A Robust and Efficient Finger Print Combination form Privacy Protection

Abdullah S. Alotaibi
Dean, Department of Computer Science, Shaqra University, Shaqra Kingdom of Saudi Arabia
E-Mail: a.shawan@su.edu.sa

https://doi.org/10.26782/jmcms.2019.06.00042

Abstract

Now a day’s fingerprint techniques are widely used in authentication systems, therefore its privacy protection becomes an important issue. Securing a stored fingerprint template is very important because once fingerprints are compromised, it cannot be easily revoked. So, we review here a new system for preserving fingerprint confidentiality. In this system, the fingerprint privacy is maintained by combining two special fingerprints keen on an original identity. In the enlistment phase, two fingerprints need aid taken from two different fingers. We acquire the minutiae positions about one fingerprint, the introduction from claiming another fingerprint, and the reference focuses starting with both fingerprints. In view of those gotten information, a joined minutiae format may be created. Also saved previously, a database. In the Confirmation phase, we utilize the fingerprints of the same fingers that need aid at that point utilized within enlistment stage. For same 2 fingerprint against a mutual minutiae template, a two-stage fingerprint matching process is used. By storing the combined minutiae template in the database, the complete minutiae characteristic of a single fingerprint will not be compromised when the database is stolen by the attackers. The joined minutiae format will be changed over under a real-look indistinguishable joined together finger impression by utilizing existing finger impression reproduction approach. These effects under another virtual character to those two different fingerprints.

Keywords: Fingerprint, Combination, Protection, Minutiae, Privacy

I. Introduction

Modern days it is very popular applications of finger print methods in authentication system, protect the privacy of the finger print become more important concern. Conventional encryption may be not addition to finger impression protection insurance on account of unscrambling will be required in the recent past the finger impres-
The greater part of the existing systems makes utilization of the magic for that finger impression protection, which makes the disservice. They might additionally a chance to be powerless at both the magic and the ensured finger impression would steal [I]. Teoh et al. Recommend a biohashing methodology toward registering those inward items between those user’s finger impression features and a pseudorandom amount (i.e., the key). The correctness from claiming this approach primarily relies on the key, which will be accepted with a chance to be never stolen or imparted. Rath et al. recommend producing cancelable finger impression by applying noninvertible transforms on the minutiae [II]. The noninvertible convert may be guided toward a key, which will normally prompt a decrease clinched alongside matching precision. The partake) energizes and more are indicated on be powerless should interruption and linkage strike when both those way and the changed format would stolen. Nanda kumar et al. recommend should execute fluffy flaw line on the minutiae, which may be defenseless of the key-inversion ambush. Our partake) energizes impalpably hiddenite those client personality card on the diminished finger impression utilizing a center. Those client personality might additionally be compromised the point when both the key and the secured diminished finger impression need aid stolen.

Those meets expectations for consolidate two diverse fingerprints under a absolute new character. Possibly in the characteristic level or in the picture level for, the idea for joining together two diverse fingerprints under another personality card is main proposed, the place the new personality card will be made by joining those minutiae positions concentrated from the two fingerprints [III]. Those unique minutiae positions of each finger impression could make secured in the new personality. However, it will be not difficult for the assailant on recognizing such another character since it holds a lot of people more minutiae positions over that of a unique finger impression. The analysis demonstrates that those EER about matching the new characters may be 2.1% the point when those unique minutiae positions need aid denoted manually from those unique fingerprints. A comparable plan may be recommended on, the place the minutiae positions concentrated from a finger impression and the simulated focuses created starting with the voice would join to prepare another character [IV]. In this work, those EER would demonstrate on a chance to be under 2% as stated by the test outcomes.

In the author's primary recommend with consolidate two separate fingerprints in the picture level. 1st from claiming all, each finger impression is decayed under the nonstop part and the winding part in view of the finger impression FM-AM model. After a few alignments, the nonstop part from one finger impression may be consolidated for those winding part from the opposite fingerprint, in this way concerning
illustration with make another virtual personality card which may be termed concerning illustration a blended finger impression.

Compared with the work energizes such a picture level built finger impression blending system need two points of interest: (i) it will be troublesome for those assailant on recognize [V] An blended finger impression from those first fingerprints, Furthermore (ii) existing finger impression matching calculations need aid relevant for matching two blended fingerprints. However, this approach produces a outwardly unlikely blended finger impression because of those varieties in the introduction Also recurrence between the two separate fingerprints. Their test effects [VI] demonstrate that the EER for matching two blended fingerprints will be something like 15% when two distinctive fingerprints would haphazardly picked to making a blended finger impression. Whether those two diverse fingerprints are deliberately decided as stated by a similarity measure, those EER might be lessened to something like 4%. In this paper, we recommend a novel framework for ensuring finger impression protection by joining two diverse fingerprints under another personality card. Throughout that enrollment, the framework captures two fingerprints from 2 special fingers.

A two-stage finger print matching process may be further suggested to matching those two inquiry fingerprints against a consolidated minutiae format. Toward utilizing the joined together minutiae template, the complete minutiae characteristic of a solitary finger impression won't be compromised at those database is stolen. For addition, the consolidated minutiae format allotment a comparative analysis of the first minutiae templates, it could make changed over under a real-look indistinguishable consolidated finger impression by utilizing a existing finger impression recreation methodology [VII].

II. Proposed Method

In a mutual minutiae pattern the minutiae position and commands are extract from two different finger prints indepedntly. The minutiae position and direction split a parallel topology to those from an unique fingerprint.

Therefore, those mutual minutiae template need a comparable topology will a unique minutiae format. Exactly existing meets expectations [VIII-X] have demonstrated that it may be time permits should recreate a full finger impression picture starting with a minutiae format. By adopting a standout among these finger impression remaking approaches, we have the ability to change over our joined together minutiae format under a joined together finger impression picture. Fig. 5 indicates our procedure with produce and joined together finger impression to two separate fingerprints. Provided for at whatever two separate fingerprints likewise input, we initial produce a consolidated minutiae format utilizing our joined minutiae format era algorithm. Then, a consolidated finger impression may be recreated from the joined together minutiae format utilizing a standout
amongst the existing finger impression reproduction methodologies.

Fig. 1 Generate a Mutual fingerprint for 2 different fingerprints

Those motivation behind may be that we set concerning illustration 0 alternating 1 haphazardly throughout the minutiae heading assignment, i.e. We include haphazardly for each minutiae heading for such a coding method. Similarly as what need been examined to area II-C2, we requirement should perform a modulo operation for those minutiae directions throughout the finger impression matching, something like that similarly as should uproot such arbitrariness. Therefore, we won't have the capacity to match the comparing joined finger impression toward utilizing a general finger impression matching calculation. Same time the reason for generating a consolidated.

Fingerprint may be to issue another virtual character for two distinctive fingerprints, which if a chance to be matched utilizing all finger impression matching calculations. "Around the existing finger impression reconstruction approaches, our past fill in accomplishes phenomenal execution. We here embrace this approach for generating a joined together finger impression starting with a joined minutiae format. However, the partake) energizes doesn't fuse a noising and more rendering step will settle on mthe recreated finger impression picture real-look indistinguishable. On make a real-look indistinguishable finger impression picture from a set of minutiae focuses.

We apply a noising and description step after adopting the work I, the following 4 stages are carried as

Approximation a course field \( O \) from the set of minutiae point by adopt the direction reconstruction algorithm planned in.

Produce a binary edge model base on \( O \) and a predefined fingerprint ridge frequency (which is set as 0.12) using Gabor filtering.

Approximation the phase image \( \psi \) of the binary ridge pattern using the finger-
print FM-AM model.
Reconstruct the permanent phase image $\psi_{c}$ by removes the spirals in the phase image $\psi$.

III. Implementation

The joined together finger impression issues another virtual personality to two different fingerprints, which could be matched utilizing minutiae based finger impression matching calculations. The preferences for our techniques again those existing finger impression mix systems [X-XIII] are as takes after: 1) Our suggested framework has the capacity on attain a low slip rate with FRR=0. 4% the point when FAR=0. 1%. 2) Compared for the characteristic level based on techniques, we have the ability on make another personality (i. E. , the joined together minutiae template) which may be challenging will a chance to be recognized from the unique minutiae templates. 3) Compared with those picture level built strategy we have the ability with make another virtual personality (i. E. , those joined fingerprint) which performs superior The point when those two separate fingerprints would haphazardly picked.

![Proposed method](image)

**Fig. 2** Proposed method

IV. Result Analysis

The association of the paper will be follows takes after. Area ii introduces our recommended finger impression security insurance framework. Area iii clarifies how on produce a consolidated finger impression to two distinctive fingerprints. Segment IV displays those test effects. Segment v analyzes the data spillage done a consolidated minutiae template, took after by the conclusions in the last segment.
Fig. 3 Reconstruct real image to fingerprint image from set of minutiae points.

Fig. 4 Performance of the proposed system for (a) Case I, and (b) Case II.
V. Conclusion

In this strategy will present a novel system for finger print security toward joining together two finger prints under a recently character. That framework might capture two finger prints from two distinctive fingers. Shared minutiae format holding just a fractional characteristic about each of the two finger prints will be generate & store in data base. Will aggravate those joined minutiae format gander genuine Concerning illustration a unique minutiae template, three different coding methodologies need aid acquainted Throughout those consolidated minutiae format era procedure. In the Confirmation process, two inquiry fingerprints from the same two fingers would oblige. A two-stage finger impression matching transform is suggested for matching those two inquiry fingerprints against those selected tem-plate. Our joined together minutiae format needs a comparable topology on a unique minutiae format. Therefore, we have the ability on consolidate two separate fingerprints under another virtual character by reconstructing a real-look indistinguishable joined together finger impression starting with those consolidated minutiae format. Those test Outcomes indicate that our framework accomplishes a low slip rate for FRR In a long way.

References

I. A. Kong, K.-H. Cheung, D. Zhang, M. Kamel, and J. You, “An analysis of biohashing and its variants,” Pattern Recognit., vol. 39, no. 7, pp. 1359–1368, 2006.

II. A. Nagar, K. Nandakumar, and A. K. Jain, “Biometric template transformation: A security analysis,” in Proc. SPIE, Electron. Imaging, Media Forensics and Security, San Jose, Jan. 2010.
III. A. Othman and A. Ross, “Mixing fingerprints for generating virtual identities,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

IV. A. Ross and A. Othman, “Mixing fingerprints for template security and privacy,” in Proc. 19th Eur. Signal Proc. Conf. (EUSIPCO), Barcelona, Spain, Aug. 29–Sep. 2, 2011.

V. B. Yanikoglu and A. Kholmatov, “Combining multiple biometrics to protect privacy,” in Proc. ICPR- BCTP Workshop, Cambridge, U.K., Aug. 2004.

VI. B. J. A. Teoh, C. L. D. Ngo, and A. Goh, “Biohashing: Two factor authentication featuring fingerprint data and tokenised random number,” Pattern Recognit., vol. 37, no. 11, pp. 2245–2255, 2004.

VII. E. Camlikaya, A. Kholmatov, and B. Yanikoglu, “Multi-biometric templates using fingerprint and voice,” Proc. SPIE, vol. 69440I, pp. 69440I-1–69440I-9, 2008.

VIII. K. G. Larkin and P. A. Fletcher, “A coherent framework for fingerprint analysis: Are fingerprints holograms?,” Opt. Express, vol. 15, pp. 8667–8677, 2007.

IX. K. Nandakumar, A. K. Jain, and S. Pankanti, “Fingerprint-based fuzzy vault: Implementation and performance,” IEEE Trans. Inf. Forensics Security, vol. 2, no. 4, pp. 744–57, Dec. 2007.

X. N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating cancelable fingerprint templates,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 29, no. 4, pp. 561–72, Apr. 2007.

XI. S. Li and A. C. Kot, “A novel system for fingerprint privacy protection,” in Proc. 7th Int. Conf. Inform. Assurance and Security (IAS), Dec. 5–8, 2011, pp. 262–266.

XII. S. Li and A. C. Kot, “Privacy protection of fingerprint database,” IEEE Signal Process. Lett., vol. 18, no. 2, pp. 115–118, Feb. 2011. [9] A. Ross and A. Othman, “Visual cryptography for biometric privacy,” IEEE Trans. Inf. Forensics Security, vol. 6, no. 1, pp. 70–81, Mar. 2011.

XIII. S. Li and A. C. Kot, “Attack using reconstructed fingerprint,” in Proc. IEEE Int. Workshop on Inform. Forensics and Security (WIFS), Foz do Iguacu, Brazil, Nov. 29–Dec. 2, 2011.

XIV. W. J. Scheirer and T. E. Boult, “Cracking fuzzy vaults and biometric encryption,” in Proc. Biometrics Symp., Sep. 2007, pp. 34–39.