

Towards a fast and secure fingerprint authentication system based on a novel encoding scheme

International Journal of Electrical Engineering
& Education
0(0) 1–13

© The Author(s) 2019


Article reuse guidelines:

sagepub.com/journals-permissions

DOI: 10.1177/0020720919883803

journals.sagepub.com/home/ije



D Harikrishnan¹ , N Sunil Kumar¹,
Shelbi Joseph¹ and
Kishor Krishnan Nair²

Abstract

Fingerprint-based authentication systems in general are prone to several security vulnerabilities. Authentication systems such as Biometric crypto systems, Cancellable templates and Bio-hashing provide a solution for addressing these vulnerabilities. But these systems are vulnerable to the unauthorized access resulting from the spoofed fingerprint templates by the fraudulent users. Hence, it is essential to enhance the features of the existing Biometric fingerprint-based authentication systems. An extensive research has been carried out by various researchers on the existing fingerprint authentication system techniques and it is found that none of them are fully capable of eliminating the security vulnerabilities. Fingerprint authentication system technique based on one time fingerprint template provides a solution for this by generating one time template from the fingerprint features. Although this method addresses vulnerability issues to a certain extent, improvements are highly essential particularly in terms of their security and performance. There are several systems based on finger code, where fingerprint features will be converted into finger code using a circular tessellation technique. Although authentication based on this technique improves security, the possibility of compromising the finger code is a huge threat, which needs to be addressed. In this paper, an innovative model is proposed which generates a secure one time finger code during every user authentication. It is generated using finger code

¹Cochin University of Science and Technology, Cochin, India

²Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa

Corresponding author:

D Harikrishnan, Cochin University of Science and Technology, Cochin, India.

Email: dharikris@yahoo.com

obtained from minutiae vectors using a circular tessellation approach, pseudo-random number generators and timestamp, which are generated during every user transaction session. This unique encoding approach makes it extremely difficult for an unauthorized user to decode the generated finger code that is used for a particular authentication session. Thus, the possibility of compromise of original fingerprint can be avoided and thus security of biometric system can be enhanced. The proposed system also provides better performance in terms of its accuracy, processing speed and complexity.

Keywords

Fingerprint authentication system, finger code, circular tessellation, one time finger code, one time template

Introduction

Biometric user authentication system identifies a person based on their physical or behavioral characteristics.¹ It operates in two phases: verification and identification. In the first phase, the system recognizes an individual by comparing the biometric input from the user opposing to the original biometric template stored in the system database. In identification phase, a person is identified against the template database.² Compared to major biometric technologies such as face and voice recognition, fingerprint authentication system (FAS) is more popular and has a higher accuracy.³ Even though FASs are very effective, a set of vulnerabilities is creating a plethora of security threats. Majority of the existing solutions to handle security vulnerabilities are in the form of crypto systems, Cancellable templates and Bio-hashing.³ Although these solutions may assist in preventing malicious attacks on the system, they do not fully eliminate it. Due to the unauthorized access by a fraudulent user, original biometrics of the user may be exposed. It will affect the security of the FAS. Furthermore, it is vital for an FAS to have a good tradeoff between performance and security. An FAS with robust security and acceptable recognition performance at the present time has remained unclear. The development of such a system is highly essential as biometric systems are beginning to flourish into the core physical and information infrastructure of our society. Therefore, it is essential to enhance system accomplishments by lifting the features of the existing FASs, without compromising the security.

With the aim of deducing the issues involved, a new framework is proposed by which a derivative of revocable biometrics approach using Bio-hashing is created. Here a novel technique is introduced for generating one time finger code (OTFC) based on pseudo-random sequence and date stamp for every user transaction session. This method uses circular tessellation for generating finger code from user's fingerprint.⁴ In this method, neighborhood of reference minutiae taken is identified first and then circular tessellation technique is applied in order to obtain circular bands and sectors.

The current research finds its use in various fields such as Banking, Commercial, Government and Forensic sectors. This scheme can enhance the security of the transactions based on bank cards. The concept can be well adapted to other biometric modalities and also multi-modal interfaces. Furthermore, it can be well adapted in biometric cardless payment systems, online shopping and e-banking. Scholars in the undergraduate and postgraduate studies can continue on this research and can take it to the next level. This paper is systematized as follows: The next section provides the related previous work on FAS based on both minutiae matching technique and finger code matching. Then, the proposed model of integrating finger code matching method based on circular tessellation with a new pseudo-random code generation technique to generate OTFC for each transaction is described. The proposed algorithm and its implementation based on authentication protocol are also given in this section. Then, the performance evaluation of the model with experimental results and its comparison with existing models using security measurement methods such as entropy are presented.

Literature survey

Among the various threats faced by the FAS, issues related with security challenges are more complicated. Various security challenges in the biometrics are well explained in the paper written by Ratha et al.³ He had given various solutions available for addressing these vulnerabilities such as Biometric crypto systems, Cancellable templates and Bio-hashing.

The basic idea of Bio-hashing and revocable biometrics are well represented in the paper authored by Teoh et al.⁵ According to the author, revocable biometric was used in the case where permanent biometric was compromised. Original template can be cancelled and replaced with new template Bio-hashing. Bio-hash technique resulted in reduced error rates when genuine token was used. Biometric data stored in the database may be compromised. Tulyakov et al. address this issue by proposing a method of decomposing fingerprint particulars. Identification of fingerprint is performed in a transformed space. Rather than transmitting original template, decomposed data is transferred and saved in the server database.⁶

Radha came up with an efficient method of adding non-invertibility (Bio-hashing) with Cancellable biometrics for enhancing fingerprint security. Cancellable biometric protects privacy of a user because user's original biometric feature is never revealed during the authentication process.⁷

Lumini and Nanni identified some drawbacks of the base Bio-hashing method. It will show low performance if pseudo-random number of a user is stolen by an imposter. Their work proposes mitigations measures to address this issue.⁸ Cheung et al. raises concern over the precision of a biometric system depending on revocable biometric. Information may be lost in the case of performing non-invertible transformation in Cancellable biometrics for feature and signal domain. This may lead to the fall of accuracy. Raw fingerprint may be protected using non-invertible

Cancellable biometric approach, but it may destroy the optimality in the representation of feature.⁹

Nair et al. proposed a new idea to tackle one of the severe attacks in FASs. In the existing systems, the original fingerprints may be compromised during the authentication as it is stored and available for the entire authentication process. Hence, an unauthorized person can access the fingerprint and can compromise the biometric system security. A robust fingerprint authentication protocol is suggested by the authors to address this vulnerability, where instead of original biometrics, only a transformed one will be used for authentication.^{10–12} Various models were proposed for generating encoded finger code (efc) from finger template using a technique known as circular tessellation. One of the popular methods was proposed by Benhammedi and Bey. They introduced a scheme for identifying features from fingerprint minutiae and convert them into binary codes known as finger code. The finger print matcher tessellate fingerprint into 32 sectors and 16 circular bands based on a center point known as core. The comparison of finger code enrolled and query finger code is performed based on hamming distance.⁴

Lim and Yuen developed a new model for calculating the entropy of the biometric systems, which is a measure of estimating security. In this model, an adversarial guessing effort was used to represent entropy, which is also known as guessing entropy.¹³

The Cancellable biometric FAS system based on finger code and one time template (OTT) provided solutions for addressing the security vulnerabilities. But the performance of these systems needs significant improvement due to the following reasons:

1. Security threat in terms of compromise of original biometric is still existing in these systems even after the transformation.
2. Although the finger code-based authentication system provides good accuracy in terms of equal error rate (EER), scope of improvement in accuracy is still there.⁴
3. The time complexity of these conventional algorithms is high.

In light of the above reasons, it is highly necessary to propose a new system.

Proposed system

The proposed system operates in two stages such as finger code generation and OTFC creation. Using circular tessellation technique, finger code will be generated from fingerprint. The fundamental reference point and its neighborhood particulars are identified from the extracted image, fingerprint is tessellated into eight sectors and five circular bands (ridge counts) using core as the center point.¹⁴ The circular tessellation is generated in matrix of order $I \times J$ as represented in

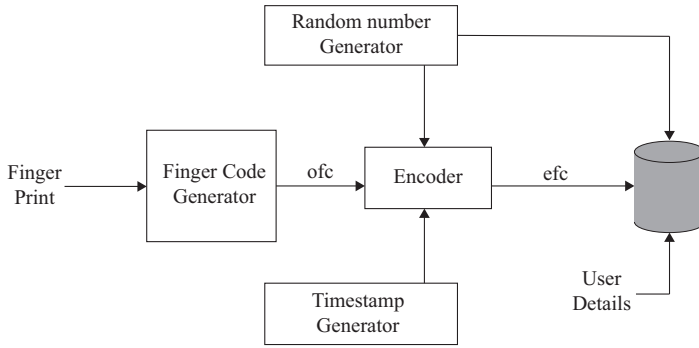


Figure 1. Flow diagram of enrollment process.

the equations given as

$$C[i][j] = \begin{cases} 1 & \text{If sector } i \text{ contains minutia at ridge } j \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

$$\text{finger code} = \{c[i][j] \text{ where } 1 \leq i \leq I; 1 \leq j \leq J\} \quad (2)$$

where I is the number of sectors and J is the number of ridge counts mapped over the finger print.

The working of the conceptual model is illustrated as a process flow diagrams as in Figures 1 and 2. The operation of the system during the enrollment and authentication are given as separate process diagrams.

Finger code generator: Generates original finger code (ofc) from the input fingerprint.

Encoder: efc is generated using ofc bits, timestamp bits are created using timestamp generator and pseudo-random numbers. The efc bits are stored in an SQL database.

For every user authentication, finger code template (FCT) is generated by applying transformation function on finger code and biometric key created from randomization process. FCT will then be stored in FCT database. This operates through two conditions, namely encoding and decoding. In the encoding state, finger print from the user is read in the form of 40 bit binary string (ofc). Along with the ofc, a timestamp is obtained in *dd/mm/yy-hh:mm:ss* format. This timestamp is also converted to 40 bit binary format. In addition to timestamp and finger code, four sorted distinct random numbers between 0 and 40 (r_1, r_2, r_3 and r_4) are generated. The 40 bit timestamp is divided into five octets. First four octets are inserted after r_1 th, r_2 th, r_3 th and r_4 th position of ofc. Fifth octet is appended

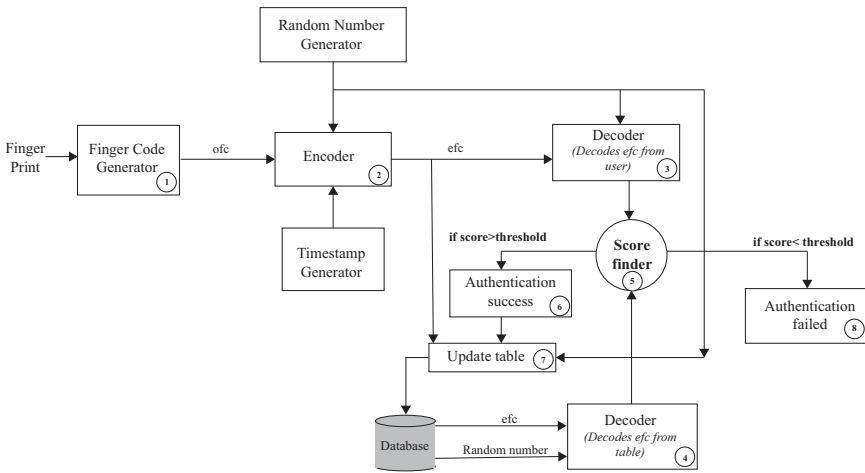


Figure 2. Flow diagram of the authentication process.

after last bit of ofc. Thus, an 80 bit efc is generated after this procedure. During the enrollment phase, user’s ofc is obtained along with user details such as username and id. Obtained ofc is converted to efc using encode procedure in client side. This efc, the pseudo-random numbers used during encoding and user’s details are stored in a database.

In the decoding phase, 80 bit efc and respective random numbers (r_1, r_2, r_3 and r_4) used during encoding will be taken as the input. ofc can be retrieved by removing timestamp octets from efc with the help of respective pseudo-random sequence. For each entry in the database, a score is calculated based on hamming distance against the ofc taken from the user. If there exists any score lower than the preset threshold value, then the one with least score is chosen as authenticated user. The entry of authenticated user in the database will be updated with new pair of efc and pseudo-random sequence. This will improve the security as the table entry of a particular user will get updated on successful login. Hence, we consider efc as one time entry.

Algorithm

The implementation of the model is based on an algorithm as illustrated. The algorithm operates in four phases, namely Encode, Decode, Enrollment and Login. The first phase shows the encoding process. Decoding operation is explained in the second phase. The procedure for the enrollment and login operations described in the algorithm is given in Figure 3.

Authentication protocol

A robust protocol is devised for transmitting biometric features of the user from the client user to the authentication server. This will represent the method of how a

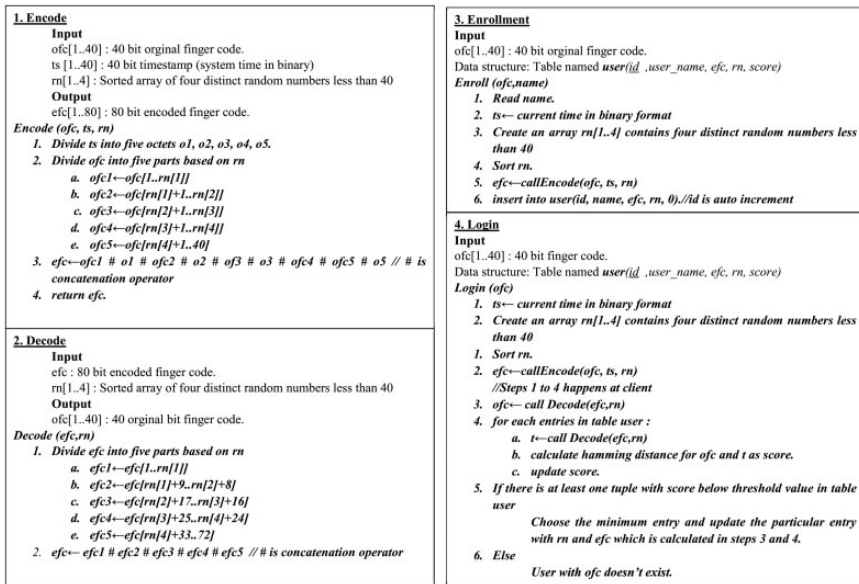


Figure 3. Algorithm.

separate OTFC is generated in every transaction session in both client and server. The authentication process of comparing OTFC created in both the client and server will be handled by the server. The authentication protocol is illustrated in Figure 4.

Performance evaluation

The proposed encoding system used in the model is highly secure. The possibility of compromising of original fingerprint is comparatively lesser than the existing model proposed by Nair et al.¹¹ Performance of our model is comparable and better than existing systems. Finger code system has high accuracy than the conventional FAS. Furthermore, comparison of finger code bits based on hamming distance yields better results, since number of comparisons will be lesser as compared to conventional systems. Execution speed of the system also will be high as well. Encoded information and random vectors are stored in the SQL database. Since matching operation is performed based on SQL queries, it enhances the system outcomes both in terms of speed and security. Complexity of the proposed algorithm is $O(\log n)$. The accuracy of the model is represented based on the EER value, which is obtained in this system as 0.37. Figure 5 shows the estimation of experimental results of false acceptance rate (FAR) and false rejection rate (FRR) over various system generated threshold values. EER is calculated on a point of

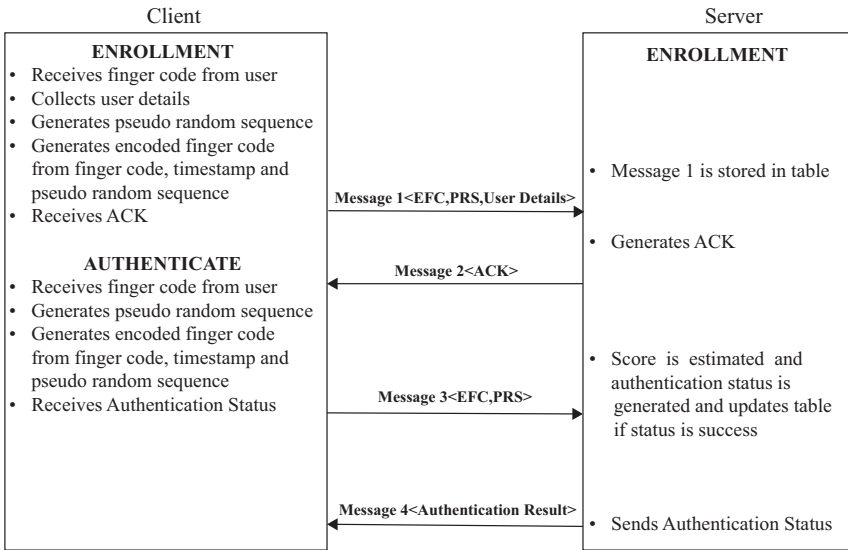


Figure 4. Authentication protocol.

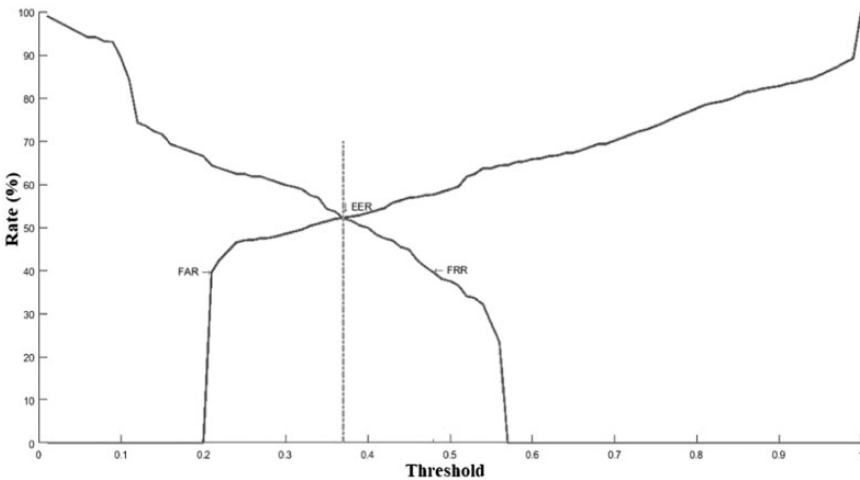


Figure 5. FAR vs. FRR.

intersection of FAR and FRR. EER is the point in which the FAR coincides with the FRR.

The quantitative measurement of the security is performed based on the analysis using Entropy.¹⁵ Entropy $H(x)$ is measured on a random variable, x based on

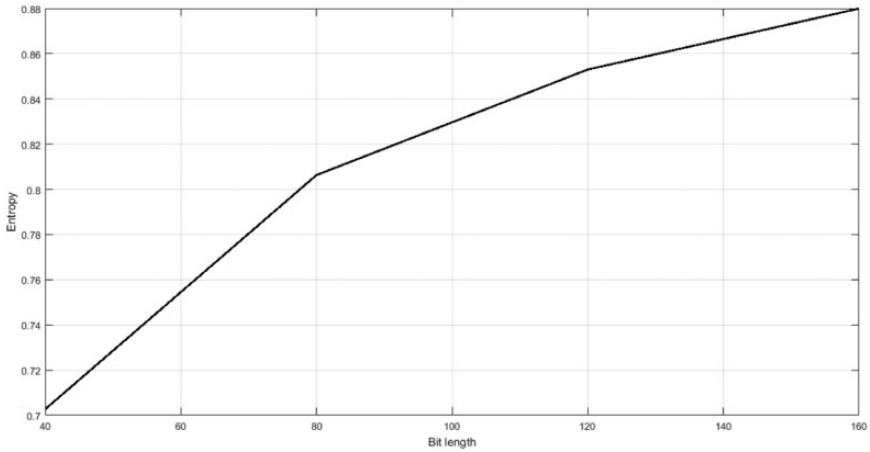


Figure 6. Entropy vs. bit length.

equations (3) and (4)

$$H_r(x) = - \sum_{r_i=1}^n \frac{r_i}{l} \log_2 \left(\sum_{r_i=1}^n \frac{r_i}{l} \right) \quad (3)$$

$$H_l(x) = -r \sum_{k=1}^n (k*l)^{-1} \log_2 \left(\sum_{k=1}^n (k*l)^{-1} \right) \quad (4)$$

where $l = I \times J$, I is the number of sectors and J is the number of circles mapped over the finger print, l is the length of the ofc, r_i is the pseudo-random vector size. $l = 0 \text{ mod } 40$, i.e. l is a number which gives remainder 0 while dividing by 40, $n = l/2$.

Entropy vs. bit length is plotted in the graph shown in Figure 6 to analyze the security limits of the analysis. This is done by forming a subset of various possibilities in terms of probability of compromise of the original finger print information by an unauthorized user. In this experiment, the change in entropy based on different finger code bit length values was analyzed. In the proposed encoding scheme, bit length of 40 is used. It can be concluded from the analysis that bit length value is directly proportional to Entropy of the system. Hence, security constraints of the analysis would be enhanced. Here, possibility of compromising the encoded data becomes merely infeasible.

The graph shown below in Figure 7 is plotted between the Entropy $H_r(x)$ and the pseudo-random vector size r_i (for instance, if $r=3$, r_1, r_2, r_3 which chooses any three random number between 1 to 40 if the ofc length is chosen as 40). Here, the Entropy is calculated by choosing the probability of any of the pseudo-random

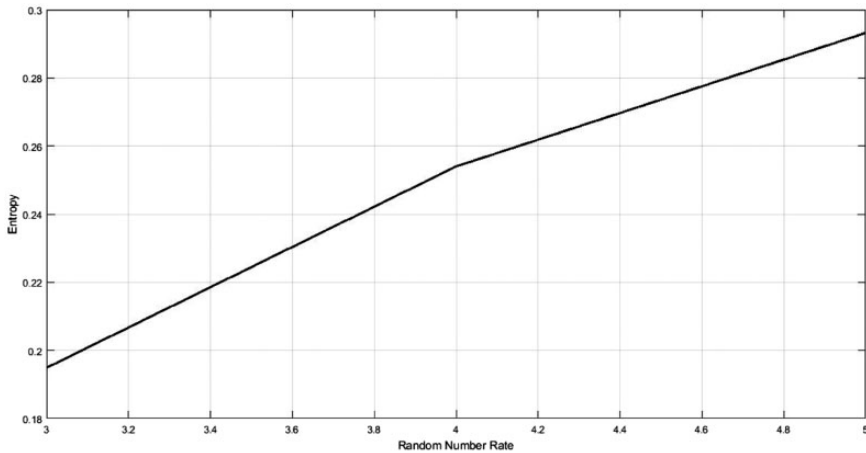


Figure 7. Entropy vs. random number size.

number for various finger code length; the pseudo-random numbers should be chosen between 1 and $1/2$. The mathematical expression of this is depicted as in equation (3).

We have taken finger print image samples from FVC 2004 DB1.¹⁶ FVC 2004 consists of 80 finger print images (eight finger print samples of 10 persons). An SQL database is used to store the encoded version of finger print images. Various test cases based on finger print images of 10 persons are considered for authentication operation. Comparison of enrolled one and login image is performed by searching the efc in the database using SQL queries. This searching operation using SQL queries has a time complexity of $O(\log n)$, which is lower than that of conventional systems. In OTT-based FAS, time complexity is $O(n)$, whereas time complexity of finger code-based FAS is $O(n^2)$. Hence, the time complexity of conventional systems is higher than the proposed system. Performance analysis based on time complexity of various systems is plotted in a graph as captured in Figure 8.

PFAS is the abbreviation of proposed FAS, OTTFAS developed by Nair et al. is the abbreviation of OTT-based FAS and FCFAS is the abbreviation of finger code-based FAS.^{10,11} This graph is plotted using search time and number of user entries as parameters. Since encoded information is stored in the SQL database, unauthorized access can be prevented to a certain level. Hence, it improves security.

The evaluation of the proposed model in conjunction with two models, namely conventional FAS based on OTT and conventional FAS based on finger code generation, is illustrated in Table 1.^{4,11}

Proposed system is less exposed to the intruder in terms of compromise of original fingerprint data even after several trials by the intruder when compared

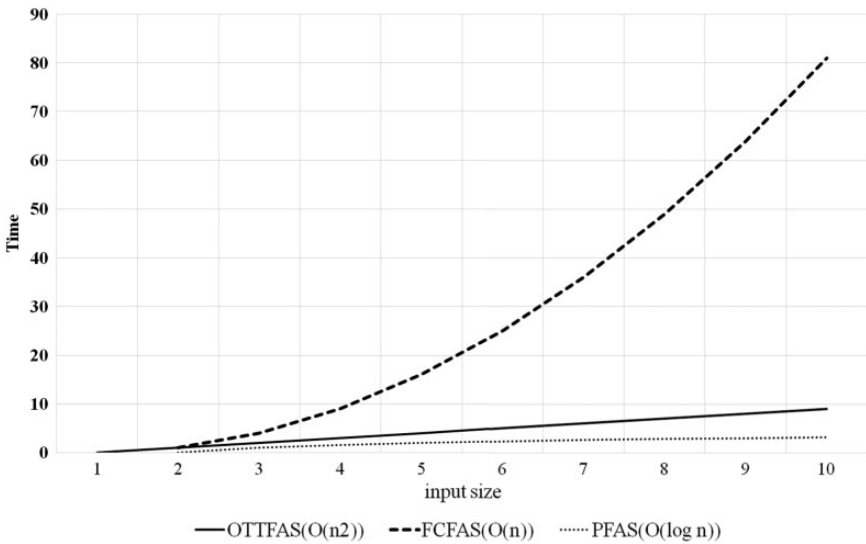


Figure 8. Time complexity comparison.

Table I. Performance comparison chart.

FAS systems	EER	Time complexity	Chance of compromise of data	Security
Proposed system	0.37	$O(\log n)$	Very low	High
Conventional FAS based on OTT	0.38	$O(n)$	Low	Medium
Conventional FAS based on finger code	0.449	$O(n^2)$	High	Low

FAS: fingerprint authentication system; OTT: one time template; EER: equal error rate.

to conventional FAS based on OTT and also finger code based FAS. The encoding scheme used in this model is highly secured. The possibility of intruder attack by accessing original fingerprint is less in OTT-based FAS. But in comparison with our model, the threat is existing when intruder makes continuous efforts to access original fingerprint and user attributes. Finger code system by Benhammadi and Bey is severely exposed to this type of attack.⁴ Hence, security of this system is marked as low.

Accuracy of this system is comparable with other conventional systems. EER of the system is 0.37, which is lower than OTT-based FAS and finger code system by Benhammadi and Bey.⁴ It is even comparable with EER of other existing fingerprint systems.

The proposed system is more superior to the existing systems in terms of its resistance to spoofing attacks and cross platform application attacks. This is

attributed to the secured encoding scheme used in the proposed system, and furthermore, the original finger templates are not stored in the system at any stage. It is also observed that the transmission overhead due to the amount of information transmitted between client and server is comparatively less in the proposed system. This system transmits only 80 bits of information between client and server during every enrollment and login process, where the conventional system based on fingerprint image and fingercode requires huge amount of information to be transmitted either in the form of image or fingercode bits.

Conclusion

It is quite common that to choose among different FASs, the prime factor to be considered is the low error rate. But the system credibility can degrade if the system is susceptible to the security vulnerabilities. A new model is proposed here which is more secured than the available FASs. A new encoding technique based on date stamp taken during user input is used by which original fingerprint will not be exposed from fraudulent users during its transmission. In the conventional fingerprint authentication schemes, it is a requirement to store the original finger template of the user in the system. This opens the door for serious security vulnerabilities as the compromise of the biometrics is of permanent nature. This research abstracted the idea of using a unique finger template using a secure encoding scheme to make the authentication process unique during each authentication session. Therefore, even if the system is compromised, it becomes near to impossible to reverse engineer the original finger template of the user. The proposed system is also comparable to other systems in terms of error rate and time complexity. This research can be further extended to other biometric systems such as iris realization system and face realization systems so that the security of those systems can also be increased.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

D Harikrishnan  <https://orcid.org/0000-0002-4489-0530>

References

1. Jinhai Z. Study and implementation of automatic fingerprint recognition technology. In: *International conference on uncertainty reasoning and knowledge engineering*, Bali, Indonesia, 4–7 August 2011. USA: IEEE.

2. Prabhakar S, Pankanti S and Jain AK. Biometric recognition: security and privacy concerns. *IEEE Secur Privacy* 2003; 1: 33–42.
3. Ratha N, Connell H and Bolle RM. Enhancing security and privacy in biometrics-based authentication systems. *IBM Syst J* 2001; 40: 615–633.
4. Benhammedi F and Bey KB. Embedded fingerprint matching on smart card. *Intern J Pattern Recognit Artif Intell* 2013; 27: 1350006.
5. Teoh A, BengJin Connie T, et al. Remarks on BioHash and its mathematical foundation. *Inf Process Lett* 2006; 100: 145–150.
6. Tulyakov S, Farooq F and Govindaraju V. Symmetric hash functions for fingerprint minutiae, https://link.springer.com/chapter/10.1007/11552499_4 (2005, accessed 10 October 2019).
7. Radha N and Karthikeyan S. An evaluation of fingerprint security using non invertible biohash. *Int J Netw Security Appl* 2011; 3: 118–128.
8. Lumini A and Nanni L. An improved BioHashing for human authentication. *Pattern Recognition* 2007; 40: 1057–1065.
9. Cheung KH, Kong A, Zhang D, et al. An analysis on accuracy of cancellable biometrics based on Biohashing. *KES* 2005; 3: 1168–1172.
10. Nair K, Helberg A and Merwe VD. An approach to improve the match-on-card fingerprint authentication system security. In: *Sixth international conference on digital information and communication technology and its applications (DICTAP)*, 2016, pp. 21–23. USA: IEEE.
11. Nair K, Helberg A and Merwe VD. Towards a robust fingerprint authentication system protocol. *J Inf Syst Secur* 2017; 13: 19–35.
12. Nair K, Helberg A and Merwe VD. An approach to authenticate magnetic stripe bank card transactions at POS terminal, <http://sdiwc.net/digital-library/an-approach-to-authenticate-magnetic-stripe-bank-card-transactions-at-pos-terminals> (2018).
13. Lim M and Yuen PC. Entropy Measurement for biometric verification systems. *IEEE Trans Cybern* 2016; 46: 1065–1077.
14. Baruni K, Helberg A and Nair K. Fingerprint matching on smart card: a review. In: *International conference on computational science and computational Intelligence (CSCI'16)*, 15–17 December 2016, pp. 15–17. USA: IEEE.
15. Sammak AJ. A unified matrix representation for calculating entropy quantities. *Int J Electr Eng Educ* 2006; 43: 164–172.
16. Maltoni D, Maio D, Jain AK, et al. *Handbook of fingerprint recognition*. 2nd ed. London: Springer, 2009.