Integration of Statistical Method and Zernike Moment as Feature Extraction in Liveness Detection

IOP Conf. Series: Materials Science and Engineering **551** (2019) 012064 doi:10.1088/1757-899X/551/1/012064

Integration of Statistical Method and Zernike Moment as Feature Extraction in Liveness Detection

A S Ahmad[1, *], R Hassan[2, *], Z Zakaria[3], R Ramlan[4]

[1,2]Software Engineering Department, School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310, Johor Bharu, Malaysia.
[3]Artificial Intelligence and Bioinformatics Research Group, School of Computing, Faculty of Engineering, Universiti Teknologi Malaysia, 81310, Johor Bharu, Malaysia.
[4]Production and Operation Management Department, Faculty of Technology Management and Business, Universiti Tun Hussein Onn Malaysia, 86400 Batu Pahat, Johor, Malaysia.

Email: asrafulsyifaa.ahmad@gmail.com, rohayanti@utm.my

Abstract. Recently, fake fingerprints have been used to defeat fingerprint recognition systems. These fake fingerprints are created without the need for any expertise and use easily found materials. In this paper, a fake fingerprint detection method is proposed that employs a combination of eleven statistical methods and integrating them with Zernike Moment as the feature extractor. Based on the experimental results, the proposed method showed average classification accuracy, sensitivity and specificity of approximately 80% for all sensors used to capture fake fingerprint images fabricated by gelatine and latex materials.

1. Introduction

A fake fingerprint is an artificial finger that is used to fool a detection system. It is categorized into two groups; cooperative which means with the cooperation of the user, and non-cooperative i.e. without user consent. There are still some issues in the fake fingerprint images despite their ability to imitate real fingerprints and fool the detection system. A fake fingerprint deforms elastically as it makes contact with the plane surface [1]. Fake fingerprint images have noise due to the presence of organic molecules in the fabrication materials. Research has been carried out to calculate the image quality of fake fingerprint images and they concluded that silgum and wood glue resulted in very low quality images due to the noise present [2]. Meanwhile, a fake fingerprint fabricated using latex shows a result that is very similar to the original fingerprint sample. These results show that all materials that are used to fabricate the fake finger have imperfections which are hard to detect by human observers[3].

Fake fingerprint images are captured by using a sensor and can be digitally analysed. Digital images consist of pixel intensities which can be represented by grey-level distribution. Different images give different readings of histogram distribution. Therefore, the statistical method was chosen as the feature extractor in our method. However, to maintain the originality of the fake fingerprint images, no image enhancement is done. Thus, in order to ensure that the noises do not affect the extraction process by the statistical method, Zernike Moment is integrated as it can help in filtering the noises. There are several fake fingerprint detection approaches using machine learning which have

been employed in previous research. Among them, the Support Vector Machine (SVM) is the most widely used [4]. Therefore, we also select and use SVM as the classification method in our research.

Therefore, the work done in this paper has two objectives. The first is to analyse which datasets in the LivDet 2015 are suitable to use as the standard benchmark for performance classification of the fake fingerprint. The second is to manipulate the use of the statistical method and Zernike Moment in terms of feature extraction. The presented analysis and exploration will provide a simple understanding of fake fingerprints and the benefit of having the feature extraction in fingerprint liveness detection. The rest of this paper is organized as follows. The dataset and statistical equation used in this research are introduced in Section 2. The result of the performance of classification is presented in Section 3. Lastly, the conclusion is drawn in Section 4.

2. Methodology

Figure 1 below shows the flow of the proposed method.

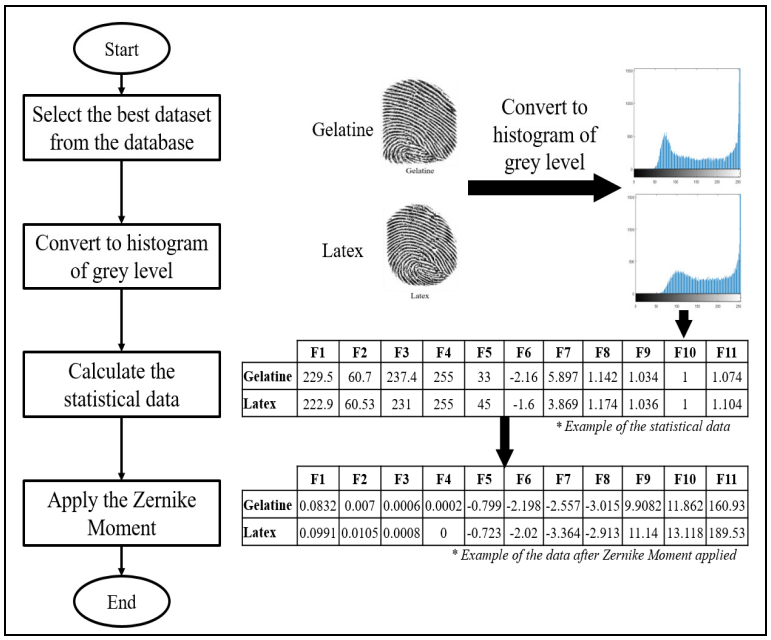

Figure 1. Flow chart of the research

2.1. Dataset Selection

The database chosen for this research is LivDet 2015. The first step in the fake fingerprint detection process is data acquisition from the databases. This step is essential as a failure in this step would lead to an inconsistency in the research objectives. The mathematical metrics approach is used in this research to calculate and evaluate the quality of the fake fingerprint images using Peak Signal to Noise Ratio (PSNR) and also Root-Mean-Square-Error (RMSE). The comparison is done by using the 250 live or known as the original fingerprint images as the references and comparing them against the 250 fake fingerprint images each made by gelatine, latex, ecoflex, and wood glue materials. The inverse relationship between PSNR and RMSE is where a lower RMSE and higher PSNR means less errors in the compared images. Table 1 shows that fake fingerprints made by latex and gelatine show the lowest RMSE values and high PSNR values. Therefore, this research will focus on latex and gelatine

materials in order to discover the characteristics that differentiates each material for a better classification process.

Table 1. Image quality assessment result

Materials	Ecoflex		Latex		Gelatine		Wood glue	
Camera	PSNR	RMSE	PSNR	RMSE	PSNR	RMSE	PSNR	RMSE
Digital	7.682	23.908	7.856	22.211	7.809	24.311	7.534	26.611
GreenBit	12.725	35.354	14.846	29.921	15.759	26.848	13.119	45.915
HiScan	10.771	32.747	11.747	30.526	10.104	21.253	12.286	41.329

2.2. Statistical Extraction Features

Generally, the extraction of features aims to reduce the dimension of the data and choose the most significant features. As the fingerprint pixels are associated with the grey-level, the statistical method is chosen to extract the meaningful information. This is due to the grey-level distribution of fingerprint images that changes according to the physical structure. Previous researchers used several statistical features to differentiate between real and fake fingerprint images [4], [5]. Thus, this research gathers eleven statistical data to be used as the features of a fake fingerprint. 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. Then the images from both datasets, gelatine and latex, were converted into a histogram of grey-level distribution and the eleven statistical data were collected for each image. The equations are as follows where $H(n)$ is equalized and normalized histogram and N is the total number of bins in the histogram.

F1: Mean, μ

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

F2: Standard Deviation, σ

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

F3: Root Mean Square, RMS

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

F4: Maximum Amplitude, $getMax$

$$getMax = \max(H(n)) \tag{4}$$

F5: Minimum Amplitude, $getMin$

$$getMin = \min(H(n)) \tag{5}$$

F6: Skewness

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

F7: Kurtosis

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

F8: Clearance Factor, CLF

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

F9: Shape Factor, SF

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

F10: Impulse Factor, IF

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

F11: Crest Factor, CF

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

2.3. Integrating Zernike Moment

To ensure the originality of the images, no enhancement is done on the images as applying image enhancement could result in many undefined or spurious minutiae being neglected and many genuine minutiae detected [6]. Thus, to handle the noise issues in the images, Zernike Moment is used as it is not sensitive at all towards the image noises. It does contain analytical invariances to rotation and luminance. Moreover, features extracted from fingerprint images are highly consistent in the change of translation since the centre of the unit disk is placed at the singular point of each image [7]. The eleven statistical data collected from each image is then applied to the Zernike Moment.

3. Performance of Classification

The table below presents the results of classification accuracy, specificity and sensitivity for the LivDet dataset based on the sensor and material fabricated. The proposed method of using the integration of Statistical Method and Zernike Moment is compared with the result of classification using Statistical Method only. Sensitivity and specificity are inversely proportional, meaning that as the sensitivity increases, the specificity decreases and vice versa [8]. Specificity is a test to define the ability of classification to detect the true negative classes while sensitivity is the ability to detect the true positive classes. In this experiment, a high specificity is needed since we want to test the specificity of the classification to specify fake classes.

Table 2 indicates that the accuracy of classification of the proposed method does show an average increment in score where the dataset of images captured by the HiScan sensor achieved a higher accuracy. It can be concluded that using a HiScan sensor that captures images in high resolution produces visible and clearer grey level distributions. This also helps in extracting the meaningful features that assist in the classification process and directly improves the accuracy score. Meanwhile, for the specificity of classification, a higher specificity means a lower sensitivity. Thus, we can see that the specificity of classification for a dataset captured using HiScan is higher compared to its sensitivity which has recorded a lower score. Meanwhile, a comparison of the accuracy of the fake fingerprint materials shows that all of them can achieve accuracy scores of more than 80%. The gelatine dataset achieves a better result when compared between the methods of extraction using the Statistical Method and the proposed method. Overall, we can see that the proposed method has a slight impact towards the classification. The presence of organic molecules affects the images captured by the sensor where each of the molecules will have their own pixel value and can be falsely detected as minutiae during the matching process. The average accuracy scores of more than 80% show that using the dataset with the most similar image quality compared to the original fingerprint images and with no image enhancement done, results in the high scores due to the usage of Zernike Moment to tackle the noise issues. Additionally, the dataset used in this research is the most similar to the original

images in terms of quality. The above 80% average scores obtained in terms of accuracy and specificity respectively is therefore a good start for another detailed research in this area.

Table 2. Classification Accuracy, Specificity and Sensitivity

			Accuracy of Classification (%)		Specificity of Classification (%)		Sensitivity of Classification (%)	
Feature Extractor			Statistical Method	Proposed Method	Statistical Method	Proposed Method	Statistical Method	Proposed Method
Sensor	Digital	Gelatine	70.61	**71.19**	84.70	71.19	84.70	**71.19**
		Latex	78.98	76.22	81.19	**86.22**	81.19	**76.22**
	GreenBit	Gelatine	83.95	**86.39**	81.88	**86.39**	81.88	**76.39**
		Latex	80.15	77.78	83.57	77.78	83.57	**77.78**
	HiScan	Gelatine	84.96	**86.77**	82.65	**86.77**	82.65	86.77
		Latex	85.03	**85.18**	82.15	**85.18**	82.15	85.18

[a]The bold value is the highest score

4. Conclusions

Throughout this study, comprehensive explanations have been justified on the improvement of fingerprint recognition. Feature extraction is one of the crucial parts in the recognition. Therefore, a set of meaningful features need to be extracted. An enhancement of the feature extractor in terms of the framework does affect the result of the accuracy. Choosing the only meaningful statistical method as recommended by various literature also plays an important role. Using Zernike Moment as another feature extractor in combination with the Statistical Method shows a slight difference in terms of accuracy, sensitivity and specificity. This work provides insights into fake fingerprints and benefits the development of fake fingerprint liveness detection research. In future, employing the feature selection might produce a better impact on the classification. The usage of sensors also plays an important role and needs to be further researched.

Acknowledgement

This work was financially supported by FRGS, Vot No: 4F973 from Ministry of Education (MOHE), and also RUG, Vot No. 16H73 from Universiti Teknologi Malaysia.

References

[1] Arunalatha G, Ezhilarasan M 2015 Fingerprint spoof detection using quality features *Int J Secur Its Appl*. **9** 83–94
[2] Rattani A, Ross A 2014 Minimizing the impact of spoof fabrication material on fingerprint liveness detector 4992
[3] Kho JB, Lee W and Choi H, Kim J 2019 An incremental learning method for spoof fingerprint detection *Expert Syst Appl* **116** 52–64
[4] Huang Q, Chang S, Liu C, Niu B, Tang M and Zhou Z 2015 An evaluation of fake fingerprint databases utilizing SVM classification. *Pattern Recognit Lett* **60–61** 1–7
[5] Park Y, Jang U, Lee EC 2017 Statistical anti-spoofing method for fingerprint recognition *Soft Comput* **22** 1–10
[6] Hong L, Wan Y and Jain A 1998 Fingerprint image enhancement: algorithm and performance evaluation *IEEE Transactions on Pattern Analysis and Machine Intelligence* **20** 777-789
[7] Jang HU, Hyun DK, Jung DJ and Lee HK 2014 Fingerprint-PKI authentication using zernike moments 5022–6
[8] Trevethan R. 2017 Sensitivity, specificity, and predictive values: foundations, pliabilities, and pitfalls in research and practice. *Front public Heal* **5** 307