International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Enhancement of Finger Vein Total Variation Decomposition by Using PAD Method

S.Logeswari[1], M.Pavithra[2], S.Kiruthika[3], P.Gopinath[4]

[1,2,3]UG student

Dept of ECE

[4]Assistant Profeesor/ ECE

Sengunthar Engineering College, Tiruchengode(India)

ABSTRACT

As an emerging biometric modality, finger vein recognition has received considerable attentions. However, recent studies have shown that finger vein biometrics is vulnerable to presentation attacks, i.e. printed versions of authorized individuals' finger veins could be used to gain access to facilities or services. In this paper, we have designed a specific for finger vein presentation attack detection (PAD). First, we use total variation (TV) regularization to decompose original finger vein images into structure and noise components, which represent the degrees of blurriness and the noise distribution. Second, a block local binary pattern (LBP) descriptor is used to encode both structure and noise information in the decomposed components. Finally, we use a cascaded support vector machine (SVM) model for classification, by which finger vein presentation attacks can be effectively detected. To evaluate the performance of our approach, we constructed a new finger vein presentation attack database. Extensive experimental results gleaned from the two finger vein presentation attack databases and a palm vein presentation attack database show that our method clearly outperforms state-of-the-art methods.

Keywords: Finger vein recognition, Presentation attack Detection, Support vector Machine

I.INTRODUCTION

In recent years, biometric techniques have attracted increased attention in various applications where correct identity assessment is crucial. Advantages over traditional authentication mechanisms such as passwords, keys, personal identification numbers, and smart cards. In the past three decades, many human traits have been investigated in depth for use with biometric techniques, including the face, iris, fingerprint, voice, palm print, and signature.

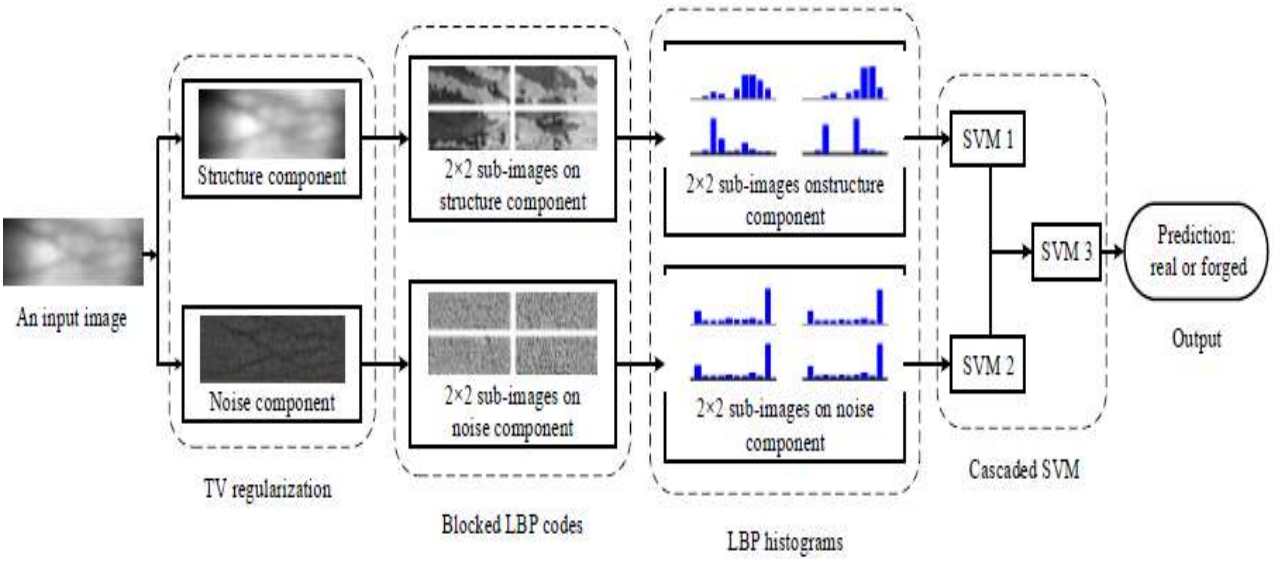
Although the above traits have been successfully taken advantage of by biometric systems in different applications, such as immigration clearance, financial payments, access control systems, and consumer electronics, they are vulnerable to presentation attacks, which can substantially decrease their level of security. Fingerprint and palm print recognition systems are also vulnerable to attacks via forged images made from commonly available materials, such as gelatin and clay With such a wide array of biometric techniques in use,

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

improving their presentation attack detection (PAD) abilities has become increasingly important for real applications. To address this problem, many PAD techniques for biometric systems based on recognizing a face iris fingerprint and palm print have been proposed.

In addition, vein recognition, including both finger vein recognition and palm vein recognition , is one of the latest emerging biometrics techniques, receiving more attention from researchers given its potential applications. Since vein patterns are almost invisible to the naked eye under natural lighting conditions and can only be acquired using infrared illumination, researchers hope that vein-based biometric systems can effectively prevent attempted spoof attacks; however, recent studies have shown that finger vein recognition systems are also vulnerable to presentation attacks from printed vein images, with a spoofing false acceptance rate as high as 86% . Hence, investigating PAD methods has become increasingly important for finger vein biometrics in the past three years. liveness or vital signs of the finger; such methods can be more accurate and reliable than texture-based methods. Through our own in-depth analysis, we found that texture-based methods perform well in preventing printed attacks because the forged finger vein images contain printing artifacts and other noise originating from the printing and imaging processing

II.BLOCK DIAGRAM



Texture-based methods only exploit noise features or extract features directly from original images, neglecting other distinctive information such as blurriness. More blurriness tends to occur in forged vein images than in real images due to the poor resolution of the forged images, defocus, and other similar factors. In this study, we found that blurriness and noise information differs to some extent between forged and real vein images. Therefore, fully utilizing both these features can further improve the discriminative power of texture-based methods.

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

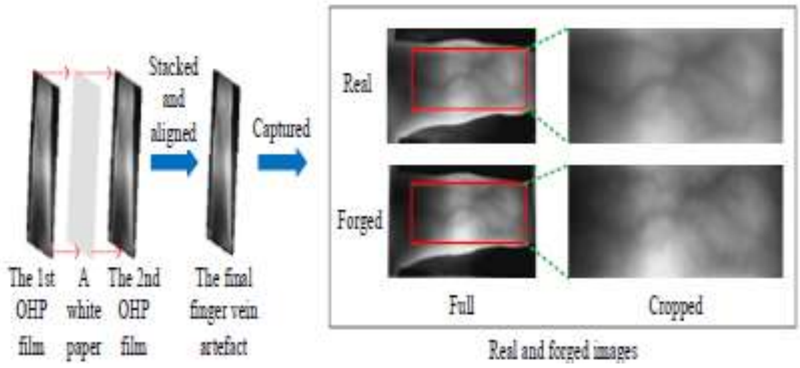
Given the above, our objective is to find a solution that effectively extracts both blurriness and noise features from forged and real vein images, and then combines these two features to better detect finger vein presentation attacks. In signal processing, total variation (TV) regularization [28], also known as total variation denoising, provides an excellent solution for noise elimination. TV regularization is based on the principle that signals with excessive and potentially spurious details have a high total variation, which is defined as the integral of the absolute gradient of the signal. This noise removal technique has advantages over simple techniques such as linear smoothing or median filtering, which not only reduce noise but also smooth away edges to a greater or lesser degree. More specifically, TV regularization is remarkably effective at simultaneously preserving edges while filtering out noise in flat regions, even at low signal-to-noise ratios (SNRs). We therefore exploit TV regularization to decompose original finger vein images.

III.DATABASES AND PERFORMANCE CRITERIA

To obtain an unbiased assessment, extensive experiments were conducted on two finger vein presentation attack databases, i.e., IDIAP FVD and SCUT FVD. The former is a publicly accessible database, while the latter was constructed by us. To further validate the effectiveness, robustness, and generalization ability of our proposed method, we conducted experiments on the Idiap Research Institute (IDIAP) palm vein presentation attack database (PVD) which is also publicly accessible. Toward the end of this section, we will briefly describe the criteria used to evaluate PAD performance.

SCUT FVD DESCRIPTION

	Clients	Hands	Fingers	Shot Number	Total
Real	100	2	3(Index, Middle and Ring)	6	3600
Forged	100	2	3(Index, Middle and Ring)	6	3600



Finger vein artefact synthesis procedure and the comparison between real and forged images in the SCUT

International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No. (01), January 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A. Databases

1) IDIAP FVD

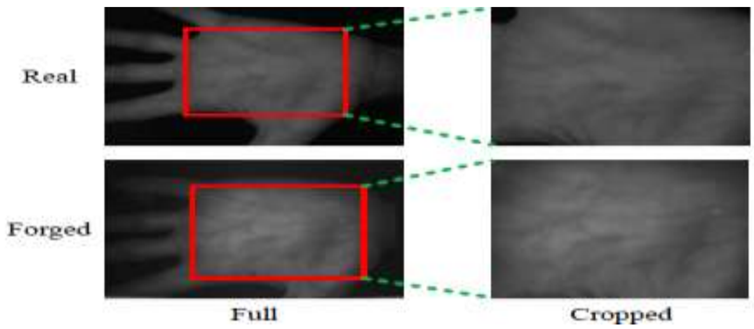
IDIAP FVD consists of cropped and full versions of real and forged images from 110 clients. The forged images were generated from corresponding real finger vein samples from the VERA Fingervein Database these forged images are simply preprocessed and printed on paper, and then recaptured using a finger vein sensor. The detailed procedure for producing the database is described in shows a comparison between the real and forged images, and Table II describes further details of IDIAP FVD.

2) SCUT FVD

Through close observation and analysis of IDIAP FVD, we found that the disparity between the real and forged finger vein images is relatively large, which reduces the difficulty of PAD to some extent. To extend IDIAP's work and narrow the disparity between the two types of images, which would be more in line with a realistically elaborate presentation attack, we improved the forgery method to produce the new SCUT FVD, which consists of cropped and full versions of 3600 real and 3600 forged The procedure for producing our database is similar to that of IDIAP FVD. A key difference between the two is that we print, at real finger size, a vein image on two OHP films rather than on thick 200 g/m_2 white paper, and then stack and align them, which significantly improves the quality of the forged images. As the intensity of near-IR light passing through two aligned OHP films is so high that the captured images tend to be overexposed, a thick 200 g/m_2 sheet of white paper is sandwiched between the two aligned OHP films to weaken the transmitted light intensity. Fig. 7 illustrates the final artifact used to attack our finger vein sensor and shows a comparison between the real and forged images in the new database; Table III provides the details image

3) IDIAP PVD

IDIAP PVD is composed of two sub-databases, the Idiap Research Institute VERA Palm Vein Database and the Idiap Research Institute VERA Spoofing Palm Vein Database. The former database consists of 2200 real images from 110 clients, but only the first 50 clients are now available. The latter database consists of 1000 forged images corresponding to the first 50 clients from the former. Both sub-databases contain cropped and full version images. The detailed procedure for producing the full database is described in shows a comparison between the real and forged images in the IDIAP PVD, while Table IV provides the details.



IV.PERFORMANCE CRITERIA

To achieve a fair and reasonable comparison between the different PAD algorithms, performance criteria are disclosed according to the PAD metrics in ISO/IEC 30107-3 [55] in terms of Attack Presentation Classification Error Rate (*APCER*) and Bona Fide Presentation Classification Error Rate (*BPCER*). *APCER* was once defined as the proportion of attack presentations incorrectly classified as bona fide presentations in a specific scenario, whereas *BPCER* was defined as the proportion of bona fide presentations incorrectly classified as attack presentations in a specific scenario. Further, we also present the results in terms of Average-Classification-Error-Rate (*ACER*) and the metric ***d*** . *ACER* is defined as the average of *APCER* and *BPCER* and can be calculated using

(APCER) / 2 ACER BPCER□.

A lower value of *ACER* indicates better PAD performance.

The metric ***d*** for decidability or decision-making power is defined as

where $\mu 1$ and $\mu 2$ are the means of the two distributions (i.e., real and forged images, respectively), while $\sigma 12$ and $\sigma 22$ are the corresponding variances. A larger value of ***d*** indicates higher separability.

V.CONCLUSION

In this paper, we proposed a novel method called TV-LBP for finger vein PAD. To our knowledge, it is the first time that both the degree of blurriness and the noise distributions of real and forged images are treated as different features. Given this, we found that we can extract discriminative features as criteria for PAD. We used TV regularization to decompose an original image into structure and noise components, representing the degree of blurriness and the noise distribution. We then exploited block LBP descriptors and a cascaded SVM model to encode and classify candidate finger vein images. We also constructed a new finger vein presentation attack database for performance evaluation. Next, we conducted extensive experiments using three databases, including our own FVD, a public FVD, and a public PVD. The results show that our proposed method can achieve complete discrimination using both cropped and full size real and forged images, outperforming state-of-the-art methods in both intra-database and inter-database test scenarios. In our future work, we intend to construct a large representative database with fewer differences between real and forged images and to conduct corresponding studies using this new database to more comprehensively meet the requirements of real applications.

REFERENCES

[1] D. T. Nguyen, Y. H. Park, K. Y. Shin, S. Y. Kwon, H. C. Lee, and K. R. Park, "Fake finger-vein image detection based on fourier and wavelet transforms," *Digital Signal Processing*, vol. 23, no. 5, pp. 1401-1413, 2013.

[2] S. Tirunagari, N. Poh, D. Windridge, A. Iorliam, N. Suki, and A. T. Ho, "Detection of face spoofing using visual dynamics," *Information Forensics and Security, IEEE Transactions on*, vol. 10, no. 4, pp. 762-777, 2015.

[3] V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," *Biometrics and identity management*, pp. 181-190: Springer, 2008.

[4] C. Sousedik, and C. Busch, "Presentation attack detection methods for fingerprint recognition systems: a survey," *IET Biometrics,* vol. 3, no. 4, pp. 219-233, 2014.

[5] N. Kose, and J.-L. Dugelay, "Reflectance analysis based countermeasure technique to detect face mask attacks," in *Digital Signal Processing (DSP), 2013 18th International Conference on*, 2013, pp. 1-6.

[6] D. Wen, H. Han, and A. K. Jain, "Face spoof detection with image distortion analysis," *IEEE Transactions on Information Forensics and Security,* vol. 10, no. 4, pp. 746-761, 2015.

[7] X. Tan, Y. Li, J. Liu, and L. Jiang, "Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model," in *European Conference on Computer Vision*, 2010, pp. 504-517.

[8] T. I. Dhamecha, A. Nigam, R. Singh, and M. Vatsa, "Disguise detection and face recognition in visible and thermal spectrums," in *International Conference on Biometrics*, 2013, pp. 1-8.

[9] S. Bharadwaj, T. I. Dhamecha, M. Vatsa, and R. Singh, "Computationally Efficient Face Spoofing Detection with Motion Magnification," in *IEEE Conference on Computer Vision & Pattern Recognition Workshops*, 2013, pp. 105-110.

[10] J. Maatta, A. Hadid, and M. Pietikainen, "Face spoofing detection from single images using texture and local shape analysis," *Iet Biometrics,* vol. 1, no. 1, pp. 3-10, 2012.

[11] S. Marcel, M. S. Nixon, and S. Z. Li, *Handbook of Biometric Anti-Spoofing*: Springer, 2014.

[12] D. Gragnaniello, C. Sansone, and L. Verdoliva, "Iris liveness detection for mobile devices based on local descriptors," *Pattern Recognition Letters,* vol. 57, pp. 81-87, 2015.

[13] K. B. Raja, R. Raghavendra, and C. Busch, "Video presentation attack detection in visible spectrum iris recognition using magnified phase information," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 10, pp. 2048-2056, 2015.

[14] R. F. Nogueira, R. D. A. Lotufo, and R. C. Machado, "Fingerprint Liveness Detection Using Convolutional Neural Networks," *IEEE Transactions on Information Forensics & Security,* vol. 11, no. 6, pp. 1-1, 2016.

[15] S. T. V. Parthasaradhi, R. Derakhshani, L. A. Hornak, and S. A. C. Schuckers, "Time-series detection of perspiration as a liveness test in fingerprint devices," *IEEE Transactions on Systems Man & Cybernetics Part C,* vol. 35, no. 3, pp. 335-343, 2005.

[16] X. Li, W. Bu, and X. Wu, *Palmprint Liveness Detection by Combining Binarized Statistical Image Features and Image Quality*