Secret Sharing based Secure Authentication System

Rupali S. Patil
Student, ME Computer
Pune University
PCCOE, Pune

Sonali Patil
Assistant Professor
Pune University
PCCOE, Pune

Sudeep D. Thepade
Assistant Professor
Pune University
PCCOE, Pune

ABSTRACT
The growth in the usage of internet has increased the demand for fast and accurate user identification and authentication. New threats, risks and vulnerabilities emphasize the need of a strong authentication system. Automated methods based on physiological characteristics of user are widely used to identify and verify the user. Biometric is the technology to deal with such methods which measures and statistically analyze the biological data. A biometric authentication system provides automatic authentication of an individual on the basis of unique features or characteristics possessed by an individual.

The authentication system can be stronger using multiple factors for authentication process. The application like Aadhar Card uses multiple factors for authentication. There are some difficulties with multi-factor authentication system such as user privacy considerations, huge size databases and centralized database which may create security threats.

To address such tribulations, the biometric authentication using secret sharing is proposed. Secret sharing will split the centralized database across the different locations. This will help in reducing the database size and removal of threats in centralized database. Also user privacy will be maintained due to decentralization of database.

General Terms
Biometrics, Authentication

Keywords
Biometric authentication, Biometric features, Secret sharing, De-centralized database.

1. INTRODUCTION
Increasing concerns over the personal information has increased the interest in computer security. Access to the internet and information resources has widely increased in our everyday life. Many people are dependent on computer systems and networks. This dependency has brought many threats to information security. As a result, information security has become an important issue and hence secure mechanisms are required to protect computers and important information against unauthorized access to computer resources. Thus authenticity of the user becomes major issue in today's internet applications. The authorized access can be provided through the various authentication methods such as providing passwords or keys. But these methods are not more secure as a password can be forgotten or guessed with bruit force attacks, a key may be lost or stolen and both can be shared. Biometric based authentication methods have significant advantages over traditional password authentication systems [1]. These methods provide an alternative to password based security systems as there are no passwords to remember and biometrics cannot be stolen and are difficult to copy.

2. LITERATURE SURVEY
This section contains the literature survey of previous work done in the area of biometric based authentication system. In the studied papers, many authentication systems use only one factor for authentication. Also most of the papers referred for the study are based on the visual cryptographic technique. Detailed description about the studied papers is given below.

2.1 Fingerprint based authentication system using threshold visual cryptography technique [2]
This paper defines an approach to overcome server side attacks. The paper uses visual cryptography technique for splitting the fingerprint template into number of shares. In this technique, one of the generated shares is stored into the database and the remaining shares are given to the user. The participants, who are having those shares, will be able to reconstruct the secret by stacking of the shares. The paper focuses on two major issues in the fingerprint based authentication systems such as costly maintenance of the huge size databases and also the falsification. The present approach is for threshold visual cryptography; hence it solves the problem of two shares scheme. In two share scheme, the intruder can easily steal one share and can reconstruct the original secret. This limitation is overcome by the system using threshold visual cryptography and it is used to protect the information about biometric which is stored in the database.

2.2 Signature based authentication using contrast enhanced hierarchical visual cryptography [3]
In this paper, application of the hierarchical visual cryptography is implemented for authentication. It is an alternative for fingerprint based authentication system. Repetitiveness in authentication and rejecting some users falsely are the two major problems in fingerprint based authentication. The implemented system in this paper, takes the signature instead of fingerprint. The signature encryption is based on hierarchical visual cryptography (HVC). HVC is the method of encryption in which signature is divided into four shares. Further any three shares are chosen to create key share. Other share is given to the user and the key share is stored in database to the administrator.

No information is visible in the shares but when both the shares are stacked or superimposed then the secret is revealed. The encryption of the secret is done stepwise in hierarchy due to which shares are more secure and does not reveal any information about secret. The scheme generates the shares

without expanding the size of shares. Secret size remains same during encryption and decryption. For authentication, user provides his or her share in the form of card, so that card reader reads the share and stacks it with the share stored in the database. After stacking, the signature is revealed and the enrolment number of the user is retrieved, which indicates that the person is authentic.

2.3 Secure Iris Authentication using Visual Cryptography [3]

The system proposed in this paper uses visual cryptography techniques to protect iris template in the database as well as providing extra layer of authentication to the existing iris authentication system. Enrolled iris template is divided into two shares using visual cryptography one is kept in the database and other with user on the ID card. Security is provided to the iris template because using only one share which is in the database, no information can be retrieved for the enrolled eye image. In this case access from unauthorized user is avoided. This system will be more secure and reliable in security-critical applications. One of the major challenges in biometric system is to protect the template securely in the database. The applicability of the system is in accessing the secure resources by only authenticated users. The system implemented in [3] has two modules.

2.3.1 Enrolment

The database administrator captures and collects the eye image from the users who are authorised to access the secure resource. Pre-processing, segmentation, normalization and feature extraction techniques are applied to extract the characteristics of the iris image provided in for enrolment and then it is stored in the database.

2.3.2 Authentication

In the authentication process, user gives the share possessed by him or her in the form of ID card. Accordingly, system retrieves the corresponding share from the database. By stacking these two shares, the iris template is generated. Further, the new eye image taken at the time of authentication is pre-processed, segmented, normalized and then features are generated. The two feature templates are compared using the hamming distance measure and then the decision is taken for granting the user or denying the user.

2.4 A multimodal biometric recognition system based on fusion of Palmprint and Fingerprint [5]

This paper is about a biometric identification system that represents an alternative to conventional approaches. In the multimodal biometric system, two or more biometric traits are used for identification. To improve the accuracy, multimodal system is used. Multimodal system proposed in paper [5] uses palmprint and fingerprint traits for identification. Each biometric trait has different information. In multimodal systems, the information from each trait is taken separately and later it is combined using some fusion techniques. The system implemented in this paper uses Euclidean distance measure for matching the database template and the input template. Matching score of the templates is used for allowing the user to access the system or denying the user from accessing the secure resource. Multimodal biometric authentication system given in [5] works in six stages which are listed below.

1. Image Capture.
2. Image Pre-processing.
3. Feature Extraction.
4. Fusion.
5. Matching.
6. Decision.

2.5 An (3, 3) – visual secret sharing scheme for hiding three secret data [6]

This paper proposes an improved (3, 3)-visual secret sharing scheme. The method is useful for sharing three secrets. Three shares are created from three secret messages. In the share creation process, first main share is created randomly. For creating the other two shares, rotation in clockwise and anticlockwise and first share is used. Depend on pixel values, fix pattern tables are designed for generating the remaining two shares.

2.6 VC of Iris Images for ATM Banking[7]

This paper proposes a method for iris recognition which is capable of comparing two digital eye-images. Here visual cryptography technique is applied to iris authentication system. In this system there are two modules enrolment and authentication. For accessing any secure resource by authenticated users this system can be used especially for ATM (automatic Teller Machine) banking. The enrolled eye image is required to be processed so characteristic iris features can be extracted using the hybrid transform (DCT+DHT), for this purpose algorithms are developed.

3. PROPOSED METHOD

In the proposed method, there are two steps involved in the process of authentication.

1. Enrolment.
2. Authentication.

In the enrolment process, biometric traits are taken using sensor or camera. After capturing the images of biometric trait, normalization is done on the data to remove the noise. The important features are extracted from the images and feature template is generated. Storing complete secret in the database is prone to the centralized database attacks. Hence, secret sharing is applied to split the secret into two shares. After generating the shares, one share is stored in the database and other is given to the user to store in the ID card. In the authentication process, the new biometric traits are captured using the sensor. After capturing images, features are extracted. Extracted feature template is compared with the template from the database share. Similarity measures are used to match the two templates and decision is made whether the user is authenticated or not.

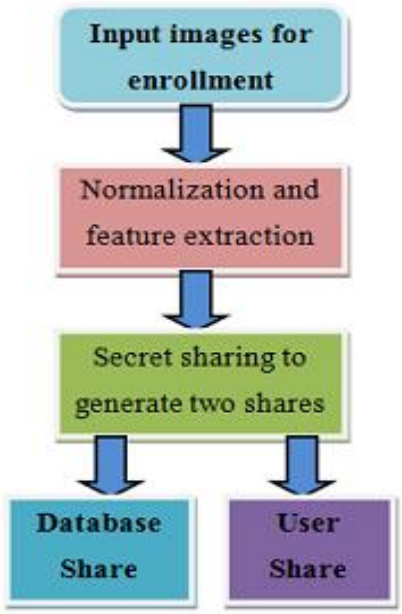

Figure 1. Enrolment Process.

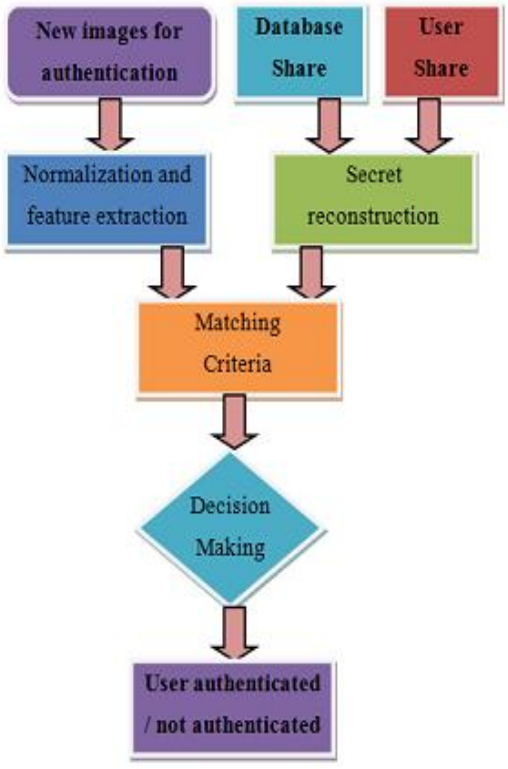

Figure 2. Authentication Process.

4. COMPARATIVE ANALYSIS

The comparative analysis of the studied papers is given in the TABLE 1 below. There are four parameters considered for the comparison. First parameter is the number of factors used for authentication, second parameter is which factor to use for authentication, third parameter is the merits of that factor in the given paper and the last parameter is the demerit of that factor in that paper.

TABLE 1. Comparative analysis of literature survey.

Parameter / Authors	No. of factors	Authentication factor	Merits	Demerits
J. Sirdeshpande et al. [1]	1	Finger print	Reduced database	False acceptance and false rejection
R. Mukesh et al. [2]	1	Finger print	Reduced database size, threshold scheme	Computational complexity
p. Chavan et al. [3]	1	Signature	Reduced gray level	Computational complexity is more
P. S. Revenkar et al. [4]	1	Iris	Permanence of iris	Subject dependent
M. D. Dhameliya et al. [5]	2	Finger print, palm print	Optimal FAR and FRR	Dependent on biometric factor weight

5. CONCLUSION

The paper proposes secure authentication system using secret sharing. The proposed system is very useful in enhancing the security of authentication system against the attacks done on centralized database. The database gets decentralized in a secure way using secret sharing. Also user privacy is taken into consideration by splitting the biometric feature vector. The proposed system uses transform domain for feature extraction which helps in not revealing the trait information. The database size gets reduced, as complete biometric feature template is not stored in the database. Also the limitations of unimodal authentication systems are overcome as proposed system uses multiple factors for authentication.

6. ACKNOWLEGEMENT

Many thanks and deep gratitude to the researchers who had given their valuable contribution in implementing biometric authentication system. Authors want to thank to computer department of Pimpri Chinchawad College of Engineering for providing the required resources. Also authors want to thank to Pimpri Chinchwad College of Engineering for continuous support for the research.

7. REFERENCES

[1] J. Sirdeshpande, S. Patil, "Amended Biometric Authentication using Secret Sharing", *International Journal of Computer Applications*, vol.98, No.21, 2014.

[2] R. Mukesh, V. J. Subashini, "Fingerprint based Authentication System using Threshold Visual Cryptographic Technique", *International Conference on Advances in Engineering, Science and Management*, pp.16-19, IEEE, 2012.

[3] P. V. Chavan, M. Atique, L. Malik, "Signature based Authentication using Contrast Enhanced Hierarchical Visual Cryptography", *Electrical, Electronics and Computer Science (SCEECS)*, pp.1-5, IEEE, 2014.

[4] P. S. Revenkar, Anisa Anjum, "secure Iris Authentication using Visual Cryptography", *Journal of Computer Science and Information Security*, vol.3, pp.217-221, 2014.

[5] M. D. Dhameliye, J. P. Chaudhari, "A Multimodal Biometric Recognition System based on Fusion of Palmprint and Fingerprint", *International Journal of Engineering Trends and Technology*, vol.4, Issue 5, pp.1908-1911, 2013.

[6] P. F. Tsai, Ming-Shi Wang, "An (3, 3) – Visual Secret Sharing Scheme for Hiding Three Secret Data", *JCIS, atlantis-press.com*, 2006.

[7] S. Koteswari, P. John Paul, S. Indrani, "VC of IRIS Images for ATM Banking", *International Journal of Computer Applications*, vol.48, No.18, pp.1-5, 2012.

[8] S. D. Thepade, P. Bidwai, "Iris Recognition using Fractional Coefficients of Cosine, Walsh, Haar, Slant, Kekre Transforms and Wavelet Transforms", *International Journal of Emerging Technologies in Computational and Applied Sciences*, pp.141-146, 2012.

[9] M. P. Dale, M. A. Joshi, N. Gilda, "Texture based Palmprint Identification using DCT features", *International Conference on Advances in Pattern Recognition*, pp.221-224, 2009.

[10] A. H. M. Al-Helali, W. A. Mahmmoud, H. A. Ali, "A Fast Personal Palmprint Authentication based on 3D-Multi Wavelet Transformation", *Transactional Journal of Science and Technology*, vol.2 No.8 pp.1-10, 2012.

[11] Adams Wai-Kin Kong, David Zhang, "Feature-Level Fusion for Effective Palmprint Authentication", *Lecture Notes in Computer Science*, vol.3072, pp.761-767, 2004.

[12] K. P. Shashikala, K. B. Raja, "Palmprint Identification based on DWT, DCT and QPCA", *International Journal of Engineering and Advanced Technology*, vol.1, Issue 5, pp.325-331, 2012.

[13] S. D. Shirke, D. Gupta, "Iris Recognition using Gabor", *International Journal of Computer Technology and Applications*, vol.4, pp.1-7, 2013.