Journal of Advanced Computer Science & Technology, 9 (1) (2020) 1-5

Journal of Advanced Computer Science & Technology

Website: www.sciencepubco.com/index.php/JACST

Research paper

Circular Gabor wavelet algorithm for fingerprint liveness detection

Olufade F.W. Onifade [1], Paul Akinde [1], Folasade Olubusola Isinkaye [2,*]

[1] Department of Computer Science, University of Ibadan, Oyo State Nigeria
[2] Department of Computer Science, Ekiti State University, Ado-Ekiti, Nigeria
**Corresponding author E-mail: folasade.isinkaye@eksu.edu.ng*

Abstract

Biometrics usage is growing daily and fingerprint-based recognition system is among the most effective and popular methods of personality identification. The conventional fingerprint sensor functions on total internal reflectance (TIR), which is a method that captures the external features of the finger that is presented to it. Hence, this opens it up to spoof attacks. Liveness detection is an anti-spoofing approach that has the potentials to identify physiological features in fingerprints. It has been demonstrated that spoof fingerprint made of gelatin, gummy and play-doh can easily deceive sensor. Therefore, the security of such sensor is not guaranteed. Here, we established a secure and robust fake-spoof fingerprint identification algorithm using Circular Gabor Wavelet for texture segmentation of the captured images. The samples were exposed to feature extraction processing using circular Gabor wavelet algorithm developed for texture segmentations. The result was evaluated using FAR which measures if a user presented is accepted under a false claimed identity. The FAR result was 0.03125 with an accuracy of 99.968% which showed distinct difference between live and spoof fingerprint.

Keywords: *Biometric; Fingerprint; Liveness Detection; Spoof; Support Vector Machine; Texture Segmentation*.

1. Introduction

Liveness detection is the ability of a system to detect if a biometric sample offered to it is live or otherwise [1,2]. Any system intended to safeguard against artificial fingerprints attacks must also be able to predict if biometric sample offered to it belongs to an active human being that was initially registered in the system. Liveness discovery could be initiated during the acquisition phase or during the processing phase. There exist four major means of introducing liveness discovery into a biometric system [3]. Extra hardware can be used to obtain life signs; information already captured with the aid of the system can be utilized to identify signs of life, liveness information embedded in the biometric can be used and finally, texture information presented to the sensor can equally be employed [4]. Some of these methods are faced with problems such as high cost of implementation, difficulty in extracting life signs without using additional hardware. Biometric systems also include facial thermograms, odor/scent, voice and gait. Despite the fact that biometric proof systems are always prone to spoof attacks [5], reliable anti-spoofing approaches could be designed to competently increase the degree of difficulty of the occurrences of the attacks. This work therefore develops a secure and better fake-proof fingerprint identification algorithm for fingerprint texture segmentation using Circular Gabor Wavelet Transform for liveness detection purpose and then classifies fingerprint into live or spoof using Support Vector Machines.

2. Related works

In recent times, biometrics verification has attracted significant attention of the researchers because of its extensive utilization in the area of safety and access control [6, 7]. Specifically, fingerprint verification appears to be the most implemented for the fact that, it is distinct and easy to obtain. Fingerprint liveness discovery is the ability to detect if the fingerprints presented to a biometric system are actually from a live fingerprint or spoofed [8]. Fingerprint liveness discovery was developed to level the vulnerability of fingerprint biometric systems to spoofing attacks [9,10,11]. Various techniques have been used to improve fingerprint liveness recognition. [12] examined the capability of feature fusion techniques in fingerprint liveness recognition. In their work, they examined how to select reliable set of matching features, and the capabilities of diverse classifiers for their aggregation. [10] suggested that for the purpose of discovering fingerprint before intruders, an automatic segmentation step ought to be done to separate the fingerprint from the main background and decide on the liveness of the fingerprint instead of doing it on the characteristics of the background. Their approach modelled the distribution of the live samples in order to predict as fake the samples that are unlikely. [13] proposed an approach that does not need user interventions, it used a nonlinear anisotropic diffusion where anti-spoofing features were achieved by computing the diffusion speed. Local speed patterns were then sent into a suitable classifier to generate results. [14] presented a unique fingerprint liveness descriptor known as Binarized Statistical Image Features (BSIF) which is a textual analysis algorithm that reacts to linear filters that are learnt from natural images by utilizing

independent component analysis (ICA). [15] used a local discriminative feature space for fingerprint liveness discovery. They utilized Weber Local Descriptor (WLD), a strong descriptor lately proposed for texture classification. The technique is made up of two divisions, differential excitation and orientation, evaluated for each pixel of image. Joint histograms of these divisions are processed to build the discriminative features used to train a linear kernel SVM classifier. [16] proposed a fingerprint liveness discovery technique that is based on a deep belief network (DBN). ADBN with multiple layers of restricted Boltzmann machine was issued to learn features from a set of live and fake fingerprints and also to identify the liveness. [17] presented a novel method for fingerprint liveness discovery by integrating low level features such as gradient features from SURF, PHOG, and texture features from Gabor wavelet.
In this work, we developed a secure and better fake-proof fingerprint identification algorithm for fingerprint texture segmentation using Circular Gabor Wavelet Transform for liveness discovery purpose. Support Vector Machines (SVM) was further used to classify the fingerprint into live or spoof.

3. Design description

The scanned fingerprint images from fingerprint capacitive and optical sensors were subjected to various image processing techniques such as the image acquisition, enhancement, filtering, and convolution, with both traditional and Circular Gabor Wavelets for feature extraction at different orientations and frequencies and classification as shown in Fig. 1.

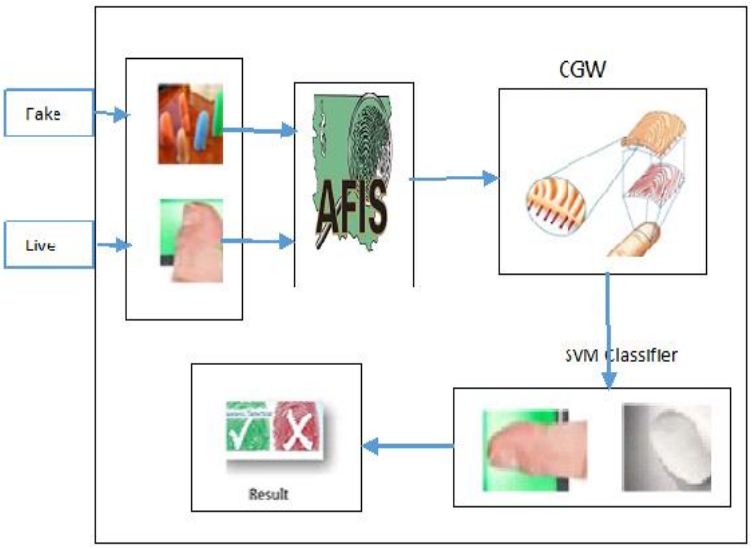

Fig. 1: Circular Gabon Wavelet (CGW) Fingerprint Liveness Detection System.

Fingerprint images were captured with capacitive sensor and optical sensor. Some samples are shown in Fig. 2 from the dataset of fake and real fingerprints. Each image was subjected to various image processing techniques.

Fig. 2: (I) Fake (Ii) Original (Iii) Fake (Iv) Original.

For pre-processing, the image was converted to double data type, and then convolution algorithm was applied to all the images after image transformation has been resized to 100×100 pixels ROI. The two-dimensional convolution matrices A and matrices B were computed, where A = resized images and B = Gabor filters. There were initialization of the filters in Gabor bank using different scales and orientations in order to extract distinct patterns in the image scanned that could assist in discriminating regular and irregular patterns. Complex numbers that have both real and imaginary parts were produced when a Gabor filter was integrated to a pixel value [18]. For every pixel of the image, Gabor filtering was performed on it hence, resulting in different orientations.
Also, the results acquired from the image processing were trained and used for classification of new image into live or spoof. This was achieved in MATLAB using Support Vector Machine (SVM) on images from Circular Gabor Wavelet.

4. Results and discussion

4.1. Scales and orientations

The selected values for frequency are, f=0.25, scales, u=[1,2,3,4,5] and orientations v=[1,2,3,4,5,6,7,8], Theta, $\theta = [0,\pi/4, \pi/2, 3\pi/4, \pi]$ for 39 elements of both the number of rows and columns in a 2-D Gabor filters using traditional Gabor and circular Gabor wavelets. Therefore,

for a Gabor array of 5 scales and 8 orientations, 40 images were generated. Fig. 3 and Fig. 4 show the traditional Gabor wavelet filter which is used in convolution with the fingerprint sample.

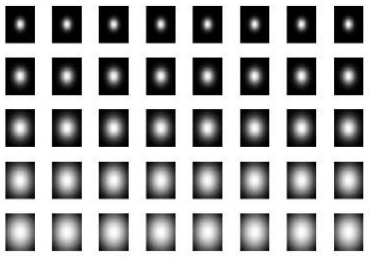

Fig. 3: Gabor Wavelets in Five Scales and Eight Orientations-Magnitudes.

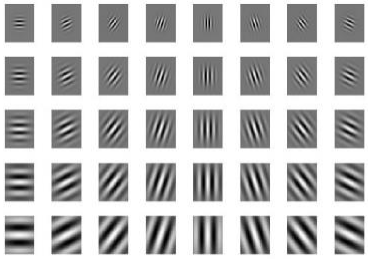

Fig. 4: Gabor Wavelets in Five Scales and Eight Orientations-Real Parts.

4.2. Circular Gabor wavelets results

The original and fake fingerprints were convolved with traditional Gabor Wavelets and the mean and the standard deviation values gotten for 40 output images. It was however, discovered that there was little discrepancies between the two. Even, the impulse responses gotten from plotting the mean and the standard deviation values showed close relations and at some point were overlapping. This mean it would be very difficult to classify. When circular Gabor Wavelet was however used, it produced better segmentation results as shown in Tables 1 and 2. The visualization graphs for the results are presented also in Fig. 5 to 8 following. The parameters used were set as follows: Frequency, f = 0.8, 1.2, 1.4, 1.5, Scale, s = 0.3, 0.6, 0.7, 0.8, Theta, θ = π/2, 5π/4, 10π/4, 17π/4. Support vector machine was developed to help in the classification of fingerprint presented to real or fake with these results.

Table 1: The Mean Values Using Circular Gabor Filter

s/n	u01_o_fc_li_04	u01_o_fo_li_04	u01_f_fc_li_04	u01_f_fo_li_04
1	9.7343	3.9854	7.8630	2.7845
2	9.5303	3.9022	7.6985	2.7280
3	9.7343	3.9854	7.8630	2.7845
4	9.5303	3.9022	7.6985	2.7280
5	14.2281	5.8232	11.4914	4.0649
6	14.0797	5.7652	11.3708	4.0286
7	14.2281	5.8232	11.4914	4.0649
8	14.0797	5.7652	11.3708	4.0286
9	12.1384	4.9669	9.8071	3.4763
10	14.9623	6.1211	12.0828	4.2645
11	12.1384	4.9669	9.8071	3.4763
12	14.9623	6.1211	12.0828	4.2645
13	10.8068	4.4192	8.7340	3.0964
14	14.4082	5.8954	11.6341	4.1097
15	10.8068	4.4192	8.7340	3.0964
16	14.4082	5.8954	11.6341	4.1097

Table 2: The Standard Deviation Values Using Circular Gabor Filters

s/n	u01_o_fc_li_04	u01_o_fo_li_04	u01_f_fc_li_04	u01_f_fo_li_04
1	5.5217	2.6844	4.3082	2.9442
2	5.4139	2.6336	4.2218	2.8871
3	5.5217	2.6844	4.3082	2.9442
4	5.4139	2.6336	4.2218	2.8871
5	7.9934	3.8768	6.2473	4.2593
6	7.9101	3.8377	6.1832	4.2173
7	7.9934	3.8768	6.2473	4.2593
8	7.9101	3.8377	6.1832	4.2173
9	6.8645	3.3328	5.3431	3.6442
10	8.3347	4.0350	6.5314	4.4460
11	6.8645	3.3328	5.3431	3.6442
12	8.3347	4.0350	6.5314	4.4460
13	6.1288	2.9781	4.7586	3.2462
14	7.9915	3.8636	6.2678	4.2590
15	6.1288	2.9781	4.7586	3.2462
16	7.9915	3.8636	6.2678	4.2590

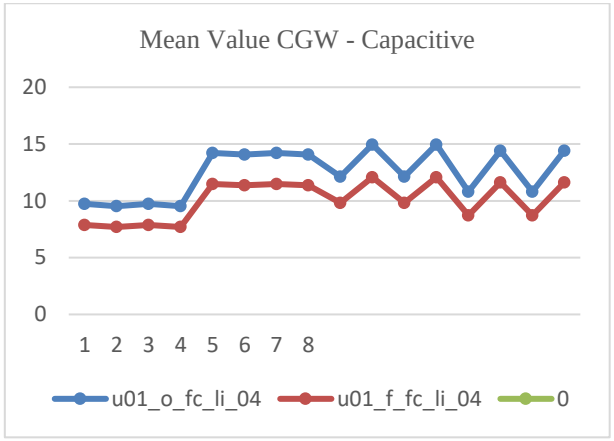

Fig. 5: Mean Value CGW – Capacitive.

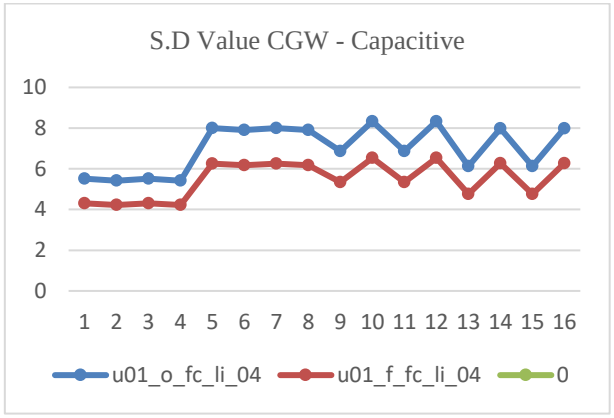

Fig. 6: Standard Deviation Value CGW.

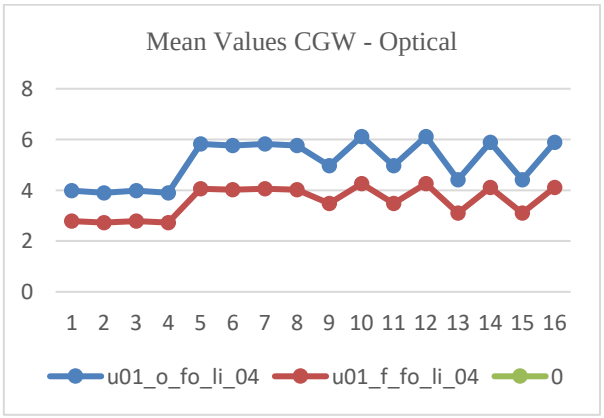

Fig. 7: Mean Value CGW – Optical.

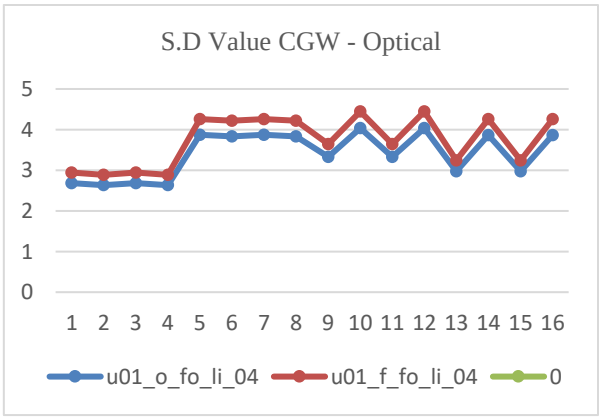

Fig. 8: Standard Deviation Value CGW – Optical

5. Evaluation of the results

The false rejection (FRR) was used to evaluate the result of the fingerprint security biometric system because it is one of the major measures in any biometric system. The FRR is the percentage of identification instances in which false rejection occurs. It is depicted as:

$$FRR\% = \frac{No\ of\ false\ rejection}{Total\ number\ of\ trials} = 0\ (none\ was\ falsely\ rejected)$$

False acceptance rate (FAR) measures the percentage of identification instances in which an illegal individuals are incorrectly accepted. FAR is in this work was used to measures if a user was accepted under a false identity.

$$FRR\% = \frac{No\ of\ false\ accepted}{Total\ number\ of\ trials} = \frac{1}{32} = 0.03125$$

From the result of evaluation, only one sample out of 32 samples was falsely classified as real. Hence the FAR is 0.03125 with the accuracy of 99.9687%

6. Conclusion

The circular Gabor wavelet algorithm was implemented using different values for the window's frequencies, scales and orientations to extract various texture segmentations from the live and fake fingerprint samples. For each set of parameters, the impulse response of 4 by 4 array of 39 by 39 filter matrix (16 filters) for filtering and convolution purposes were computed. Then, 272 fingerprint samples were converted to 2D matrix using MATLAB codes. The 2D image was convolved with all the wavelets to get a filtered output. The statistical mean, standard deviation values of output images were derived and plotted. We performed image analysis with those statistical values that were used to train the Support Vector Machine (SVM). 32 out of 272 images were used to train the SVM in order to classify the image into live or fake. Out of the 32 samples, one was falsely acceptance as real. Also, it was observed that when the orientations ranged from 0 to 360^0, the output performance of our algorithm was more. The texture segmentation using our algorithm was discrete and fingerprint samples can be separated by SVM into live or spoof with improved better segmentation results as compare to traditional Gabor wavelets. We were able to realize accuracy of 99.9687%. This shows that the algorithm outperforms existing ones.

References

[1] A. Czajka, Pupil Dynamics for Iris Liveness Detection. *IEEE Trans. Information Forensics and Security 10*(4) (2015) 726-735. https://doi.org/10.1109/TIFS.2015.2398815.

[2] C. Yuan, X. Sun, R. and Lv, Fingerprint Liveness Detection based on Multi-scale LPQ and PCA. *China Communications 13*(7) (2016) 60-65. https://doi.org/10.1109/CC.2016.7559076.

[3] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, A High Performance Fingerprint Liveness Detection Method based on Quality Related Features. *Future Generation Computer Systems 28*(1) (2012) 311-321. https://doi.org/10.1016/j.future.2010.11.024.

[4] T. de Freitas Pereira, J. Komulainen, A. Anjos, J. M. De Martino, A. Hadid, M. Pietikäinen, and S. Marcel, Face Liveness Detection using Dynamic Texture. *EURASIP Journal on Image and Video Processing*, *2014*(1), 2. https://doi.org/10.1186/1687-5281-2014-2.

[5] B. Tan, and S. Schuckers, Spoofing Protection for Fingerprint Scanner by Fusing Ridge Signal and Valley Noise. *Pattern Recognition 43*(8), (2010) 2845-2857. https://doi.org/10.1016/j.patcog.2010.01.023.

[6] Z. Xia, C. Yuan, R. Lv, X. Sun, N. N. Xiong, andY. Q. Shi, A Novel Weber Local Binary Descriptor for Fingerprint Liveness Detection. *IEEE Transactions on Systems, Man, and Cybernetics: Systems* (2018). https://doi.org/10.1109/TSMC.2018.2874281.

[7] R. P. Sharma, and S. Dey, Fingerprint Liveness Detection using Local Quality Features. *The Visual Computer* (2018) 1-18. https://doi.org/10.1007/s00371-018-01618-x.

[8] H. U. Jang, H. Y. Choi, D. Kim, J. Son, and H. K. Lee, Fingerprint Spoof Detection using Contrast Enhancement and Convolutional Neural Networks. In *International Conference on Information Science and Applications (2017)* (pp. 331-338). Springer, Singapore. https://doi.org/10.1007/978-981-10-4154-9_39.

[9] L. Ghiani, D. A. Yambay, V. Mura, G. L. Marcialis, F. Roli, and S. A Schuckers, Review of the Fingerprint Liveness Detection (Livdet) Competition Series: 2009 to 2015. *Image and Vision Computing 58* (2017) 110-128. https://doi.org/10.1016/j.imavis.2016.07.002.

[10] A. Sequeira, and J. Cardoso, Fingerprint Liveness Detection in the Presence of Capable Intruders. *Sensors*, *15*(6), 2015, 14615-14638. https://doi.org/10.3390/s150614615.

[11] E. Marasco, and A. Ross, A survey on anti-spoofing schemes for fingerprint recognition systems. *ACM Computing Surveys (CSUR) 47*(2) (2015) 28. https://doi.org/10.1145/2617756.

[12] A. T.oosi, A. Bottino, S. Cumani, P. Negri, and P. L. Sottile, Feature Fusion for Fingerprint Liveness Detection: A Comparative Study. *IEEE Access 5* (2017) 23695-23709. https://doi.org/10.1109/ACCESS.2017.2763419.

[13] S. P. Potty, V. Rohith, and S. V. Sylish, Fingerprint Liveness Detection. *International Journal of Pure and Applied mathematics* 18(20) (2018) 283-287. https://acadpubl.eu › hub › 2018-118-21.

[14] L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, Fingerprint Liveness Detection using Binarized Statistical Image Features. In *2013 IEEE sixth international conference on biometrics: theory, applications and systems (BTAS)* (2013) (pp. 1-6). IEEE. https://doi.org/10.1109/BTAS.2013.6712708.

[15] D. Gragnaniello, G. Poggi, C. Sansone, L. Verdoliva, Fingerprint Liveness Detection Based on Weber Local Image Descriptor. In *2013 IEEE work-shop on biometric measurements and systems for security and medical applications* (2013) (pp. 46-50). IEEE. https://doi.org/10.1109/BIOMS.2013.6656148.

[16] S. Kim, B. Park, B. S. Song, and S. Yang, Deep Belief Network based Statistical Feature Learning for Fingerprint Liveness Detection. *Pattern Recognition Letters 77*, (2016) 58-65. https://doi.org/10.1016/j.patrec.2016.03.015.

[17] S. Khan, M. Hussain, H. Aboalsamh, G. Bebis, A comparison of different Gabor feature extraction approaches for mass classification in mammography. *Multimedia Tools and Applications 76*(1) (2017) 33-57. https://doi.org/10.1007/s11042-015-3017-3.

[18] R. K. Dubey, J. Goh, and V. L. Thing, Fingerprint Liveness Detection from Single Image Using Low-Level Features and Shape Analysis. *IEEE Transactions on Information Forensics and Security 11*(7) (2016) 1461-1475. https://doi.org/10.1109/TIFS.2016.2535899.