Checking User Authentication by Biometric One Time Password Generation using Elliptic Curve Cryptography

Dr.R.Sridevi
Assistant Professor in Computer Science
PSG College of Arts & Science, Coimbatore, India
srinashok@gmail.com

***Abstract*— Fingerprint recognition or fingerprint authentication refers to the automated method of verifying a match between two human fingerprints. Fingerprints are one of many forms of biometrics used to identify individuals and verify their identity. Also Face recognition becomes one of the popular biometric identification systems used in identifying or verifying individuals and matching it against library of known faces. Also it finds its application in wide variety of areas like criminal identification, human - computer interaction, security systems, credit- card verification, teleconference, image and film processing. They are fused together by score level fusion. Score level fusion is a method in which the weights of multiple Biometric features are compared against the images in the database and a new weight will be generated. If the weight is above threshold, then the user will be recognized and the first level of authentication will be completed. The second level of authentication for a user is done using One Time Password. But normally these are just random numbers that can be easily judged and hence may pose threat to some sensitive information. As a solution for this problem, the scheme proposed in this paper makes use of Elliptic Curve Cryptography, a public key cryptographic method, to generate One Time Password. As Elliptic Curve Cryptography is a strong asymmetric algorithm it is difficult to hack them in the reverse direction due to computational complexity and the uniqueness of the final fused weight value that is used as private key. Hence this proposed system is more reliable than any other conventional systems.**

Keywords-biometric fusion; user authentication; one time password; score level fusion;

I. INTRODUCTION

Random passwords and ID cards have been some of the few traditional methods that are used for identifying an individual. But these methods have become less secure as the threats to hack them are escalating [1]. Security is needed for two reasons, to identify the legitimate users and to protect privacy [2].Biometric technology makes use of the subject's biometric traits such as palm print, palm lines, fingerprint, face, iris, etc of the individuals. Each individual poses unique traits. Even identical twins have different biometrics features. So they are very difficult to be replicated and hence they can be reliably used for authentication purposes. Two types of biometrics are uni-instance biometrics and Multi-instance biometrics. Conventional multi-instance biometrics methods treat different traits independently [3] multiple biometric features can be fused at different levels such as image level, feature level, decision level and matching score level. One of the more efficient fusion methods is score level fusion[4]. This is the first level of authentication provided in our proposed model. The next level of authentication is provided by means of using One Time Password. Nowadays all the systems are using One Time Password to provide authentication [5]. But they are normally generated randomly. To make the generated OTP stronger, Elliptic Curve Cryptography (ECC), a very powerful technique is used.

Proposed work is enhancing the security using fingerprint and facial biometrics and OTP generation using ECC. The preference given to ECC over other methods is that it offers high security even with smaller size key, thus reducing computation power, memory and bandwidth [6].

II. RESEARCH OBJECTIVES

The main objective of the paper is to design a system that could check the authenticity of the user. To achieve this, concept of biometrics and OTP are utilized to enhance security. Two levels of authentication are provided .Multiple biometric feature of an individual is used to authorize the user to access the confidential data of the system. This is the first level authentication. OTP is generated using Elliptic Curve Cryptography(ECC) method. ECC is preferred because of its trapdoor function. This is the second level of authentication. A user who passes both levels of authentication successfully, is identified as a legitimate user and is allowed to access the system.

III. SURVEY OF LITERATURE

Yong Xu et al explained various fingerprint identification methods. Most notable methods are line based method, coding based method, sub spaced based method and representation based method. Our paper focuses on the use of line based method. David Zhang et al explain the use of gober function to capture the orientation of palm lines. Raghavendra et al has given a overview of ROI extraction. The accurate extraction of ROI plays a crucial role in improving the performance of the overall fingerprint recognition. Yong Xu et al has explained processing of sub bands of the image identification. JitendraChaudhari et al explains about the orientation based approach,a best method in palm print matching.

The second level of authentication involves the ideas of OTP and ECC. Many authors have exploited the strength of ECC and came up with implementation in various tasks of public key cryptography like authentication, digital signature, key agreement and encryption. Victor S. Miller explains the use of Elliptic curves in Cryptography. He proposed an encryption scheme similar to Diffie-Hellman key exchange protocol but faster by around 20 percent. Neal Koblitz explained about the elliptic curves over finite fields for public key cryptosystems. He explained that the discrete logarithm problem is harder for finite group field compared to binary field. He also gave a theorem for non smoothness existing in cyclic subgroup generated by a global point. Neal Koblitz et al extended the idea of discrete logarithmic problem used in public key cryptography of Diffie-Hellman to elliptic curve group.

S.S.Tyagi et al enlightens the use of RSA algorithm along with its strengths, weakness and the reason to move to Elliptic Curve Cryptography method (ECC). Nick Sullivan et al explains the security of ECC over RSA algorithm. LaiphrakpamDolendro Singh et al explained the implementation of elliptic curve cryptography. It also explains the various mathematical operations such as point addition, multiplication, subtraction and inverse modulo operation using elliptic curve. Darrel Hankerson et al explained the various elliptic curve arithmetic, issue with implementation and cryptographic protocols in details. Lawrence C. Washington gave proofs to various theories related to elliptic curve.

In order to securely transfer image across the network various techniques have been develop in recent years using ECC. Ahmed et al presented an image encryption technique using cyclic elliptic curve and chaotic system. They proposed a technique to generate a pseudo random key stream using cyclic elliptic curve point and chaotic system which in turn is used for encryption of data stream from the image. Hong Liu et al gave a cryptanalysis of image encryption scheme based on hybrid chaotic system and cyclic elliptic curve. They found that known-plain text attack and choosing a plain image with all the pixel value 0 can generate the encrypted image.

Maria Celestin Vigila et al proposed an algorithm to perform image encryption using ECC. They use a coupled linear congruential generator to generate the private key and a random integer ‘k’. To obtain the cipher image point multiplication is performed for each pixel value with the generator to fit into the elliptic curve coordinate. A mapping table is required while performing decryption.

Ali Soleymani et al proposed an encryption technique using Elliptic Curve over Prime Group field. They created a mapping table which has values of 0 to 255 along the row and the corresponding row contains the elliptic curve coordinate. Pixel value of the image are mapped onto elliptic curve coordinate using the table and encrypted using the public key of the receiver. To view the encrypted data as cipher image the table is used again to map the values back to the range of 0 to 255. HimikaParmar et al gave a basic idea about one time passwords (OTP). In Wikipedia, advantages of static passwords over dynamic passwords were explained. Tamanna Saini et al, a onetime password generation system is introduced. HimikaParmar et al has explained about the various methods of one time password generation. This paper also focuses on the generation of OTP using image encryption.

IV. PROPOSED RESEARCH WORK

To overcome the limitation of the uni-modal biometric technique[7] and to improve the performance of the biometric system, multimodal biometric methods are designed by using multiple biometrics or using multiple instants of the same biometric trai[8]t, which can be fused at four levels such as image (sensor) level, feature level, matching score level and decision level[9]. OTP authentication method has been prevalent in various applications and it is widely accepted and trusted [10]. But nowadays, OTP generated are eavesdropped and are used for unethical activities. Hence, a strong method is needed to avoid this OTP hacking[11] .A novel framework is proposed that combines the fingerprint and facial images at the matching score level and this is followed by the use of OTP that is generated using ECC. Three types of matching scores, which are respectively obtained from the fingerprint and facial images, are fused to make the final decision. If the decision is favourable then the OTP will be generated and will be sent through mail to the registered mail ID. The user is expected to enter the ID. If there is a match, then the user is identified as a legitimate person.

V. BIOMETRIC FUSION BASED DECISION MAKING

Fusion techniques integrate different data sources or multiple classifiers to improve the performance of the system. In multi-instance biometric systems, unlike Uni-instance biometric systems, combines multiple biometric features to improve the reliability of the system[12]. A multi-instance biometric system requires an integration scheme to fuse the information obtained from the individual modalities. Fusion technique can be used to address a number of issues faced in the deployment of biometric systems: Accuracy, Efficiency, Robustness, Applicability and universality.

A. Types of Biometric Fusion

The fusion can be done at 4 different levels.

(1) Image level fusion: Many images can be combined to form a single image. The image fusion method tries to solve the problem of combining information from several images taken from the same object to get a new fused image [13]. The wavelet-based approach is widely used in image fusion.

(2) Feature level fusion: The data obtained from each biometric modality is used to compute a feature vector. If the features extracted from one biometric indicator are somewhat independent of those extracted from the other, it is reasonable to concatenate the two vectors into a single new vector, provided the features from different biometric indicators are in the same type of measurement scale. The new feature vector has a higher dimensionality and represents a person's identity in a different and hopefully, more discriminating feature space[14]. Feature reduction techniques may be employed to extract a small number of salient features from the larger set of features.

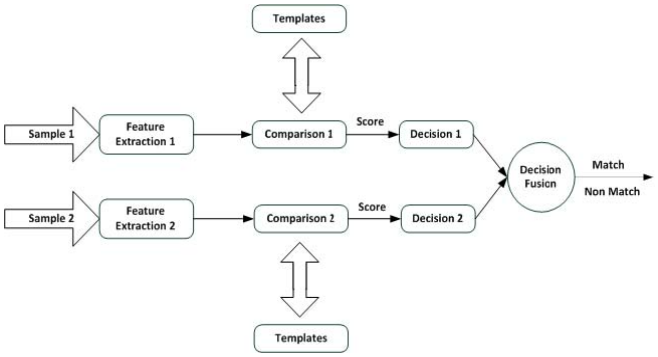

Fig.1 Feature Level Fusion

(3) Score level fusion: Each biometric matcher provides a similarity score indicating the proximity of the input feature vector with the template feature vector. These scores can be combined to assert the veracity of the claimed identity. Techniques such as weighted averaging may be used to combine the matching scores reported by the multiple matchers [15].

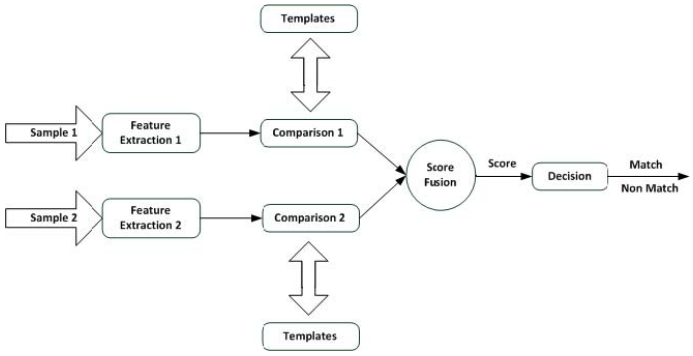

Fig.2 Score Level Fusion

(4) Decision level fusion: It is similar to score level fusion, except that the scores are turned into match / non-match decisions before fusion. Each biometric system makes its own recognition decision based on its own feature vector. A majority vote scheme can be used to make the final recognition decision[16].

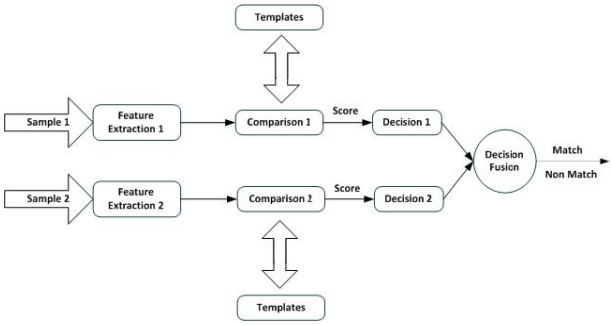

Fig.3 Decision Level Fusion

In the work proposed both score level and decision level fusion techniques are used and thus increases reliability. This provides the first stage of authentication. Prior to matching, two methods can be used. One is sensor level which provides raw data and the other method is the feature level which provides feature sets[17]. After matching, classifier can be selected randomly or either of the classifier fusion methods can be performed. The fusion used is confidence level fusion (i.e.) fusion is performed based on matching score.

B. Score level Fusion Matching

Match scores output by multiple matchers are consolidated. Two approaches exist in the context of verification: A feature vector is constructed using the match scores; feature vector is assigned to one of two classes: "genuine" or "impostor". A single scalar score is generated from multiple matching scores; a classifier operates on the new score. Scalar score is the method used here.

C. Weighing Biometric Traits

Each biometric trait provides a matching score based on the input feature set and the template against which the input is compared with[18]. These scores are weighted in order to reduce the importance of less reliable biometric traits and increase the importance of more reliable traits. Weighting all traits equally and using a user-specific matching threshold is used in order to obtain a new score. The user specific threshold fixed commonly for the entire fusion and decision making process.

D. Fusion Methodology

Sum rule (i.e.) weights of the individual scores are used to improve the system performance:

$$W = m_1 + m_2$$

Where,

m_1 = Matching score of fingerprint image.

m_2 = Matching score of facial image.

W = Total score.

Total score is calculated against all the images in the database. So this implies that the time complexity depends on the number of enrolments in the database. After all the computations are over, the maximum of all the values are chosen as the final weight for the input palm images.

E. Decision Methodology

Decision is based on the threshold value that is set commonly for the entire system. If the final weight obtained is above threshold, then the user is identified as a legitimate user. If it is less then the threshold, then the user is determined to be a illegitimate user.

If, Weight > Threshold, Recognized user

If, Weight < Threshold, Unrecognized user

VI. ECC BASED OTP GENERATION

The private key used in the ECC is not any binary or hexadecimal value but is the value driven from the previous level of authentication and the public key is only a constant. Weight from the score level fusion step is used as private key. It is multiplied along with the public key values in order to obtain the arbitrary constants to be used in the Elliptic curve equation.

Compute the Elliptic curve equation,

$$y^2 = x^3 + ax + b$$

OTP generated based on the above equation is transmitted via mail service to the registered mail ID. The private key is the weight value obtained as a result of score level fusion. This value is unique for each user. The private key is nothing but the common multiplier value chosen for a and b used to satisfy the elliptic curve. Since the private key used is the weight from the previous level of authentication which can be computed only when

calculating key value in the forward direction. If it tracked from the opposite direction, it will be nearly impossible to crack it due to the computational complexity of the elliptic curve equation and also due to the fact that the score value is purely private. Due to these reasons, it is considered as a trapdoor function. Hence, it very difficult for the adversaries to crack it.

A. User Enrollment

In any biometric authentication process, enrolment is the first process to be carried out. The users, who wish to enrol use the system, must register themselves in the database. This is done at the server side. Two databases are maintained. One for fingerprint images and other is for facial databases. The procedure followed for each individual is as follows: Biometric images of the individual are captured using a web camera. The pre - processing process in this level involves the extraction of ROI. It is done by using function in MATLAB software. Due to the extraction of the required feature ,the memory for storage is reduced. Only the users, enrolled in the database can access the system in the future.

B. Verification and Authentication

The fusion performed is score level fusion. All the scores are fused by weighted binary fusion method.

$$W = m1 + m2$$

A threshold value is set. If the fused value is above the threshold, then second level of authentication is carried out. On the contrary, if the value is below threshold, then the user is identified as an unauthorized user and the process is terminated.

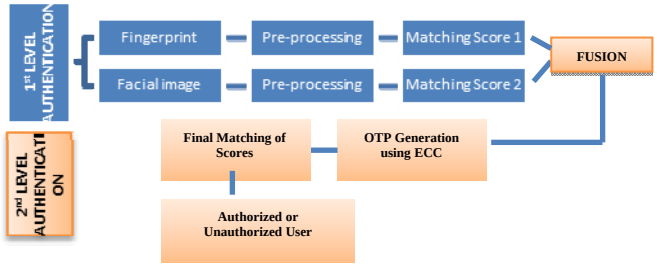

Fig.4 Verification and Authentication

OTP is generated by means of using ECC equation.

$$y^2 = x^3 + ax + b \text{ where,}$$

a = weight * constant

b = weight * constant

y = sqrt (x^3 + (weight * constant) x + (weight * constant)) and

x = random number.

The OTP thus generated is sent to the receiver's registered mail ID. If the entered OTP matches with the transmitted OTP, the user is identified as an authenticated legitimate user.

VII. EXPERIMENTAL RESULTS

The first level of authentication involves the authentication using multi instance biometrics technique. If there is a match, OTP will be generated. Matching is determined by the weight value obtained as decision making. If the obtained weight is above threshold of 0.7, then it is determined that there is match and the second level of authentication is carried out or else the user is not accepted by the system to access the data.

Second level of authentication starts with the generation of OTP .The generated OTP is sent to the mail ID mentioned. If the OTP generated by the user matches with the OTP generated recently, then the user is identified as a legitimate user.

VIII. CONCLUSION AND FUTURE WORK

The Proposed work shows that One time password is an efficient technique for generating dynamic passwords due to which new passwords are generated each time thus making it difficult for attackers to judge the OTP in a stipulated time. Moreover the use of ECC has improved the security of the system.. This model can be used for more sensitive applications even in an IoT environment .In the future, even more number of traits can be combined in order to make the system more reliable.

IX. REFERENCES

[1] Anil. K. Jain, Arun Ross and SalilPrabhakar, 2004, "Introduction to Biometric Recognition", IEEE Transaction on Circuits and Systems for Video Technology, vol 14, January.

[2] Austin Hicklin, Brad Ulery and Craig Watson, 2006, "A Brief Introduction to Biometric fusion", www.noblis.org, June.

A. Morales, M. A. Ferrer, and A. Kumar, 2011, "Towards contactless fingerprint authentication," *IET Comput. Vis.*, vol. 5, no. 6, pp. 407–416, November.

[3] Arun Kumar Gandhi, S.S.Tyagi, 2011, "Security Enhancement in Elliptic Key Cryptography Using Character Based Method", International Journal of Soft Computing and Engineering (IJSCE), ISSN: 2231-2307, Vol 1, July.

[4] Adams Wai-Kin Kong and David Zhang, 2004,"Competitive Coding Scheme for Palmprint Verification", Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04), 1051-4651/04, IEEE.

[5] D. Zhang, Z. Guo, G. Lu, D. Zhang, and W. Zuo, 2010 "An online system of multispectral palmprint verification," *IEEE Trans. Instrum. Meas.*, vol. 59, no. 2, pp. 480–490, February.

[6] D. Han, Z. Guo, and D. Zhang, 2008, "Multispectral palmprint recognition using wavelet-based image fusion," in *Proc. IEEE 9th Int. Conf. Signal Process.*, October, pp. 2074–2077.

[7] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid, 2012, "Recommendation for key management part 1: General (revision 3)" NIST Special Publication 800-57, pages 1–147, July.

[8] G. Feng, K. Dong, and D. Hu, 2004, "When faces are combined with palmprints: A novel biometric fusion strategy," in *Biometric Authentication* (Lecture Notes in Computer Science). Berlin, Germany: Springer-Verlag, pp. 701 -707.

[9] HimikaParmar, Nancy Nainan and SumaiyaThaseen, 2012, "Generation Of Secure One-Time Password Based On Image Authentication", CoNeCo, WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07, pp 195–206, 2012. © CS & IT-CSCP.

[10] JitendraChaudhari, Pradeep M Patil, Y P Kosta, 2015, "Comparative Study Of Radon Based Low Resolution Palmprint Image Matching", ICICES 2014, ResearchGate, DOI: 10.1109/ICICES.2014.7034035, February.

[11] Johannes Merkle, Tom Kevenaar, and Ulrike Korte ,"Multi-Modal and Multi-Instance Fusion for Biometric Cryptosystems", unpublished.

[12] Joshua E. Hill, 2013, "The Dual Elliptic Curve Deterministic RBG", Unpublished, June.

[13] Koblitz N, 1987, Elliptic curve cryptosystems. Mathematics of Computation, 48(177):203–209.

[14] Kien Nguyen, SridhaSridharan, 2015, "Score-Level Multi biometric Fusion Based on Dempster–Shafer Theory Incorporating Uncertainty Factors", IEEE Transaction on Human Machine Systems, vol 45, February.

[15] L. Hong, A. K. Jain, and S. Pankanti, 1999, "Can multibiometrics improve performance ?," in Proc. AutoID'99, Summit, NJ, October, pp. 59–64.

[16] L. I. Kuncheva, C. J.Whitaker, C. A. Shipp, and R. P.W. Duin, 2001, "Is independence good for combining classifiers?," in Proc. Int. Conf. Pattern Recognition (ICPR), vol. 2, Barcelona, Spain, pp. 168– 171.

[17] L. Hong and A. K. Jain, 1998, "Integrating faces and fingerprints for personal identification," IEEE Trans. Pattern Anal. Machine Intell., vol. 20, pp. 1295–1307, Dec.

[18] LaiphrakpamDolendro Singhand KhumanthemManglem Singh, 2015, "Implementation of Text Encryption using Elliptic Curve Cryptography", Eleventh International Multi-Conference on Information Processing-2015 (IMCIP-2015), Procedia Computer Science 54 (2015) 73 – 82, Elsevier.