

Halftone Visual Cryptography

Shruti Dusane, Sushant Gaikwad, Neha Adne, Prajakta Gore, Prof. P.A Patil

Department of Information Technology.

All India Shri Shivaji Memorial Society's, Institute of Information Technology

Abstract: Visual cryptography is a secret sharing scheme which uses images distributed as shares such that, when the shares are superimposed, a hidden secret image is revealed. In extended visual cryptography, the share images are constructed to contain meaningful cover images, thereby providing opportunities for integrating visual cryptography and biometric security techniques. In this project, we propose a method for processing halftone images that improves the quality of the share images and the recovered secret image in an extended visual cryptography scheme for which the size of the share images and the recovered image is the same as for the original halftone secret image. The resulting scheme maintains the perfect security of the original extended visual cryptography approach.

Keywords: Visual cryptography, share generation, share embedding, secret sharing

Introduction:

Visual cryptography (VC), is a secret sharing scheme, based on black and-white or binary images. Secret images are divided into share images which, on their own, reveal no information of the original secret. Shares may be distributed to various parties so that only by collaborating with an appropriate number of other parties, can the resulting combined shares reveal the secret image. Recovery of the secret can be done by superimposing the share images and, hence, the decoding process requires no special hardware or software and can be simply done by the human eye. Visual cryptography is of particular interest for security applications based on biometrics. For example, biometric information in the form of facial, fingerprint and signature images can be kept secret by partitioning into shares, which can be distributed for safety to a number of parties. The secret image can then recovered when all parties release their share images which are then recombined. A basic 2-out-of-2 or (2; 2) visual cryptography scheme produces 2 share images from an original image and must be noted that the recovered image has a degradation in visual quality (specifically, the contrast between white and black is decreased) since a recovered white pixel is actually comprised of 2 white and 2 black subpixels, while a black pixel is represented by 4 black subpixels in the recovered image. It is also obvious that, while the shares appear to be random (and, in fact, can be shown to contain no informational content that can be used to recover the original secret image on their own), the shares also have no interesting content that could be used to carry other information (such as a biometric image) that might be helpful in a security context. For example, if a share image could be selected to be the fingerprint of the share holder, this could be useful in authenticating a user's right to hold that share when the parties meet to combine their share images to reveal the secret.















Pixel		
Prob.	50% 50%	50% 50%
Share 1	 	 
Share 2	 	 
Stack share 1 & 2	 	 
	FOR WHITE PIXEL	FOR BLACK PIXEL

Fig 1: . Scheme for generation of 2-out-of-2(2,2)VC scheme: a selected secret pixel can be encrypted with two sub-pixels in each of the two shares.

HALFTONE VISUAL CRYPTOGRAPHY

A. Visual cryptography scheme

Here we present some basic definitions below which are required to understand before actually learning the VCS model and its further applications.

1. Secret image: It is defined as the original secret image which has to be obscured. .
2. Hosts: These are kinds of images which are used to encode the secret image.
3. Shares: The secret image(SI) is encrypted and disintegrated into n separate images that sometimes looks as random images that contains noise only (in the case of (k, n)VCS) or sometimes as a raw host image.
4. Target: These are the images which are reconstructed by super imposing the different shares.
5. Sub pixel: Each pixel P of an image is divided into a specific number of sub pixels during the encryption steps.
6. Pixel Expansion (m): It is related to the increase in the number of pixels. When the size (width or height) of the decrypted image is bigger when compared to the (SI) original secret image, this change called as "*pixel expansion*" for example: if each of the pixels is boomed into 2subpixels inside each of the share as depicted in Fig. 1. Here pixel expansion $m=2$.
7. Relative Contrast: The difference in intensity measurement between black pixels and white pixels in the target image

System Analysis:

Existing

System:

In visual cryptography, the decoding process is performed directly by the human eyes; while in existing, the shared images need some processing to reconstruct the secret image. The increasing numbers of possibilities to create, publishes, and distribute images calls for novel protection methods, new sharing and access control mechanisms for the information contained in the published images. Secure image sharing techniques overcome the traditional cryptographic approach, providing new solutions for the development of new and secure imaging applications.

Proposed System:

We have proposed a (t, n) VC scheme with flexible value of (n) . From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies, which reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of (t, n) VC with unlimited. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic model is adopted in the scheme.

Working :

Each pixel of the images is divided into smaller blocks. There are always the same number white (transparent) and black blocks. If a pixel is divided into two parts, there are one white and one black block. If the pixel is divided into four equal parts, there are two white and two black blocks. The example image uses pixels that are divided into four parts.

In the following table we can see that a pixel divided into four parts can have six different states. If a pixel on layer 1 has a given state, the pixel on layer 2 may have one of two states: identical or inverted to the pixel of layer 1. If the pixel of layer 2 is identical to layer 1, the overlaid pixel will be half black and half white. Such overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be completely black. This is an information pixel.

We can now create the two layers. One transparent image, layer 1, has pixels which all have a random state, one of the six possible states. Layer 2 is identical to layer 1, except for the pixels that should be black (contain information) when overlaid. These pixels have a state that is opposite to the same pixel in layer 1. If both images are overlaid, the areas with identical states will look gray, and the areas with opposite states will be black.

The system of pixel can be applied in different ways. Each pixel can be divided into four blocks. However, we can also use pixels, divided into two rectangle blocks, or even divided circles. Also, it doesn't matter if the pixel is divided horizontally or vertically. There are many different pixel systems, some with better contrast, higher resolution or even with color pixels.

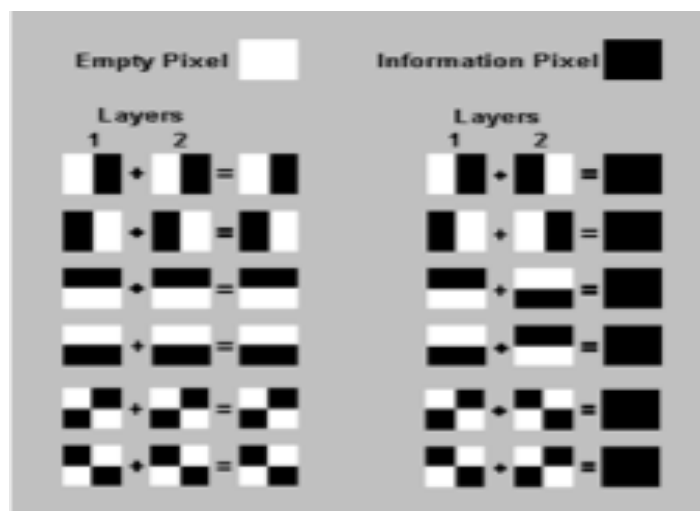
If the pixel states of layer 1 are truly (crypto secure) random, both empty and information pixels of layer 2 will also have completely random states. One cannot know if a pixel in layer 2 is used to create a grey or

black pixel, since we need the state of that pixel in layer 1 (which is random) to know the overlay result. If all requirements for true randomness are fulfilled, visual cryptography offers absolute secrecy according to the Information Theory.

If visual cryptography is used for secure communications, the sender will distribute one or more random layers 1 in advance to the receiver. If the sender has a message, he creates a layer 2 for a particular distributed layer 1 and sends it to the receiver. The receiver aligns the two layers and the secret information is revealed, this without the need for an encryption device, a computer or performing calculations by hand. The system is unbreakable, as long as the two layers don't fall together in the wrong hands. When one of both layers is intercepted it's impossible to retrieve the encrypted information.

So we can conclude that for a set of n participants, a secret image S is encoded into n shadow images which are called shares. Each participant gets one share. If there are n participants, then k out of n participants are needed to combine shares and the secret image will be seen.

Fig 2: Working of pixels on embedding



Results:

Halftone images of a secret image are used to bring out the 2 sharing images. No hint of the secret picture (SI) can be comprehended may be from one of the sharing images only, here comes the problem that the constituents of the picture are identifiable even now, from the superimposed image. This framework is convenient as it needs only two sharing images for a encrypting a secret picture. Further since these 2 sharing images comprise similar privilege, so such framework is not able to offer a 2-level control. Moreover, the intensity of the colors on the superimposed image is confined in the range of $(1/4, 1/4, 1/4)$ to $(1/2, 1/2, 1/2)$, where $(1/4, 1/4, 1/4)$ represents white-colored pixel and the black pixel is $(1/2, 1/2, 1/2)$. Or we can say that, after superimposition process on the sharing images produced as output by this framework, the scope of color contrast becomes 25 percent of secret picture so, the color saturation of superimposed image brought out by this framework will be worsened. The composite image brought out by this framework will look slightly brighter when compared to original image.

Conclusion:

We have proposed a VC scheme with flexible value of. From the practical perspective, the proposed scheme accommodates the dynamic changes of users without regenerating and redistributing the transparencies,

which reduces computation and communication resources required in managing the dynamically changing user group. From the theoretical perspective, the scheme can be considered as the probabilistic model of VC with unlimited. Initially, the proposed scheme is based on basis matrices, but the basis matrices with infinite size cannot be constructed practically. Therefore, the probabilistic model is adopted in the scheme.

Reference:

1. Z. Zhou, G.R. Arce, and G. Di Crescenzo, "Halftone Visual Cryptography", IEEE Transactions on Image Processing.
2. N. Askari, H.M. Hays, and C.R. Moloney, "An extended visual cryptography scheme without pixel expansion for halftone images" 26th annual IEEE Canadian conference on electrical and computer engineering year 2013.
3. Swati Yadav, Rajesh Kumar rai, "A Probabilistic Model of Visual Cryptography" International Journal of advancement in electronics and computer engineering (IJAECE) 9, December 2012.
4. ANNIE DAISY.V, VIJESH JOE. C, SHINLY SWARNA SUGI.S "An Image Based Authentication Technique Using Visual Cryptography Scheme" International Conference on Inventive Systems and Control (ICISC-2017)