Finger vein Liveness Detection Using Motion Magnification

R. Raghavendra[*], Manasa Avinash[†], Sébastien Marcel[#], Christoph Busch[*]
[*]Norwegian Biometrics Laboratory, Gjøvik University College, 2802 Gjøvik, Norway
[†] Vidya Vikas Institute of Engineering and Technology, Mysore - India
[#]Idiap Research Institute, Centre du Parc, 1920-Martigny, Switzerland
Email: {raghavendra.ramachandra;chrishtoph.busch}@hig.no; marcel@idiap.ch; manasar.hsn@gmail.com

Abstract

Finger vein recognition has emerged as an accurate and reliable biometric modality that was deployed in various security applications. However, the use of finger vein recognition also indicated its vulnerability to presentation attacks (or direct attacks). In this work, we present a novel algorithm to identify the liveness of the finger vein characteristic that is presented to the sensor. The core idea of the proposed approach is to magnify the blood flow through the finger vein to measure its liveness. To this extent, we employ the Eulerian Video Magnification (EVM) approach to enhancing the motion of the blood in the recorded finger vein video. Next, we further process the magnified video to extract the motion-based features using optical flow to identify the finger vein artefacts. Extensive experiments are carried out on a relatively large database that is comprised of 300 unique finger vein videos corresponding to 100 subjects. The finger vein artefact database is captured by printing the real (or normal) presentation image of the finger vein on a high-quality paper using two different kinds of printers namely laser and inkjet. Extensive comparative evaluation with four different well-established state-of-the-art schemes demonstrated the efficacy of the proposed scheme.

1. Introduction

Biometric systems are widely used in various applications that demand reliable user identity authentication based on either physical and/or behaviour characteristics. Even though biometric systems are known for their reliable biometric performance, at the same time they have also demonstrated a vulnerability to various kinds of attacks. The attacks on biometric systems can be broadly classified into two types namely: (1) Direct Attack (2) Indirect Attack.

This work is funded by the EU 7th Framework Program under grant agreement n^o 284862 for the large-scale integrated project FIDELITY.

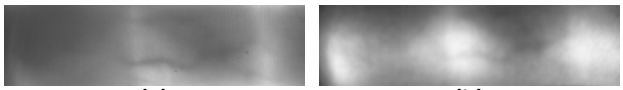

Figure 1: Illustration of finger vein artefact (a) Real Image (b) Artefact (print)

The direct attack is also called presentation attack and merely involves in presenting a biometric artefact to the sensor to gain access. The indirect attack involves in attacking the different working components of the biometric system and hence demands the need for understanding the process flow of biometric systems. When comparing these two kinds of attacks, the direct attack or presentation attack appears not only feasible but also more cost effective for the attacker to break a biometric system.

Most of the biometrics modalities have demonstrated the vulnerability for presentation attacks [2][8]. Among the various biometric modality, the finger vein biometrics is gaining more popularity because of its robustness and accuracy. Furthermore, the finger vein biometric is considered as a trustworthy modality since the vein pattern is present inside the skin and thus no latent prints are left unintentionally. Further, the characteristic is not visible to the naked eyes and hence not easy to capture in a non-intrusive manner unlike other biometric modalities such as the face, iris or fingerprint. Also, the finger vein biometric is considered to be more stable since the persons finger vein pattern remain relatively stable during his/her lifetime [1] although no definitive scientific studies exist.

Recently, the vulnerability of finger vein biometric systems has been investigated in [10] for presentation attacks using a print artefact. The finger vein print artefacts are generated by printing the finger vein image using a conventional printer. In the next step, this is further enhanced in terms of contours using a black ink white board marker. This artefact is then presented to the finger vein sensor to capture the artefact samples. Extensive analysis is pre-

sented using a finger vein artefact database comprised of 50 subjects indicated the vulnerability of the finger vein biometrics with a Spoof False Acceptance Rate (SFAR) of 86%. More recently, the 1st Competition on Counter Measures to Finger Vein Spoofing Attacks was organised in conjunction with the International Conference of Biometrics 2015. Figure 1 illustrates the finger vein artefact sample from the Spoofing-Attack finger vein database [9] used in this competition. Early results available from this competition introduced three different Presentation Attack Detection (PAD) algorithms using (1) Binarized Statistical Image Features (BSIF), (2) Riesz transform and (3) Local Phase Quantization (LPQ) [14] and Weber Local Descriptor (WLD). All these schemes have used Support Vector Machine (SVM) as a classifier. The best result is noted for the third scheme based on the combination of Local Phase Quantization (LPQ) [14] and Weber Local Descriptor (WLD) as a feature extraction and SVM as a classifier. Since all the available PAD techniques are constructed on a learning based schemes, they may have difficulties to generalise. Furthermore, the use of texture based features are highly sensitive to noise and thus less robust on unseen attacks.

Hence, this paper presents a liveness measure based on the motion magnification for finger vein PAD. To the best of our knowledge, there is no similar prior work for use as a finger vein liveness measure. For this purpose, we developed a new finger vein video artefact database comprised of 100 subjects whose videos are recorded in two different sessions. We generate two different artefacts by printing a real finger vein image using inkjet and laser printer. We then propose a novel scheme based on Eulerian Video Magnification (EVM) [11] to magnify the motion of the blood in the finger vein. We then compute the optical flow between the first and the last frame in the EVM video to compute the motion magnitude that in turn is compared against the pre-set threshold to make the decision on whether the presented video is an artefact or a normal presentation. Extensive experiments are presented that include the vulnerability assessment as well as the comparative evaluation of the proposed liveness measure with four well-established finger vein PAD algorithms. Experimental results demonstrated the efficacy of the proposed finger vein PAD algorithm with the lowest ACER of 2.20% on inkjet print artefact and ACER of 3.60% on laser jet print artefact.

The rest of the paper is structured as follows: Section 2 presents the finger vein artefact data collection, Section 3 presents the proposed scheme, Section 4 presents the experimental results and discussion. Finally, Section 5 draws the conclusion of this work.

Figure 2: Example of the finger vein artefact (a) Back view (b) Side view (c) Top view

2. Finger vein artefact data collection

We collect a new large scale finger vein artefact database in which artefacts are generated using two different kinds of printers such as inkjet and laser printer. Our database is comprised of 100 subjects for which we capture the finger vein from four different fingers namely right index, right middle, left index and left the middle. However, some of the subjects were not able to provide all four fingers due to the various reasons. Thus, the collected database has 300 unique finger vein samples that correspond to 100 subjects. All samples are collected in our laboratory using our GUC finger vein sensor. The finger vein sensor used in this work will capture the finger vein image by penetrating the near infrared light through the finger. Thus, the subject will position the finger inside the sensor, the LED light is illuminating the dorsal part of the finger so that it will penetrate through the finger and the ventral vein pattern is captured by the camera located on the opposite side.

2.1. Real sample capture

The real sample database is collected by asking the user to place the finger on the sensor. We capture the video for the duration of 1.67 seconds at a rate of 15 frames per second that will result in 25 frames for each video capture. The data capture process is carried out in two different sessions to have two independent video captures for every subject. Thus, we have a total of 600 videos with $600 * 25 = 15000$ frames corresponding to a real finger vein.

2.2. Finger vein artefact generation

Figure 3: Illustration of Finger vein presentation attack (a) working vein sensor with LED glowing (b) Attack on the sensor with finger vein artefact and external light

In this work, we generated the artefacts by printing the real sample using different kinds of printers such as inkjet and laser. The motivation for using the print attack is by because it is very easy to generate, cost effective and already proven to be efficient in a previous study [9]. In order to generate the finger vein artefacts using inkjet printer, we first perform the pre-processing on each of the captured frame of the video by extracting the Region of Extract (ROI) and then rescaling the ROI finger vein to have dimension of 100×300 pixels. We then carry out the contrast enhancement using histogram equalisation to improve the contrast of the real image before printing using high-quality glossy paper with 300 gr. A similar procedure is also followed to generate the laser print artefact, which also uses high-quality paper with 200gr on which a real finger vein sample is printed using a laser printer.

After we generated the artefact, we present it to the finger vein sensor as presentation attack instrument. Our main idea is to present this artefact to the sensor such that it will block the LED illumination and then we use the external visible light source to illuminate the artefact so that the attack instrument is successfully captured by the camera. However, in a real scenario the finger vein sensor uses the LED illumination to illuminate the finger through sideways or back penetration for a normal image capture. Thus, we designed the final artefact to block both sides and any back illumination. To this extent, we have used a thick plastic base on which the print finger vein artefact is placed and presented to the sensor. Figure 2 shows the final artefact used to attack the GUC finger vein sensor. Figure 3 shows the presentation attack on the vein sensor using the artefact showed in the Figure 2.

Figure 4 shows both real (normal) finger vein images and artefact finger vein images (one frame from the video) captures using our GUC finger vein sensor. Here one can observe the good quality of a finger vein artefact image collected by following our outlined procedure.

3. Proposed scheme

Figure 5 shows the block diagram of the proposed finger vein PAD scheme that can be structured in two main components namely: The PAD module and the finger vein verification module. Given the finger vein video $F_v = \{F_{v1}, F_{v2}, \ldots, F_{vn}\}$, where n indicates the number of frames. We then process each frame F_{vn} to extract the Region Of Interest (ROI). Since the GUC sensor has dedicated space to place the finger, the ROI extraction is carried

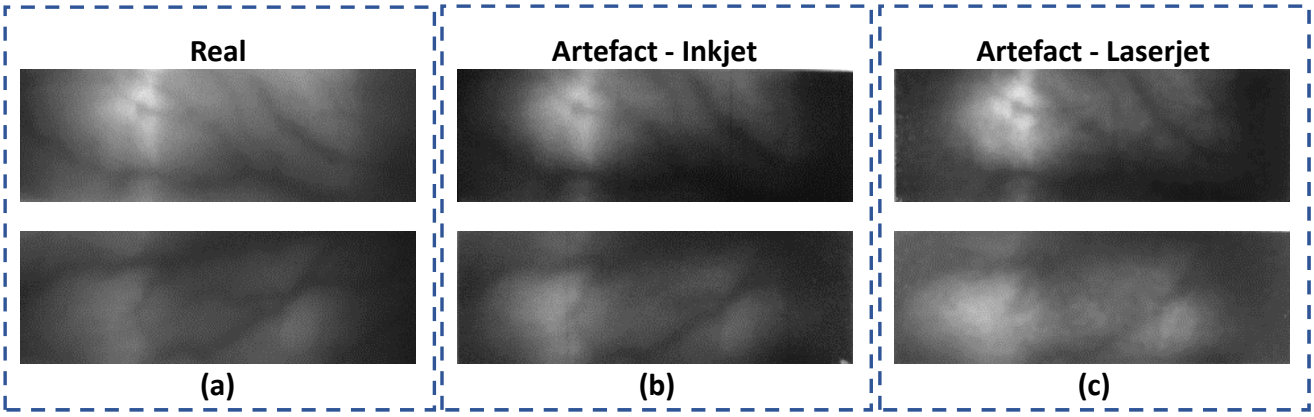

Figure 4: Comparison between real and artefact capture (a) Real Image (b) Inkjet print artefact (c) Laser print artefact

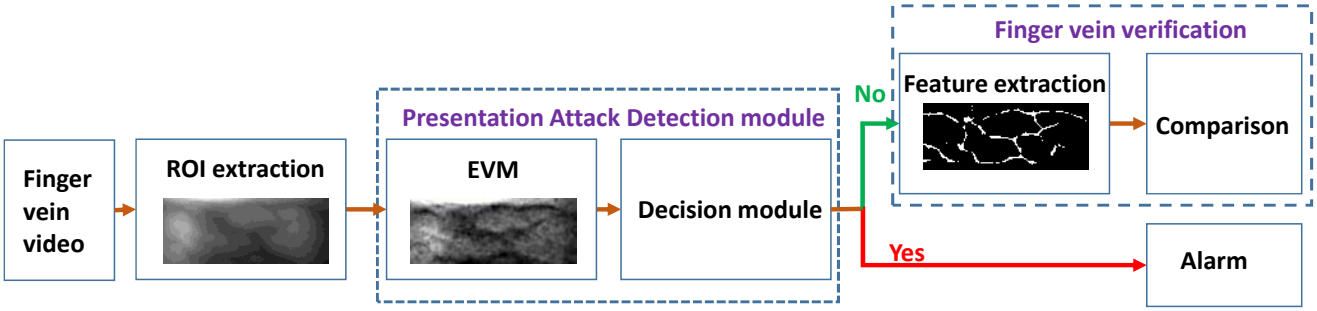

Figure 5: Block diagram of the proposed finger vein PAD scheme

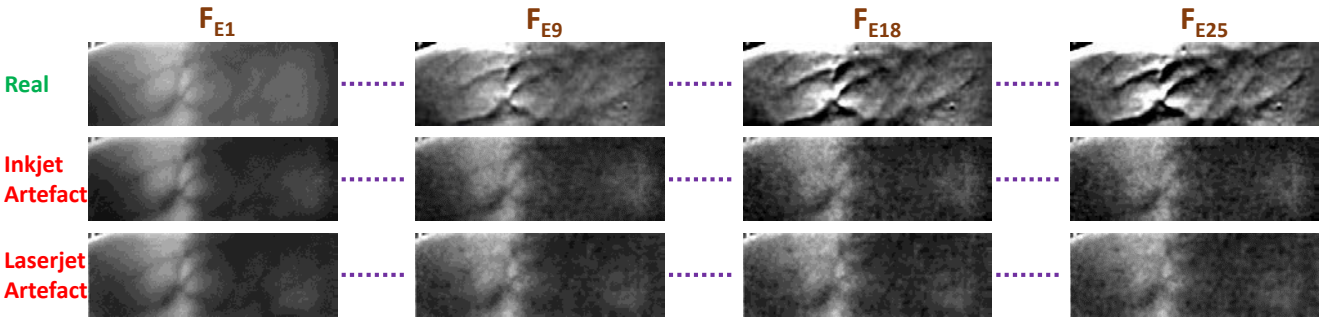

Figure 6: Qualitative illustration of the EVM motion magnification on real, inkjet print and laser print finger vein video

out by setting a pre-assigned rectangular area to cover the region of interest for the finger. The obtained ROI finger vein image Fr_{vn} is further re-sized to have a dimension of 100×300 pixels before passing it to the PAD module.

3.1. PAD module

The core idea of the proposed finger vein PAD module is to explore the motion of blood that flows through the finger vein F_v. To this extent, we employ the Eulerian Video Magnification (EVM) [11] that can amplify the inherent motion. The EVM algorithm is based on processing both temporal and spatial filtered information that can localise and magnify the inherent motion using Taylor expansion assumption. For each ROI frame Fr_{vn}, the first step involves in decomposing the ROI frame Fr_{v1} into spatial Laplacian bands which are then processed using an ideal temporal bandpass filter to isolate the desired temporal motion in each band. Finally, the isolated bandpass signal is then multiplied by an amplification factor α and added to the original signal. The motion magnification is depended on both filter and the value of the magnification factor α. In this work, we choose the α value as 250 based on the visual inspection of the processed finger vein frames from the training set. The value of α is kept constant throughout our experiment. Thus, the enhanced motion will provide a significant information on the liveness of the finger vein by magnifying the motion of the blood that flow through the finger vein. Let the EVM processed video corresponding to the input video F_v be denoted as $F_E = \{F_{E1}, F_{E2}, \ldots, F_{En}\}$.

Figure 6 shows the quantitative results of the motion magnification obtained using EVM algorithm on both real and artefact finger vein video at four different instances starting from Frame 1, Frame 9, Frame 18 and Frame 25. It is quite interesting to observe from Figure 6 that, the use of EVM on the real finger vein video shows a significant magnification of the blood flow by emphasizing the finger vein parts in the frames. Furthermore, the magnification of the blood flow increases with time as we can observe a most significant motion enhancement in the Frame 25 when compared to that of Frame 1. However, it is also interesting to observe at the same selected frames almost zero motion magnification in the case of the artefact finger vein videos. These qualitative results demonstrate the applicability of the EVM method for the finger vein liveness detection.

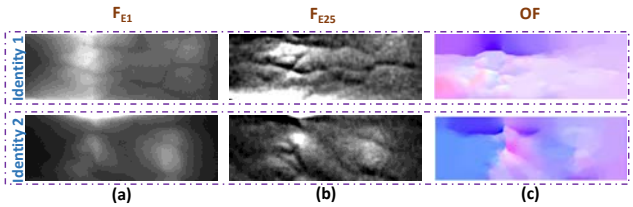

Figure 7: Qualitative results of motion features on real finger vein sample illustrated on two different finger vein videos (a) First frame (b) Last EVM frame (c) Motion computed using optical flow

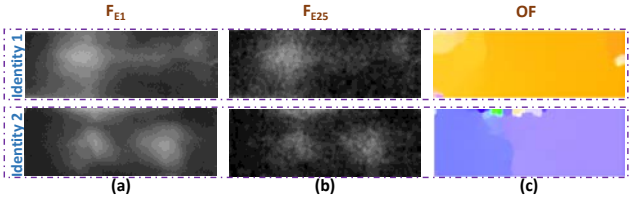

Figure 8: Qualitative results of motion features on inkjet print artefact finger vein sample illustrated on two different finger vein videos (a) First frame (b) Last EVM frame (c) Motion computed using optical flow

In the next step, we further process the motion magnification finger vein video F_v to classify each presented video as either real or artefact by extracting the motion-based features. We employ optical flow [4] to extract the motion-based features. The optical flow will compute the motion of each pixel by solving the optimisation problem. In this work, the successive over-relaxation (SOR) [4] is used to solve the optimisation problem due to its low computational complexity. However, computing the optical flow for every frame of F_E is highly computational. Thus, we propose to

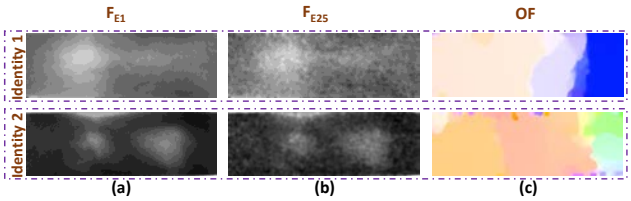

Figure 9: Qualitative results of motion features on laser print artefact finger vein sample illustrated on two different finger vein videos (a) First frame (b) Last EVM frame (c) Motion computed using optical flow

compute the optical flow between the first and last frame of F_E. Since the use of EVM requires a first couple of frames to enhance the motion, the use of the first frame F_{E1} represents the normal frame where the last frame F_{E25} represents the motion enhanced frame. Thus, it is our assertion that the optical flow computation between these two frames will provide a significant information about the motion of blood that can form the evidence of liveness of a captured finger vein characteristic. Figure 7 illustrates the qualitative results of the optical flow between F_{E1} and F_{E25} on real finger vein video where Figure 8 and 9 shows the qualitative results on inkjet print and laser print artefact finger vein video. Thus, one can observe the significant change in the motion magnitude (Figure 7 (c)) of the real presentation when compared with the artefact presentation (and Figure 8 (c) and 9 (c)). Finally, we obtain the final decision by simply comparing the motion magnitude to the preset threshold as follows:

$$[Mx, My] = OF(F_{E1}, F_{E25}) \tag{1}$$

Where, OF indicates the optical flow operation on the first frame F_{E1} and the last frame F_{E25}, Mx indicates the flow in horizontal direction and My indicates the flow in vertical direction.

$$Motion_{Mag} = \sum_j \sum_k \left(\sqrt{[(Mx)^2 + (My)^2]} \right) \tag{2}$$

Where, $Motion_{Mag}$ indicates the quantitative value of the motion magnitude, j indicates the number of rows and k indicates the number of columns.

$$D_e = \begin{cases} Real, & \text{if, } Motion_{Mag} \geq Th, \\ Attack, & \text{otherwise} \end{cases} \tag{3}$$

Where, D_e indicates the final decision and Th is the predetermined threshold value on the training set.

3.2. Finger vein verification

The finger vein verification system (or baseline system) employed in this work is based on the Maximum Curvature Points (MCP) [5] as a feature extraction and correlation as a comparator. This choice is made by considering the high performance and fewer computation characteristics exhibited by the MCP features [6].

4. Experiments and Results

This section describes the experimental protocols and the experimental results obtained by comparing the proposed scheme with four different state-of-the-art finger vein presentation attack detection algorithms.

4.1. Evaluation protocols

For the experiments, each finger is considered as a unique finger instance that will result in 300 unique samples. For each unique instance, we have collected two videos in two separate sessions. We then divided the whole database into two independent subsets namely: training and testing set. The training set is comprised of first 50 unique

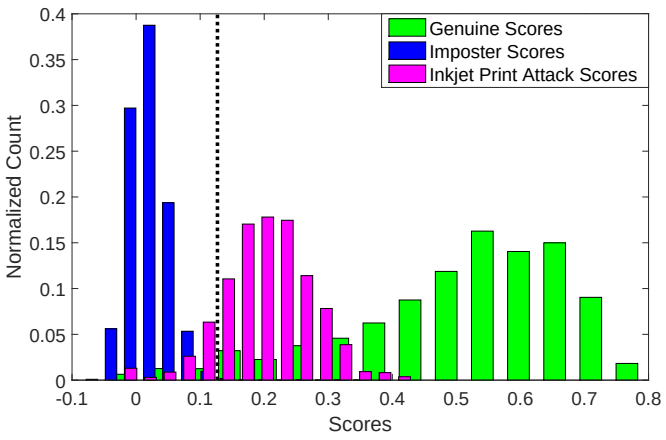

Figure 10: Score distribution with inkjet print artefact

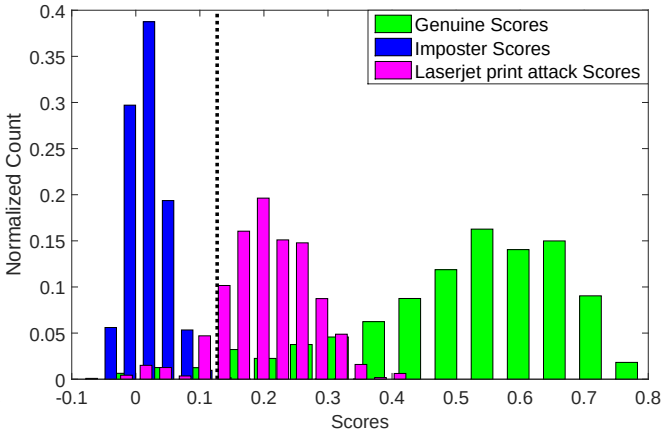

Figure 11: Score distribution with laser print artefact

instances and the testing set is comprised of remaining 250 instances. The training set is used for multiple purpose in this work that includes (1) To set the threshold value based on the Equal Error Rate ($EER\%$) for vulnerability analysis (2) Used to set the Threshold value Th (see Equation 3) with the proposed PAD scheme (3) used as the training set to evaluate the state-of-the-art finger vein PAD algorithms. The testing set is solely used to evaluate the performance of the proposed as well as state-of-the-art finger vein PAD schemes.

4.2. Results and discussion

We first present the vulnerability study on our GUC finger vein sensor [7] to 2 different kinds of finger vein print artefacts. The main goal of this vulnerability study is to obtain the Spoof False Acceptance Rate (SFAR$\%$) that indicates the applicability of the artefact samples collected in this work to spoof the sensor. To this extent, we consider the baseline finger vein recognition system that operates in two modes namely: *normal mode* and *attack mode* to obtain the comparison scores. In the normal mode, we have used one frame of a real video from the first session as the reference and we have used all 25 frames of a real video from the second session as the probe. This will generate $25 \times 250 = 6250$ genuine scores and $250 \times 249 \times 25 = 1556250$ zero-effort impostor scores. For the attack mode, we have used one frame of a real video (same image that we have used with normal mode) while the probe sample corresponds to the finger vein artefact video that is comprised of 25 frames. Thus, here also we have $25 \times 250 = 6250$ genuine scores and $250 \times 249 \times 25 = 1556250$ impostor scores.

Figure 10 shows the score distribution obtained on both normal and inkjet print artefact obtained using the baseline finger vein system. The black vertical line in Figure 10 and 11 indicates the threshold value obtained on the training dataset that corresponds to the EER value of the baseline finger vein system operating in the normal mode (i.e. with real presentation). As observed from the Figure 10, the inkjet print artefact scores lies between impostor and genuine scores of the real presentation and shows an SFAR of 90.62%. A similar observation can also be noted for the laser print finger vein artefact where the corresponding score distribution is shown in Figure 11. Here also it can be observed that spoof scores show significant overlapping with genuine and imposter scores obtained using real presentation and thereby indicating an SFAR of 91.87%. The obtained SFAR shows the vulnerability of the finger vein sensor to the artefacts generated in this work and thereby motivates the need for presentation attack detection (or countermeasure) techniques to mitigate these attacks.

In the following, we present and discuss the results obtained on the proposed PAD scheme on the finger vein verification system. The quantitative performance of the presentation attack detection algorithms are presented according to the ISO/IEC WD 30107-3 [3] in terms of: (1) Attack Presentation Classification Error Rate (APCER), which is defined as a proportion of attack presentation incorrectly classified as normal (or real) presentation (2) Normal Presentation Classification Error Rate (NPCER) which is defined as proportion of normal presentation incorrectly classified as attack presentation. Finally, the performance of the overall PAD algorithm is presented in terms of Average Classification Error Rate (ACER) such that,

$$ACER = \frac{(APCER + NPCER)}{2} \tag{4}$$

The lower the values of ACER, the better is the PAD performance.

Table 1: Performance of the proposed scheme on inkjet print artefact. (* reimplemented in Matlab)

Method	APCER (%)	NPCER (%)	ACER (%)
Riesz transform-SVM* [9]	9.20	84.40	46.8
LPQ+WLD-SVM * [9]	22.80	0.40	11.6
LBP-SVM * [9]	34.40	2.40	18.40
M-BSIF-SVM * [9]	20.00	5.60	12.80
Proposed scheme	**2.40**	**2.00**	**2.20**

Table 1 and 2 indicates the quantitative performance of the proposed method when compared to 4 different state-of-the-art schemes that was employed in 1st Competition on Counter Measures to Finger Vein Spoofing Attacks [9]. Since the state-of-the-art schemes are based on frame based feature extraction and learning, we have used the training set (see Section 4.1) that comprised of first 50 unique instances with video frames to train the SVM classifier. A final decision is obtained for the probe video by using majority voting that is, if the majority of the frames in the probe video is classified as a real then the probe video is considered as real - otherwise as an attack. However, the proposed scheme does not use any classifier based on learning, but it still requires to compute the value of a threshold Th (see Equation 3). We computed the threshold value using the training set incorporating real (or normal) finger vein video frames and kept constant on both types of artefacts used in this work. This further justifies the generalisation capability of the proposed scheme. Based on the quantitative results obtained on the inkjet print artefact as tabulated in Table 1, the proposed scheme outperforms the existing state-of-the-art schemes with the best ACER of 2.20%.

Table 2 shows the results obtained on the laser print finger vein artefact. Here also it can be observed that the proposed scheme outperforms the existing state-of-the-art schemes with the best ACER of 3.60%. Thus, based on

Table 2: Performance of the proposed scheme on laserjet print artefact. (* reimplemented in Matlab)

Method	APCER(%)	NPCER (%)	ACER (%)
Riesz transform-SVM * [9]	7.20	79.60	43.40
LPQ+WLD-SVM * [9]	13.20	1.60	7.40
LBP-SVM * [9]	10.00	6.00	8.00
M-BSIF-SVM * [9]	8.00	14.00	11.00
Proposed scheme	**5.20**	**2.00**	**3.60**

the above experiments it can be observed that the proposed scheme based motion magnification using EVM emerged as the best finger vein presentation attack detection algorithm. Kindly refer to http://youtu.be/aXEoS7u63XY for more comprehensive results.

5. Conclusion

A presentation attack detection algorithm in finger vein recognition must produce both a reliable and a robust solution to improve the practicality for finger vein biometrics. In this research, we present a novel solution to identify an attack on finger vein recognition based on magnifying the blood motion in the finger vein. The proposed method is tailored using Eulerian Video Magnification (EVM) to magnify the motion and optical flow to compute the motion features. We then used a simple classification scheme by comparing the motion magnitude obtained using optical flow to the pre-set value of the threshold Th. The pre-set threshold value is computed on the training set and kept constant on the testing set. Since the proposed method is based on the liveness measure by checking the blood flow, it can be generalised for any unseen attack. Extensive experiments are carried out on two different kinds of finger vein artefacts generated by printing a real finger vein images using laser and inkjet printer. A comparative evaluation is presented by evaluating the performance of the proposed scheme along with four different state-of-the-art schemes. The experimental results demonstrate the best performance of the proposed framework with the lowest ACER of ACER of 2.20% on inkjet print artefact and ACER of 3.60% on laser jet print artefact.

References

[1] Finger Vein description. http://www.mofiria.com/en/about. Accessed: 2015-04-04.

[2] J. Galbally, S. Marcel, and J. Fierrez. Biometric antispoofing methods: A survey in face recognition. *IEEE Access*, 2:1530–1552, 2014.

[3] ISO/IEC JTC1 SC37 Biometrics. *ISO/IEC WD 30107-3:2014 Information Technology - presentation attack detection - Part 3: testing and reporting and classification of attacks*. International Organization for Standardization, 2014.

[4] C. Liu, W. T. Freeman, E. H. Adelson, and Y. Weiss. Human-assisted motion annotation. In *Computer Vision and Pattern Recognition, IEEE Conference on*, pages 1–8, 2008.

[5] N. Miura, A. Nagasaka, and T. Miyatake. Extraction of finger-vein patterns using maximum curvature points in image profiles. *IEICE Transactions on Information and Systems*, 90(8):1185–1194, 2007.

[6] R. Raghavendra, K. Raja, J. Surbiryala, and C. Busch. Finger vascular pattern imaging; a comprehensive evaluation. In *Asia-Pacific Signal and Information Processing Association, 2014 Annual Summit and Conference (APSIPA)*, pages 1–5, Dec 2014.

[7] R. Raghavendra, K. B. Raja, J. Surbiryala, and C. Busch. A low-cost multimodal biometric sensor to capture finger vein and fingerprint. In *International Joint Conference on Biometrics (IJCB)*, pages 1–7, Sep 2014.

[8] C. Sousedik and C. Busch. Presentation attack detection methods for fingerprint recognition systems: a survey. *IET Biometrics*, 3(4):219–233, 2014.

[9] P. Tome, R. Raghavendra, C. Busch, S. Tirunagari, N. Poh, B. H. Shekar, D. Gragnaniello, C. Sansone, L. Verdoliva, and S. Marcel. The 1st competition on counter measures to finger vein spoofing attacks. In *The 8th IAPR International Conference on Biometrics (ICB)*, May 2015.

[10] P. Tome, M. Vanoni, and S. Marcel. On the vulnerability of finger vein recognition to spoofing. In *International Conference of the Biometrics Special Interest Group (BIOSIG)*, pages 1–10, Sept 2014.

[11] H.-Y. Wu, M. Rubinstein, E. Shih, J. Guttag, F. Durand, and W. T. Freeman. Eulerian video magnification for revealing subtle changes in the world. *ACM Trans. Graph. (Proceedings SIGGRAPH 2012)*, 31(4), 2012.