

# Visual Cryptography Technique for Banking Application

Mr. Kumbhar Omkar Ashok<sup>1</sup> Miss.Karke Ashwini Namdev<sup>2</sup> Miss.Kotakar Nikita Narayan<sup>3</sup>

Prof. Nikumbh Darpana M<sup>4</sup>

<sup>1,2,3</sup>Student <sup>4</sup>Professor

<sup>1,2,3,4</sup>Department of Electronics & Telecommunication Engineering

<sup>1,2,3,4</sup>SCSCOE, Rahuri, India

*Abstract*— Information is increasingly important in our day to day life. It gets more value when shared with others. It is possible to share the information like audio, video and image easily, due to advances in technologies related to networking and communication. It may give rise to safety related issues. Attackers may try to access unauthorized data and misuse it. Certain techniques are required to solve this problem. For sharing information secretly, some techniques are used termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme. A technique used for protecting image-based secrets is Visual cryptography (VC). In visual cryptography scheme secret image is split into some shares, which separately reveals no knowledge about the secret information. Then participants gets the shares. By stacking these shares directly, secret information can be revealed and visually recognized. To combine to reveal the secret image, all shares are necessary. Many visual cryptographic techniques have been evolved day by day.

**Key words:** Banking Application, Visual Cryptography

## I. INTRODUCTION

In visual cryptography scheme (VCS), where  $k \leq n$ , a visual secret image is divided into  $n$  shadow images (referred to be shadows). Each shadow image can be made on a transparency, in  $(k,n)$ -VCS. By stacking any  $k$  transparencies on an overhead projector, user can visually decode the secret through human visual system without the assistance of any hardware or computation. We cannot recover the secret image, in stacking  $k-1$  or fewer shadows. This novel decoding quality may serve to securely and cheaply share alphanumeric characters where users hope to recover the key when no computer is temporarily available or without using computer for some security reasons. Recently, a attention has attracted to this stacking-to-see property. VCS is not only an important and active research area, but also can provide practical applications in combining watermark, Google street view, fingerprint and bar code. Visual Cryptography is a special encryption technique that hides the information in images in such a way that it can be decrypted by the human vision if the correct key image is used. The technique was proposed by Naor and Shamir. Visual Cryptography uses two transparent images. One image contains the latent information and the other image contains random pixels. Both transparent images and layers are required to exhibit the information. It is impossible to retrieve the secret information from one of the images. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet.

In the overlay animation user can look the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this, copy the example layers 1 and 2, and print them onto a transparent

sheet or thin paper. Always use a program that shows the black and white pixels accurate and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). User can also copy and paste them on each other in a drawing program like paint and see the result soon, but make sure to select transparent drawing and align both layers exactly over each other.

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

In this example a pixel, divided into four parts, can have six different stages. If a pixel on layer 1 has a given stage, 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 same to layer 1, the overlaid pixel will be half black and half white. The overlaid pixel is called grey or empty. If the pixels of layer 1 and 2 are inverted or opposite, the overlaid version will be fully black. This is an information pixel.

User can now create the two layers. One transparent image, layer 1, has pixels which all have a random stage, one of the six possible stages. Layer 2 is identical to layer 1, except for the pixels that must 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 stages will be black.

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

## II. LITERATURE SURVEY

Visual Cryptography (VC) is not adequate in terms of providing color meaningful shares with high visual quality. This paper induces visual cryptography encryption method for color images which use the error diffusion and visual information pixel (VIP) techniques to generate meaningful color shares with high visual quality. In Error diffusion method, low frequency differences between the input and output images are minimized and consequently it produces agreeable halftone images to human vision. Synchronization of the VIPs across the color channels improves visual contrast of shares. Comparison of Floyd halftone with Jarvis halftone shows good result of Jarvis method.

With rapidly growing network, internet has become a initial source of transmitting latent or secret data such as

military information, financial documents, etc. In such cases, techniques addicted to protect such kind of information are needed and they play an important role in providing secret and secure transmission over network. Visual Cryptography is also one of them which is used to cover secret visual information (such as image, text, etc) in which secret sharing scheme is used. Secret sharing is used to encrypt a latent image into customized versions of the original image. There are many secret sharing algorithms in literature to divide the image into number of shares. These sharing schemes lead to computational difficulty and also generate shares like clamorous images. Then afterwards Lin & Tsai proposed a scheme which creates significant shares but having same computational complexity as like Shamir's scheme. Along with this, in these schemes, as decryption is done using Human Visual system, the latent can be retrieved by anyone if person get at least k number of shares. To outbrave all above problems, we are suggesting one new method in which a symmetric secret key is used to encrypt the image and then latent shares are generated from this image using Novel secret sharing technique with steganography. So, finally this method will produce significant shares and use of secret key will ensure the security of scheme. This scheme can become a secure solution suitable for today's authentication challenges.

Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human visual system. The benefit of the visual secret sharing scheme is in its decryption process where without any complex cryptographic computation encrypted data is decrypted using Human Visual System (HVS). But the encryption technique needs cryptographic computation to divide the image into a number of parts let n. k-n secret sharing scheme is a special type of Visual Cryptographic technique where at least a group of k shares out of n shares reveals the secret information, less of it will reveal no information. In our paper we have proposed a new k-n secret sharing scheme for color image where encryption (Division) of the image is done using Random Number generator.

### III. BLOCK DIAGRAM & DESCRIPTION

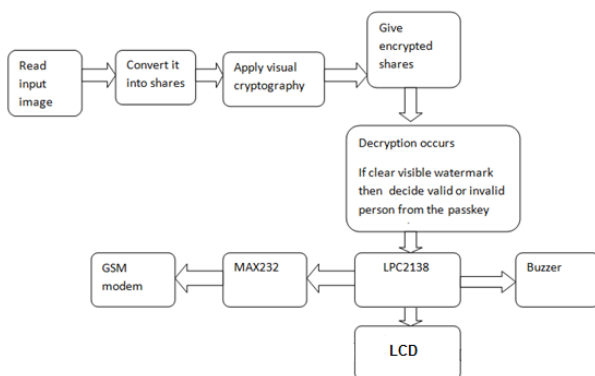


Fig. 1: Hardware Control Block

Read input color image convert it into shares, envelop the gray scale image and encrypt image and add the passkey. At the decryption side, add the passkey combined the decrypted share images and get the output result get the inserted image back. If user enter the wrong passkey, then image will not be clear. If enter passkey is ok then only user will be able to

view the clear image and then can access the system and system will send the message to user that system has been access if locker system will be there. If any security system is there, invalid user enter the wrong key he may not be able to access the system and the message will send to police via gsm modem.

Hardware used:

- 1) ARM7:LPC2138
- 2) LCD
- 3) MAX232
- 4) GSM module
- 5) Buzzer

#### A. ARM7LPC2138

The LPC2138 microcontrollers are 32/16 bit ARM7TDMI-S CPU with real-time rivalry and embedded trace support, that combines the microcontroller with embedded high speed flash memory ranging from 32 KB to 512 KB. A 128-bit wide memory interface and unique accelerator architecture enable 32-bit code execution at the maximum clock rate. For critical code size applications, the alternative 16-bit Thumb mode reduces code by more than 30 % with minimal performance penalty.

Due to their tiny size and low power consumption, LPC2141/2/4/6/8 are ideal for applications where miniaturization is a key requirement, such as access control and point-of-sale. A blend of serial communications interfaces ranging from a USB 2.0 Full Speed device, multiple UARTS, SPI, SSP to I2Cs and on-chip SRAM of 8 KB up to 40 KB, make these devices very well suited for communication gateways and protocol converters, soft modems, voice recognition and low end imaging, providing both large buffer size and high processing power. Various 32-bit timers, single or dual 10-bit ADC(s), 10-bit DAC, PWM channels and 45 fast GPIO lines with up to nine edge or level sensitive external interrupt pins make these microcontrollers particularly suitable for industrial control and medical systems.



Fig. 2: LPC2138

#### B. Liquid Crystal Display

LCDs are the most popular electronic display device. LCD flat full color panels are now challenging the CRT as displays for television and computers. While even a tiny LED display consumes a few milliwatts of power, the LCD consumes just microwatts of power. Hence, the LCDs are over 1000 times more efficient at their job than the LEDs.

#### C. RS232 pins

RS232 connector commonly referred to as the DB-25 connector. In labeling, DB-25S refers to the socket connector (female) and DB- 25P is for the plug connector (male). Since not all the pins are used in PC cables, IBM

introduced the DB-9 Version of the serial I/O standard, that uses 9 pins only.

#### D. GSM Module

The SIM900 is a complete Quad-band GSM solution in a SMT module. Featuring an industry-standard interface, the SIM900 delivers GSM 850/900/1800/1900MHz performance for SMS, voice, Fax and Data in a small form factor and with low power consumption. With a tiny configuration, SIM900 can fit almost all the space requirements in your M2M application, especially for slim and compact demand of design.

- 1) It is designed with a very powerful single-chip processor integrating AMR926EJ-S core.
- 2) Quad - band GSM module with a size of 24mmx24mmx3mm.
- 3) An embedded Powerful TCP/IP protocol stack.
- 4) SMT type suit for customer application.
- 5) Based upon mature and field-proven platform, backed up by our support service, from definition to design and production.



Fig. 3: SIM900

#### E. Buzzer

The piezo buzzer produces sound based on reverse of the piezoelectric effect. The underlying principle is the generation of pressure variation or strain by the application of electric potential across a piezoelectric material. These buzzers can be used to alert a user of an event corresponding to a switching action, counter signal or sensor input.

Software used:

- 1) Keil $\mu$ vision4
- 2) MATLAB7

#### F. Keil $\mu$ vision4

The  $\mu$ Vision IDE from Keil combines project management, make facilities, program debugging, source code editing, and complete simulation in one powerful environment. The  $\mu$ Vision development platform is easy-to-use and helps to quickly create embedded programs that work. The  $\mu$ Vision editor and debugger are integrated in a single application which provides a seamless embedded project development environment.

- 1) The new Keil  $\mu$ Vision4 IDE has been designed to, enabling faster, more efficient program development and to enhance developer's productivity.
- 2) A flexible window management system is introduced, that enables you to drag and drop individual windows anywhere on the visual surface including support for Multiple Monitors.
- 3) Language used: Embedded C

#### G. MATLAB

MATLAB, short for MATrixLABoratory is a programming package specially designed for quick and easy scientific

calculations and I/O. It has literally hundreds of built-in functions for a wide variety of computations and many toolboxes designed for specific research disciplines, including optimization, statistics, solution of partial differential equations, data analysis. For CME200, you need a deep knowledge of basic MATLAB commands and several more advanced features including two- and three-dimensional graphics, solution of ordinary differential equations, solution of algebraic equations, solutions of linear systems of equations and calculations with matrices. Most of what you need is discussed here.

## IV. SYSTEM OVERVIEW

### A. Advantages:

- 1) It hides message and privacy is safe.
- 2) No one would be able to know what it says unless there's a key to code.
- 3) We can write whatever we want to keep a code secret.
- 4) Efficient power consumption
- 5) The visual cryptography schemes are used as secret images tools.
- 6) Fast transmission of images in compressed form.

### B. Disadvantages:

- 1) Images are available only in few formats.
- 2) It takes long time to figure out the code.
- 3) It takes long time to create the code.

## V. CONCLUSION

This system uses Colour Image Visual Cryptography for data protection and it is not able to break this protection with present technology. This system will be a boon for the Banking Application and the bank customers are feel free from the password hacking problems. Once this system is deployed in web Server, all the computer in the network can able to access this application through browser without any software installation in their computer.

## REFERENCES

- [1] Tzung-Her Chen, Kai-Hsiang Tsao, and Kuo-Chen Wei, —“Multi-Secrets Visual Secret Sharing”<sup>l</sup>, Proceedings of APCC2008, IEICE, 2008.
- [2] F. Liu<sup>1</sup>, C.K. Wu<sup>1</sup>, X.J. Lin,—“—Colour visual cryptography schemes, IET Information Security”, July 2008.
- [3] M. Shirali-Shahreza, — “Steganography in MMS,<sup>l</sup> in Multitopic Conference”, 2007. INMIC 2007. IEEE International, 2007, pp. 1-4.
- [4] Li Bai,—“A Reliable (k,n) Image Secret Sharing Scheme”, IEEE,2006.
- [5] C. K. Chan and L. M. Cheng, — “Hiding data in images by simple LSB substitution”, I Pattern Recognition, pp. 469—474, Mar. 2004.
- [6] M. Kutter and S. Winkler, — “A vision-based masking model for spread- spectrum image watermarking”,<sup>l</sup> IEEE Trans. Image Processing, vol. II, pp. 16-25, Jan. 2002.
- [7] M. Naor and A. Shamir, — “Visual cryptography, <sup>l</sup> Advances in Cryptology-Eurocrypt’94”, pp. 1–12, 1995.