Remote Voting System Using Extended Visual Cryptography

Tridib Chakraborty[1], Mizan Md Chowdhury[2]

[1]Department of Information Technology, Guru Nanak Institute of Technology

[2]Department of Information Technology, Guru Nanak Institute of Technology

Abstract: ***Establishing trust is one of the most important human-human and human-computer interactions. Authentication can be done using something we know (for example, a password), something we have (for example, a mechanical key), or something we are (a living, breathing human). These may be combined to provide stronger authentication. In this paper, we discuss some of the issues associated with Internet-based remote voting and argue that visual cryptography offers a promising way to provide both satisfactory authentication and secret ballot guarantees.***

Keywords: Remote voting, Extended Visual Cryptography, Authentication

1. Introduction

People all over the world are starting to take a hard look at their voting equipment and procedures, and trying to figure out how to improve them. There is a strong inclination towards moving to Electronic Voting in order to enhance voter convenience, increase voter confidence and voter turnout.

Voting systems must be certified before they are used. Election officials must have confidence that the voting system will prevent fraud and perform reliably.

[1]Visual cryptography was originally invented and pioneered by Moni Naor and Adi Shamir in 1994 at the Euro crypt conference. Visual cryptography is "a new type of cryptographic scheme, which can decode concealed images without any cryptographic computation". No computer participation is required, thus demonstrating one of the distinguishing features of VC. VC is a unique technique in the sense that the encrypted message can be decrypted directly by the human visual system (HVS).

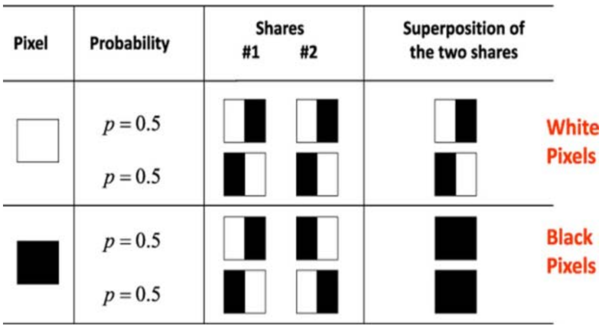
In Remote voting system before an election, the election officials need to generate and send image transparencies to eligible voters. A voter visits the election website. The election web site maintains a list of unique ids and associated passwords. The entered id must be on the list and has not been used already. If the entered id is valid, the election server then allows entering a random string. The complementary image to the password image for the voter's [3]transparency is generated and displayed on a web page. After the web server displays the corresponding image generated, the voter holds the transparency (share1) up to the screen to reveal the password. To continue the voting process, the voter enters the revealed password. This protocol serves to both authenticate the voter to the election server and the election server web site to the voter.

2. Approach

We propose to provide remote authentication for both voters and voting systems using visual cryptography.

Visual Cryptography

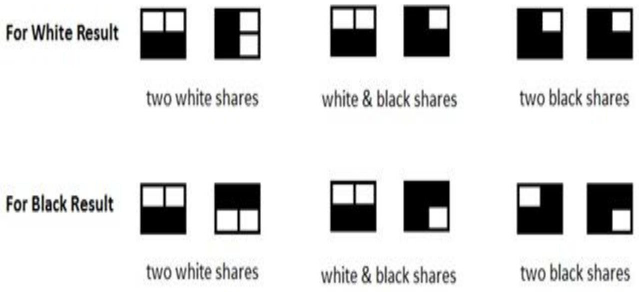
Generally speaking, images, audio, and video files are usually much bigger than text files. Therefore, using complicated conventional cryptography to encrypt/decrypt them seems to be rather wasting processing time. Naor and Shamir [1] proposed a new cryptography paradigm, called visual cryptography (VC) or visual secret sharing (VSS), which attempts to recover a secret image via the human visual system by stacking two or more transparencies. In their approach, the secret was partitioned into n shadow images (shares), and each participant would receive only one share. Once any k or more shares of a secret are stacked together, the secret image will be visually retrieved without the help of the computer. That is to say that the secret image will be invisible if the number of stacked shares is less than k. This is known as (k, n)-threshold mechanism.



Extended visual cryptography:

The extended visual cryptography scheme (EVCS) was introduced by Mizuho NAKAJIMA, Yasushi YAMAGUCH.[2], where a simple example of (2,2)-EVCS was presented.

Generally, an EVCS takes a secret image and original share images as inputs, and outputs shares that satisfy the following three conditions: 1) any qualified subset of shares can recover the secret image; 2) any forbidden subset of shares cannot obtain any information of the secret image other than the size of the secret image; 3) all the shares are meaningful images.



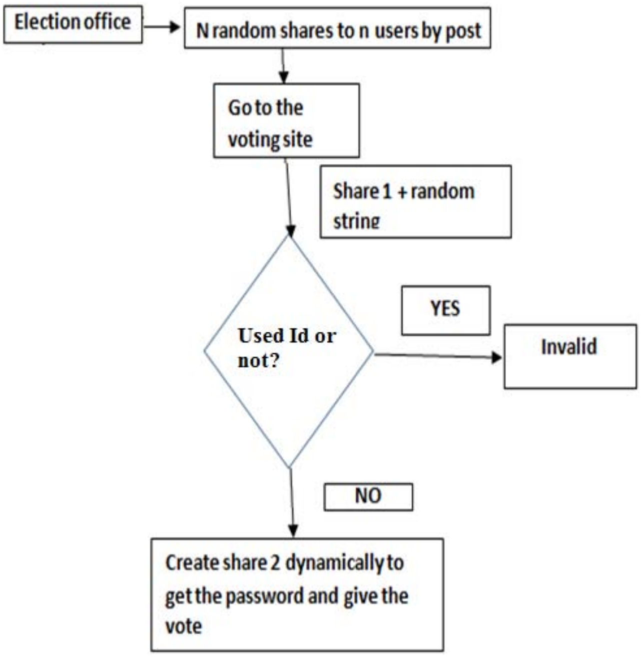
Remote Voting Authentication Process

In this process, before an election the election officials generate the shares[3]. After the generation of transparencies, the election officials send the generated transparencies to eligible voters through a third party who sends each eligible voter a randomly selected transparency along with a unique id. There is no mapping between voter identities and the transparency they receive. The user will go to the voting site and will enter the unique id. After that, server will check whether the unique id is new or used. If the id is used then it means the user has already casted his vote and is not allowed anymore to cast vote. If the user is new, then the voter is allowed to enter a random string. After this, share2 is generated and displayed on the password screen along with the random string. Now using the transparency provided to user, the user gets to see the password to cast the vote.

Previous studies have analyzed how much a user needs to know in order to make rational decisions in the security of computer services, and the users showed they did not have a solid grasp on the security aspects of the system. With our system, voters do not need to understand how visual cryptography works, but are directly involved in performing the decryption in an intuitive and physical way.

Our authentication scheme ensures that the voter cannot continue with the voting process without also verifying the server is legitimate.

Process Logic


Election office
N random shares to n users by post
Go to the voting site
Share 1 + random string
Used Id or not?
YES
Invalid
NO
Create share 2 dynamically to get the password and give the vote

3. Conclusion

In order to hide the secrecy we go for expansion and increasing of the number of shares, but this affects the resolution. Therefore an optimum number of shares are required to hide the secrecy. At the same time security is also an important issue. Hence research in visual cryptography (VC) using extended visual cryptography is maintaining the contrast and at the same time maintaining the security. So the system which we have developed not only provides security but also authenticates the system in two ways and is also very easy to use and understand.

4. Future Work

Contrast of the image can be improved. The share size is getting doubled for our algorithm, the size of the image should remain same. A module need to be developed to deal with the different device specific resolution.

References

[1] Visual Cryptography, Moni Naor and Adi Shamir, Copyright © 1998, Springer-Verlag
[2] Extended Visual Cryptography For Natural Images, Mizuho NAKAJIMA, Yasushi YAMAGUCHI, 2002
[3] Remote Voting System for Corporate Companies using Visual Cryptography, Anusha MN Srinivas B K., 2012