A VISUAL CRYPTOGRAPHY SCHEME WITH LAYERED EXPANSION FOR SECRETHALFTONE IMAGES

M. KarthikBabu1 S. Amarnath Babu2
Pursuing M.Tech, SACET, Chirala, Andhra Pradesh, India1
Assoc. Professor, SACET, Chirala, Andhra Pradesh, India2

Abstract - Visual cryptography may be a cryptographical technique that permits the visible data like pictures, words etc., to be hidde in such a way that decipherment becomes a mechanical operation that doesn't need a laptop. Secret pictures area unit divided into share pictures that, on their own, reveal no data of the initial secret. Shares could also be distributed to numerous parties in order that solely by collaborating with Associate in nursing acceptable range of different parties, willthe ensuing combined shares reveal the key image. Recovery of the key is done by superimposing the share pictures and, hence, the decipherment method needs no special hardware or software package and might be merely done by the human eye. Visual cryptography is of specific interest for security applications supported life science

Key Words — cryptography, image processing, visual cryptography, secret sharing.

INTRODUCTION

Visual cryptography is a cryptographic technique which allows the visible information like images, words etc., to be hidde in such a way that decoding becomes a mechanical operation that does not require a computer. 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 [3]. The secret image can then be recovered when all parties release their share images which are then recombined.

Visual Cryptography provides a friendly setting to subsume the photographs. Typically cryptography tools support only 1 reasonable format. Our application supports .gif and .png formatted pictures.

VCS of Associate in Nursing EVCS, we tend to mean a standard VCS that have an equivalent access structure with the EVCS. Generally, Associate in Nursing EVCS takes a secret image and original share pictures as inputs, and outputs shares that satisfy the subsequent 3 option:

1. Any qualified set of shares will recover the key image;
2. Any verboten set of shares cannot acquire any info of the key image apart from the key image apart from the scale of the image.
3. All the shares are important pictures.

An example of ancient (2, 2) VCS will be found in Fig., where, typically speaking, a VCS suggests that any out of shares might recover the key image. Within the theme of Fig., shares (b) and (c) are distributed to 2 participants on the Q.T., and every participant cannot get any info regarding the key image, however when stacking shares (b) and (c), the key imagewill be determined visually by the participants.

(a) Secret image (b) Share 1 (c) Share 2 (d) Stacked result

Fig: a) Secret Image b) Share 1 c) Share 2 d) Result after placing the share 1 and share2.

PRE-PROCESSING HALFTONE IMAGES

The applying of visual cryptography to grey scale pictures by 1st changing the photographs to a binary image employing a halftoning algorithmic program. The task of the project is to implement an algorithm, which should be fast and the printed images must look good based, on human visual perception. In this project, we survey some of the existing methods. Further, based on2-by-2 block replacement method, we propose an improved algorithm. Their improvements can be divided into three major parts. They are:
1. Adaptive gray level region definition
2. Inclusion of the nearest neighbours in the analysis before halftoning
3. Parallelize the algorithm in order to speed up the conversion.

WHAT IS HALFTONING AND HOW IT WORKS

The grayscale digital image consists of 256 gray levels, while the black and white printers only have one colored ink. So, there is a need to replace wide range of grayscale pixels for printers. These 256 levels of gray should somehow be represented by placing black marks on white paper. Halftoning[6] is a representation technique to transform the original continuous tone digital image into a binary image only of 1's and 0's consisting. The value 1 means to fire a dot in the current position and 0 means to keep the corresponding position empty.

Since the human eyes have the low pass spatial-frequency prosperity, human eyes perceive patches of black and white marks as some kind of average grey when viewed from sufficiently far away. Our eyes cannot distinguish the dots patterns if they are small enough. Instead, our eyes integrate the black dots and the non-printed areas as varying shades of gray. Fig 2(b) shows a typical halftoning image. Zooming in a part of the halftoning image, we can see that the image is actually structured by a certain strategy of distributed black dots.

Fig 2: (a) The original image; (b) The halftoning image; (c) An enlargement of (b)

Here we are using the Block Replacement Method for pre-processing the halftone images.

AN IMPROVED PRE-PROCESSING SCHEME

Block replacement halftoning is a commonly used halftoning technique. In this method each pixel in the original image is replaced by one of the defined set of binary blocks. The dimension of the patterns is determined by screen frequency and the print resolution [1]. For simplicity, assume that each pixel is going to be replaced by a 2X2 matrix. Since the dimension of the matrix is 2X2 then only five different gray levels can be represented by the set of matrices, see Fig 3. The pixel belong to one of the five gray level regions is replaced by the corresponding predetermined candidate. Fig 3 illustrates how this method works. In this illustration the representation for the first and the last pixel are shown. The same is done for the rest of the original image. In Fig 2 the left is the image halftoned by a 2-by-2 block replacement halftoning, and the right is by a 3-by-3 block replacement. The 3-by-3 block replacement can represent ten different gray levels. Comparing the two images (a) and (b), we see that the 3-by-3 block replacement can keep more details than 2-by-2 replacement, the bigger number of gray levels, the higher resolution. In contrast to the ordered dithering method, the arrangement of the black micro dots in the patterns does not have necessarily to be clustered or to be dispersed. Due to the low-pass spatial frequency property of the human eye, the same gray level can be represent by two different patterns, any of which can possibly be arranged as a clustered dot and another as a dispersed dot. The choice of the patterns has an impact on the characteristics of the final halftoning image. This will be described in detail in the next section.

Fig 3: Halftoning images by block replacement. In (a), the candidates are 2 x 2, hence five levels of gray. In (b), the candidates are 3 x 3, hence 10 levels of gray.

Example for Block Replacement is shown in the following Fig.
Visual cryptography may be a quite cryptography that may be decoded directly by the human sensory system with nonspecial calculation for coding. As shown in below Fig, our visual cryptography system takes 3 footage as an input and generates 2 pictures that correspond to 2 of the 3 input footage. The third image is reconstructed by printing the 2 output pictures onto transparencies and stacking them along, this sort of visual cryptography, that reconstructs the image by stacking some substantive pictures along, is especially called Extended Visual Cryptography [5]. In this project, the pictures shown on the output images are called sheets and the resulting image reconstructed by stacking the two sheets together is called the target. Previous works on the extended visual cryptography deal with binary images such as text images, but natural images such as photographs are difficult to handle in such scheme. This project establishes the extended visual cryptography themetor natural pictures. Generally, visual cryptography suffers from the deterioration of the image quality. This project additionally describes the tactic to enhance the standard of the output image.

Proposed system Visual cryptography provides friendly surroundings to troy out pictures. Our application has been developed exploitation swing and applications programme technologies, thus provides a friendly surroundings to users.

VISUAL SECRET SHARING SCHEME:

The basic model of the visual cryptography consists of a several number of visible sheets. On everyvisibility a cipher text is written that is different from random noise. The hidden message is reconstructed by stacking a particular variety of the transparencies and viewing them. The system can be used by anyone without any knowledge of cryptography and without performing any cryptographic computations. Naor and Shamir have developed the Visual Secret Sharing Scheme (VSSS) to implement this model. In $k$ out of $n$ VSSS (which is also called $(k, n)$ scheme), a binary image (picture or text) is transformed into $n$ sheets of transparencies of random images. The original image becomes invisible when any $k$ sheets of the $n$ transparencies are put together, but any combination of less than $k$ sheets cannot reveal the original binary image. In the scheme, one pixel of the original image is reproduced by $m$ sub pixels on the sheets. The pixel is considered “on” (transparent) if the number of transparent sub pixels is more than a constant threshold, and “off” if the transparent sub pixels is less than a constant lower threshold, when the sheets are stacked together. The contrast $\alpha$ is the difference between the on and off threshold number of transparent pixels. Atienese et
al. has extended the \((k, n)\) VSSSto general access structures where everwill specify all qualified and out subsets of \(n\) participants. Droste thought about the matter of sharing more than one secret image among a set of participants and proposed a method to reconstitute different images with different combinations of sheets.

The Basic Idea of the Proposed System

EXTENDED VISUAL CRYPTOGRAPHY:

Naor associating in nursing and Shamir [2] have mentioned an extension of the model which conceals the terribly existence of the key image. That is, each sheet carries some meaningful images rather than random dots. They referred to the \((2, 2)\) example with the number of sub pixels \(m = 4\). Ateniese has formalized this framework as the Extended Visual Cryptography [8] and developed a Scheme for general access structures. They also discuss the trade-off between the contrast of the each images on the sheets and that of the resulting image when stacked together in \((k, k)\) cases.

APPLICATION TO EXTENDED VC

GRAY SCALE CONVERSION:

In photography and computing, a grayscale digital image is a picture which the worth of every pixel may be a single sample, that is, it carries solely about the picture information. Images of this sort, also known as black-and-white [8], are composed having the shades of gray, varying from black at the weakest intensity to white at the strongest.

The grayscale images are different from black and white images, which in the context of computer imaging are images with only the two colors, black and white images, which in the context of computer imaging are images with only the two colors, black and white. Grayscale images have many shades of gray in between. Grayscale images are also called monochromatic, denoting the presence of only one (mono)color (chrome).

Conversion of a color image to grayscale is not unique; a common strategy is to match the luminance of the grayscale image to the luminance of the color image. In fact a gray color is one in which the red, green and blue components all have equal intensity in RGB space. The grayscale intensity is stored as an 8-bit integer giving 256 possible different shades of gray from black to white. Gray-level conversion is the process which converts the given original image to a 256 bits gray-level bitmap image.

Steps of grayscale algorithm:
Step 1: Give the height and width of the image.
Step 2: X and Y axis are declared.
Step 3: The starting position of the X and Y axis are ‘0’.
Step 4: Now the starting position is incremented to ‘1’.
Step 5: Now we are getting the position of x and y values of X and Y axis.
Step 6: Check the color of the getting position whether it is black or white.
Step 7: If the color of the position is near to black change it as to pure black.
Step 8: Else if the color of the position is near to white change it as to pure white.
Step 9: Procedure will continued until the process completed.

IMAGE ENCRYPTION:

In cryptography, encryption is the process of the conversion of information from a readable state to a non-readable state. In an encryption scheme, the message or information is encrypted using an encryption algorithm, turning it into an unreadable cipher-text. The aim of this technique is to cover the information and the code will be sent to the exact user. The user only sees the hidden image.
Step 2: Horizontal block = image width / 2
Step 3: Vertical block = image height / 2
Step 4: Number of block = horizontal block X vertical block
Step 5: For n=0 to no.of.block-1
   For x=0 to n-1
   For y=0 to n-1
       Encrypt pixel using position (x, y)

**IMAGE DECRYPTION:**

The decryption of the image will be done by overlapping the shares, without removing cover images by means of that we can avoid pixel expansion problems. Where removing cover images results in change in the display quality of the recovered image. When we place both the shares one over another with proper alignment, we can interpret the original image.

**FOR BLACK AND WHITE IMAGES:**

In the original encryption, the problem can be considered as a (2, 2) secret sharing. The solution of the (2, 2) black-and-white VCS scheme by either dividing one pixel into two subpixels or four subpixels in the two shares. So the size of the superimposed image is expanded by a factor of 4. The following Fig. shows all the possible arrays of the four subpixels.

![Four Subpixels Arrays](image)

The Six Arrays of Four Subpixels

Randomly choose an array from Fig. for a pixel in the secret image, as the first share. The second share is identical with the first one if the original pixel is white and if the original pixel is black, the second share is complementary with the first one. When we superimpose the two shares, the white color is recovered as medium gray and the black color is recovered as completely black. Secret sharing improves the reliability and robustness of secure key management.

Example: Consider the following situation: If the only key that provides access to some important data is lost somewhere, then that important data will become inaccessible. Thus this problem can be resolved by dividing the key into pieces and then distributing them to different persons so that any pre-specified set of persons can recover the key jointly.

**CONCLUSION**

In this paper, we’ve explored extended visual cryptography while not enlargement. We’ve shown that using an intelligent pre-processing of halftone pictures supported the characteristics of the first secret image, we tend to square measureable to manufacture smart quality images within the shares and therefore the recovered image. Note that alternative applications may also enjoy the pre-processing approach, like multiple image visual cryptography, that hides multiple pictures in shares.

**REFERENCES**


**AUTHORS:**

**Amarnath Babu S** is presently working as associate professor, Dept of Computer Science and Engineering, in St.Ann’s College of Engineering and Technology, Chirala. He Guided Many UG and PG Students. He has More than 11 Years of Excellence in Teaching. He published 6 International Journals.

**Karthik Babu Manam** received the B.Tech degree in Electronics & Instrumentation Engineering from AcharyaNagarjuna University, in 2011 & pursuing his M.Tech in Computer Science & Engineering from JNTU Kakinada.