Chapter 5

TAMPERPROOF QUESTION PAPERS—AN APPLICATION USING VISUAL CRYPTOGRAPHY SCHEMES

5.1 Introduction

This chapter explains new applications of tamperproof preparation and transmissions of online question papers using visual cryptography schemes. The present method of conducting various competitive examinations like UPSC exams, IIT-JEE, UGC-NET, GATE, MAT etc. and also regular school and university examinations is by using printed question papers. These types of question papers can be easily leaked out or tampered with and we often hear of such incidents and subsequent cancellation of examinations. This causes loss of money and time and also creates political and social embarrassment. The genuine students and candidates become upset and are put under pressure. The Kerala SSLC Examination 2005, All India Medical Entrance Examination 2005 and AIEEE 2011 are examples. Nowadays, people are very conscious and concerned about their education and in our system the ability of an individual is assessed through examinations. So the reliability and security of question papers is of paramount importance to ensure educational and social justice. This chapter discuss the security of
question papers and suggest a new technique for preparing tamperproof e-question papers. The technique is perfectly secure using visual cryptographic techniques and is also very easy to implement.

The secure transmission of fingerprint images with the help of visual cryptography schemes is included in this chapter. This technique provides a very secure way to encrypt and decrypt fingerprint images without any complex computations.

5.2 The Tamperproof Question Paper

The presented Tamperproof Question Paper (TQP) provides a very secure way to hide a question paper in different shares. In this application, the question paper is broken up into \( n \) pieces, which individually yield no information about the question paper. These pieces of the question paper, called shares or shadows, may then be distributed among a group of \( n \) participants/dealers. By combining any \( k \) of these shares the question paper can be recovered, but combining less than \( k \) of them will not reveal any information about the question paper. In this method, the reconstruction of the question paper is based on XOR operation. This will enable one to obtain back a perfect question paper completely true to the original.

The schematic diagram for preparation and transmission of tamperproof question papers using visual cryptography is shown below:

**Figure 5.1** The implementation model for TQP using VCS

The question papers are normally set up by a trusted authority who computes all the shares (unintelligent pieces of the question papers) and distributes them to participants via secure channels. The trusted authority who sets up the scheme is called a *dealer*. The participants hold their shares until some of them have to pool together their shares and recreate the question papers. The recovery of the question papers is done by the *combiner* who on behalf of the cooperating group compute the question papers. The combiner is successful only if the cooperating group has at least *k* members. The medium is used to transmit shares from the dealer to participants and participants to the combiner. It may be secure communication channels, email or direct handing over to participants/combiner using any portable devices (CD/DVD/Pen drive etc.).
The major attractions of this application are:

- The scheme is perfectly secure and very easy to implement.
- Very low computational complexity.
- The devices required are also very economical.

5.2.1 General Phases of the TQP

The basic idea for the method is to divide a question paper (QP) according to a given access structure. The access structure of a given scheme is the collection of authorized subsets of shareholders/participants that are allowed to reconstruct the QP. The QP is divided into a number of shares \( S_1 \) to \( S_n \) such that only pre-specified subsets of \( S_i \)'s are eligible to rebuild the QP. Thus, the proposed method will have three phases:

1. QP shares building phase
2. QP shares distribution phase
3. QP reconstruction phase

The details of the three phases are given below.

5.2.2 QP Shares Building Phase

During this phase, a trusted entity, usually called the share builder/dealer, is supplied with the required input to produce a share for each shareholder/participant (See Figure 5.2). It requires the following information:

1. The QP: usually the question paper is represented as a binary image.
2. The trusted participants (shareholders): the people/machines that will be given shares of the QP to keep.

3. The qualified subsets (access structure): A qualified subset is a subset of the shareholders that is able to rebuild the QP.

![Figure 5.2 The Schematic representation of shares builder phase](image)

Based on the qualified subsets, the share-builder will produce one share for each participant. In some schemes giving more than one share to a higher privileged participant is suggested.
5.2.3 QP Shares Distribution Phase

In the shares distribution phase, the shares produced in the first phase are delivered to the participants (see Figure 5.3). Usually secure channels are used for communication between share-builder and participants.

Figure 5.3 The Schematic diagram for shares distributing phase

5.2.4 QP Reconstruction Phase

In the shares reconstruction phase, a qualified subset of participants (any $k$ participants) will pool their shares with a trusted entity, usually called QP builder, to reconstruct the QP (Figure 5.4). Reconstructing the QP needs to be secure and hence the required shares should be submitted to the QP builder over secure channels to insure privacy.
5.2.5 The Execution of Different Phases of the TQP

The executions of different phases of TQP are explained with the help of the University examination system. The execution of TQP system is shown in figure 5.5. In this system, the Controller of Examinations (CE) of the University is the share builder/dealer. The Principal/Head of examination centers and external examiner posted by the University are the participants. The CE is responsible for the generation and distribution of shares to the participants via a secure medium.

The CE generates two shares from the QP by using 2-out-of-2 visual cryptography scheme. Then the first share is sent to the Center Head (CH) and the second share is sent to the External Examiner (EE) via
a secure medium. If there are more than one centres of examination, this process will be repeated for each centre. In this case, the CE generates two separate sets of shares for each examination centre. The same sets of shares will not be used for more than one center, which will affect the security of the QP.

On the day of examination, the CH and EE pool their shares to reconstruct the QP. That is:

\[ QP = \text{Share}_1 \oplus \text{Share}_2 \]

where the symbol \( \oplus \) represents XOR operation. Share 1 and share 2 are kept by CH and EE respectively. The representation for the TQP model is shown below:
Figure 5.5 The execution of TQP model
From the figure 5.5, we can see that the QP can be reconstructed by CH and EE in their respective center only. Even if EE of one centre and CH of another centre pool their shares, it will not reveal any information about the QP. Similarly EE of two different centers are also unable to reconstruct the QP. If the shares kept by EE or CH are lost or damaged, the CE can generate two new shares and send them to CH and EE via a secure channel. Therefore, this model provides perfect security and reliability.

**5.2.6 Experimental Result**

For the experiment, the QP considered is a binary image file. To perform the encryption process, the QP is encrypted into two shares so that the original image is visible only when the two shares are overlaid using XOR operation. The Figure 5.6 depicts the encryption and decryption processes of the QP using VCS based on XOR operation.
### Part III: Computer Science

#### 3.2 Data Communications & Computer Networks

_for 2008 admission only_

**Time:** Three Hours  
**Maximum WGP:** 100

**Section - A**

Answer any Seven questions  
(Weightage: 1 each)

1. Define bandwidth.
2. Explain multiplexing.
3. What is parallel communication?
4. What is RS-32?
5. Explain Co-axial cable.
6. What is Huffman Coding?
7. What are the functions of Data link layer?
8. What is network topology?
10. What is a virtual terminal?

**Section - B**

Answer any Seven questions  
(Weightage: 2 each)

11. Explain RZ and NRZ.
12. Describe PCM and DPCM.
14. Explain Error detection and correction
15. Explain data compression.
17. Explain IEEE 802 standard.
20. Explain client server model.

---

**Figure 5.6a** Copy of actual question paper (Sample)
Figure 5.6b Share 1
Figure 5.6c Share 2
Part III: Computer Science
3.2 Data Communications & Computer Networks

[For 2008 admission only]

Time: Three Hours Maximum WGP: 100

Section - A
Answer any Seven questions
[Weightage: 1 each]

1. Define bandwidth.
2. Explain multiplexing.
3. What is parallel communication?
4. What is RS-232?
5. Explain Co-axial cable.
6. What is Huffman Coding?
7. What are the functions of Data link layer?
8. What is network topology?
10. What is a virtual terminal?

Section - B
Answer any Seven questions
[Weightage: 2 each]

11. Explain RZ and NRZ.
12. Describe PCM and DPCM.
14. Explain Error detection and correction
15. Explain data compression.
17. Explain IEEE 802 standard.
20. Explain client-server model.

Figure 5.6d Decrypted QP using VCS with XOR operation
5.3 Fingerprints and Visual Cryptography\textsuperscript{2}

A fingerprint has its own distinctiveness and this property has been used for personal identification for several years. Fingerprint identification is based on two basic premises:

- Persistence: the basic characteristics of fingerprints do not change with time.
- Individuality: everybody has a unique fingerprint.

Fingerprint can be used in one of two modes: the identification mode, in which the identity of an unknown user is determined, and the verification mode, in which a claimed identity is either accepted or rejected. Fingerprints are applied in many high end applications with governments, defense and airport security being major customers. However, there are some areas in which fingerprints are increasingly being used in commercial and administrative applications, namely, network/PC login security, web page security, employee recognition, time and attendance systems, voting etc. The fingerprint systems also enhance user convenience by alleviating the need to design and remember passwords. Fingerprint information is being stored and transmitted increasingly using computer systems and networks everyday. Therefore secure and reliable transmission of fingerprint has great importance.

Visual cryptography provides a secure way to transmit fingerprint image without any computational complexity.

In this method the fingerprint image is combined with visual cryptography; the resulting cipher will become very hard to break, because it uses two different security techniques.

**Figure 5.7** A diagrammatic description for fingerprint and VCS system

In this system the fingerprint image is encrypted into ciphertext (C) by using visual cryptography schemes. The ciphertext (C) is a collection of shares which individually yield no information about the fingerprint image. In many cases, multiple encryptions do not strengthen the cipher and hence it is a waste of time; but in this case, it strengthens the cipher considerably. This type of cryptosystem easily overcomes any type of attacks.

5.3.1 Experimental Result

Experiments were conducted using 2-out-of-2 VCS. In this experiment, consider the fingerprint in binary image format. In the encryption process, the fingerprint image files are encrypted into two shares so that the original image is revealed only by stacking the two shares using XOR operation. The Figure 5.8 depicts the experimental results.
The scheme is perfectly secure and very easy to implement. To decode the encrypted information, i.e., to get the original information back, the shares are stacked and the fingerprint image pops out. The major advantage of this method is that the decryption process (fingerprint reconstruction phase) does not require any complex algorithm and computations.
5.4 Conclusion

The application of ‘2-out-of-2’ VCS has been demonstrated and explained here using a simple example. Variations of this method are also possible to various needs. Very sensitive and strategically important information is being stored and transmitted increasingly using computer systems and networks everyday. This revolution, however, has brought with it new threats and computer crimes as evidenced by the increasing number of computer attacks and break-ins. Therefore, there is a great need to keep information in a secure and reliable manner. This method also leaves open the scope for future expansions, which address emerging examination needs and security requirements, especially in the context of the ever-increasing applicability and relevance of online learning programs and examinations.

The fingerprint has direct application in individual identity verification and security requirements for e-documents, because online fingerprint transactions and applications are increasing in all areas of exchange in geometric proportions.