International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 7831-7836

http://www.ripublication.com

Counterfeit Currency Detection Using Visual Cryptography

Nishanth N Janadri, Najeerahamed S, Kunal Pagare, Brindha.K

M.Tech Information Technology (Networking), Assistant Professor(Senior)
SITE, VIT University, Vellore
SITE, VIT University, Vellore

Abstract

There is almost no country in the world which faces the problem of counterfeit currency notes. This problem is severe especially in countries like India which is hit hard by this wrongdoing. Counterfeit notes of all denominations even smaller ones Rs.10 and 50 have been flooding into the system. In order to deal with problems like this much detection systems have been introduced, which are not portable and easily deployed. An automated recognition system is much in need in present day scenario. This can be achieved by visual cryptography. In this method currency note will be provided with a share(s) of the secret image, which will be decided by the governing body and the other share(s) will be given to the user through an application on any mobile platform and thus it can be determined whether the currency note is genuine or not.

Keywords: counterfeit currency detection, shares, key shares, visual cryptography scheme**.**

Introduction

Visual cryptography scheme is a powerful secret image sharing scheme which allow users to share image over a shared medium in encrypted manner so that third party will be clueless about the hidden image. Visual secret sharing scheme proposed by Moni Naor and Adi Shamir. A secret sharing scheme involves distribution of a secret among n parties so that a particular set of authorized persons will be able to reconstruct the secret. The reconstruction is usually achieved by superimposition of the shares. Secret sharing in visual cryptography is totally different from typical cryptography scheme where in each party is allowed to keep a portion of the secret and part of secret image can be reveled with the minimum shares available. The same thing is totally prohibited in typical cryptography schemes. There has been steady

growth of interest in visual cryptography due to its simplicity, effectiveness and security. The most highlighting aspect of visual cryptography is the elimination of complex computation problem during decryption process which is performed by human visual system.

The existing system in counterfeit detection system includes the various measure in the currency note in which some are visual to human eye and some are detected through the CCM (currency counting machine). A common man cannot make use of this machine as it is not portable, affordable and it is not usable for general purposes. A portable and handy device is required which can be used by a common man on day to day basis not involving any high-tech gadgetry. This is an attempt to design an alternative for common people using the concept of visual cryptography.

Basic visual cryptography generally involves image sharing which is a part of secret sharing as it is a well thought approach to the general secret sharing problem. In this case concealed images are the secrets. Image sharing defines a scheme that is identical to general secret sharing. In (k, n) visual secret sharing scheme the secret image is split up into n shares so that the decryption is successful if k shares are stacked together. It will be unsuccessful fewer than k shares are superimposed. Another advantage of visual cryptography is that the decryption allows anyone to use the system with least knowledge of cryptography involving least computations whatsoever. The secret image consists of black and white pixels which are separately handled. Each pixel is represented by m subpixels, subpixels being black and white pixels. These subpixels are visible to human eye which averages the number of subpixels. The shared image size increases m times larger than the original image resulting in a n×m Boolean matrix. The matrix is represented as S= [s_{ij}] where s=1 if and only if *j*th subpixel is black in the *i*th shared image and s=0 if and only if *j*th subpixel is white in the *i*th shared image.

Literature Survey

Currency notes are provided with built-in security measure. They are in number such as:

Figure1: 500 Rupees note with various Identification Marks

See through register*:*
The small floral design printed both on the front and back of the note near to the watermark in the middle of the vertical strip has an accurate back to back registration. The design will look exactly the one in the light because they are perfectly aligned.

Identification mark:
Each note has a unique sign of it such as 100-Triangle, Rs.500-Circle, and Rs.1000-Diamond. These shapes are designed with special printing technique intaglio special feature has been introduced on the left of the watermark window. This feature helps the visually impaired to identify the denomination.

Fluorescence:
Currency notes are provided with fluorescent ink in the number panel and also with the optical fiber threads. Both can be seen when they are exposed to the ultra violet light.

Water marking:
The currency notes are provided with water marking picturing the Mahatma Gandhi om the front side of the notes.

Optically variable ink:
The currency notes of 1000/500 are introduced with optical variable ink which changes the color of number printed if seen with different angle.

Intaglio printing:
The portrait of Mahatma Gandhi, the Reserve Bank seal, guarantee and promise clause, Ashoka Pillar Emblem on the left, RBI Governor's signature are printed in intaglio i.e., which can be felt by touch, in Rs.20, Rs.50, Rs.100, Rs.500 and Rs.1000 notes.

Security thread*:*
The security thread appears to the left of the Mahatma's portrait. The Rs.500 and Rs.100 notes have a security thread with similar visible features and inscription in Hindi “Bharat”, and “RBI”. When held against the light, the security thread on Rs.1000, Rs.500 and Rs.100 can be seen as one continuous line. The Rs.5, Rs.10, Rs.20 and Rs.50 notes contain a readable, fully embedded windowed security thread with the inscription “Bharat” (in Hindi), and “RBI”.

Micro lettering
This feature can be seen well under a magnifying glass. This feature appears between the vertical band grafted with pattern and value of currency and Mahatma Gandhi portrait. It always contains the word “RBI” in Rs.5 and Rs.10. The notes of Rs.20 and above also contain the denominational value of the notes in micro letters.

Latent Image:
The vertical band on right side of Mahatma Gandhi is encrypted with the latent image. Same value as that of currency, which can be seen when holding the currency notes horizontal at the eye level.

There are many schemes in Visual Cryptography schemes that have been proposed. The popular ones being as follows:

(2, 2) Visual Cryptography Scheme involves the division of the original image into 2 shares. Each pixel from the original image is represented in each share in the form of a block of 2 or 4 sub-pixels. These blocks of sub-pixels are usually non-overlapping. On overlapping of two shares if 2 white pixels are superimposed the resulting pixel will be a white pixel and if any other combination is superimposed with, the resultant pixel will be a black one. This implies that the superimposition works like the Boolean OR function. This scheme totally depends on two shares and if even a single share is damaged the secret image cannot be retrieved.

In *(k, n) Visual Cryptography Scheme*, n shares are generated out of which only k shares are sufficient to retrieve the secret image. The value of k can vary from 2 to n. If there are shares less than k it is impossible to retrieve the secret image. This overcomes the drawback in (2, 2) VCS (Visual Cryptography Scheme). If user loses any of the shares there is still an easy way to retrieve the secret image. But this scheme faces problem of security of the system since any k shares can help reveal the secret image.

General Access Structure is another VCS which overcomes the problem of security faced in (k, n) VCS. In this scheme the n shares are divided into two subsets namely forbidden set and qualified set. The concept here is any k shares only from qualified set of shares can reveal the secret and is not possible even if there are more than k shares in the forbidden subset.

The Recursive Threshold VCS overcomes another problem of (k, n) VCS. A secret image of 'c' number of bits is divided into n shares having the least size of 'c' bits each. But only k among n shares are necessary and hence it results in inefficiency in terms of bits from secret present in per bit of shares. Hence this scheme hides smaller shares in larger shares recursively leading to doubling of secret sizes at every proceeding.

Halftone VCS is one of the popular visual cryptography schemes proposed by Zhi Zhou, Gonzalo R. Acre, and Giovanni Di Crescenzo. In this every binary pixel from the secret is encoded into an array of sub-pixels namely halftone cell in every share. The use of halftone cells results in better contrast, quality and security.

There are also VCS for *Grey images and Color images*. Since many of the visual cryptography schemes are limited to black and white pixels, these techniques were insufficient for real life applications. Hence VCS for Grey images was proposed by Chang-Chou Lin, Wen-Hsiang Tsai and VCS for Color images by Verheul and Van Tilborg. In case of gray images a technique is used to convert it into binary image and then the existing VCS are applied. In case of color images one pixel is divided into m sub pixels and those in turn are converted into c color regions. There is only one color region in each sub-pixel and the remaining are black.

Objective and Methodology

The approach proposed in this paper towards counterfeit detection is through the concept of Visual Cryptography. A foolproof application system is to be developed in such a way that it helps common people to end their suspicion or confusion in a blink.

A novel approach is proposed involving the currency regulators. These authorities first decide on a secret image. This secret image is split into a fixed number of shares. Among these a few number of shares are stacked together and it is impregnated into the currency bill. The other remaining shares of the total shares that are produced are stacked together separately and released as the key to the public for the decryption on the user friendly application developed for the counterfeit currency detection. This is where the regulators' part ends. At the user end the currency under suspicion is scanned from the smartphone. The public is notified which part of the currency bill has to be scanned. So all the user has to do is scan that portion of the bill. Once scanned the application stacks the shares together both from the currency note and the key in the application. On stacking if the secret image is revealed then it can be considered an authentic currency bill and the user can be free from worry.

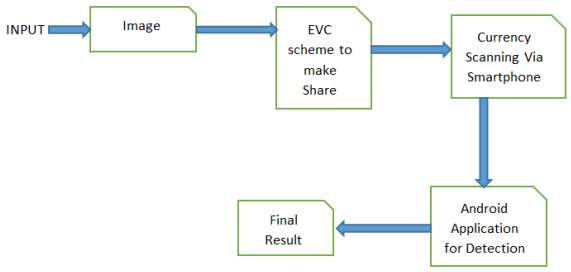

Figure 2: Workflow of Counterfeit detection system

The Visual Cryptography Scheme being applied is the Extended Visual Cryptography (EVCS). In this scheme all the shares that are split from the secret image are meaningful images. The shares are categorized into two subsets namely Qualified subset and Forbidden subset. This contributes towards the security of the system i.e., anyone attempting to meddle or malpractice can never know which actually is the secret key expected.

The secret image is basically considered a matrix of pixels. This matrix is split into shares where splitting is usually done horizontally, vertically or diagonally. Once splitting is done, the shares generated are embedded with shadow images which enable the shares gain meaning. During decryption the halftone method is used to get better decrypted image. If this decrypted image tallies with the secret image it is an indication of a genuine currency bill.

Conclusion

With the implementation of this application the currency detection will get far easier than existing system and loss towards the economic growth may decrease as less

number forged currency notes will be regulated in the market. The currency will not be detected unless it is being scanned by the authorized application not by the other application because authorized application will carry the key for the decryption of shares involved in the currency.

References

1. Moni Naor and Adi Shamir, "Visual cryptography". In Proceedings of Advances in Cryptology, EUROCRYPT 94, Lecture Notes in Computer Science, 1995, (950):pp. 1-12.
2. Shamir, A. 1979. How to Share a Secret. Communications of the ACM. 22: 612-613.
3. Sanjana, Manoj Diwakar, Anand Sharma . "IJCSMS International Journal of Computer Science & Management Studies". Vol. 12, Issue 02, April 2012.
4. 4. Suhas B. Bhagate, P J Kulkarni, "An overview of various visual cryptographic schemes. International Journal of Advanced Research in Computer and Communication Engineering". Vol. 2, Issue 9, September 2013.
5. A Comprehensive Study of Visual Cryptography, Jonathan Weir and WeiQi Yan Queen's University Belfast, Belfast, BT7 1NN, UK.
6. An introduction to different types of visual cryptographic schemes. International Journal of Science and Advanced Technology (ISSN 2221-8386) Volume 1 No 7 September 2011.
7. Z. Zhou, G. R Arce, and G. Di Crescenzo, "Halftone Visual Cryptography," in Proc. of IEEE International Conference on Image Processing, Barcelona, Spain,Sept 2003, vol. 1, pp. 521–52.
8. "Design and Implementation of Hierarchical Visual Cryptography with Expansionless Shares. International Journal of Network Security & Its Applications". (IJNSA), Vol.6, No.1, January 2014.
9. Binod Prasad Yadav, C. S. Patil, R. R. Karhe, P.H Patil "An automatic recognition of fake Indian paper currency note using MATLAB". International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 3, Issue 4, July 2014.