International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 1 155 - 158

A Review on an Authentication System using Secret Sharing

Nitesh M. Agrawal[1]
M.E. Student, Department of Electronics and Tele- communication,
Sipna C.O.E.T, S.G.B. Amravati University,
Amravati(Maharashtra State), India.
nitesh11391@gmail.com

Dr.Prashant R. Deshmukh[2]
Professor, Department of Electronics and Tele-communication,
Amravati(Maharashtra State), India
pr_deshmukh@yahoo.com

Abstract: Security using Authentication system is an important concern in the field of information technology. It is an important thing as per as concern to the ruling of internet over people today. The growth in the usage of internet has increased the demand for fast and accurate user identification and authentication. This New threats, risks and vulnerabilities emphasize the need of a strong authentication system. The cryptography is a secret sharing scheme where a secret data gets divided into number of pieces called shares and not a single share discloses any information about secret data. There are some automated methods to identify and verify the user based on the physiological characteristics. To deal with such methods, there is a technology called biometrics which measures and statistically analyses the biological data. The biometric samples which are stored in the database as a secret are unique for each user so that no one can predict those samples. 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 more than one factor for authentication. There is some difficulty with authentication systems such as user privacy considerations in case of multiple biometric features, huge size databases and centralized database which may create security threats.
To address such tribulations, the Authentication System using Secret Sharing is proposed, Secret sharing splits the centralized database across the different locations. This helps in reducing the database size and removal of threats in centralized database. Also user privacy is maintained due to the decentralized database.

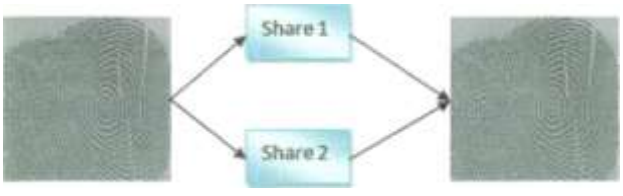
Keywords-*Authentication System, biometric features, secret sharing, decentralized database, MATLAB.*

*****

I. INTRODUCTION

The authenticity of the user becomes major issue in today's internet applications as per 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. 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.

A biometric authentication system provides the automatic authentication of an individual based on the unique characteristics possessed by an individual. Biometric authentication systems use physical and behavioral features of an individual for authentication. Physical features include fingerprint, palm print, iris, facial features, etc. Behavioralfeatures are voice, gait, signature are used for authentication. Biometric features are widely used due to its characteristics are Universality, Uniqueness, Permanence, Performance, User's acceptability. Biometric system work by first capturing sample of the feature; such as digital sound signal for voice recognition or taking a digital color image for face recognition. The sample is then transformed using some sort of mathematical function into a biometric template. The biometric template will provide a normalized, efficient and highly criminating representation of the feature, which can be objectively compared with the other templates in order to determine the identity. Most of the biometric systems allow two modes of operation. An enrolment mode for adding templates to a database and authentication mode, where a template is created for an individual and then one to one match is performed for the template in the database. Concept of secret sharing is shown below



Secret trait image Reconstructed secret

II. LITERATURE REVIEW

This section contains the literature survey of previous work done in the following fields are Biometric systems, Feature extraction methods for biometric trait, Image Fusion and Secret sharing schemes. It contains the literature survey of

various biometric based authentication systems. 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.

Shamir [1]proposed the idea of a (k,n) threshold based secret sharing in 1979. The technique used a polynomial function of order (k-l) Constructed as $f(x) = d_0 + d_1x + d_2x^2 + - - - - - + d_{k-1}x^{k-1} \pmod p$,where the secret is d_0 and p is prime number. The secret share are the pairs of values (x_i, y_i) where $y_i = f(x_i)$, $1 \le i \le n$ and $0 < x_1 < x_2 \ldots\ldots < x_n \le p-1$. The polynomial function /(x) is destroyed after distributing the pair of values (x_i, y_i) to each participant. Not a single participant can reveal the original secret. Also no group of (k-1) or fewer shares can reveal the secret. When k or more than k shares are available, then we can have at least k linear equations $y_i = f(x_i)$. The solution to those linear equations can be obtained using Lagrange's interpolation formula which is given below.

$$d_0 = \sum_{i=1}^{k} yi \prod_{1 \le j < k, j \ne i} \frac{xj}{xj - xi}$$

Thien and Lin [2,11] proposed a scheme based on Shamir's secret sharing method. Instead of using the random numbers for generating linear equations, Thien and Lin uses the pixel values of the secret image. In the (2, 4) threshold scheme, two pixel values are taken for generating the polynomial. The polynomial function can be generated as $S_x(i,j) = (110+112x) \pmod{251}$,where 110 and 112 are the values of first two pixels of the secret image. Hence four share values are computed as (l , 222), (2, 83), (3, 195) and (4, 56). These values become the first pixel of four shares. The next pixel of shares can be computed in the similar manner by taking the next two pixels of the secret image. The process repeats till all pixels of the secret are encoded. Hence in the Thien and Lin scheme, the share size becomes the half of the original secret image size. As like Shamir's secret sharing scheme, for reconstruction of the secret, the Lagrange's interpolation formula is used.

Sonalipatil ,PrashantDeshmukh [3] introduced an idea of secret sharing is to start with a secret, divide it into pieces called shares, which are then distributed amongst participants by the dealer. Only certain authorized subsets of participants can reconstruct the original secret. Applications for secret sharing schemes seem to be getting more important nowadays. For many circumstances, secret sharing has to provide more flexibility and functionality as per the need of an application. Secret Sharing has been an active research field for many years. Various secret sharing techniques have been developed to secure data, but there is a need to implement a secret sharing scheme with all augmented capabilities like general access structure, robustness against cheating shareholders, verifiability of the shares, proactive redistribution of shares etc. The intent of this paper is to explain the extended capabilities of secret sharing schemes and analyze the relation in application semantics and multifarious secret sharing schemes.

Rejeswari Mukesh, V. J. Subashini [4] defines an approach to overcome server side attacks in which visual cryptography technique uses is 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 system, such as costly maintenance of the hugesize 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.

P.V. Chavan, M. Atique, L. Malik [5] proposed an 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 createkey share. Other share is given to the user and the key share is stored in database to the administrator.

The system proposed by P. S. Revenkar, AnisaAnjum [6] uses visual cryptography techniques to protect iris temp late 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 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 [6] has two modules.

Enrolment**:** The database administrator captures and collects the eye image from the users who are authorized 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.

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.

M. D. Dhameliya,, J. P. Chaudhari [7] proposed 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 [7] uses palmprint and fingerprint traits foridentification. Each biometric trait has different information. In multimodal system 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 [7] works in six stages which are Image Capture, Image Pre-processing, Feature Extraction, Fusion, Matching, Decision.

In the biometric systems, there are various methods for extracting the important features of the biometric traits. The following section contains the literature survey of the various feature extraction techniques in the field of biometrics. In paper [8], multimodal biometric recognition using iris and fingerprint by texture feature extraction using hybrid wavelets is implemented. The work is focusing on correlation based fingerprint. The method is robust but less accurate. For accuracy improvement, multimodal system using Hybrid wavelet is implemented. In paper [9] survey of palmprint feature extraction algorithms is given. There are four approaches for feature extraction, which includes structure, statistics, subspace or appearance and texture and transform domain. Structure based approach includes the features such as principal lines, wrinkles, delta points, minutiae etc.

Dr. G Raghavendra Rao, P. Devaki [10] proposed an algorithm for protecting the secret image whose confidentiality needs to be maintained, and also to authenticate the distributor who distributes that secret image to multiple users. The secret image will be fused with the fingerprint of the dealer for authentication purpose. Fusion of the finger print will be done by using image fusion technique to generate a single image consisting of the secret image as well as the finger print image of the dealer. The fused image will be divided in to number of shares based on the threshold secret sharing technique. This provides both confidentiality of the secret image and as well as the authentication of the dealer who has sent the image. The verification will be done during reconstruction of the secret image.

III. PROPOSED WORK

In the proposed method , two objective are considered for the experiment .Firstly to automate the threshold value for making decision on the basis of similarity measurement and second is to achieve the higher accuracy in authentication process. There are two steps involved in the process of authentication system.

1. Enrolment
2. Authentication

In the enrolment process, Images are taken using sensor or camera. After capturing the images and, normalization is done on the data to remove the noise. Using the transform domain, the important texture features are extracted from the images and feature vector is generated. Then fusion of the images will be done by using image fusion technique to generate a single image consisting of the secret image as well as the image of the dealer. Hence, secret sharing is applied to split the feature vector into two shares. After generating the shares, are stored in the database.

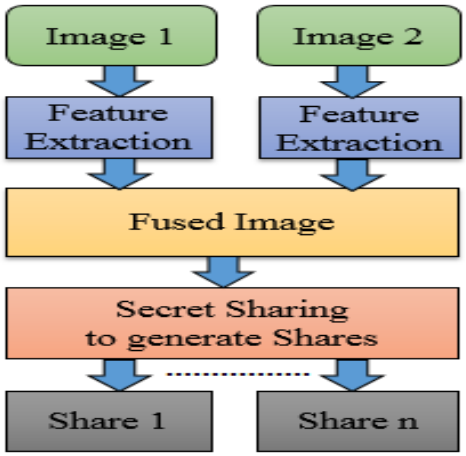


Fig:- User Enrolment Process

In the authentication process, the shares are received at receiver. After receiving shares, Images are reconstructed using templet reconstruction. Thus Fused Image is generated using Fusion Rule. Using the inverse transform domain, the important

texture features are extracted from the fused images and feature vector is generated. Hence secured data, in form of an images are obtained

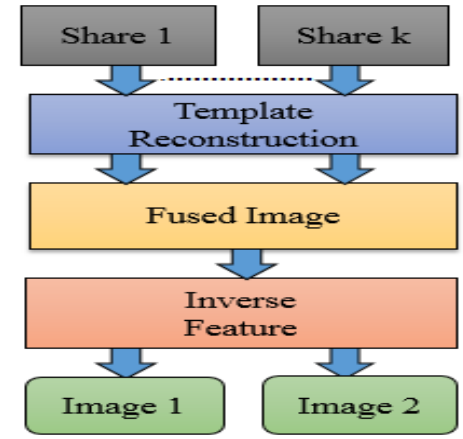


Fig: User Authentication Process

IV. 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

V. References

[1] Adi Shamir, "How to share a secret", Communication of the ACM, vol. 22, No. 11, pp. 612613, 1979.

[2] C. C. Thien, J.C. Lin, "Secret image sharing", Computers Graphics, vol. 26, pp. 765-770, 2002.

[3] SonaliPatil, PrashantDeshmukh, "An Explication of Multifarious Secret Sharing Schemes", International Journal of Computer Applications, vol. 46, No. 19, pp. 610, 2012.

[4] Rejeswari 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.

[5] 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, IE`EE, 2014.

[6] P. S. Revenkar, AnisaAnjum, "Secure Iris Authentication using Visual Cryptography", International Journal of Computer Science and Information Security, vol. 3 pp. 217-2215 2010.

[7] M. D. Dhameliya, 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. 1908-191 1, 2013.

[8] Vinayak Ashok Bharadi, BhaveshPandya, BhushanNemade, "Multimodal Biometric Recognition using Iris and Fingerprint — By Texture Feature Extraction using Hybrid Wavelets", Confluence- The Next Generation Information Technology Summit, pp. 697-702, IEEE, 2014.

[9] PengXinrong, TianYangmeng, Wang Jiaqiang, "A survey of Palmprint Feature Extraction Algorithms", International Conference on Intelligent Systems Design and Engineering Applications, pp. 57-63, IEEE, 2013

[10] Dr G RaghavendraRao , P. Devaki – "A Novel Algorithm to Protect the Secret Image through Image Fusion and Verifying the Dealer and the Secret Image'' Fifth International Conference on Signals and Image Processing,pp.77-80,IEEE, 2014

[11] Li Bai, S. Biswas, A. Ortiz and D. Dalessandro, "An Image Secret Sharing Method", International Conference on information Fusion, pp. I -6, IEEE, 2006.

[12] B Siva Kumar, S Nagarai-" Discrete and Stationary Wavelet Decomposition for IMAGE Resolution Enhancement" International Journal of Engineering Trends and Technology (IJETT) - Volume4 Issue7- July 2013