cs.jhu.edu/ fabian/courses/CS600.624/NaorShamir-VisualCryptography.pdf
(used for understanding Shamir's visual crypto algorithm)

[2] An overview of visual cryptography techniques: https://www.researchgate.net/publication/353374619_An_overview_of_visual_cryptography_techniques
(used for looking into more visual cryptography algorithms)

[3] Visual Cryptography website: https://www.ciphermachinesandcryptology.com/en/visualcrypto.htm
(used for extracting the animation on title slide of presentation and understanding pixel expansion)

[4] Visual Cryptrography for Color Images: https://www.sciencedirect.com/science/article/pii/S0031320302002583#SEC3
(used for understanding the visual crypto algorithm for color images and also several figures from the paper are included in the presentation)

[5] Visual Cryptography PPT - University of Bristol:
https://homes.esat.kuleuven.be/ fvercaut/talks/visual.pdf
(used for obtaining images to create our example for how shamir's VC scheme works)

[6] A Comprehensive Study of Visual Cryptography: https://fardapaper.ir/mohavaha/uploads/2018/12/Fardapaper-A-Comprehensive-Study-of-Visual-Cryptography.pdf
(used for explaining the proof for Shamir's visual secret sharing scheme in this document)

[7] Visual Crytography Tool: https://www.101computing.net/visual-cryptography/
(used to generate the encryption and decryption of 'Discrete Math' figure for Shamir's VC in the presentation)