ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

BIOMETRIC AUTHENTICATION USING PARTIAL HIERARCHICAL VISUAL CRYPTOGRAPHY

Rekha R , Selin M

[*] Department of Computer Science and Engineering, KMEA College of Engineering, India

ABSTRACT

The importance of a strong authentication is very crucial in almost all applications now. User authentication is a method in which the identity of the individual is verified for accessing certain information .Using biometric information for authentication will be a better proposal as biometric information will be unique for each individuals. The project proposes to implement a signature based authentication using partial hierarchical visual cryptography. Visual cryptography encrypts secret information into different portions known as shares. Hierarchical visual cryptography encrypts the signature in different levels.

KEYWORDS: Visual cryptography, secret sharing, shares, authentication

INTRODUCTION

User authentication is an important security measure for protecting confidential data. Without a means of verifying a potential requester, data access may be granted to unauthorized individuals or groups that can steal confidential information for malicious purposes, or in the case of businesses, use the information to their financial advantage. Unauthorized access to data can also lead to file corruption or the downloading of viruses, both of which can cause a system or entire network to crash . Therefore data needs to be protected from unauthorized users as there are many threats to data security .

The purpose of computer security is to devise ways to prevent the weakness from being exploited. When computer security is concerned we are addressing three main aspects of the computer related system namely confidentiality, integrity and availability. Confidentiality ensures that the resources of the system are only accessed by the authorised parties. By the term access means it covers reading, viewing, or well defined methods of covering the resources.

Confidentiality can be sometimes called as secrecy or privacy.

Integrity means that the assets can be modified only by authorised parties in authorised ways, so the changes that can be brought to the system include writing, changing, deleting, creating. Availability means the resources are accessible to authorised parties at appropriate times. Information is increasingly important in our daily life. Information gets more value when shared with others. Due to advances in technologies related to networking and communication, it is possible to share the information like audio, video and image easily. It may give rise to security related issues. Attackers may try to access unauthorized data and misuse it. To solve this problem certain techniques are required. Techniques to provide security, while sharing information are termed as Secret sharing schemes. When it comes to visual information like image and video, it is termed as Visual secret sharing scheme.

Visual cryptography (VC) is a technique used for protecting image-based secrets. The basic concept of visual cryptography scheme is, to split secret image into some shares, which separately reveals no knowledge about the secret information. Shares are then distributed to participants. By stacking these shares directly, secret information can be revealed and visually recognized. All shares are necessary to combine to reveal the secret image. Starting from the basic model, many visual cryptographic techniques have been evolved day by day.

Visual cryptography is a technique which allows information such as images, text, diagrams etc to be encrypted and then it can be decrypted by the eyes. Visual cryptography scheme was proposed by Naor and Shamir in 1994. Basic idea is hiding the secret image in n distinct images called as shares. The secret image can be then later revealed by staking together these shares. Superimposing of one image on top of another image is called stacking of the image. Different schemes are available for Visual cryptography.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

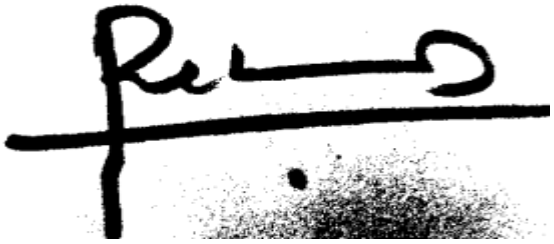
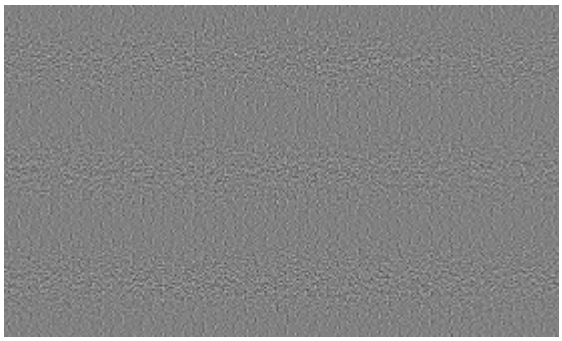
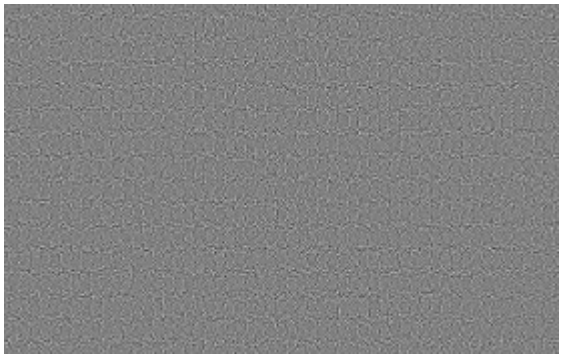


Image to be encrypted



One share after encryption



Second share after encryption

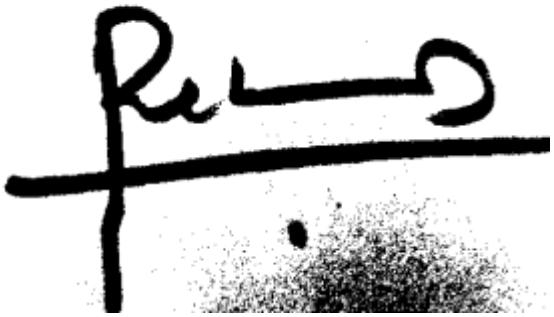


Image after visual cryptography based decryption

In (2, 2) visual cryptography, the main constraint is both the shares are required to reveal secret information. If one share gets lost due to some technical problem, secret information cannot be revealed. So there is a restriction of keeping all the shares secure to reveal information and user can not afford to lose a single share. To give some flexibility to user, basic model of visual cryptography proposed by Naor and Shamir can be generalized into a visual variant of k out of n visual cryptography scheme. In (k, n) visual cryptography scheme, n shares can be generated from original image and distributed. Original image is recognizable only if k or more shares stacked together, where value of k is between 2 to n. If fewer than k shares stacked together, original image cannot be recognized. It gives flexibility to user. If user loses some of the shares still secret information can be revealed, if minimum k number of shares is obtained.

PROPOSED WORK

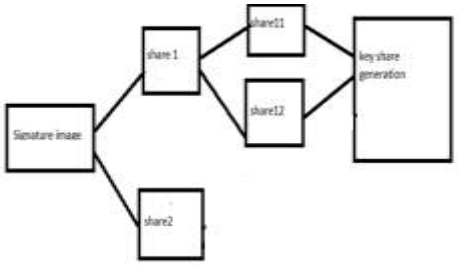
A signature can be defined as handwritten depiction of someone's name which is normally treated as proof of identity.Traditional functions of a signature are to prove the identity of a document or to give evidence to an individual with regard to a document. Signature verification is the process used to recognize an individual's handwritten signature. There are two types of signature verification: static and dynamic. Static signature verification system is when a signature is written offline such as bank cheques and the system reads the image scanned, and then verifies it with the signatures in database of the customer. Dynamic signature verification system is when a signature is written onto a hand held device such as a tablet and is read at run time, and compared to the signatures in database of the person to check for authenticity.

Prevailing methods of authentication are linked to passwords, user Ids, PIN. Authenticating using signature is considerably more secure than traditional password authentication mechanism. In conventional password authentication mechanism if the server is hacked or connection to the server is spooled then an attacker can learn your password. Security is always an evolving concept and it never relies completely on any algorithm. In traditional password based authentication mechanism, user has to remember the password and it prone to dictionary attack. Here, signature is unique pattern presented by user and two way authentication is taking place i.e. user authenticate to the system and system authenticate to user. The user has to enroll as a registered user to become a part of authentication system.

ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

During enrollment, the signature of the user is scanned and applied as an input to the hierarchical visual cryptography. HVC then divides the signature in to two shares. This is the first stage of the hierarchical visual cryptography. Then at the next stage again the share1 ie the data share is again encrypted again to generate the second level shares. This work is only implementing partial hierarchy as only one share at the stage one is encrypted again to form the second level shares.The user should have an id proof which has a key share generated out of hierarchical visual cryptography .

The simple share is that share which is kept as a part of database in the system. Since the database of the entire authentication system includes the scrambled form of the share, there exist least possibility of various attacks like dictionary attack and brute force attack. During authentication the key share from user is superimposed over the corresponding simple share available in the system. For verification of a user, revealed signature is matched with user id . The user id along side with the decrypted signature image will beef up the security level. In this authentication system, unauthorized user can not authenticate.



Proposed method of key share generation

The signature image which is selected is of the PNG format. PNG is portable network graphics format. PNG file format supports lossless data compression. All the shares generated should also be of PNG file format.

CONCLUSION

Authenticating using signature is considerably more secure than traditional password authentication mechanism. In conventional password authentication mechanism if the server is hacked or connection to the server is spooled then an attacker can learn your password. The signature authentication is proposed to implement with hierarchical visual cryptography. Through hierarchical visual cryptography the security of the system would be very much higher compared to traditional (2,2) visual cryptography scheme. The increase in number of shares is the main reason behind the improved security. Large amount of shares can diminish the quality of the decrypted image.

REFERENCES

[1] Pallavi Vijay Chavan,Dr.Mohammed Atique,Dr.Latesh Malik, "*Signature based Authentication using contrast enhanced Hierarachial Visual Cryptography*," 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science.

[2] A. Shamir, "How to share a secret", Communications of ACM vol. 22, no. 11, pp. 612–613, 1979.

[3] S. Jaya, Malik Aggarwal, "Novel authentication system using visual cryptography", World Congress on Information and Communication Technologies-2011, pp. 1181–1186, October 2011.

[4] P. L. Yi Chen, "Authentication mechanism for secret sharing using boolean operation", International Journal of Electronic Science and Technology, vol. 10, no. 3, pp. 195–198, September 2012

[5] Zdenek Riha, Vaclav Matyas "*Biometric Authentication Systems*," FIMU Report Series ,November 2000.