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

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

MULTI-MODEL BIOMETRICS AUTHENTICATION FRAMEWORK

Sneha Kurhekar*, Harshvardhan Upadhyay
Department of Electronics and Telecommunication Engineering, SRCOE, Pune, Maharashtra, India

DOI:

ABSTRACT

Authentication is the process to conform the truth of an attribute claimed by real entity. Biometric technology is widely useful for the process of authentication. Today, biometric is becoming a key aspect in a multitude of applications. So this paper proposed the applications of such a multimodal biometric authentication system. Proposed system establishes a real time authentication framework using multi-model biometrics which consists of the embedded system verify the signatures, fingerprint and key pattern to authenticate the user. This is one of the most reliable, fast and cost effective tool for the user authentication.

KEYWORDS: Authentication, biometric, embedded system, signature, fingerprint and key pattern.

INTRODUCTION

Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. Authentication is relevant to multiple fields. In computer science, verifying a person's identity is often required to allow access to confidential data or systems. Now a day, biometric technologies are widely used for authentication purpose. Today, the security requirements of society have placed biometrics at the center of a large debate as it is becoming a key aspect in a multitude of applications [1]. There are many more other personal authentication techniques as well. Some of them uses the possession of the token (i.e ID cards) and some of them are knowledge based (i.e password, key-phase etc). But, the token based technique whose attributes can be stolen or lost whereas knowledge based approaches whose attributes can be forgotten, which become major drawback of such techniques. But the biometrics attributes, do not suffer from such disadvantages. Authentication factor covers the elements used to authenticate or verify a person's identity prior to being further process.

- Knowledge factors: Something which is well known to user, like a password, personal identification number (PIN), challenge response, Security question etc.
- Ownership factors: Something the user has like wrist band, ID card, security token, cell phone with built-in hardware token, software token, or cell phone holding a software token etc.
- Inherence factors: Something the user does like fingerprint, retinal pattern, DNA sequence signature, face, voice etc.

Proposed system is used Two-factor authentication process**.** Historically, fingerprints have been used as the most authoritative method of authentication. But now there are many more parameters was discovered for authentication. Here we used fingerprint, signature and key pattern verification to authorize user. Proposed biometric authentication system built up by knowledge factor (key pattern) and inherence factor (signature and fingerprint). On the other hand as per the biometrics is concern proposed system used both traits of biometrics physiological trait (fingerprint) and behavioral trait (signature). So, we say proposed system is a multi-model biometric system. Fig 1 represents the generic architecture of signature and fingerprint verification process [2]. This generic architecture acts as a basic platform for our proposed work. In general, signature and fingerprint verification process consists of two phase enrolment phase and evaluation phase. During the enrolment phase, each user provides several training Signatures and fingerprints, which are processed for extracting a set of distinguishing features that are stored into a database. Afterwards, during the evaluation phase, the user presents a new signature and fingerprint whose features are extracted and compared against those previously stored into the database during the enrolment phase. The result of this comparison produces a score or degree of similarity which is used to determine the authenticity of the user.

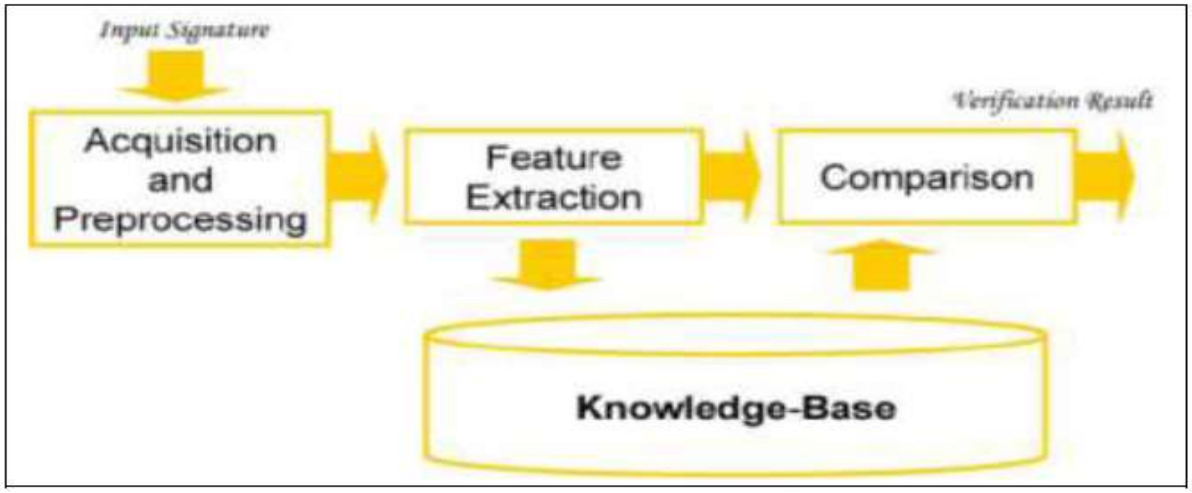

Fig 1. Generic architecture of signature and fingerprint verification process

PROPOSED SYSTEM

Fig. 2 shows the architecture adopted by proposed system. As shown in fig. 2 data acquisition process is performed by android mobile Phone and Finger Print Sensor R305. Data acquisition is the process of collecting input data from input devices. So, the signatures are collected using android mobile phone whereas, the finger prints are collected from the Finger Print Sensor R305.

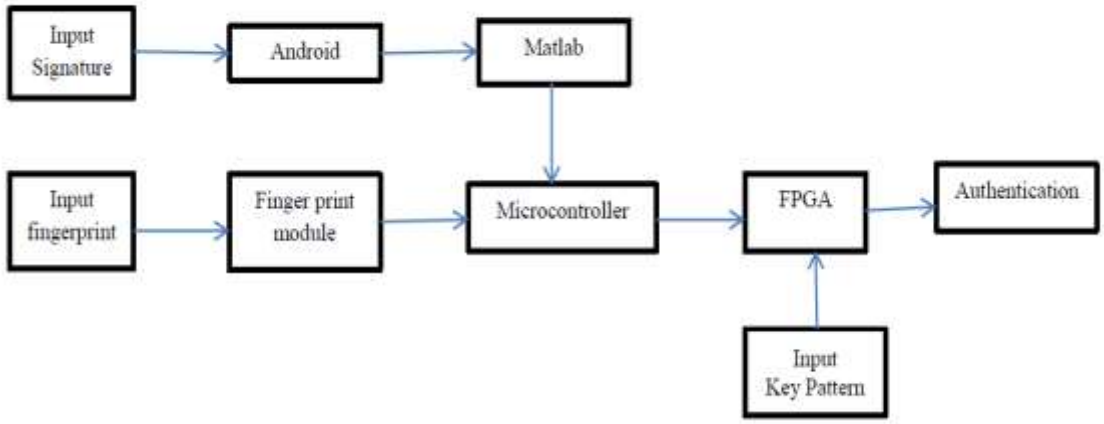

Fig. 2 Architecture of proposed system

A. Working:

Proposed biometric authentication framework worked on following stages:

1. Data Acquisition**:** android mobile phone and Finger Print module R305 are used for data acquisition process.

2. Image preprocessing: In this stage segmentation of signature is carried out. Pre saving of segmentation of signature is done with the help of gesture builder library on android: In gesture builder library emulator save the gesture file. It provide extra layer of security.

3. Feature Extraction: Feature extraction is the efficiency measure tool for the signature verification process. In proposed system A Hidden Markov Modeling (HMM) is used for signature and dynamic time wrapping (DTW) is for fingerprint. DTW minimize the effects of distortion and times shift between two signatures collected in different sessions. A Hidden Markov Modeling (HMM) process consist of two processes, they are an underlying process and an observable process. So, HMM is called as a doubly stochastic process. For signature, the stroke, length and shape

feature is used for matching whereas for finger print, minutia is used for matching. Minutia is the unique feature of the ridges.

4. Classification: In verification process, authentication of signature, fingerprint and key pattern are done. In these, the features of signature and finger print and key pattern which stored in dada based during enrolment stage are matched with test signature, fingerprint and key pattern. K nearest neighbors (KNN) classifier used for the classification stage.

APPLICATION OF PROPOSED SYSTEM

One of our highest priorities in the world of information security is verification and conformation that a person accessing sensitive, confidential, or classified information is authorized to do so. Such access is usually accomplished by a person's proving their identity by the use of some means or method of authentication. Simply, a person must be able to validate who they say they are before accessing information, and if the person is unable to do so, access will be denied. Generally speaking, a system can identify you as an authorized user in one of three ways: what you know, what you have, or what you are. And the last method is what we are - biometrics technology.

Now a day, biometric technology can use for large number of applications. Specially security is very important for today's society in such cases biometric authentication systems can help to make operations, transactions and everyday life both safer and more convenient. When biometrics technology is used for the purpose of verifying a user's identity, it is important to know that not everyone within an organization or department needs access to all information. While biometrics is considered the most reliable form of user authentication, we must remember that user authentication is complex, especially when applied to a network where one person may need to have access to various applications or systems. People within organizations who need access to sensitive, confidential, or classified information will need the strongest form of authentication - three-factor authentication. This level of authentication will necessitate use of passwords, smart cards or tokens, and personal identifiers. Those who need to have rapid access to a particular application or system might need to use a smart card or token. A password may be the only authentication needed for those with minimal security needs.

From the casual user of the home computer, to businesses, corporations, medical professionals/providers, and government, there is a great concern about the security of files, systems, and the ability of technology to protect us from unauthorized access. Some areas where we can implement proposed authentication system are listed below:

1. Biometric Security: Old security methods are simply not strong enough to provide best protection. Biometric technology is more accessible than ever before, ready to bring enhanced security and greater convenience to whatever needs protecting. Only 2% of human subjects do not have fingerprints that can be reliably measured. And variation in the signatures produced by individual is too high.
2. Border Control/Airports: Border Control and Airport are the key area of application for biometric authentication system. Anyone who's traveled by air can tell you security checkpoints border crossings are some of the most frustrating places to have to move through. Thankfully, biometric technology is helping automate the process.
3. Financial: It can't be overstated how much biometrics authentication system can benefit financial transactions. With recent implementations of mobile and online payments protected by biometrics it's clear that the security and convenience are welcomed by the consumer when it comes to buying goods and those benefits are gradually making their way into the higher risk world. So in the financial issues authentication is must.
4. Physical Access Control: Proposed system provides great physical access control solutions which are stronger authentication methods than keys, cards and PINs because it have its own property, it cannot be lost or stolen. While a key can be lost or stolen and used by someone else. So we can use proposed system in such cases where physical access control exist.
5. Time and Attendance: Proposed biometric authentication system will bring efficiency to the workplace by keeping better tabs on the employees in a given workforce.

So simply we can say we can used proposed system in all areas where authentication is play vital role like all type of offices, banks, hospital, colleges, institute etc to make user authorized. Also we can used it in above mentioned places to maintain employees record, in college and institute for student etc. Concluding all, we can say proposed system provide extra layer of security since it is not depend only on one parameter. We used three parameters which provide its more security and only real user is get authenticated.

CONCLUSION

This paper proposed a system which is a real time authentication framework using multi-model biometrics. It consists of the embedded system to verify the signatures, fingerprint and key pattern for authentication of user. Proposed framework provides a strong user authentication solution. When a high level of security is needed, it is necessary that you combine more than authentication factors. Proposed system combines three authentication factors. We combine knowledge factors and inherence factors also so that it have achieved the highest level of security across multiple applications and systems. We can used it widely.

ACKNOWLEDGEMENT

First and foremost I would like to express my deepest gratitude to my guide respected **Prof. H. Upadhyay** for his valuable support, guidance, motivation and encouragement throughout the period this work was carried out. I wish to express my gratitude to **Prof. Sujatha Rao** (HOD) for her valuable guidance, motivations and helpful attitude.

REFERENCES

[1] Anil Jain, Arun Ross and Salil Prabhakar, "Introduction to Biometric Recognition", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 4-20,January 2004.
[2] D. Impedovo and G. Pirlo, "Automatic signature verification: The state of the art," IEEE Trans. Syst., Man, Cybern.—Part C: Appl. Rev., vol. 38, no. 5, pp. 609–635, Sep. 2008.
[3] M. Fons, F. Fons, and E. Cantó-Navarro, "Fingerprint image processing acceleration through run-time reconfiguration hardware," IEEE Trans. Circuits Syst. II: Exp. Briefs, vol. 57, no. 12, pp. 991–995, Dec. 2010.
[4] Gruber C, Gruber T, Krinninger S, Sick B, "Online Signature Verification With Support Vector Machines Based on LCSS Kernel Functions", IEEE transaction on System, Man, and Cybematics, Part B: Cybemetics, Vol. 40, PP. 1088 – 1100, June 2010.
[5] Enrique Argones Rúa,, José Luis Alba Castro, *M* "Online Signature Verification Based on Generative Models", IEEE Transactions on Systems, Man, and Cybernetics—Part B: Cybernetics, Vol. 42, No. 4, pp 1231 - 1242 August 2012.
[6] Mariano lópez-garcía, Rafael ramos-lara, Oscar miguel-hurtado, and Enrique cantó-navarro, "Embedded system for biometric online signature verification", IEEE Transactions on Industrial Informatics, Vol. 10, No. 1, PP 491 – 501 February 2014.
[7] Miguel A. Ferrer, J. Francisco Vargas, Aythami Morales, and Aarón Ordóñez, ―Robustness of Offline Signature Verification Based on Gray Level Features‖. IEEE Transactions on Information Forensics and Security, Vol. 7, No. 3, June 2012.
[8] M. Fons, F. Fons, E. Cantó-Navarro, and M. López-García, "FPGA based personal authentication using fingerprints," *J. Signal Process. Syst.*, vol. 66, no. 2, pp. 153–189, Feb. 2012.
[9] O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, "A new algorithm for signature verification system based on DTW and GMM," in *Proc. 42nd. Annu. IEEE Int. Carnahan Conf. Security Technol.*, Oct. 2008, pp. 206–213.
[10] B. Ly Van, S. Garcia-Salicetti, and B. Dorizzi, "On using the Viterby path along with HMM likelihood information for online signature verification," IEEE Trans. Syst., Man, Cybern. Part B: Cybern., vol. 37, no. 5, pp. 1237–1247, Oct. 2007.
[11] J. Fierrez-Aguilar, J. Ortega-García, D. D. Ramos, and J. Gonzalez-Rodríguez, "HMM-based on-line signature verification: Feature extraction and signature modeling," Pattern Recognit. Lett., vol. 28, no. 16, pp. 2325–2334, Dec. 2007.
[12] Eric Monmasson , Marcian Cirstea, "Guest Editorial Special Section on Industrial Control Applications of FPGAs" IEEE Transactions on Industrial Informatics, Vol. 9, No. 3, pp 1250-1252, August 2013.
[13] S. Jin, D. Kim, T. T. Nguyen, D. Kim,M. Kim, and J. W. Jeon, "Design and implementation of a pipelined datapath for high-speed face detection using FPGA," IEEE Trans. Ind. Inf., vol. 8, no. 1, pp. 158–167, Feb. 2012.
[14] E. Monmasson, L. Idkhajine, M. N. Cirstea, I. Bahri, A. Tisan, and M. W. Naouar, "FPGAs in industrial control applications," IEEE Trans. Ind. Inf., vol. 7, no. 2, pp. 224–243, May 2011.

[15] Y. Komiya, T. Ohishi, and T. Matsumoto, "A pen input on line signature verifier integrating position, pressure and inclination trajectories," IEICE Trans. Inf. Syst., vol. E84 D, no. 7, pp. 833–838, Jul. 2010.
[16] S. Impedovo and G. Pirlo, "Verification of handwritten signatures: An overview," in *Proc. 14th Int. Conf. Image Anal. Process.*, Sep. 2007,pp. 191–196.
[17] T. Ahonen, A. Hadid, and M. Pietikainen, ―Face description with local binary patterns: Application to face recognition, IEEE Trans. Pattern Anal. Machine Intell., vol. 28, no. 12, pp. 2037–2041, Dec. 2006.
[18] H. Ketabdar, J. Richiardi, and A. Drygajlo, "Global feature selection for on-line signature verification," in Proc. 12th IGS Conf., Salerno, Italy, Jun. 2005, pp. 59–63
[19] J. Richiardi, H. Ketabdar, and A. Drygajlo, "Local and global feature selection for on-line signature verification," in Proc. IAPR 8th ICDAR, Seoul, Korea, Aug. 2005, vol. 2, pp. 625–629.
[20] J. Fiérrez Aguilar, L. Nanni, J. López-Pe´nalba, J. Ortega García, and D. Maltoni, "An on-line signature verification system based on fusion of local and global information," in Proc. IEEE Int. Conf. Audio Video-Based Person Authentication, Halmstad, Sweden, Jun. 2005, pp. 523–532.
[21] J. Y. Kim, D. Y. Ko, and S. Y. Na, "Implementation and enhancement of GMM face recognition systems using flatness measure," in Proc. IEEE Int. Workshop Robot Human Interact. Commun., Sep. 2004, pp. 247–251.
[22] J. J. Igarza, L. Gómez, I. Hernáez, and I. Goirizelaia, Searching for an Optimal Reference System for On-Line Signature Verification Based on (x, y) Alignment, D. Zhang and A. K. Jain, Eds. Berlin, Germany: Springer-Verlag, 2004, pp. 519–525, ICBA 2004, LNCS 3072.
[23] G. Dimauro, S. Impedovo, M. G. Lucchese, R. Modugno, and G. Pirlo, "Recent advancements in automatic signature verification," in Proc. 9th Int. Workshop Frontier Handwriting Recognit., Oct. 2004, pp. 179–184, IEEE Comput. Society Press.
[24] B. Fang, C. H. Leung, Y. Y. Tang,K.W. Tse, P.C.K.Kwok, andY.K. Wong, "Off-line signature verification by tracking of feature and stroke positions," IEEE Trans. On Pattern Recognit., vol. 36, no. 1, pp. 91–101, Jan. 2003.
[25] B. Bhanu, X. Tan, "Fingerprint indexing based on novel features of minutiae triplets", IEEE Trans. Pattern Recog. Anal. Mach. Intell. 25(5) (2003) 616–622.
[26] M. Diligenti, P. Frasconi, and M. Gori. Hidden tree markov models for document image classification. IEEE Transactions on Pattern Analysis and Machine Intelligence, 25(4):519–523, 2003.
[27] A. K. Jain, F. D. Griess, and S. D. Connell, "On-line signature verification," Pattern Recognit., vol. 35, no. 12, pp. 2963–2972, 2002.
[28] Y. Komiya, T. Ohishi, and T. Matsumoto, "A pen input on line signature verifier integrating position, pressure and inclination trajectories," *IEICE Trans. Inf. Syst.*, vol. E84 D, no. 7, pp. 833–838, Jul. 2001.
[29] N. K. Ratha, A. W. Senior, and R. M. Bolle, "Automated biometrics," in Proc. 2nd Int. Conf. Adv. Pattern Recog., Rio de Janeiro, Brazil, Mar. 2001, pp. 445–474
[30] J. Li, A. Najmi, and R. Gray. "Image classification by a two dimensional hidden markov model". IEEE Transactions on Signal Processing, 48(2):517–533, 2000.
[31] D. Impedovo and G. Pirlo, "On-line signature verification by stroke-dependent representation domains," in Proc. 12th ICFHR, Kolkata, India, Nov. 2010, pp. 623–627, 16–18.
[32] R. Bajaj and S. Chaudhury, "Signature verification using multiple neural classifiers," Pattern Recognit., vol. 30, no. 1, pp. 1–7, Jan. 1997
[33] R. Kashi, J. Hu, W. L. Nelson, and W. Turin, "On-line handwritten signature verification using hidden Markov model features," in Proc. 4th Int. Conf. Doc. Anal. Recog., Ulm, Germany, Aug. 1997, pp. 253–257.
[34] L. L. Lee, T. Berger, and E. Aviczer, "Reliable on-line human signature verification systems," IEEE Trans. Pattern Anal. Mach. Intell., vol. 18, no. 6, pp. 643–647, Jun. 1996.
[35] S. Nabeshima, S. Yamamoto, K. Agusa, and T. Taguchi, "MEMOPEN: A new input device," in Proc. Int. Conf. Companion Human Factors Comput. Syst. (CHI'95), 1995, pp. 256–257.
[36] G. Pirlo, "Algorithms for Signature Verification," in Proc. NATO-ASI Series Fund. Handwriting Recognit., S. Impedovo, Ed., Berlin, Germany, 1994, pp. 433–454, Springer-Verlag.
[37] O. Miguel-Hurtado, L. Mengibar-Pozo, and A. Pacut, "A new algorithm for signature verification system based on DTW and GMM," in Proc. 42nd. Annu. IEEE Int. Carnahan Conf. Security Technol., Oct. 2008, pp. 206–213.

[38] R. Ramos-Lara, M. López-García, E. Cantó-Navarro, and L. Puente- Rodriguez, "Real-Time speaker verification system implemented on reconfigurable hardware," J. Signal Process. Syst., vol. 71, no. 2, pp.89–103, May 2013.
[39]] M. López-García, J. Daugman, and E. Cantó-Navarro, "Hardware-software co-design of an iris recognition algorithm," IET Inf. Security, vol. 5, no. 1, pp. 60–68, Apr. 2011.
[40] J. Liu-Jiménez, R. Sánchez-Reillo, L. Mengibar-Pozo, and O. Miguel Hurtado, "Optimisation of biometric ID tokens by using hardware/software co-design," IET Biometrics, vol. 1, no. 3, pp. 168–177, Sep. 2012.