

# Foolproof Examination System through Color Visual Cryptography and Signature Authentication

Ms. Siddhi Shinde<sup>1</sup>, Ms. Prachi Shetti<sup>2</sup>, Ms. Tejaswini Ahire<sup>3</sup>, Ms. Hemyani Gosavi<sup>4</sup>,  
Prof S. N. Bhadane<sup>5</sup>

Students, Department of Information Technology<sup>1,2,3,4</sup>

Professor, Department of Information Technology<sup>5</sup>

Pune Vidyarthi Griha's College of Engineering & S.S. Dhamankar Institute of Management, Nashik, India

**Abstract:** *There have been widespread allegations about the question papers leakage for a number of subjects in the recently held Secondary School Leaving Certificate examinations. The leakage is due to the practice of using printed question papers. Such incidents and subsequent cancellation of examinations are happening frequently. This creates political and social embarrassment and causes loss of money and time. This paper proposes a new system of fool proof examination by tamperproof e-question paper preparation and secure transmission using secret sharing scheme. The application is perfectly secure because the proposed method automatically embeds the corresponding institute seal in the form of the key. As a result, it is easy to trace out the source culprit for the leakage of question papers. This scheme has reduced reconstruction time because the reconstruction process involves only Exclusive-OR (XOR) operation apart from authentication. 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 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.*

**Keywords:** Visual cryptography, secret sharing scheme, examination system, information security, authentication. Secret Sharing, Random Number

## I. INTRODUCTION

Visual Cryptography is a special type of encryption technique to obscure image-based secret information which can be decrypted by Human Visual System (HVS). This cryptographic system encrypts the secret image by dividing it into  $n$  number of shares and decryption is done by superimposing a certain number of shares ( $k$ ) or more. Simple visual cryptography is insecure because of the decryption process done by human visual system. The secret information can be retrieved by anyone if the person gets at least  $k$  number of shares. Watermarking is a technique to put a signature of the owner within the creation. In this current work we have proposed Visual Cryptographic Scheme for color images where the divided shares are enveloped in other images using invisible digital watermarking. The shares are generated using Random Number. Visual Cryptography is the method used for secret-sharing that encrypts a secret image into several shares; intervention of computer, or calculations are not to decrypt the secret image. The hidden secret image can be retrieved visually by overlaying the encrypted shares and then the secret image becomes clearly visible. Each share after printing on a separate transparencies can be super imposed to decrypt the secret image. When all  $n$  shares were superimpose, the original image would appear. In this scheme the binary image is divided into two shares, for the white pixel in the secret image, one of the upper two rows of table I is chosen to make share1 and share2. If the pixel of the secret image is black, one of the lower two rows of table I is used to make share1 and 2. This scheme consists of pixel expansion where every pixel from the secret image is expanded to 4 pixels, so when the shares are generated and superimposed together the reconstructed image will be four times the original secret image size because of this pixel expansion. Also the resolution of the reconstructed image will be less than the original secret image as every

white pixel is decomposed into two white & two black pixels. Only one secret could be hidden using this technique. The main aim of this is to overcome this drawback by employing a secret sharing scheme for this application. The main concept of the original Visual Secret Sharing (VSS) scheme is to encrypt a secret image into a number of meaningless shared images. Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used. Confidentiality is the assurance that only the intended recipient of a message can read it. This is what most people think of when they hear "cryptography".

## II. RELATED WORK

This paper describes the secret information can be retrieved by anyone if the person gets at least  $k$  number of shares. Watermarking is a technique to put a signature of the owner within the creation. Simple visual cryptography is insecure because of the decryption process done by human visual system. In this current work we have proposed Visual Cryptographic Scheme for color images where the divided shares are enveloped in other images using invisible digital watermarking. The shares are generated using Random Number.

[1]. Abdalbasit Mohammad, Nurhayat Varola, "A review paper on Cryptography"(2007)

With the internet having reached a level that merges with our lives, growing explosively during the last several decades, data security has become a main concern for anyone connected to the web. Data security ensures that our data is only accessible by the intended receiver and prevents any modification or alteration of data. In order to achieve this level of security, various algorithms and methods have been developed. Cryptography can be defined as techniques that cipher data, depending on specific algorithms that make the data unreadable to the human eye unless decrypted by algorithms that are predefined by the sender. Susan et al. pointed out that network and computer security is a new and fast-moving technology within the computer science field, with computer security teaching to be a target that never stops moving. Algorithmic and mathematic aspects, such as hashing techniques and encryption, are the main focus of security courses. As crackers find ways to hack network systems, new courses are created that cover the latest type of attacks, but each of these attacks become outdated daily due to the responses from new security software. With the continuous maturity of security terminology, security techniques and skills continue to emerge in the practice of business, network optimization, security architecture, and legal foundation.

[2]. Shyamalendu Kandar, "K-N Secret Sharing Visual Cryptography Scheme for Color Image using Random Number" (2011)

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 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.

[3]. Dipesh Vaya, Sarika Khandelwal, Teena Hadpawat, "Visual Cryptography: A Review" (2017)

Visual Cryptography is a technique, which is used to conceal the secret image into transparencies and these transparencies are distributed to the intended recipients. They demonstrated a visual secret sharing scheme, where an image was broken up into  $n$  shares so that only someone with all  $n$  shares could decrypt the image, while any  $n-1$  shares revealed no information about the original image. In this paper we have used a  $(n, n)$  visual cryptographic scheme half toning algorithm is used to divide the secret image into transparencies with the help of Jarvis Filter. Here, the encrypted transparencies are concealed in host image and then it can be sent to the intended person by other means. During authentication the secret image is verified. Experimental results reveal that the retrieved secret image after post filtering has 70% accuracy when compared to the retrieved secret image before post filtering whereas it as an accuracy between 50 to 60%.

## III. PROPOSED SYSTEM

Visual Cryptography is a special type of encryption technique to obscure image-based secret information which can be decrypted by the (HVS). This cryptographic system encrypts the secret image by dividing it into  $n$  number of shares

and decryption is done by superimposing a certain number of shares(k) or more. To achieve secure transmission of data, usually the data is concealed using symmetric or asymmetric key cryptography, which involves high computation and is cost effective in the encryption and decryption process. Simple visual cryptography is insecure because of the decryption process done by the human visual system. The secret information can be retrieved by anyone if the person gets at least k number of shares. The main aim of this is to overcome this drawback by employing a secret sharing scheme for this application. The main concept of the original (VSS) scheme is to encrypt a secret image into a number of meaningless shared images. It cannot leak any information of the shared secret by combination of the shared images except for all of the shares. This paper proposes a security system for tamper proof e- question paper sharing scheme using simple arithmetic operations. Visual cryptography is a cryptographic technique where visual information gets encrypted in such a way that the decryption can be performed by the human visual system without the aid of computers.

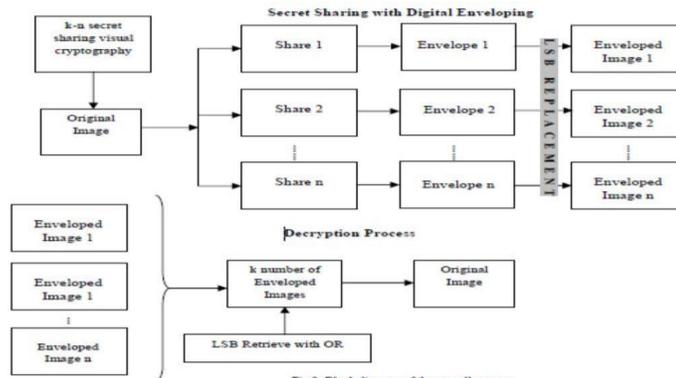


Fig 2: Block diagram of the overall process

#### IV. PROJECT MODULES

##### 4.1 Encryption Module

**Input:** Enter the no of shares (N) and Number of shares to be taken (K), browse the image, Image shares produced after applying visual, Enveloping using watermark, final image, enter email id and send the image.

**Output:** Image encrypted and divide in to different mail.

**Algorithm:** Input: Secret image I of size m\*n Number of shares N  
Image of any size K

##### 4.2 Decryption Module

**Input:** open mail, unwrap envelope, enter valid key and take output image.

**Output:** Decryption text (original text).

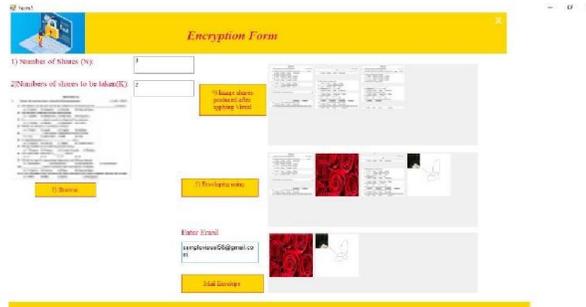
**Algorithm:** In the receiver side, the following one-step formula reconstructs the secret image Secret Image = S1XOR S2XOR S3XOR ...SN.

**V. RESULT**

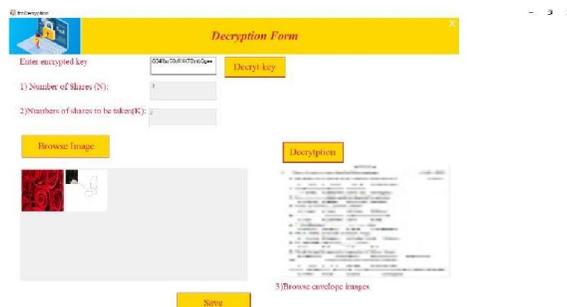
**5.1 Login Module**



**5.2 Encryption Module**



**5.2 Decryption Module**



1. Cryptography is the art of achieving security by encoding messages to make them non-readable.
2. Currently this particular cryptographic technique is being used by several countries for secretly transfer of hand written documents, financial documents, text images, internet voting etc.
3. Visual cryptography is used in many applications like bank customer identification, biometric security & remote electronic voting etc.

**VI. CONCLUSION**

This suggests the automation of examination system by securing question paper using secret sharing scheme. The main advantage of this proposed scheme with authentication is high visual quality of the color image with PSNR reduced

computational complexity and no pixel expansion. The proposed method without authentication recovers the original image without any loss (PSNR value infinity) which is not possible with the existing visual cryptographic schemes. The alternative methods for authentication will further enhance visual quality of images. To the best of our knowledge, for the first time, color secret sharing scheme without half toning is applied for secure transmission of Examination question papers

#### **REFERENCES**

- [1]. Chen G., Liu J., and Wang L., "Color Image Sharing Method Based on Lagrange's Interpolating Polynomial," in Proceedings of International Conference on Health Information Science, Beijing, pp. 63-75, 2012.
- [2]. Fathimal M. and Jansirani A., "(N, N) Secret Color Image Sharing Scheme with Dynamic Group," International Journal of Computer Network and Information Security, vol. 7, no. 7, pp. 46-52, 2015.
- [3]. Thien C. and Lin J., "Secret Image Sharing," Computers and Graphics, vol. 26, no. 5, pp. 765-770, 2002.
- [4]. Ulutas M., Ulutas G., and Nabiye V., "Invertible Secret Image Sharing for Grey Level and Dithered Cover Images," Journal of Systems and Software, vol. 86, no. 2, pp.485-500, 2013.
- [5]. Verheul E. and Tilborg H., "Constructions and Properties of K out of N Visual Secret Sharing Schemes," Designs, Codes and Cryptography, vol. 11, no. 2, pp. 179-196, 1997.
- [6]. Guo C., Chang C., and Qin C., "A hierarchical Threshold Secret Image Sharing," Pattern Recognition Letters, vol. 33, no. 3, pp. 83-91, 2012.