International Journal of GEOMATE, Dec., 2017, Vol. 13, Issue 40, pp. 118-123
Special Issue on Science, Engineering & Environment, ISSN: 2186-2990, Japan
DOI: https://doi.org/10.21660/2017.40.92748

ANALYSIS OF GALTON-HENRY CLASSIFICATION METHOD FOR FINGERPRINT DATABASE FVC 2002 AND 2004

Riki Mukhaiyar[1]

[1]ISPAI Research Group, Universitas Negeri Padang, Indonesia

*Corresponding Author; Received: 27 July 2017, Revised: 20 Aug. 2017, Accepted: 30 Sept. 2017

ABSTRACT: According to Galton-Henry, fingerprint classification varies into arch, tented arch, left loop, right loop, whorl, and twin loop schemes. The approach is depended on the existence of a core and delta of each fingerprint. If this method is implemented for all fingerprint benchmark databases, then less than 41% of the fingerprint is being classified, by 37.19% for FVC 2002 and 40.31% for FVC 2004. Therefore, in this research, three requirements are needed to improve the classification result of the fingerprint, i.e. core point and its number, ridge frequency and ridge direction, and tented arch as additional requirement. This approach improves the result which is only 5.94% and 1.56% that is unclassified for FVC 2002 and 2004 consecutively. Then, to evaluate the time taken in executing the algorithm, this research does the evaluation by offering two possible conditions of the input of the fingerprint. The first type is without the fingerprint classification, while the second type is with the classification step along the algorithm process. The latter type requires an additional step namely RoI selection process to select a desired area of the fingerprint.

Keywords: Fingerprint, Fingerprint classification, FVC2002, FVC2004, Galton-Henry

1. INTRODUCTION

Securing and protecting private information of personal identity by ensuring the confidentiality, integrity, and availability of information in all forms is a growing concern in today's society. There are many tools and techniques in term of supporting the information security management. However, biometric-based system has evolved to support some aspects of this kind of information such as the facet of identification, authentication, and non-repudiation in information security.

Two different distinctions need to be made regarding biometrics are biometric authentication and biometric identification [1]. The first one is the means of identifying someone based on their enrolment biometric. For example, requiring employees to enroll into a fingerprint biometric scanning procedure is to enable the biometric device acquiring necessary biometric template information in order to authenticate the user in the future. Meanwhile, the latter is the means of identifying someone within a large grouping of biometrics by comparing an individual's biometric with an existing database of non-process-enrolled biometric templates. The identification process provides a high rate of errors [2].

The objectives of biometric authentication systems are to provide a reliable verification measures as indicated via the different rates discussed earlier and the ability to be non-obtrusive to the individual users. The biometric system must be able to quickly gather the biometric information from the user and process that information to provide or deny access [1]. Acceptability is another factor that must be examined when researching biometric systems [2]. The biometric data used for verification purposes cannot be utilized to determine if a particular individual might have a physical ailment [1].

Nevertheless, slow authentication or verification processing is a negative factor that affects the end users. Companies that employ biometric systems, such as fingerprint technology, do not want their end users to have negative effects from authentication devices. Moreover, depending on the fingerprint access point, the system must be able to provide rapid authentication to allow for steady throughput. Based on this case, an alternative approach to reduce the time consuming along the verification step will be introduced in this paper. And the case is in term of a biometric fingerprint.

2. RELATED WORKS

As mentioned previously, time consumption required along a verification process is the case to be discussed along this paper, not the verification process. Fast and accurate processes are required to minimize a vulnerable gap time for imposter to hack system whilst identifying an enquired fingerprint. Several approaches had been proposed to verify the fingerprint. Jain et al introduced a filterbank-based to match the fingerprint [3]. Then, result of this method was compared with a minutia-based method. Meanwhile, Bazen and Veldhuis [4] offered a likelihood-ratio-based

approach for the verification. In their approach, the likelihood ratio of the feature of the fingerprint was optimized to find out the average error rates.

In this paper, an alternative method is offered to determine the time consumption along the verification process by considering a classification step along the whole process. The classification step will reduce the coverage data when the verification process scans the database. The two previous reference methods used all their fingerprint data in the database to find out the truth of the fingerprint owner. However, the classification process will create a classification database to reduce the number of the fingerprint data determined along the verification process.

Many previous researchers had introduced their method to classify the fingerprint. For example, Ezin in 2010 proposed an artificial intelligent procedure to classify the fingerprint in database [5]. The artificial intelligent, known as well as an artificial neural network, uses a brain working philosophy to analyze and recognize the need of a system. Based on it, its implementation could be applied into many areas [6].

3. PROPOSED METHOD

Fingerprint classification is needed to support the idea to reduce the time consuming in the verification step. In this authentication process, a queried fingerprint is compared with all fingerprints in the database i.e. FVC2002, FVC2004, and BRC [7], [8], [9]. If the database is huge, this step becomes "bottleneck" in terms of speed complexity. This condition is not accepted in a busy online application such as bank, office, and security. Therefore, the classification step helps the verifying systems to reduce the number of fingerprint to be verified.

The uncommon distribution of fingerprint classes based on human interpretation can make the classification process of the fingerprint less efficient [2]. Instead of combining the fingerprint based on its visual appearance to generated more classes such as tented, arc tented, right loop, left loop, and whorl; a classification scheme which is basically can be implemented in a long term as result of different impression from the same fingerprint, will consistently distributed to the same classes. However, there are fingerprints which its classes are always been different although they are located near the classification line by less determining the quality of its database. In the end, these fingerprints are misclassified since the vary impressions over the same fingerprints. To solve this issue, the fingerprints are not being pre-classified, yet they are associated with vectors of numerical features. Besides, the classes formed will be given a query fingerprint by regaining part of fingerprint that has feature of vectors in the database in which the database has proximity with the query fingerprint. This approach is also called continuous classification [10], [11], [12]. Field orientation that is commonly used in building the vectors of numerical features containing local orientations [13], [14], [15], [16]. Besides that, the average range of the fingerprint is also used as an assistance feature in certain researches [11], [17].

4. RESULTS AND DISCUSSIONS

4.1. Results

The classification process is conducted by implementing fingerprint classes proposed by Henry-Galton. There are six different classes used in Henry-Galton classification scheme i.e. arch, tented arch, left loop, right loop, whorl, and twin loop whorl. All these categorize are classified based on the appearance of core and delta of each fingerprint.

However, if this approach is used for all the benchmark databases, then less than 41% of the fingerprints have the possibility to be classified because not all of the fingerprint images have tented arch (TA). For example, in BRC DBI-Test database, there are only 21.55% of the 1480 fingerprint images with TA. Meanwhile, FVC2002 database and FVC2004database, have just 37.19% and 40.31% fingerprint images, respectively. Therefore, in this fingerprint classification image process, there are three requirements i.e. core point and its number, ridge frequency, and ridge direction whilst TA is just as an additional requirement.

In this experiment, for FVC2002, of 320 fingerprint images, only 51.25% of them are classified. Meanwhile, 5.94% is unclassified because several causes like no/unidentified-core, no/unidentified-TA, and un-clear ridge/valley. Still, 35.94% of the input fingerprints are indicated likely as a left/right loop classes and 1.25% of them are judged as a false classification. This false classification happens because the fingerprints do not have some needed criterions. For instance, some fingerprints do not have either core or TA, so then it is difficult to identify the fingerprint either as left/right loop- and tented arch- classes. In another case, several fingerprints have uncertain number of core point. Thus, it is classified just as whorl class and not twin loop whorl. Lastly, short ridge-line after the core and false-core identification can obtain a false classification as well for all classes. Especially for likely left/right loop classes, this decision is based on core position and upper- and lower-ridge furrow form and direction as following pictures.

The Fig. 1.shows how a fingerprint without TA is indicated as either left/right loop classes fingerprint. In the above fingerprint, by using left up-angle as a predicted core-point and the pattern of ridge furrows are shown by red and blue arrows, accordingly. The ridge pattern shown by red arrow is straight and to the right side whilst the other side shown by blue arrow is a curved line and to the left side, so then this fingerprint is likely to be a right loop class fingerprint, and vice versa.

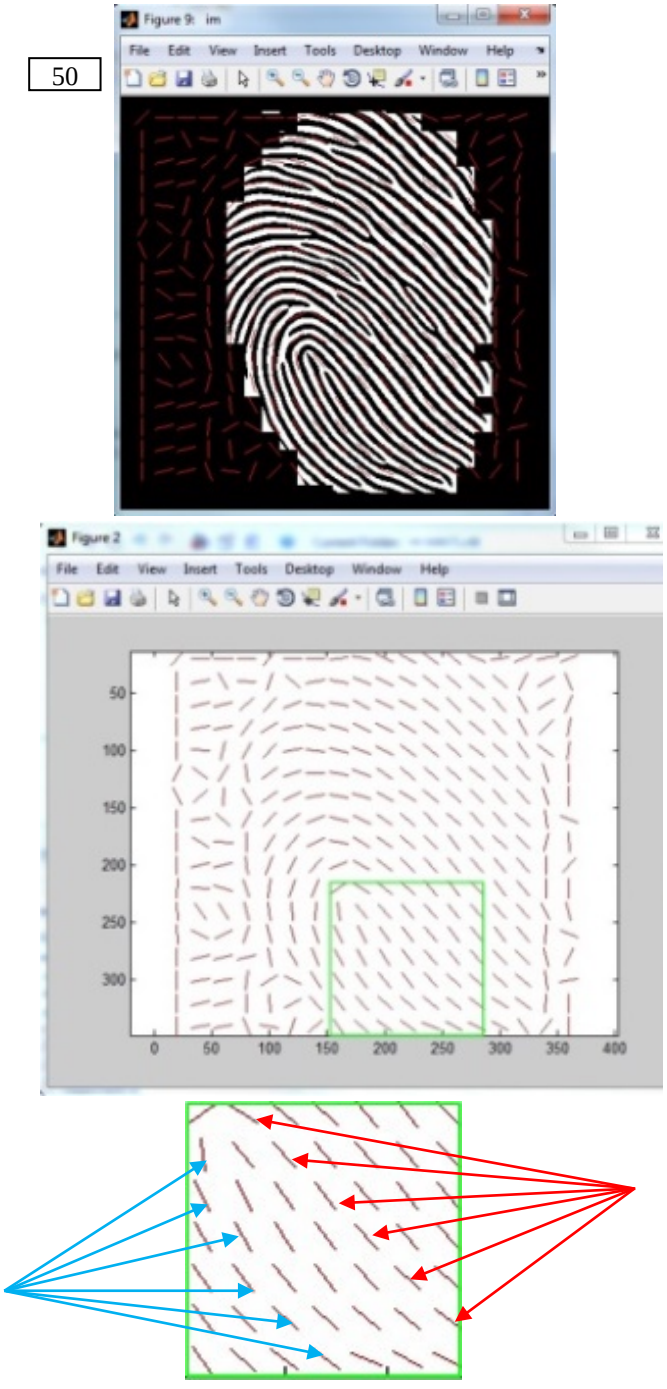

Fig. 1 Ridge-Orientation for Classification Direction

Furthermore, for FVC2004, as shown in Table 1, the percentage of the classified fingerprint is slightly higher than FVC2002. The reason is because the fingerprint input size in FVC2004 is bigger, so that fingerprint details like core and TA are covered well rather than in FVC2002. Yet, since the acquisition quality of FVC2004 is lower than 2002, so then the percentage of false classification in FVC2004 is higher than in FVC2002.

Table 1. The comparison result of three different databases

No.	Classification Decision	FVC2002	FVC2004
		in percent	
1.	Classified	51.25	59.06
2.	Unclassified	5.94	1.56
3.	Indicated as left/right loop	41.56	35.94
4.	False classification	1.25	3.44

However, in this database, it is found four new fingerprint types as follows.

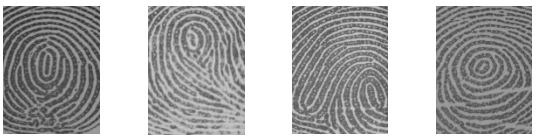

Fig. 2 Indicated as a new type of fingerprint

The fingerprint classification process is influenced by the quality and the feature covered region of the fingerprint. If the fingerprint acquisition gives a good quality image or at least image enhancement step improve the quality well, the detailed information required to classify the fingerprint is available, as well as for the covered region. Moreover, to improve the number of a classified fingerprint, the use of tented arch (TA) as a requirement can be maximized by using another approach: ridge frequency and ridge direction whilst TA is just as an additional requirement.

The second thing to be evaluated is duration needed to execute the proposed algorithm. Time consuming is a concerning issue to be determined since there are two different algorithm of the fingerprints adapted in its verification process i.e. without and with classification. Furthermore, the total times of each combination are compared to see which combination is better. The approach has been tested by using Intel Core i5-2430M CPU@2.40GHz; 4.00 GB installed RAM; and MATLAB version 7.10.0 (R2010a).

Table below illustrates time taken by system to execute all steps of the research. From each table, the comparison among different sub-databases in the same database is shown to provide the different percentage.

Table 2. Time Needed for Database FVC 2002 and FVC 2004 (in second)

No	Data bases	FVC2002		FVC2004	
		w/out Classification	w/ Classification	w/out Classification	w/ Classification
1.	DB1	0.7269	0.5048	0.6966	0.4829
2.	DB2	0.7592	0.5255	0.6820	0.4725
3.	DB3	0.6941	0.4811	0.6878	0.4772
4.	DB4	0.6855	0.4751	0.7009	0.4860

4.2. Discussions

For databases FVC2002 and FVC2004, the performances of one fingerprint are examined against seven variant of itself and 72 variant from the other fingerprints. Totally, this research exploits 576 type of fingerprint. Based on the result showed previously, several observations can be highlighted as follows.

The performance of a biometric system cannot be separated from the verification process. This stage becomes important because it aims to check the authenticity of a fingerprint. So then the system can decide which input of fingerprint should be either accepted (genuine) or rejected (impostor). However, it has become commonplace in the verification step that not all the accepted or rejected fingerprints are true genuine and true impostor. These conditions are known as false genuine and false impostor. False genuine and impostor would create a problem if its rates (EER) are huge. Hence, fingerprint with the lowest EER has a chance to become a better fingerprint in the database. However, EER is not the only requirement to acknowledge of which fingerprint has a better error rate. In this research, threshold value is also determined as a parameter to know which fingerprint in the same database has the lowest error rate. The reason is because threshold value would show an excuse level for the authentication system to decide the authenticity of the fingerprint.

Finding an error rate for each fingerprint in the database is required to discover the characteristic of the database after imposed by the proposed algorithm. The lowest level of the error rate for databases FVC2002 and FVC2004 is in 0.063. Meanwhile, the highest EER and the threshold of each EER could be dissimilar. In term of the threshold score, the highest score would represent a better condition of the fingerprint. If a fingerprint has a high threshold score, it means that the enquired fingerprint would be recognized by the system as an authorized fingerprint even with a high qualification matching score. However, the threshold rate does not become a prior regulation to decide which fingerprint has a better error rate but EER with the lowest score does. For example, in database FVC2002DB2, fingerprint 4 has a better error rate with 0.063 EER score and 0.475 threshold score; compared with the other fingerprints. Notwithstanding, fingerprint 108 has the highest threshold score i.e. 0.525. Similarly with fingerprint 107 in database FVC2002DB3, this fingerprint has a better error rate with 0.063 EER score and 0.375 threshold score. Besides, fingerprint 108 has 0.525 threshold score which is 40% higher than fingerprint 107.

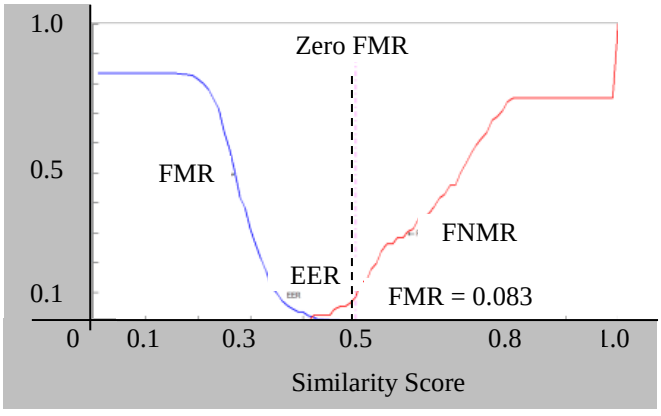

Fig. 3 Classification and EER

Obviously, databases FVC2002 (DB1, DB2, DB3, DB4) and FVC2004 (DB1, DB2, DB3, DB4) use a different scanner to obtain the fingerprint. Based on the EER score; the threshold score; and the type of scanner used to acquire the fingerprint, it is obvious that the clarity of the input of fingerprint plays an important role to minimize the error rate. In other word, the quality of the fingerprint influences how many fingerprints would be classified as a genuine owner of as an impostor and how minimum the error rate is. For example, the highest threshold score for databases FVC2002DB1; DB2; DB3; DB4, FVC2004DB1; DB2; DB3; DB4, are 0.475, 0.525, 0.525, 0.425, 0.525, 0.175, 0.275, and 0.375, respectively. Referring to these score, it can be seen that the score for FVC2002 databases have a better rate than the other databases since their fingerprints have a better quality of images.

In order to evaluate the time taken in executing the algorithm, this research does the evaluation by offering two possible conditions of the input of the fingerprint. The first type is without the fingerprint classification, while the second type is with the classification step along the algorithm process. The latter type requires an additional step namely RoI selection process to select a desired area of the fingerprint. It is obvious that an augmented step would require an additional time taken to complete the algorithm. However, in this research, the size of the input of fingerprint plays an important role to reduce the time consuming. However, the additional step of the process does not affect the total time taken along the execution.

5. CONCLUSIONS

In the fingerprint classification of image process, there are three requirements i.e. core point and its number, ridge frequency, and ridge direction whilst TA is just as an additional requirement. In this paper, for FVC2002 database, out of 320 fingerprint images, only 51.25% of them are classified. Meanwhile, 5.94% of them are unclassified because several causes like no/unidentified-core, no/unidentified-TA, and un-clear ridge/valley. Furthermore, for FVC2004, the percentage of the classified fingerprint is slightly higher than FVC2002. The reason is because the fingerprint input size in FVC2004 is bigger, so that fingerprint details like core and TA are covered well rather than in FVC2002. Yet, since the acquisition quality of FVC2004 is lower than 2002, so then the percentage of false classification in FVC2004 is higher than in FVC2002. Moreover, to improve the number of a classified fingerprint, the use of tented arch (TA) as a requirement can be maximized by using another approach: ridge frequency and ridge direction whilst TA is just as an additional requirement.

In term of to evaluate the time taken in executing the algorithm, this research does the evaluation by offering two possible types of the input of the fingerprint. The first type is just by using the original fingerprint as an input. Meanwhile, the second type is by selecting a particular area of the original fingerprint to reduce an unneeded feature captured along the algorithm process. The latter type requires an additional step namely RoI selection process to select a desired area of the fingerprint. It is obvious that an augmented step would require an additional time taken to complete the algorithm. However, in this research, the size of the input of fingerprint plays an important role to reduce the time consuming. The additional step of the process does not affect the total time taken during the execution.

6. REFERENCES

[1] R. Mukhaiyar, S.S. Dlay, and W. L. Woo, Cancellable Biometric using Matrix Approaches, Newcastle University, UK, Thesis, pp. 10–17, 2015.

[2] R. Mukhaiyar, S.S. Dlay, and W. L. Woo, “Alternative Approach in Generating Cancellable Fingerprint by using Matrices,” in Proceeding of 56th International Symposium of ELMAR, Zadar: Croatia, pp. 1–4, 2014.

[3] A. K. Jain, S. Prabhakar, L. Hong, and S. Pankanti, “Filterbank-Based Fingerprint Matching,” IEEE Transaction on Image Processing, Vol. 9, No. 5, pp. 846-859, May 2000.

[4] A. M. Bazen and R. N. J. Veldhuis, “Likelihood-Ratio-Based Biometric Verification,” IEEE Transactions on Circuits and System for Video Technology, Vol. 14, No. 1, pp. 86-94, January 2004.

[5] E. C. Ezin, “Pyramidal Structure Algorithm for Fingerprint Classification Based on Artificial Neural Network,” Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol.14, pp. 63, 2010.

[6] R. Mukhaiyar, “The Comparation of Back Propagation Method and Kohon Method for Gas Identification,” International Journal of GEOMATE, Vol.12, pp. 97-103, 2017.

[7] http://bias.csr.unibo.it/fvc2002/databases.asp.

[8] http://bias.csr.unibo.it/fvc2004/databases.asp.

[9] Biometrics Research Center, Department of Computing,The Hong Kong Polytechnic University, cslzhang@comp.polyu.edu.hk.

[10] R.M. Bolle, J.H. Connell, and N.K. Ratha, “Biometric Perils and Patches,” Pattern Recognition, Vol. 35, No. 12, pp. 2727-2738, 2002.

[11] S. Huckemann, T. Hotz, and A. Munk, "Global Models for the orientation Field of Fingerprints: An Approach Based on Quadratic Differentials", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 30, No. 9, pp. 1507-1519, 2008.

[12] R. Cappelli, A. Lumini, D. Maio, D. Maltoni, "Fingerprint Classification by Directional Image Partitioning", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 21, No. 5, pp. 402-421, 1999.

[13] C.H. Park, J.J. Lee, M.J.T. Smith, S.I. Park, and K.H. Park, "Directional Filter Bank-Based Fingerprint Feature Extraction and Matching", IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14, No. 1, pp. 74-85, January 2004.

[14] R. Mukhaiyar, "Core-Point, Ridge-Frequency, and Ridge-Orientation Density Roles in Selecting Regional of Interest of Fingerprint," International Journal of GEOMATE, Vol.12, Issue 30, pp. 146-150, 2017.

[15] A. Senior, "A Combination Fingerprint Classifier", IEEE Transaction of Pattern Analysis and Machine Intelligence, Vol. 23, No. 10, pp. 1165-1174, 2001.

[16] B. Bhanu, X. Tan, "Fingerprint Indexing Based on Novel Features of Minutiae Triplets", IEEE Transaction of Pattern Analysis and Machine Intelligence, Vol. 25, No. 5, pp. 616-622, 2003.

[17] S. Yoon, J. Feng, and A.K. Jain, "On Latent Fingerprint Enhancement", In SPIE Biometric Technology for Human Identification VII", Vol. 7667, No. 1, pp. 766-707, 2010.

This paper is a genuine and authentic work and contains unpublished materials. There is not conflict interest on this paper. The author confirms that no ethical issues involved.