November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

Different Feature Representation for Fake Fingerprint Classification

Asraful Syifaa' Ahmad*[1], Rohayanti Hassan*[2], Shahreen Kasim[3], Rohaizan Ramlan[4]
[1,2]*School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310 Johor Bharu, Johor, Malaysia*
**Corresponding author: *asrafulsyifaa.ahmad@gmail.com, rohayanti@utm.my*
[3]*Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, Malaysia.*
shahreen@uthm.edu.my
[4]*Production and Operation Management Department, Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, Malaysia.*
rohaizan@uthm.edu.my

Article Info
Volume 81
Page Number: 956 - 963
Publication Issue:
November-December 2019

Article History
Article Received: *3 January 2019*
Revised: *25 March 2019*
Accepted: *28 July 2019*
Publication: *25 November 2019*

Abstract

Existing studies show the fake fingerprint detection faced a problem in dealing with a variety of materials that can be used to fabricate the fake fingerprints, type of sensor and the noises. These cause a lack of meaningful features extracted to represent the fake fingerprints. Continuous advancement in this domain does lead to the introduction of new materials for fake fingerprint fabrication. Meanwhile, the performance of classification shows a low accuracy when classifying the fake fingerprint fabricate by the unknown materials. Therefore, a good extraction method able to extract meaningful features is needed. This work aims to use two different based of features representation; pixel intensity-based and ridge length-based in order to gain the variant meaningful features. The idea is to represent both features gain from two different based on representation using the data statistical method, then select the best features before fused the features together.

Keywords*: Pixel intensity, Ridge length, Feature extraction, Classification, Fake fingerprint detection*

1. INTRODUCTION

Fingerprint recognition is known as the most successful recognition and has been widely applied in many domains such as government, civilians and commercial. However, the existing fingerprint recognition faced some issues and be threatened by the existing of fake fingerprints. Three types of fake fingerprints are categorized by the automated fingerprint identification system (AFIS); the fingerprint film, the altered fingerprint and synthetic fingerprint. The fake fingerprint film means the fake fingerprint that is created and fabricated in low-cost production. The materials used to fabricate the fake fingerprints are easily

TEST Engineering & Management
November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

found such as wood glue, gelatine, latex, silicone and ecoflex. The variety of materials used to cause the minutiae hard to be detected. Nevertheless, the quality of these fake fingerprint can be varying depending on the materials used to fabricate it [1], [2]. Thus, a good feature extraction process needs to be done in order to ensure only the meaningful minutiae be detected and represented the fingerprint images. This is because the performance of classification and detection depends on the input of image and the detection system did shows the low performance when using new or unknown materials in real life situation. Therefore, it is a need to have a good set of features to represent the fingerprint images and to prepare a method that robust to any set of fake fingerprint images. As for that the classification process will play an important role to classify either the image is fake or not, the classifier used need to be the best[3], [4].

Our work extract features using two different based extractors and yet select and combine the features. The dataset used is the fake fingerprint images fabricated by gelatine and latex from the LiveDet 2015 database. Thus, our work has two objectives in this paper:

- Explore two different based on feature representation to represent the fake fingerprint images
- Analyse several data statistical method that can be used to represent the fake fingerprint features

The rest of this paper is organized as follows. The features representation method for enhanced features fusion framework for fake fingerprint classification is proposed in Section 2. The experimental results are discussed in Section 0 and the conclusion is drawn in Section 4.

2. METHODOLOGY

Generally, the fake fingerprint detection undergoes three main stages which are image enhancement, feature extraction, and classification. Meanwhile, our work skipped the image enhancement steps in order to ensure there are no features being neglected during the enhancement of images. The process starts with the feature extraction process. Feature extraction consists of a set of steps to obtain a set of features that able to properly represent an object for the next process [5].

Next, our work undergoes the feature selection and feature fusion. There are three level of fusions and two different fusion strategies identified; data level fusion, feature level fusion and also decision level fusion[6]. Data level fusion is at where two different images are gained from the sensor at once. While for feature level fusion is where the result from the different extractor is combined to achieve higher classification score. Meanwhile, decision level fusion is where the result gained from the different classification process is combined.

Lastly, the classification step. Classification usually refers to the learning classifier develop by several features but different things go to the classification of fingerprint where feature extraction is included in the pipeline [7]. Compared to fingerprint recognition, it ends with the template matching process. The difference between the classification and template matching are their aims where classification aims to claim the identity of a person by their fingerprint. Meanwhile, template matching or verification aim is to check whether two

TEST Engineering & Management
November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

fingerprints are the same using a set of compared images in the database [8].

The features representation method of enhanced features fusion framework for fake fingerprint classification are consist of two different based on representation which is done to improve the discoverability of meaningful and variant features. The illustration of the method is shown in Figure 1 below.

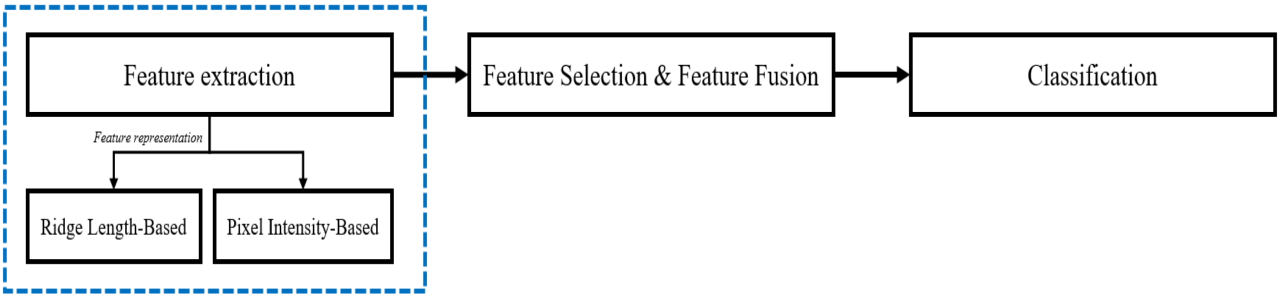


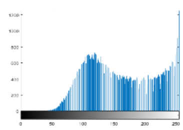
Figure 1. Enhanced features fusion framework

For the feature representation step, there were two parallel extraction methods were run at the same time. The feature extraction using the pixel intensity and the feature extraction using the ridge length was run parallel in order to gain variant and meaningful features. Both methods were run in order to get the most significant features in a different approach by considering another variant of features. The first extraction is done by converting the images to pixel intensity value graph and second is by extracting the ridge features. Then, only ridge length features are chosen and be tabulated in graph distribution. The idea is to represent both features gain from two different based on representation using the data statistical method, then select the best features before fused the features together. The details of the feature representation are explained in the next sub-sections.

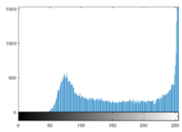
2.1 Pixel Intensity-based

For the first method, the feature extraction using the pixel intensity is chosen as the pixel intensity represented the fingerprint images can be converted to the valuable information. Each pixel does contain a single numerical value that will represent the signal level of the pixel point. By converting the images to the gray scale which means it involved the intensity images that changed from black to white. The images are then converted to the pixel intensity graph before undergoing the statistical method. The details of extraction can be summarized as in Table 1.

Table 1. Example of pixel intensity value graph

Material	Fake fingerprint images	Pixel Intensity Level	Description
Gelatine			• Pixel value 250 is the background • The pixel value is distributed over the entire

November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

			intensity range
Latex			• Pixel value 250 is the background • Most of the pixels rather low-intensity value

2.2 Ridge Length-based

In order to maintain the originality of the images, our work does not apply any enhancement method towards the image. This is because by applying the image enhancement many undefined or spurious minutiae be neglected and many genuine minutiae were detected. Therefore, the ridge extraction was used to ensure that no meaningful features be neglected. Ridge length itself brings the uniqueness to each person as different people will have a different set of ridge lengths. The ridge features were invariants to any geometric transformation. These features were concise as it can maintain the ridge structure and the minutiae can be obtained by further extracting the ridges. The ridge extraction usually contains four elements which are ridge count, ridge length, ridge angle of direction and also ridge type[9], [10]. The different aim would bring to different usage of features extracted. Our work only uses the ridge length as features extracted as the benefit is to obtain variant meaningful features. Ridge length was calculated from one end to another end of the line by considering the angle of the ridge orientation and the coordinate of the points. The ridge line is unique as minutiae. Another advantage of using the ridge line extractor is to neglect the spurious minutiae and also noises in the images[11]. The ridge length data were then tabulated and converted into ridge length distribution graph.

2.3 Data Statistical Methods

The eleven statistical methods as the chosen features to be extracted for this work are from the previous literature[4], [12]–[14]. The previous study by Abhyankar and Schuckers demonstrated the pixel intensity that can represent the physical and inherent information thus can differentiate the fake and real fingerprints by using typical first order image features which are energy, entropy, median, variance, skewness, kurtosis, and coefficient of variation. However, the resulting classification was not high enough. Therefore, the number of features was tested by adding another feature from another literature. A significant improvement has been proposed by modifying the number of features. To support the proposed selected features, an experiment was done in order to see the differences in term of accuracy score by using seven features, eight features, nine features, ten features and also eleven features. The increments number of features are calculated and tested by using SVM classification.

The features are Mean, Standard Deviation, Root Mean Square (RMS), Maximum Amplitude, Minimum Amplitude, Skewness, Kurtosis, Clearance Factor, Shape Factor, Impulse Factor, and Crest Factor. As the gray level distribution of the fingerprint images can be represented as the fingerprint information, the equations for all eleven

TEST Engineering & Management
November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

features are presented as follow, Eq. (1)- Eq. (11).

F1: Mean

$$\mu = \frac{\sum_{n=1}^{N} H(n)}{N} \quad (1)$$

F2: Standard Deviation

$$\sigma = \sqrt{\frac{\sum_{n=1}^{N}(H(n)-\mu)^2}{N-1}} \quad (2)$$

F3: Root Mean Square

$$RMS = \sqrt{\frac{\sum_{n=1}^{N}(H(n))^2}{N}} \quad (3)$$

F4: Maximum Amplitude

$$getMax = \max\big(H(n)\big) \quad (4)$$

F5: Minimum Amplitude

$$getMin = \min\big(H(n)\big) \quad (5)$$

F6: Skewness

$$skewness = \frac{1}{\sigma^3}\sum_{n=1}^{N-1}(n-\mu)^3 H(n) \quad (6)$$

F7: Kurtosis

$$kurtosis = \frac{1}{\sigma^4}\sum_{n=1}^{N-1}(n-\mu)^4 H(n) \quad (7)$$

F8: Clearance Factor

$$CLF = \frac{getMax}{\sum_{n=1}^{N}|H(n)|} \quad (8)$$

F9: Shape Factor

$$SF = \frac{RMS}{\sum_{n=1}^{N}|H(n)|} \quad (9)$$

F10: Impulse Factor

$$IF = \frac{\mu}{\sum_{n=1}^{N}|H(n)|} \quad (10)$$

F11: Crest Factor

$$CF = \frac{getmax}{RMS} \quad (11)$$

where

$H(n)$	is equalized and normalized histogram
N	is the total number of bins in the histogram
μ	is the mean
σ	is the standard deviation

3. EXPERIMENTAL RESULTS

In order to gain the number of suitable meaningful statistical features, an experiment is done an be motivated to show that by considering extra data statistical features able to increase the possibility of more meaningful features vector. This experiment

November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

is done for both set of features gained from the two different extraction method; Pixel Intensity-based and Ridge Length-based.

Accuracy has been evaluated using SVM classifier on a different set of features (F1-F7, F1-F8, F1-F9, F1-F10 and F1-F11) for each sensor. F1-F7 refers to the pixel intensity value that was represented using seven common data statistical features (Mean, Standard Deviation, Root Mean Square (RMS), Maximum Amplitude, Minimum Amplitude, Skewness, Kurtosis). F1-F8 refers to the pixel intensity value that was represented using seven common data statistical features with the addition of Clearance Factor. F1-F9 refers to the pixel intensity value that was represented using seven common data statistical features with the addition of Clearance Factor and Shape Factor. F1-F10 refers to the pixel intensity value that was represented using seven common data statistical features with the addition of Clearance Factor, Shape Factor and Impulse Factor. F1-F11 refers to the pixel intensity value that was represented using seven common data statistical features with the addition of Clearance Factor, Shape Factor, Impulse Factor and Crest Factor.

Table 2 shows the result gained from the Pixel Intensity-based features and

Table 3 shows the result gained from the Ridge Length-based. The fake fingerprint images had been categorized into three parts according to the sensor type. This due to the variants sensors gives a different resolution of images which also affect the quality of images. For Table 2, the average score of classification obtained by the Digital sensor, using features set F1-F7 to F1-F11, both materials show an increment of the accuracy even though there are slightly different in score between both materials. While for GreenBit sensor, the accuracy score also shows the increment pattern for both material gelatine and latex. Both results show almost the same score for both materials however when using features set, F11, the accuracy score latex rose up to 0.9015. Meanwhile, for the HiScan sensor, the accuracy score by latex shows quite different in between when using F1-F7 features and F1-F11 features. This shows that the additional statistical features which are F8: Clearance Factor, F9: Shape Factor, F10: Impulse Factor and F11: Crest Factor succeed to demonstrate a better accuracy that implied a meaningful feature. The advantage of using extra features is to have more features that could increase the possibility to have meaningful features to be extracted. Therefore, eleven statistical data are chosen in this research.

For

Table **3**, the average score of classification obtained by the Digital sensor, using features set F1-F7 to F1-F11, both materials show an increment of the accuracy even though there are slightly different in score between both materials. While for GreenBit sensor, the accuracy score also shows the increment pattern for both material gelatine and latex. Both results show almost the same score for both materials however when using features set, F11, the accuracy score latex rose up to 0.7091. Meanwhile, for the HiScan sensor, both materials also show an increment of the accuracy even though there are slightly different in score between both materials. This shows that the additional statistical features which are F8: Clearance Factor, F9: Shape Factor, F10: Impulse Factor and F11: Crest Factor succeed to demonstrate a better accuracy that implied a meaningful feature.

TEST Engineering & Management

November-December 2019
ISSN: 0193-4120 Page No. 956 - 963

Table 2. Comparison of the average accuracy features gained from Pixel Intensity-based Method

Setof Features	Digital		GreenBit		HiScan	
	Gelatine	Latex	Gelatine	Latex	Gelatine	Latex
F1-F7	0.8089	0.7901	0.8334	0.8324	0.8429	0.8171
F1-F8	0.8107	0.7908	0.8355	0.8345	0.8479	0.8439
F1-F9	0.8119	0.7952	0.8405	0.8415	0.8503	0.8446
F1-10	0.8127	0.7959	0.8428	0.8471	0.8509	0.8449
F1-11	0.8136	0.8017	0.8432	0.9015	0.8526	0.8503

Table 3. Comparison of the average accuracy features gained from Ridge Length-based Method

Set of Features	Digital		GreenBit		HiScan	
	Gelatine	Latex	Gelatine	Latex	Gelatine	Latex
F1-F7	0.7358	0.7438	0.7008	0.6783	0.7179	0.6449
F1-F8	0.7361	0.7446	0.7017	0.686	0.7193	0.6487
F1-F9	0.7388	0.7458	0.706	0.6987	0.7233	0.6523
F1-10	0.7404	0.7465	0.7064	0.6994	0.7274	0.656
F1-11	0.7424	0.7472	0.7094	0.7091	0.7286	0.6666

4. CONCLUSION

Recent studies show that fingerprint recognition faces a threatened from fake fingerprint. Meanwhile, fake fingerprint detection shows a low accuracy toward the classification process when classifying the fake fingerprint fabricate by the unknown materials. Therefore, our work aims to provide a framework that able to classify the fake fingerprint by having an optimal set of features. In this article, we proposed a scheme of feature extraction process using two different based on features extraction and eleven data statistical method. The performance shows that variant set of meaningful features gained from the two different based on feature representation. Meanwhile, the additional statistical features were chosen up to 11 which are F8: Clearance Factor, F9: Shape Factor, F10: Impulse Factor and F11: Crest Factor succeed to demonstrate a better accuracy that implied a meaningful feature. This preliminary work shows a good accuracy result exhibited by the state-of-the-art feature representation methods. Future work will involve investigating the selection method in order to choose an optimal feature that able to represent all type of materials fabricated the fake fingerprints.

ACKNOWLEDGEMENT

This research is funded by the Fundamental Research Grant Scheme (FRGS) and Universiti Teknologi Malaysia under Vote No:RJ130000.7851.5F037.

REFERENCES

[1] A. Rattani, Z. Akhtar, and G. Foresti, “A preliminary study on identifying

fabrication material from fake fingerprint images," *Proc. - 2015 IEEE Symp. Ser. Comput. Intell. SSCI 2015*, pp. 362–366, Dec. 2016.

[2] A. Rattani and A. Ross, "Minimizing the Impact of Spoof Fabrication Material on Fingerprint Liveness Detector," in *21st IEEE International Conference on Image Processing (ICIP)*, 2014, no. October.

[3] R. K. Dubey, J. Goh, and V. L. L. Thing, "Fingerprint Liveness Detection From Single Image Using Low-Level Features and Shape Analysis," *IEEE Trans. Inf. Forensics Secur.*, vol. 11, no. 7, pp. 1461–1475, Jul. 2016.

[4] Q. Huang, S. Chang, C. Liu, B. Niu, M. Tang, and Z. Zhou, "An evaluation of fake fingerprint databases utilizing SVM classification," *Pattern Recognit. Lett.*, vol. 60–61, pp. 1–7, Aug. 2015.

[5] M. Galar *et al.*, "A survey of fingerprint classification Part I: Taxonomies on feature extraction methods and learning models," *Knowledge-Based Syst.*, vol. 81, pp. 76–97, Jun. 2015.

[6] R. Fischer, T. Kiertscher, S. Gruhn, T. Scheidat, and C. Vielhauer, "From biometrics to forensics: A feature collection and first feature fusion approaches for latent fingerprint detection using a Chromatic White Light (CWL) sensor," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2012, vol. 7394 LNCS, pp. 207–210.

[7] M. Nixon, "Basic image processing operations - In Feature Extraction and Image Processing for Computer Vision," Academic Press, 2012, pp. 83–136.

[8] M. Galar *et al.*, "A survey of fingerprint classification Part II: Experimental analysis and ensemble proposal," *Knowledge-Based Syst.*, vol. 81, pp. 98–116, 2015.

[9] D. Yambay *et al.*, "Sex differences from fingerprint ridge density in Chinese and Malaysian population," *Forensic Sci. Int.*, vol. 6, no. 4, pp. 328–332, 2013.

[10] H. Choi, K. Choi, and J. Kim, "Fingerprint matching incorporating ridge features with minutiae," *IEEE Trans. Inf. Forensics Secur.*, vol. 6, no. 2, pp. 338–345, Jun. 2011.

[11] Y. Ha, T. H. Nguyen, R. Li, and Y. Wang, "Performance and security-enhanced fuzzy vault scheme based on ridge features for distorted fingerprints," *IET Biometrics*, vol. 4, no. 1, pp. 29–39, Mar. 2015.

[12] A. Abhyankar and S. Schuckers, "Fingerprint Liveliness Detection Using Local Ridge Frequencies And Multiresolution Texture Analysis Techniques," *2006 Int. Conf. Image Process.*, pp. 1–4, Oct. 2006.

[13] A. K. Mahamad and T. Hiyama, "Fault Classification based Artificial Intelligent Methods of Induction Motor Bearing," *Int. J. Innov. Comput.*, vol. 7, no. 9, pp. 5477–5494, 2011.

[14] L. F. A. Pereira *et al.*, "A fingerprint spoof detection based on MLP and SVM," in *Proceedings of the International Joint Conference on Neural Networks*, 2012, pp. 1–7.