International Journal of Scientific Research and Engineering Development-– Volume3 Issue 1, Jan-Feb 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Privacy Preserving Biometric Template Generation

Jitty Merin Mathew[1], Vineeth M V[2],Smita C Thomas[3]

[1]P G Scholar,Computer Science and Engineering, Mount Zion College of Engineering, Kadammanitta

Email: jittymerin2@gmail.com

[2]Computer Science and Engineering, Mount Zion College of Engineering, Kadammanitta

[3]Research scholar,Computer Science and Engineering,Vels University, Chennai

----------**********----------

Abstract:

The use of human biometric traits such as fingerprint and fingervein for the purpose of automatic user recognition has gained a lot of attention in the recent years. The paper proposes a deep-learning method for finger-vein identification and template generation, able to achieve stable and highly accurate performance when dealing with finger-vein images of different quality and a fingerprint template generation. There is increased concern over the loss of privacy and misuse of biometric data held in central repositories, as biometric applications gain popularity. So in order as a solution to this template protection schemes are also implemented in this paper.

Keywords **— Biometric, template, authentication, fingerprint, fingervein, deep-learning, security**

----------**********----------

I. INTRODUCTION

Biometrics is used for body measurements and calculations. Biometrics authentication is a form of identification and access control. It is also used to identify individuals in groups that are under surveillance.Two biometric traits are used here for template generation such as fingerprint and fingervein. As most of these modalities are prone to spoof attacks there is a high growth in demand for more user-friendly, yet secure, biometric modalities such as finger vein, hand vein and palm vein, since they are harder to forge and difficult to acquire without the users' willingness.

Most of the current state-of-the-art models suffer from some shortcomings, mainly related to the associated feature extraction approaches. In order to overcome such limitations, in this paper we propose to perform finger-vein-based identification by exploiting deep-learning techniques. Deep-learning methods such as convolutional neural networks (CNNs) consist of a number of convolutional and sub-sampling layers producing a fully connected layer, which in turn can be used as a robust feature extractor and classifier module. In order to verify the effectiveness of the designed CNN, we have tested our approach over four publicly-available finger-vein databases, characterized by different image quality levels. The achieved performance shows that the proposed method is able to guarantee stable and highly-accurate identification results, irrespective of the quality of the considered finger-vein images. Additionally, the proposed CNN-based identification system requires negligible manual effort for feature selection. In the implementation of fingerprint template generation two fingerprints are superimposed to form a multi-biometric template comprised of two biometric layers.

II. PROPOSED SYSTEM

The proposed scheme consist of template generation for fingervein and fingerprint and their protection.

A. Employed Fingervein Template Generation

1) FINGER VEIN DATABASES

The effectiveness of our proposed CNN-based identification system is evaluated on four publicly-available fingervein databases, namely t' Hong Kong Polytechnic University (HKPU), the University Sains Malaysia (FV-USM), the Shandong University (SDUMLA) and the University of Twenty Finger Vascular Pattern (UTFVP) database.

1) HKPU database: The HKPU finger-vein image database consists of images from 156 male and female volunteers. It has been acquired between April 2009 and March 2010 using a contact-less imaging device at the Hong Kong Polytechnic University campus..

2) FV-USM database: The FV-USM database is from University Sains Malaysia.

3) SDUMLA database: The SDUMLA database has been collected by Shandong University of China.

4) UTFVP database: The UTFVP database has been collected by the University of Twenty, Netherlands.

2) Finger-Vein Based Biometric Template Generation System

- Preprocessing:

The original images are gathered and then pre-processed for ROI extraction and image enhancement.Firstly, all the images area taken from the databases and are subsampled to guarantee uniformity.The upper and lower boundaries of the finger are detected using two masks from the images obtained from four publicly available databases.Then the part of the image which contains the interested finger is then extracted.

- Template Generation:

By selecting images from a single session or by selecting combination of images from all available sessions, templates are generated. The next method is used because the same data can be acquired in different sessions. The results made us to find the best possible combination of templates to be used for person identification.

B. Employed Fingerprint Template Generation

A fingerprint recognition system gets an image of your and then determines whether the patterns of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

- Phases Of Template Generation:

There are two phases in template generation:

1) Enrollment of valid subjects

All the valid subjects get enrolled in the system. The procedure of enrollment is as follows:
The acquired biometric signals (fingerprint captured) are processed and each one is converted into a set of unordered feature points to create multi biometric template. Biometric templates are encoded descriptions of the finger ridge patterns and helps in the comparison of the fingerprints.

2) Verification phase

In the Verification phase, the user is verified when she presents query samples of each of the constituent biometric modalities; whose features are matched and removed from the multi-biometric template ie, the biometric template captured from the enrollment phase will then be compared to all the stored biometric templates in the central databases. If a match is found, then the identity of the subject will be established and he/she will be allowed to enter. If there is no match found in the biometric database, then the subject can be asked to make a re attempt.

- Proposed Template Protection Schemes:

The biometric recognition techniques have been developed for several years. Most of the biometric

systems store the extracted biometric template during a centralized database for authentication applications. Although the convenience of a biometric system is increasing, the biometric template protection becomes more and more important.Two approaches are used for template protection.

i) Key-Mixed Template For Fingerprint

In this approach a Key-mixed Template (KMT) protection scheme is used which mixes a person's template with a secret key to generate every other shape of template that's more secured. The biometric template is been combined with a secret key to save lots of you the returned stop assault, spying and tampering attack for a cross fit assault. Inside the feature extraction method, the person given secret key should be blended with the permanently biometric template to make a Key-blended-Template (KMT). The integration feature M (.) can mix the key-decided random vector Vi and therefore the template Ti as: M (Ti, Vi) = Ti + Vi. The KMT is beneficial while a user authorized the template is legal. The key for exclusive databases ought to be set to be distinct by using the identical consumer.There are exceptional carriers incorporate two one-of-a-kind databases DB1 and DB2. Inside the enrollment phase, the distinct key-blended-template KMT1 and KMT2 are correspondingly saved in DB1 and DB2.

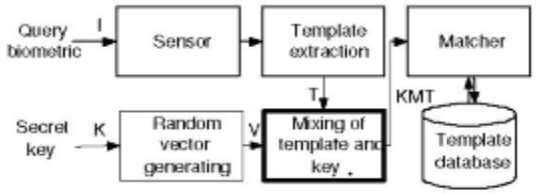

Fig. 1 Proposed biometric system

Think that an attacker successfully carried out a returned give up assault, snoop or tampering assault from DB1 and going to DB2 for authentication. This technique will no longer suit KMT1 for KMT2 in database DB2. Consequently, the cross in shape attack cannot be successful while an authentic one that owns the permanently biometric and a secret key are able to do the robustness against the lower back stop attack, snooping, and tampering assault. Because the number of attackers in returned stop attack is restrained, involvement from specific attackers should no longer be as clean because the known plaintext attack in cryptography and extra secured than it. The key and KMT generation are the extra essential operations, which can be incorporated to the prevailing biometric structures easily . This scheme is mainly designed to address the back stop assault, spying, and tampering attacks in a positive degree and might be followed via the present biometric structures to decorate the security of template safety.

This proposed KMT scheme can efficiently prevent the back end attack, snooping, and tampering attack, without reducing the performance of the original biometric system.

ii) Random Distance Method For Fingervein

Let a feature vector fv be represented as a point in the Cartesian coordinate system. It is proposed to use the distance of fv from some random point for matching purposes.Let the feature vector be divide into two equal halves such that the j^{th} feature belonging to the first half maps as the abscissa, and the corresponding feature at jth position in the second half maps as the ordinate to define a point in the Cartesian space as $(x, y) \in fv$. Let (x1,y1), (x2,y2), and (x3,y3) are such point representations belonging to three different feature vectors fv1, fv2, and fv3; and (x0, y0) is a random point derived from user-specific key. Assuming that the same key is assigned to each user (worst-case scenario), Euclidean distances d1, d2, and d3 between feature points and random point are used as transformed features. If the feature vectors fv1 and fv2 belong to the same user, then the difference in their values would be small, i.e., $\|x1 - x2\| < \delta$ and $\|y1 - y2\| < \delta$, then it can be shown that $d2 - d1 \propto \delta$.

III. CONCLUSION

The present work proposed a CNN based fingervein template generation and a fingerprint template generation which can perform effectively irrespective of the environmental conditions.The present work is one of the comprehensive study analyzing the fingervein based biometric template generation with more than two publicly available databases. This work is to use key mixed biometric template for increased performance, template security and enhanced privacy and another method called random distance transformation is used which also increases the privacy of the template.This approach is simple and easy to implement.Important requirements like revocability, unlinkability, and non-invertibility are also satisfied The main aim of this work has been to fully explore the potential of this idea.The results show that the proposed scheme is effective for template security.The protection of the generated template is inevitable.As a result of this, to increase the privacy,security and performance of the template,a key-mixed template scheme is implemented which can effectively prevent the backend attack,snooping and tampering attack.

REFERENCES

[1] Rig Das,Member,IEEE,Emanuela Piciucco, Student Member,IEEE,Emanuele Maiorana,Senior Member,IEEE,and Patrizio Campisi,Senior Member,IEEE "Convolutional Neural Network For Fingervein Based Biometric Identification System"IEEE Transactions On Information Forensics and Security, 2018.

[2] Muhammet Yildizi,BerrinYanikoglu,Alisher Kholmatov,Alper Kanak,Umut Uludag And Hakan Erdogani "Biometric Layering With Fingerprints:Template Security And Privacy Through Multi-Biometric Template Fusion" Security In Computer Networks The Journal, 2016.

[3] Shih-Wei Sun,Institute of Information Science,AcademiaSinica,Taipei,Taiwan,ROCDept,Electrical Engineering,National Central Univ,Chung-Li,Taiwan,ROC,"Biometric Template Protection:A Key-Mixed Template Approach",IEEE,2007.

[4] Harkeerat Kaur and Pritee Khanna,"Random Distance Method For Generating Unimodal and Multimodal Cancelable Biometric Features", IEEE Transactions on Information Forensics and Security,2018.

