IEICE TRANS. INF. & SYST., VOL.E102–D, NO.7 JULY 2019

LETTER

Weber Centralized Binary Fusion Descriptor for Fingerprint Liveness Detection

Asera WAYNE ASERA[†], *Nonmember and* Masayoshi ARITSUGI[††a)], *Senior Member*

SUMMARY In this research, we propose a novel method to determine fingerprint liveness to improve the discriminative behavior and classification accuracy of the combined features. This approach detects if a fingerprint is from a live or fake source. In this approach, fingerprint images are analyzed in the differential excitation (DE) component and the centralized binary pattern (CBP) component, which yield the DE image and CBP image, respectively. The images obtained are used to generate a two-dimensional histogram that is subsequently used as a feature vector. To decide if a fingerprint image is from a live or fake source, the feature vector is processed using support vector machine (SVM) classifiers. To evaluate the performance of the proposed method and compare it to existing approaches, we conducted experiments using the datasets from the 2011 and 2015 Liveness Detection Competition (LivDet), collected from four sensors. The results show that the proposed method gave comparable or even better results and further prove that methods derived from combination of features provide a better performance than existing methods.

key words: *fingerprint classification, liveness detection, machine learning, support vector machines, image processing*

1. Introduction

Currently, biometric systems are widely used for authentication in applications, such as security, surveillance, and forensic investigations. These systems rely on physical human attributes or characteristics that are distinctive and unique in individuals, such as the face and fingerprints. Although biometric systems offer robust security, they exhibit flaws and weaknesses. One of their weaknesses is known as spoofing; they are vulnerable to some form of sophisticated spoofing. Given that fingerprint-based systems are commonly used, they are more susceptible and subjected to attacks. The spoofing method is an attack that creates a replica of a latent or real fingerprint; it has a success rate of above 70% [1]. Therefore, it is important to further investigate preventative methods that can distinguish between live and fake fingerprints. In the last decade, various methods have been proposed to combat spoofing. These methods are known as liveness detection techniques.

In fingerprint liveness detection, methods incorporating machine learning as a component and local descriptors have become popular [2]. Local descriptor methods are software-based methods; they analyze the information obtained locally in an image by observing its statistical behavior using histograms (frequencies of occurrence). They are known to be excellent and stable to various kinds of alterations and have gained particular attention because of their potential capability [3].

Among the best and well-known local descriptors is the local binary pattern (LBP) [4], which has been proven to yield impressive results for fingerprint liveness detection [5]. It compares each pixel of the neighborhood with the central pixel to generate a binary number. To calculate the LBP value of the center pixel, the binary number is converted into a decimal number. However, even with its advantages, some disadvantages still exist, such as, it involves long histograms that can decelerate feature extraction, it is sensitive to noise, and the central pixel containing important information is not considered. Another simple and powerful local descriptor is the Weber local descriptor (WLD) proposed by Chen et al. [6]. This is inspired from Weber's law in psychophysics; it has two components, differential excitation and orientation. In the differential excitation component, the numerator is the intensity difference between the target pixel and the average intensity of its neighbors; the denominator is the intensity of the current pixel. The second component is the orientation, or the gradient orientation of the current pixel. Although it is a robust descriptor, its orientation component only considers the four surrounding pixels around the center pixel, which can lead to not fully obtaining and representing the local information of the center pixel. In addition, it is reasonable to hypothesize that by integrating multiple features, the accuracy could be improved. However, only a few methods utilize the combination or fusion features in fingerprint liveness detection.

In this paper, we propose the Weber centralized binary fusion (WCBF), a new combination of feature descriptors for fingerprint liveness detection. It is a novel combination of two existing and individual methods [7], [8] and is inspired by the WLD. It also contains two components: differential excitation and centralized binary pattern (CBP) [8]. CBP is a discriminative and highly efficient local descriptor. In comparison to the orientation component of the WLD, the CBP extracts local features better. The orientation component of the WLD uses four surrounding pixels for the calculation; however, CBP uses all of the surrounding pixels including the central pixel for calculation. Therefore, for a given fingerprint image, two components of the proposed descriptor are computed and subsequently the extracted fea-

Manuscript received March 5, 2019.
Manuscript publicized April 17, 2019.

[†]The author is with Department of Computer Science and Electrical Engineering, Graduate School of Science and Technology, Kumamoto University, Kumamoto-shi, 860–8555 Japan.
[††]The author is with Big Data Science and Technology, Faculty of Advanced Science and Technology, Kumamoto University, Kumamoto-shi, 860–8555 Japan.
a) E-mail: aritsugi@cs.kumamoto-u.ac.jp

DOI: 10.1587/transinf.2019EDL8044

tures are used to generate a two-dimensional (2D) histogram to statistically represent the local information of the differential excitation, and CBPs of the input image. To decide whether the fingerprints are live or fake, the proposed descriptor is processed using a machine-learning algorithm known as SVM for training.

2. Weber Centralized Binary Fusion

2.1 Differential Excitation

In WLD, the original differential excitation $\xi(x_c)$ of a current pixel x_c is calculated as follows:

$$\Delta I = \sum_{i=0}^{p-1} \Delta(x_i) = \sum_{i=0}^{p-1} (x_i - x_c) \tag{1}$$

$$G_{ratio}(x_c) = \frac{\Delta I}{I} \tag{2}$$

$$\begin{aligned} \xi(x_c) &= \arctan[G_{ratio}(x_c)] = \arctan\left[\frac{\Delta I}{I}\right] \\ &= \arctan\left[\frac{\sum_{i=0}^{p-1} \Delta(x_i)}{x_c}\right] \end{aligned} \tag{3}$$

where x_i is the i-th neighbor pixel of the current pixel x_c, I is the intensity of the current pixel x_c, and ΔI is the intensity differences of the current pixel against its neighbors. Equation (3) is derived from Weber's law because the differential component is inspired from it. As the values from calculating the differential excitation are large, in Eq. (3) the arctangent function is used to limit the values of $\xi(x)$ in the range of $[-\pi/2, \pi/2]$, and it could also partially suppress noise. Therefore, if the value of $\xi(x)$ is positive, this indicates that the surroundings are lighter than the current pixel; otherwise, if it is negative, the surroundings are darker than the current pixel.

In the proposed method, the differential excitation component is different from that used in the original WLD. It adopts the Laplacian of the Gaussian from [7] by applying the Gaussian filter to the image, as shown in Eq. (7). The Laplacian operator is expressed as in Eq. (4), where $f(x, y)$ is the image, and (x, y) is the position of the current pixel x_c.

$$\Delta I = \nabla^2 = \frac{\delta^2 f}{\delta x^2} + \frac{\delta^2 f}{\delta y^2} \qquad \text{Laplacian operator} \tag{4}$$

As stated, the Laplacian operator in the original WLD is sensitive to noise. As such, [7] used the Laplacian of the Gaussian (LoG) to compute ΔI, which is expressed and shown by the following formulas:

$$h(x, y) = exp\left(-\frac{x^2 + y^2}{2\sigma^2}\right) \qquad \text{2D Gaussian} \tag{5}$$

$$g(x, y) = h(x, y) \otimes f(x, y) \qquad \text{Result of Convolution} \tag{6}$$

$$\begin{aligned} \Delta I &= \nabla^2 g = \nabla^2[h(x, y) \otimes f(x, y)] \\ &= \frac{1}{\pi\sigma^4}\left(\frac{x^2 + y^2}{2\sigma^2} - 1\right) exp\left(-\frac{1}{2\sigma^2}(x^2 + y^2)\right) \end{aligned} \tag{7}$$

Finally, the differential excitation of the current pixel x_c is computed as follows.

$$\begin{aligned} \xi(x_c) &= \arctan[G_{ratio}(x_c)] = \arctan\left[\frac{\Delta I}{I}\right] \\ &= \arctan\left[\frac{\nabla^2 g}{I}\right] \end{aligned} \tag{8}$$

Given that the results from calculating the differential excitation is normalized to the intensity of the central pixel, the output will produce continuous values. To obtain discrete values with a limited range, a uniform quantizer is necessary. Hence, the mid-tread quantizer is used with an odd number of levels S.

2.2 Centralized Binary Pattern (CBP)

The CBP was first proposed by Fu and Wei [8]. It is a powerful texture descriptor that alleviates some disadvantages of the LBP. In the CBP, the corresponding pairs of neighboring pixels are compared, only if their connecting lines pass through the center pixel g_c. Further, the center pixel and the average value of all the pixels within the window are compared. Therefore, using the threshold C, pixels greater than or equal to C are assigned to 1, otherwise 0. Therefore, the CBP value of the center pixel is obtained by calculating the value of each pixel using Eq. (9). It is subsequently converted into a decimal number in the range of $[0, 32]$. Hence, the CBP reduces the histograms' dimensionality by comparing the pairs of neighbors. As an example, consider M=8, R=2 for a conventional LBP. Its histogram's dimensionality is 256; a uniform LBP can be 59 while a CBP is only 32. In other methods, feature extractions miss the local structure because the center pixel is set to 0 and is used as a threshold. In the CBP, it considers the importance of the center pixel and the information it provides. Hence, by giving it the largest weight, the CBP's discrimination is improved.

$$\begin{aligned} CBP_{M,R} = &\sum_{m=0}^{(M/2)-1} s\left(g_m - g_{m+(M/2)}\right) 2^m \\ &+ s(g_c - \frac{1}{M+1}(\sum_{m=0}^{M-1} g_m + g_c))2^{M/2} \end{aligned} \tag{9}$$

$$s(x) = \begin{cases} 1, & |x| \geq C \\ 0, & |x| < C \end{cases}$$

2.3 Combination

The proposed descriptor is the combination or fusion of two individual features, differential excitation and CBP patterns. For each pixel of a fingerprint image, it is analyzed in the two components, the differential excitation and CBP components, and used to extract the features simultaneously. To express the descriptors, histograms are often used. Therefore, using the two features extracted, a 2D histogram of dimensions MxS is generated. Further, S is the number of intervals of the differential excitation ξ, and M is the total number of CBP values. In other words, each column corresponds to a CBP m, and each row corresponds to a differential excitation interval s. Thus, the value of each cell corresponds to the frequency of the specific differential excitation interval s and the CBP pattern m. Finally, the feature vector is processed using the SVM machine learning under three different kernels to classify and determine the live and fake fingerprints.

3. Experimental Results

3.1 Experiments and Datasets

In this section, the performance of the proposed method is evaluated on the available datasets provided by the 2011 and 2015 Liveness Detection Competitions [9], [10]. Refer to Table 1 for information on the datasets and their characteristics. We subsequently compared the results of the proposed method with state-of-the-art methods, the winner of the 2011 LivDet Competition, and the winner, first runner up, and second runner up of the 2015 LivDet Competition, respectively. For the CBP component, the neighborhood (M), radius (R), and threshold (C) are set to 8, 2, and 0.15, respectively.

The metrics adopted from the Liveness Detection Competition for the performance evaluation are the following:

- *Ferrlive*: Rate of misclassified live fingerprints
- *Ferrfake*: Rate of misclassified fake fingerprints
- *Average Classification Error (ACE)*:

$$= \frac{Ferrlive + Ferrfake}{2}$$

- *Fcorrlive*: Rate of correctly classified live fingerprints
- *Fcorrfake*: Rate of correctly classified fake fingerprints
- *Accuracy*: Rate of correctly classified live and fake fingerprints

3.2 Results

In Table 2, the results of the state-of-the-art methods, winner of the 2011 LivDet competition, and the proposed method, are shown. The lowest error rates or best performances values for each scanner are in bold. Therefore, for the Biometrika scanner, the LBP+LPQ method performed the best with an error rate of 6.90%. For the Digital and Italdata scanners, the proposed method exhibits the lowest error rates of 6.00% and 7.00% respectively. WLD+LPQ exhibits the best result of 3.66% for the Sagem scanner. However, the proposed method outperforms all of the other methods in the overall performance, as shown by Fig. 1.

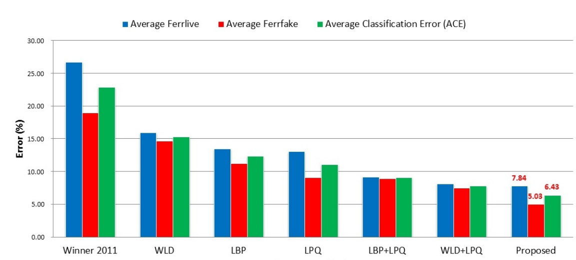
The LivDet 2015 datasets included spoof images of unknown materials. The aim is to test the reliability of the methods because in real-life scenarios, the materials used by attackers could be considered unknown and never been tested or used before. Therefore, the liveness detection methods should be able to function regardless of the materials used. Another specific challenge is the image quality. The Biometrika HiScan-PRO has a sensor with a resolution of 1000 dpi instead of 500 dpi that was used in the LivDet 2011. It is natural to say that increasing the image resolution should present positive benefits to the performance. Table 3

Table 1 Characteristics of the datasets used in the 2011 LivDet competition [9] and 2015 LivDet competition [10]

2011 LivDet	#1	#2	#3	#4
Scanner	Biometrika	Digital	Italdata	Sagem
Model no	FX2000	400B	ET10	MSO300
Resolution	500	500	500	500
Image size	312×372	355×391	640×480	352×384
Live samples	2000	2000	2000	2000
Fake samples	2000	2000	2000	2000
2015 LivDet	**#1**	**#2**	**#3**	**#4**
Scanner	Biometrika	Digital	Green Bit	Cross
Model no	HiScan	U5160	DScan26	LScanG
Resolution	1000	500	500	500
Image size	1000×1000	252×324	500×500	640×480
Live samples	2000	2000	1977	3010
Fake samples	2500	2500	2500	2921

Table 2 Error rates on 2011 LivDet test sets for live and fake samples separately

Methods	Error	Biometrika	Digital	Italdata	Sagem
Winner [2]	Ferrlive	11.00	15.10	15.10	66.00
	Ferrfake	29.00	28.50	12.50	6.20
	ACE	20.00	21.80	13.80	36.10
WLD [2]	Ferrlive	19.30	13.40	22.50	8.60
	Ferrfake	7.20	14.10	32.84	4.73
	ACE	13.25	13.75	27.67	6.66
LBP [2]	Ferrlive	8.40	13.40	18.50	13.80
	Ferrfake	11.90	13.40	16.47	4.44
	ACE	10.15	12.80	17.48	9.12
LPQ [2]	Ferrlive	15.70	11.90	16.00	8.70
	Ferrfake	9.90	7.50	15.28	3.96
	ACE	12.80	9.70	15.64	6.33
LBP+LPQ [2]	Ferrlive	6.50	10.30	13.30	6.80
	Ferrfake	7.30	8.80	14.29	5.41
	ACE	**6.90**	9.55	13.80	6.11
WLD+LPQ [2]	Ferrlive	9.80	6.30	11.80	4.90
	Ferrfake	4.60	9.70	13.49	2.41
	ACE	7.20	8.00	12.64	**3.66**
Proposed	Ferrlive	9.80	6.49	8.90	6.18
	Ferrfake	5.05	5.50	5.10	4.45
	ACE	7.43	**6.00**	**7.00**	5.32



Error types	Winner 2011	WLD	LBP	LPQ	LBP+LPQ	WLD+LPQ	Proposed
Average Ferrlive	26.80	15.95	13.53	13.08	9.23	8.20	**7.84**
Average Ferrfake	19.05	14.72	11.25	9.16	8.95	7.55	**5.03**
Average Classification Error	**22.93**	**15.33**	**12.39**	**11.12**	**9.09**	**7.88**	**6.43**

Fig. 1 Average classification error

Table 3 Summary results of accuracy rates of 2015 LivDet methods and the proposed method

Methods	Green Bit	Biometrika	Digital	Cross	Overall
Winner [10]	95.40	94.36	93.72	98.10	95.51
2nd [10]	95.80	95.20	85.44	96.00	93.23
3rd [10]	94.44	94.08	88.16	94.34	92.82
Proposed	94.75	94.18	93.96	97.57	95.11

Table 4 Breakdown or detailed results of Table 3

Methods	Error	Green Bit	Biometrika	Digital	Cross
Winner [10]	Fcorrlive	96.50	91.50	91.90	99.07
	Fcorrfake	94.67	96.27	94.93	97.10
	known	95.70	97.30	95.40	97.88
	unknown	92.60	94.20	94.00	95.98
	Accuracy	95.40	94.36	93.72	98.10
2nd [10]	Fcorrlive	93.50	89.10	64.30	98.93
	Fcorrfake	97.33	99.27	99.53	92.96
	known	98.00	99.60	99.60	97.77
	unknown	96.00	98.60	99.40	86.10
	Accuracy	95.80	95.20	85.44	96.00
3rd [10]	Fcorrlive	92.50	96.20	89.30	98.07
	Fcorrfake	95.73	92.67	87.40	90.47
	known	97.50	92.40	90.80	91.89
	unknown	92.20	93.20	80.60	88.44
	Accuracy	94.44	94.08	88.16	94.34
Proposed	Fcorrlive	92.97	92.35	92.60	96.94
	Fcorrfake	96.16	95.64	95.04	98.22
	known	96.50	95.75	95.65	97.85
	unknown	94.80	95.20	92.60	99.66
	Accuracy	94.75	94.18	93.96	97.57

is a summary of the results of the winner, the first runner up, and the second runner up methods from the 2015 LivDet competition, and the proposed methods, respectively. Compared to Table 2 specifically for the Biometrika scanner, a slight increase occurred in the performance even though in the 2015 LivDet dataset, the images were obtained using a higher resolution device. Note, however, that the methods in the 2015 LivDet competition had the opposite effect that there was a decrease in classification performance. Further, the small image sizes of the digital scanner in the 2015 LivDet dataset resulted in a slight degradation in performance. However, despite these challenges, the overall performance of the proposed method is the second best with an accuracy rate of 95.11%.

More details or the results breakdown are provided in Table 4. This table shows the results of the metrics used for evaluating the performance, as provided in one of the previous subsections. Row **Fcorrfake** includes the percentage of correctly classified fakes for all fake images (including known and unknown). As for the rows, **known** and **unknown**, they are the percentages of correctly classified fakes from the known materials and unknown materials, respectively. As shown by the results, no significant difference occurred in the accuracy rates between the fake fingerprints created from the known and unknown materials. The proposed method can identify fake fingerprints regardless the type of material used.

4. Conclusions

It is considered that as liveness detection improves, spoofing attacks and the methods used thereof also improve. Therefore, it is necessary to introduce new methods of fingerprint liveness detection. Herein, the proposed method is a new combination or fusion of features. We investigated its performance by analyzing and testing it using criteria and datasets adopted from the 2011 and 2015 LivDet competitions. The results show that the proposed method provides better and improved performance in comparison with state-of-the-art methods and other methods from the 2011 and 2015 LivDet competitions. It also proves and confirms that methods derived from a combination of features offer better performance in terms of discriminative power, or distinguishing live and fake fingerprints, as opposed to methods with individual features.

For future work, we are considering the investigation of the effects of the parameters on the reliability of the proposed method, and further plan to apply and test the proposed method on other forms of biometric liveness detection, such as the iris and face.

References

[1] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial "gummy" fingers on fingerprint systems," Proc. SPIE, pp.4677–4677–15, April 2002.

[2] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Fingerprint liveness detection based on weber local image descriptor," 2013 IEEE Workshop on Biometric Measurements and Systems for Security and Medical Applications, pp.46–50, Sept. 2013.

[3] J. Li and N.M. Allinson, "A comprehensive review of current local features for computer vision," Neurocomputing, vol.71, no.10, pp.1771–1787, 2008. Neurocomputing for Vision Research Advances in Blind Signal Processing.

[4] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," IEEE Trans. Pattern Anal. Mach. Intell., vol.24, no.7, pp.971–987, July 2002.

[5] S.B. Nikam and S. Agarwal, "Local binary pattern and wavelet-based spoof fingerprint detection," Int. J. Biometrics, vol.1, no.2, pp.141–159, Aug. 2008.

[6] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikäinen, X. Chen, and W. Gao, "WLD: A robust local image descriptor," IEEE Trans. Pattern Anal. Mach. Intell., vol.32, no.9, pp.1705–1720, Sept. 2010.

[7] D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Local contrast phase descriptor for fingerprint liveness detection," Pattern Recognition, vol.48, no.4, pp.1050–1058, 2015.

[8] X. Fu and W. Wei, "Centralized binary patterns embedded with image euclidean distance for facial expression recognition," 2008 Fourth International Conference on Natural Computation, pp.115–119, Oct. 2008.

[9] D. Yambay, L. Ghiani, P. Denti, G.L. Marcialis, F. Roli, and S. Schuckers, "Livdet 2011 — fingerprint liveness detection competition 2011," 2012 5th IAPR International Conference on Biometrics (ICB), pp.208–215, March 2012.

[10] V. Mura, L. Ghiani, G.L. Marcialis, F. Roli, D.A. Yambay, and S.A. Schuckers, "Livdet 2015 fingerprint liveness detection competition 2015," 2015 IEEE 7th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp.1–6, Sept. 2015.