Texture-based Finger Vein Presentation Attack Detection with Optimal Gray Level Co-Occurrence Matrix Features and Light-GBM

Kashif Shaheed
Department of Multimedia Systems, Faculty of Electronics, Telecommunication, and Informatics, Gdańsk University of Technology, Gdańsk, Poland *kashif.shaheed@pg.edu.pl*

Piotr Szczuko
Department of Multimedia Systems, Faculty of Electronics, Telecommunication, and Informatics, Gdańsk University of Technology, Gdańsk, Poland *piotr.szczuko@pg.edu.pl*

Inam Ullah
School of Computer Science and Engineering, Shandong Jianzhhu University, Jinan, Shandong China *inamullah538@sdjzu.edu.cn*

Hammed Adeleye Mojeed
Department of Computer System Architecture, Faculty of Electronics, Telecommunication and Informatics, Gdańsk University of Technology
Gdańsk, Poland *hammed.mojeed@pg.edu.pl*
Department Department of Computer Science, University of Ilorin,
Ilorin, Nigeria *mojeed.ha@unilorin.edu.ng*

Abdullateef Oluwagbemiga Balogun
Department of Computer and Information Science, Universiti Teknologi PETRONAS, Bandar Seri Iskandar, 32610 Perak, Malaysia *abdullateef.ob@utp.edu.my*

Luiz Fernando Capretz
Department of Electrical and Computer Engineering, Western University, London, Ontario, N6A 5B9, Canada *lcapretz@uwo.ca*

Abstract

Presentation Attack Detection (PAD) is crucial in biometric finger vein recognition. The susceptibility of these systems to forged finger vein images is a significant challenge. Existing approaches to mitigate presentation attacks have computational complexity limitations and limited data availability. This study proposed a novel method for identifying presentation attacks in finger vein biometric systems. We have used optimal Gray-Level Co-occurrence Matrix (GLCM) features with the Light-Gradient Boosting Machine (LGBM) classification model. We use statistical texture attributes, namely, energy, correlation, and contrast, to extract optimal features from counterfeit and authentic finger-vein images. The study investigates cluster-pixel connectivity in finger vein images. Our approach is tested using K-fold cross-validation and compared to existing methods. Results demonstrate that Light-GBM outperforms other classifiers. The proposed classifier achieved low APCER values of 2.73% and 8.80% compared to other classifiers. The use of Light-GBM in addressing presentation attacks in finger vein biometric systems is highly significant.

Keywords: Presentation Attack Detections, Finger Vein Recognition, Biometric, Machine

Learning, Spoof Attack Detection

1. Introduction

Biometric technology is rapidly expanding and has become a prominent part of our daily lives. Biometric authentication could be used in healthcare systems for patient identification and health data protection. Biometric systems identify individuals automatically based on their biological and behavioural characteristics. Various biometric methods are employed for user identification, including but not limited to fingerprint [19], facial [13], and iris [3] recognition techniques. Among the most promising and widely adopted forms of biometrics is finger-vein recognition, owing to its unique and immutable patterns and high resistance to alteration or forgery [4]. Furthermore, each finger's vein pattern is entirely distinct and permanent, making it a highly reliable and secure modality for biometric identification purposes [1]. Despite the high success rate of finger vein recognition methods for authentication, these techniques have limitations. Finger Vein Recognition (FVR) encounters two significant challenges: the influence of image-acquiring conditions and the potential risk of spoofing attacks. Previous studies have emphasized the crucial role of image-acquiring conditions in authentication performance, underscoring its significance.

Several research endeavors have focused on improving the quality of finger-vein images to enhance the efficiency of finger vein recognition technology [5], [11], [18], [23]. These efforts have aimed to enhance the accuracy of finger vein recognition systems for improved security. Fortunately, due to extensive research, the adverse impacts of these challenges have been substantially reduced. Various studies have confirmed that biometric systems are vulnerable to presentation attacks, such as the use of counterfeit images and the presence of spoofing attacks. According to recent studies [2], [7], FVR classification is susceptible to presentation attacks involving printed graphics that mimic FV sensors and enable unauthorized access to individuals and any identification management system. Consequently, it is imperative to implement appropriate measures to enhance the security of the FVR system against such attacks. Figure 1 provides a visual example of both finger vein spoof and real images. Ensuring the safety of FV technology for deployment in sensitive areas like finance, immigration, and access control systems is of utmost importance. To achieve this, verifying and confirming the effectiveness of the technology's security measures is crucial. Once this has been accomplished, FV technology can be trusted to perform effectively in these critical domains.

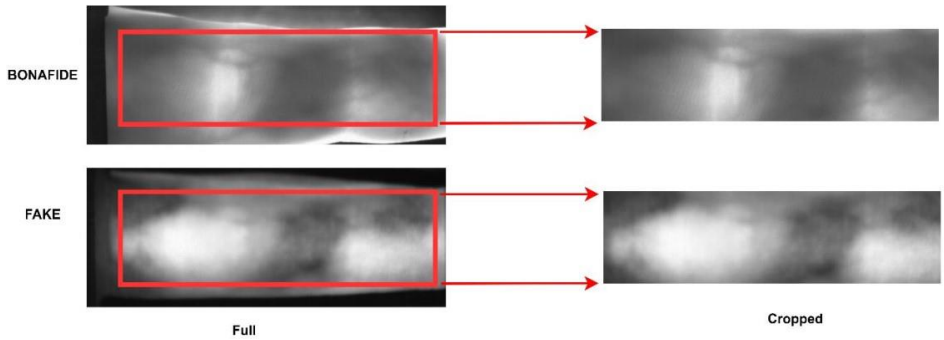

Fig. 1. A visual example of a fake and bonafide image in a complete and cropped scenario.

Recently, a novel biometric authentication method known as the FVR system has undergone significant improvement and validation for its effectiveness [21, 22]. Compared to other biometric verification techniques, the FV biometric authentication method reliably establishes a person's identity by utilizing the unique blood vessel patterns beneath the skin of their fingers. However, capturing finger vein features can be challenging due to the need for a near-infrared light source, which minimally impacts the skin's condition. Despite advancements in the FVR system, it remains susceptible to exploitation through compromised finger-vein images. Studies conducted in [13] and [14] have demonstrated

that spoofing attacks can be executed by creating printed FV images on various media, such as paper or film, and applying them to a real finger during image acquisition using carbon-based ink. To prevent deceptive actions and uphold the authenticity of biometric information, it is imperative to incorporate Presentation Attack Detection (PAD) schemes into FV biometric technology. This measure is a crucial safeguard against spoofing attacks, thereby preserving the integrity of the FVR system.

Considering the manifold challenges associated with deep learning and conventional finger vein PAD methods, such as limited amounts of labeled data, inherent complexity, and performance improvement problems, our study uses various machine learning classifiers. Specifically, we leverage optimal GLCM features for finger vein PAD and evaluate the performance of diverse machine learning models in addressing this issue.

Our proposed methodology differs from earlier approaches by including four distinctive aspects listed below.

1. The study presents a new method for detecting presentation attacks in FV biometric systems. It utilizes GLCM features and LGBM for classification. This method effectively tackles challenges in PAD methodologies like dataset scarcity.
2. To achieve optimal feature extraction from the spoof and genuine finger-vein images, we employ an approach that leverages specific GLCM characteristics. In particular, we utilize Energy, Correlation, and Contrast characteristics in our Optimal GLCM technique. Notably, this marks the first application of the Optimal GLCM technique for feature extraction in finger veins to detect presentation attacks.
3. The Light-GBM classification model and K-fold cross-validation are used to categorize finger vein presentation attacks. The model was chosen for its fast training, accurate prediction performance, and efficiency in classification tasks. Various performance criteria were used to test the IDIAP and SCUT-FVD PAD benchmarks. A comparative analysis is presented to compare the effectiveness of the suggested approach to existing machine learning techniques.

2. Related works

Early studies on PAD primarily relied on traditional heuristic-based methods. For instance, Qin et al. [9] conducted pioneering research in this field, utilizing dynamic data from successive images to authenticate genuine finger vein (FV) images. This approach was grounded in the observation that subtle changes in vein pattern size occur as the heart rate fluctuates. Nguyen et al. [8] explored FV images in spatial and frequency domains, employing Fourier and wavelet transforms. Their method incorporated frequency data to identify potential fraudulent activities associated with finger veins. A set of procedures for PAD in FV images was proposed in [17]. In [24], several algorithms have been proposed for PAD in FV images, such as the usage of average vertical energy, utilization of binarized statistical image features (BSIF) and SVM, as well as the Fourier spectrum, the use of a monogenic scale space-based global descriptor, and the usage of an application of a local binary pattern (LBP). Raghavendra & Busch [12] and Tirunagari et al. [16] introduced the use of windowed dynamic mode decomposition (DMD) and a steerable pyramid feature to mitigate presentation attacks, surpassing traditional PAD approaches like Local Binary Pattern (LBP) and Binary Structural Similarity Index (BSIF) in performance. Qiu et al.[10] demonstrated the use of blurring and noise dispersion to detect presentation attacks. They applied a total variation regularization approach to extract noise information and utilized the Local Binary Pattern (LBP) descriptor to remove uneven brightness distribution from the finger vein region. Then, these features were input into the Support Vector Machine (SVM) model for data classification, achieving an impressive 0% Attack Presentation Classification Error Rate (APCER). Another study [2] focused on determining the optimal set of presentation attack features by fine-tuning hyperparameters for LBP. This research aimed to extract valuable information from images to detect presentation attacks. The study reported that the most effective result for APCER and BPCER was less than 0.5%. Another conventional FV presentation attack detection method, based on a hybrid FV texture analysis space, was detailed in the reference [1]. It involved preprocessing images using

the watershed algorithm for segmentation and extracting textural statistics from finger vein images. Multiple feature spaces, including grayscale and color regions, were analyzed using a Histogram of Oriented Gradients (HOG). Photo classification was carried out using the SVM algorithm, resulting in an ACER of less than 0.60%. The latest investigation of finger veins incorporated the PAD technique [15], focusing on threat analysis utilizing various feature and matching strategies from prior studies on the SCUT-FVD and IDIAP datasets. The experiment in this study concluded that score-level combinations from various matching algorithms could be effectively employed for PAD. All the methods mentioned above were traditional approaches.

A few research have employed deep learning methods to detect presentation attacks in finger vein images. For instance, Nguyen et al. [8] used a deep learning architecture for finger vein presentation attacks for the first time. The VGG-16 Network model was initially employed in this work to extract characteristics from photos. Next, use the Principal Component Analysis (PCA) approach to minimize the feature's dimension. Lastly, the classification operation is performed using an SVM classifier. However, compared to the prior method, this one is more complex and requires much computation. Another work [20] uses a multi-tasking strategy to combine the recognition and anti-spoofing tasks into a single CNN model, focusing on finger vein recognition and presentation attack detection. They employed an embedded system with a multi-intensity illumination strategy approach to automatically determine the most useful feature for finger vein identification. Yet, there is still a problem with the system's computational complexity, which compromises the proposed work's reliability.

Our proposed methodology presents a unique approach to mitigating presentation threats in finger vein (FV) biometric systems, distinguishing it from prior methodologies in various aspects. We outline an innovative approach for integrating optimal Gray-Level Co-occurrence Matrix (GLCM) attributes with the Light Gradient Boosting Machine (LGBM) machine-learning classification model. This innovative fusion effectively addresses the limitations of previous methodologies, such as limited dataset availability. Subsequently, we leverage specific GLCM attributes - Energy, Correlation, and Contrast - to extract characteristics from both authentic and counterfeit finger-vein images, marking the inaugural implementation of the Optimal GLCM technique in this domain.

3. Methodology

In the following section, we aim to explain the methodology we have meticulously employed to detect presentation attacks on finger vein patterns. To facilitate a better understanding of our approach, we have included a flowchart of our work in Figure 2. The proposed approach implemented in our work is presented in Algorithm 1.

Algorithm 1: Finger vein presentation attack detection by using Optimal GLCM features and Light-GBM classifier

1. Preprocess image, i.e., image=X, and the Preprocessing step is applied by using:
    1.1 Reshape image (X) to Desired shape to remove the irregular detail.
    1.2 Remove Noise using the Gaussian smoothing operator and
    1.3 *Enhance the local contrast using the CLAHE enhancement method.*

2. Extract Features:
   The optimal texture feature of GLCM is used, including Contrast, Energy, and Correlation, and we keep the distance 1 and 5, angle=0, to reduce the computational complexity in feature contraction using GLCM.
3. *Classification uses the output of previous feature extraction map steps, and the Light-Gradient Boosting Machine Learning classifier is used to classify the images into Bonafide and Presentation Attack.*
4. *Validation: K-Fold Cross-validation approach is used to validate the performance of the proposed method*
5. *Evaluation: Several performance metrics and machine learning were used to evaluate the proposed model's performance comprehensively.*

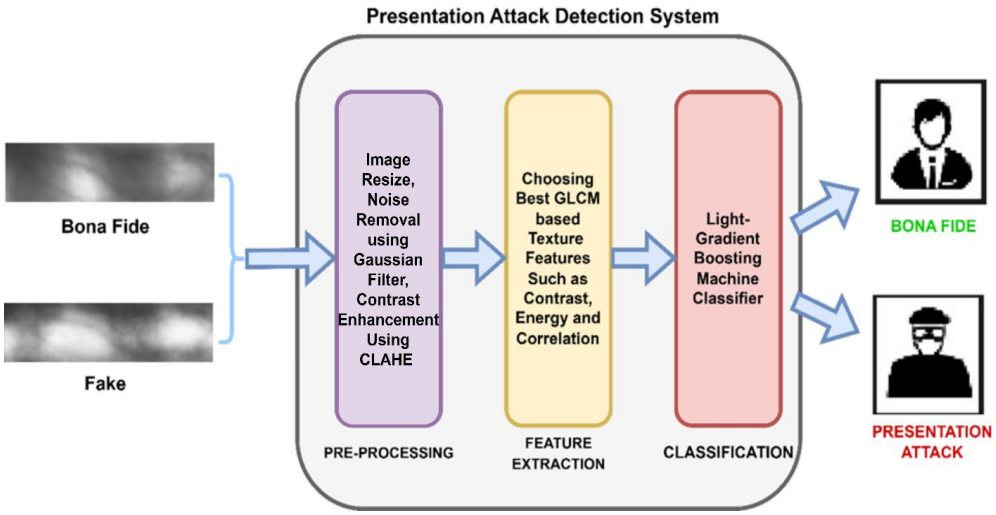

Fig. 2. A systematic framework of the proposed work.

3.1. Preprocessing

The preprocessing stage is critical for detecting and correcting image errors. It is especially crucial for finger vein images, which often have noise and low contrast. Our process for data preparation includes simple actions such as scaling and noise reduction. Resizing datasets guarantees that they meet model criteria and remain consistent in size by removing unnecessary elements from the images.

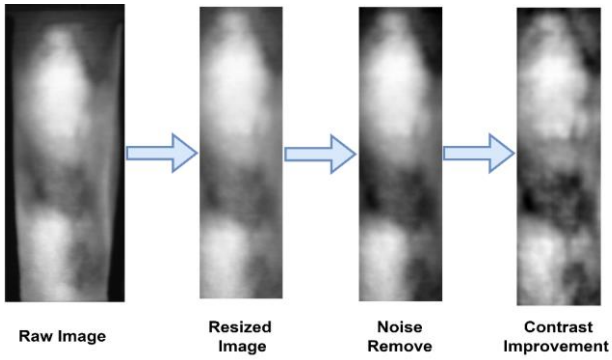

Fig. 3. A systematic framework of the proposed work.

3.2. Feature Extraction

This study identified the optimal combination of statistical GLCM features from finger vein images, encompassing energy, correlation, and contrast. To derive these statistical texture qualities, we have implemented a second-order method that considers the connectivity of clustered pixels in an image of finger veins, denoted as image I. This approach has found widespread application across diverse fields and applications.

To build a GLCM, we calculate the time for every couple of quantized gray levels to appear as neighbours in the quantized image. Each element of the GLCM can be calculated in more technical terms as follows.

$$P_{ij} = \sum_{k=1}^{K}\sum_{t=1}^{T}\{1, \quad If \quad QI(k,t) = i, QI(k+\Delta x, t+\Delta y) = j, 0, \tag{1}$$

Otherwise, where $\delta = (\Delta x, \Delta y)$ represents a displacement vector in pixels along the x- and y-axes, i and j represent the rows and columns of the matrix, and k and t represent the intensities of pixels. One thing to remember is that a GLCM feature vector can be produced by combining a variety of displacement vectors. For example

$$\begin{aligned}\Delta_{0^\circ} &= (1,0)\\ \Delta_{45^\circ} &= (1,1)\\ \Delta_{90^\circ} &= (0,1)\\ \Delta_{135^\circ} &= (-1,-1)\end{aligned} \tag{2}$$

If the feature vector is inverted, the result is

$$\begin{aligned}\Delta_{0^\circ} &= (-1,0)\\ \Delta_{45^\circ} &= (-1,-1)\\ \Delta_{90^\circ} &= (0,-1)\\ \Delta_{135^\circ} &= (1,-1)\end{aligned} \tag{3}$$

GLCM captures the frequency of similar patterns from various angles, extracting discriminative information from input images. Figure 4 [4] illustrates the GLCM calculation process. It consists of two matrices: the transformation matrix and the host image matrix. For instance, consider a pair of pixels at coordinates (2, 2) in the host image. Looking at a distance of one and an angle of zero, we can identify three red-highlighted positions in the matrix. Consequently, the transformation matrix should represent this pixel pair as three. We can also generate pixel pairs for other cases using a similar method.

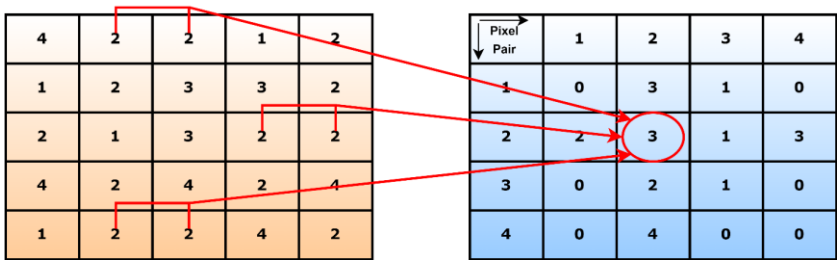

Fig. 4. An example of GLCM calculation.

To reduce computing complexity in this research, we employed a perfect set of features with a distance of 1 and an angle of 0. Below is a description of them:

Energy: Homogeneity in digital image processing relates to uniform grey-level distribution. It is quantified through the GLCM attributes.

$$Energy = \sum_{a,b}^{N-1}(P_{a,b})^2 \tag{4}$$

Correlation: This metric is used to determine authenticity in finger vein images. Correlation values assist with biometric authentication by discriminating between attacks. Correlation in images measures pixel relationships. It specifies the GLCM's correlation features.

$$Correlation = \frac{\sum_{a,b}^{N-1}(a,b)p(a,b)-\mu_a\mu_b}{\sigma_a\sigma_b} \tag{5}$$

Contrast: Contrast in images estimates the intensity of neighbouring pixels. Low-contrast images show low-frequency distributions. GLCM contrast is related to spatial frequencies, not grey levels.

$$Contrast = \sum_{i,j=0}^{N-1} P_{ij}\,(i-j)^2 \tag{6}$$

3.3. Light Gradient Boosting Classifier

The Gradient-Boosting Decision Tree (GBDT) is a widely adopted machine learning technique with efficient implementations like XGBoost and parallel Gradient-Boosted Regression Trees (pGBRT) [29][30]. These implementations include numerous

engineering optimizations but have relatively limited efficiency and scalability, especially when dealing with high-dimensional feature spaces and large datasets. A significant factor contributing to this limitation is the extensive computation time required to assess all data records for each feature to determine potential split points. As a solution to these challenges, Ke et al. [31] introduced Light-GBM, designed for efficient distributed computing, employing two distinct techniques: gradient-based one-sided sampling (GOSS) and exclusive feature bundling (EFB). The Light Gradient Boosting Machine (LGBM) is a machine learning algorithm that utilizes tree-based learning methods. The authors leverage two innovative methodologies, GOSS and EFB, to enhance the flexibility and efficiency of their approach [31]. GOSS evaluates information access by discarding a substantial portion of data instances with minor gradients. GOSS can accurately estimate information access even with a small dataset because instances with higher gradients are pivotal in the assessment.

EFB is used to group exclusive features to reduce their number. LGBM, a Gradient Boosting Decision Tree algorithm, provides various advantages like speed, efficiency, memory reduction, and support for parallel processing. LGBM is a high-performance algorithm based on decision trees that are suitable for tasks like ranking and classification. LGBM's leaf-wise tree-splitting strategy is a distinguishing feature compared to other algorithms. This algorithm eliminates more loss and achieves higher accuracy than level-wise tree-splitting. These unique features make LGBM stand out from other boosting techniques. Table 1 represents the hyperparameters used in our proposed model.

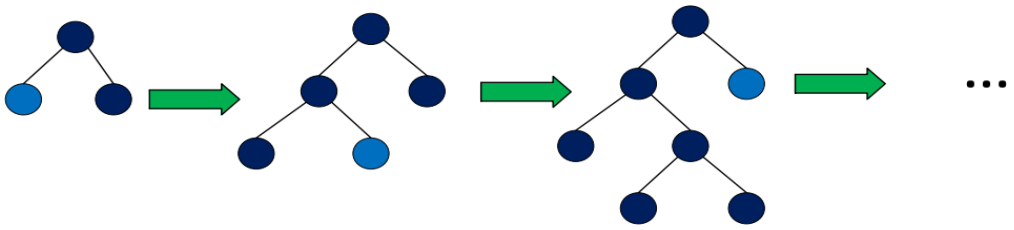

Fig. 5. Leaf-wise tree growth in LGBM [6].

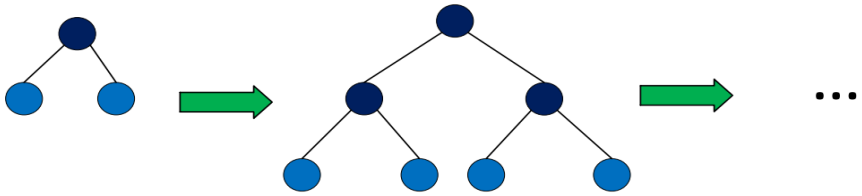

Fig. 6. Level-wise tree growth in other boosting algorithms[6].

Table 1. Hyperparameters are used in the Light-GBM model.

Learning Rate	Number of Leaves	Boosting Type	Metric
0.13	20	GBDT	Binary_Logloss

4. Experimental results and analysis

We have employed three distinct metrics: the Bona Fide Presentation Classification Error Rate (BPCER), the Attack Presentation Classification Error Rate (APCER), and the Average Classification Error Rate (ACER). To quantify these metrics, we have employed the equations provided below.

$$\mathrm{APCER} = 1 - \left(\frac{1}{\mathrm{Num_{PA}}}\right) \sum_{i=1}^{\mathrm{Num_{PA}}} (\mathrm{R_i}) \tag{7}$$

$$BPCER = \left(\frac{\sum_{i=1}^{Num_{BF}}(R_i)}{Num_{BF}}\right) \tag{8}$$

$$ACER = \frac{APCER+BPCER}{2} \tag{9}$$

In the above equations, Num_{PA} denotes the number of presentation attacks for the given presentation attack instrument species. Num_{BF} denotes the quantity of bona-fide presentations, and *Ri* takes the value of 1 if the i^{th} presentation is classified as an attack presentation and a value of 0 if it is classified as a bona-fide presentation. As shown by these equations, decreased values of APCER and BPCER indicate improved detection performance.

The model's performance suggested in this study was additionally evaluated through the utilization of widely accepted and standardized assessment metrics, which consist of accuracy, precision, recall, and f-score (F1). It is important to note that these metrics are defined in the following manner.

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive+False Positive}} \tag{10}$$

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive+False Negative}} \tag{11}$$

$$\text{F1} - \text{score} = 2 \times \frac{\text{Precision} \times \text{recall}}{\text{Precision} + \text{recall}} \tag{12}$$

$$\text{Accuracy} = \frac{\text{True Postive+True Negative}}{\text{True Positive+False Positive+True Negative+False Negative}} \tag{13}$$

According to the above equations, True Positive represents the number of correctly predicted positive sample outcomes, True Negative represents the number of correctly predicted negative sample outcomes, and False Negative indicates the number of incorrectly predicted positive sample outcomes. False Positive represents the number of incorrectly predicted negative sample outcomes.

In this study, three primary experiments were conducted. The first experiment aimed to identify the best feature combination and confirm the top three GLCM features out of the five available for the PAD task in the finger vein biometric system. This evaluation was performed on the IDIAP [17, 25] and SCUT-FVD[24] datasets. A total of 880 images were used from IDIAP and 1000 images from SCUT-FVD. Among 880 images from VERA, 440 were fakes, and 440 were genuine. And, among 1000 images in SCUT-FVD, 500 were fake, and 500 were real. In the second experiment, we assessed the effectiveness of the proposed model using these three optimal features. Lastly, the third experiment focused on evaluating the performance of various Machine Learning models to enhance the overall performance of the PAD system.

4.1 Performance of machine learning algorithms on all features

In this experimental study, we will assess the performance of GLCM features such as Energy, Correlation, Dissimilarity, Homogeneity, and Contrast to understand how individual classifiers perform. Figure 7 shows varying accuracy levels among the classifiers used. The energy texture feature of GLCM performed exceptionally well, while other features had consistent performance. Determining the best features for accuracy with machine learning classifiers using the IDIAP dataset is challenging.

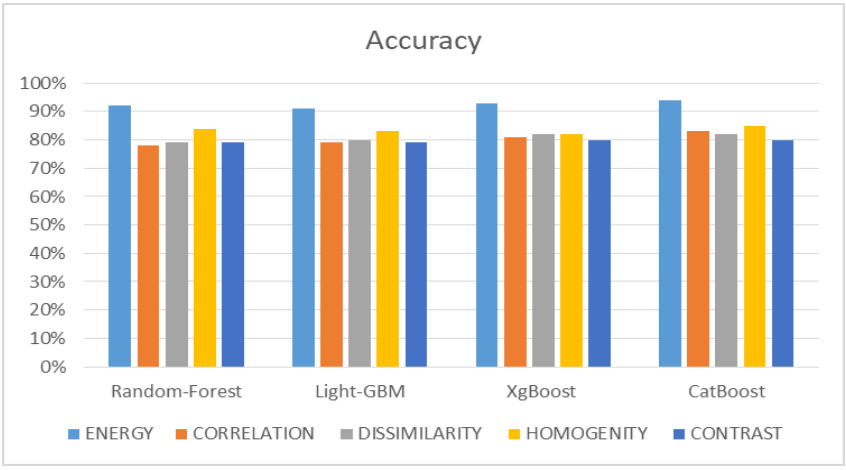

Fig. 7. Accuracy of various Machine Learning Models employing distinct features

As illustrated in Figure 8, different classifiers yield varying levels of precision when employing a variety of distinct features on the SCUT-FVD presentation attack finger vein dataset. It has come to our attention that diverse features produce differing outcomes with machine learning classifiers. However, it remains challenging to determine which specific feature performs optimally across all machine learning classifiers. Therefore, our upcoming experiment will focus on identifying the most optimal combination of features for the classification task.

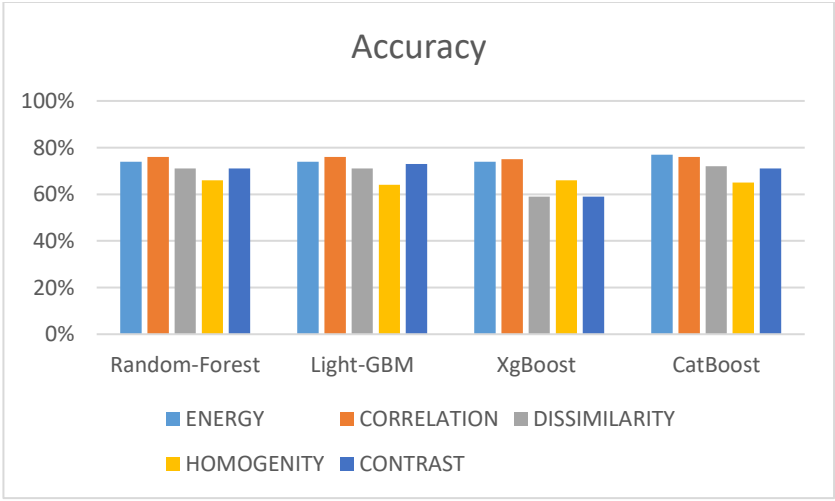

Fig. 8. Accuracy of various Machine Learning Models employing distinct features

In this experiment, we meticulously evaluated feature accuracy across various datasets and different machine-learning classifiers. Upon analyzing Figure 9, presented below, we observed that the Energy and Correlation features achieved an average accuracy of 84% and 78%, respectively. Furthermore, the Contrast feature also outperformed Homogeneity and Dissimilarity in terms of accuracy. Consequently, this experiment confirmed that Energy, Correlation, and Contrast features yield the best results regarding machine learning classifier accuracy.

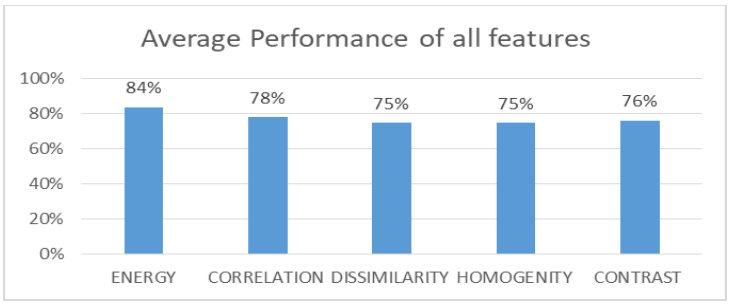

Fig. 9. The accuracy of different machine learning models using various features across two datasets.

4.2 Performance of ML algorithms on optimal features

Figure 9 shows that XGBoost performs poorly on the IDIAP dataset compared to other classifiers. Random forest does somewhat worse than CAT Boosting and Light-GBM. CAT Boosting and XGBoost perform similarly under k-fold cross-validation. Figure 10 shows that XGBoost performs worse than other classifiers on the IDIAP dataset. Random forest underperforms CAT Boosting and LGBM. CAT Boosting and XGBoost perform similarly under k-fold cross-validation. Light-GBM and CAT Boosting perform better on the IDIAP dataset than Random Forest and XGBoost.

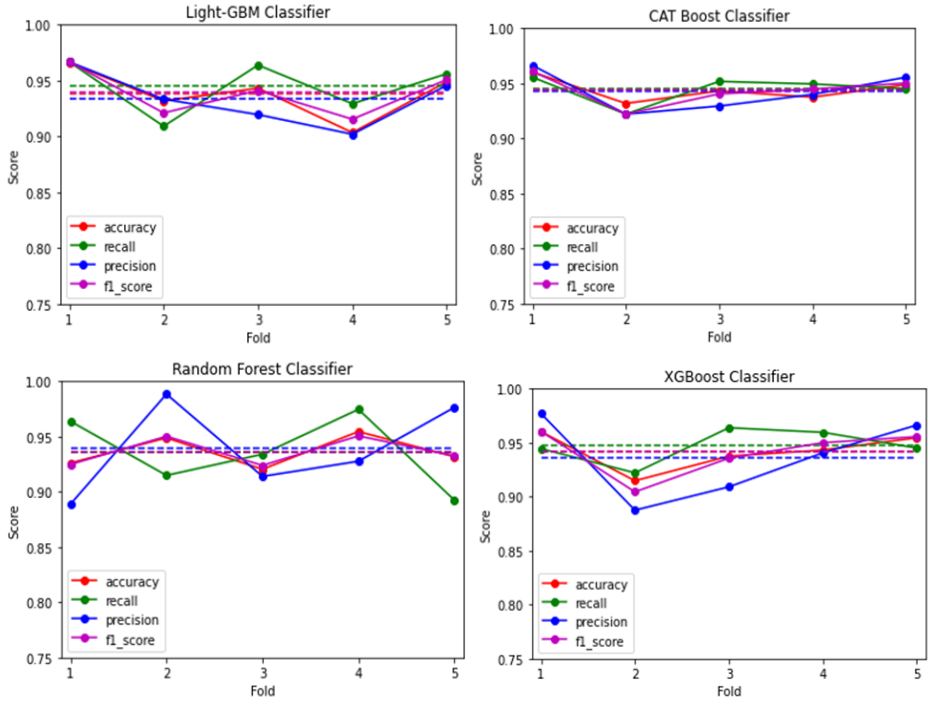

Fig. 10. Performance comparison of different machine learning classifiers using optimal features

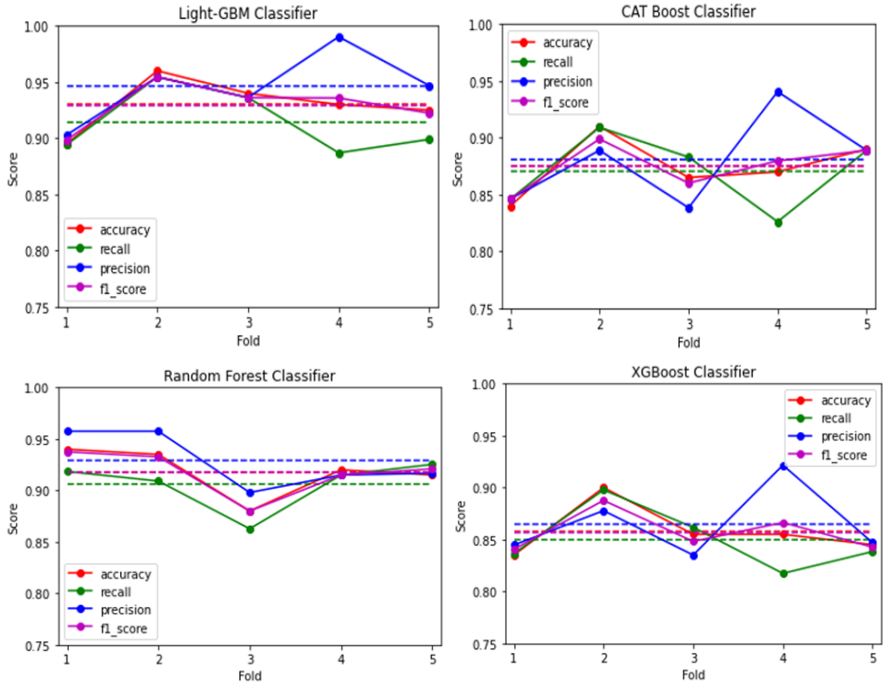

Fig. 11. Performance comparison of different machine learning classifiers using optimal features

Figure 11 demonstrates that XGBoost performs poorly compared to other machine learning classifiers. Random Forest and LGBM outperform CAT Boosting. Using k-fold cross-validation, Random Forest underperforms LGBM. LGBM outperforms all other

classifiers on the SCUT-FVD dataset. LGBM outperforms other models' predictions for accuracy, precision, recall, and F1 score on the IDIAP and SCUT-FVD datasets. Light-GBM is proposed for biometric finger vein recognition to address the presentation attack issue.

From Figure 11, we conclude that the Light GBM classifier demonstrates impressive performance on the SCUT-FVD dataset, outperforming the Random Forest, XGBoost, and CAT Boosting classifiers across all performance measures. Therefore, we can confidently conclude that the LGBM classifier's performance is outstanding in the IDIAP and SCUT-FVD datasets.

4.3 Performance evaluation using presentation attack metrics using IDIAP and SCUTFVD dataset

Experiment 3 aims to assess a classifier for finger vein biometrics against presentation attacks, focusing on APCER, BPCER, and ACER metrics. The classifier is tested on IDIAP and SCUT-FVD datasets with a 75%-25% split ratio. The Light-GBM classifier performs excellently, with APCER, BPCER, and ACER values of 2.73%, 12.73%, and 7.73% on the IDIAP dataset, surpassing other classifiers. The random forest classifier also exhibited reasonable performance. Table 2. Illustrate the performance of our proposed method using IDIAP dataset.

Table 2. Finger vein presentation attack detection performance on the IDIAP dataset

Model	**APCER (%)**	**BPCER (%)**	**ACER (%)**
Random Forest	2.73	13.64	8.18
XgBoost	6.36	12.73	9.55
Cat Boosting	5.45	10.91	8.18
Proposed (Light-GBM)	**2.73**	**12.73**	**7.73**

We also evaluated our proposed classifier using the SCUTFVD dataset. Table 3 clearly demonstrates the impressive performance of our approach compared to other classifiers. Our proposed classifier reported an APCER of 8.80%, BPCER of 11.20%, and ACER of 10.00%, showcasing the effectiveness of our method compared to other classifiers.

Table 3. Finger vein presentation attack detection performance on the SCUTFVD dataset

Model	**APCER (%)**	**BPCER (%)**	**ACER (%)**
Random Forest	10.40	36.00	23.20
XgBoost	12.00	32.80	22.40
Cat Boosting	10.40	22.40	16.40
Proposed (Light-GBM)	**8.80**	**11.20**	**10.00**

5. Discussion

PAD, which stands for Presentation Attack Detection, is a highly significant and pressing concern within the realm of biometric finger vein recognition systems. The current study introduces a novel and sophisticated approach to effectively identify and thwart presentation attacks within FV biometric systems. The method put forth in this research capitalizes on the myriad benefits offered by optimal GLCM features, strategically combined with the utilization of LGBM for the purpose of machine-learning-based classification.

The experimental investigation conducted within the scope of this study encompassed a thorough and detailed evaluation of GLCM features alongside an array of different machine learning classifiers utilizing both the IDIAP and SCUTFVD datasets. Upon scrutinizing the IDIAP dataset, it was observed that various classifiers showcased diverse levels of accuracy, with some features maintaining a consistent performance level throughout the analysis, as visually depicted in Figure 7. To further enhance the feature selection process, an additional experiment was carried out, the findings of which are illustrated in Figure 9. An intriguing

observation was made regarding the Random Forest classifier, which exhibited a marginally lower performance compared to CAT Boosting and Light-GBM, as illustrated in Figure 10. Furthermore, the examination through k-fold cross-validation unveiled that CAT Boosting and XGBoost displayed relatively similar performance across all metrics, albeit XGBoost fell short compared to the other models. Significantly, the CAT Boosting classifier also displayed a weaker performance when juxtaposed with the Random Forest and Light-GBM classifiers. This discovery underscores the exceptional performance delivered by the Light-GBM classifier across the IDIAP and SCUT-FVD datasets, excelling in numerous evaluation metrics, including accuracy, precision, recall, and F1-score.

6. Conclusion and Future Work

This paper presents a novel approach to solving PAD problem in biometric finger vein recognition systems, combining GLCM features with LGBM to overcome problems. By utilizing optimal GLCM characteristics along with the LGBM algorithm for classification, the method presented in this research effectively addresses the challenges that have been previously faced in methodologies for PAD methods. These obstacles encompass the limited availability of datasets and the substantial model complexity involved. The strategy employed in this investigation entails the extraction of statistical textural attributes, such as energy, correlation, and contrast, from both genuine and fake finger-vein images, ensuring the optimal extraction of features for precise detection of presentation attacks. To assess the efficacy of the proposed method, a K-fold cross-validation technique was implemented, with a comparison made against alternative machine learning approaches. This assessment procedure highlighted the superiority of the proposed method in the realm of presentation attack detection. Through the utilization of K-fold cross-validation for evaluation, the results of this research indicate that the method proposed, which integrates the Light-GBM classifier, showcases superior performance in comparison to other machine learning algorithms, including Random Forest, XGBoost, and CAT classifiers. This research improves the security and reliability of FV biometric systems by advancing Presentation Attack Detection.

Further research can help biometric systems detect presentation attacks more accurately. More information about real and fraudulent images is required. Additional data will increase the system's defenses against various types of attacks. The concept also applies to other biometric features, such as the iris and the face.

References

1. Ashari, N.N., Teng, J.H., Ong, T.S., Kalaiarasi, S.M.A.: Finger Vein Presentation Attack Detection Based on Texture Analysis. Springer Singapore
2. Lee, W.Q.J., Ong, T.S., Connie, T., Jackson, H.T.: Finger Vein Presentation Attack Detection with Optimized LBP Variants. Springer Singapore (2021)
3. Boyd, A., Yadav, S., Swearingen, T., Kuehlkamp, A., Trokielewicz, M., Benjamin, E., Maciejewicz, P., Chute, D., Ross, A., Flynn, P., Bowyer, K., Czajka, A.: Post-mortem iris recognition - A survey and assessment of the state of the art. IEEE Access. 8 136570–136593 (2020)
4. Garg, M., Dhiman, G.: A novel content-based image retrieval approach for classification using GLCM features and texture fused LBP variants. Neural Comput. Appl. 33 (4), 1311–1328 (2021)
5. Guo, X. jing, Li, D., Zhang, H. gang, Yang, J. feng: Image restoration of finger-vein networks based on encoder-decoder model. Optoelectron. Lett. 15 (6), 463–467 (2019)
6. Ke, G., Meng, Q., Finley, T., Wang, T., Chen, W., Ma, W., Ye, Q., Liu, T.Y.: LightGBM: A highly efficient gradient boosting decision tree. Adv. Neural Inf. Process. Syst. 2017-Decem (Nips), 3147–3155 (2017)
7. Kolberg, J., Gomez-barrero, M., Venkatesh, S., Ramachandra, R., Busch, C.: Presentation Attack Detection for Finger Recognition. Springer International Publishing (2020)
8. Nguyen, D.T., Park, Y.H., Shin, K.Y., Kwon, S.Y., Lee, H.C., Park, K.R.: Fake finger-

vein image detection based on Fourier and wavelet transforms. Digit. Signal Process. A Rev. J. 23 (5), 1401–1413 (2013)
9. Qin, B., Pan, J.F., Cao, G.Z., Du, G.G.: The anti-spoofing study of vein identification system. CIS 2009 - 2009 Int. Conf. Comput. Intell. Secur. 2 357–360 (2009)
10. Qiu, X., Kang, W., Tian, S., Jia, W., Huang, Z.: Finger Vein Presentation Attack Detection Using Total Variation Decomposition. IEEE Trans. Inf. Forensics Secur. 13 (2), 465–477 (2018)
11. Qiu, X., Tian, S., Kang, W., Jia, W., Wu, Q.: Finger Vein Presentation Attack Detection Using Convolutional Neural Networks. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics). 10568 LNCS 296–305 (2017)
12. Raghavendra, R., Busch, C.: Presentation Attack Detection Algorithms for Finger Vein Biometrics: A Comprehensive Study. Proc. - 11th Int. Conf. Signal-Image Technol. Internet-Based Syst. SITIS 2015. 628–632 (2016)
13. Ramachandra, R., Busch, C.: Presentation attack detection methods for face recognition systems: A comprehensive survey. ACM Comput. Surv. 50 (1) (2017)
14. Schuiki, J., Prommegger, B., Uhl, A.: Confronting a Variety of Finger Vein Recognition Algorithms With Wax Presentation Attack Artefacts. 1–6 (2021)
15. Schuiki, J., Wimmer, G., Uhl, A.: Vulnerability Assessment and Presentation Attack Detection Using a Set of Distinct Finger Vein Recognition Algorithms. 1–7 (2021)
16. Tirunagari, S., Poh, N., Bober, M., Windridge, D.: Windowed DMD as a microtexture descriptor for finger vein counter-spoofing in biometrics. 2015 IEEE Int. Work. Inf. Forensics Secur. WIFS 2015 - Proc. (2015)
17. Tome, P., Raghavendra, R., Busch, C., Trungarari, Poh, N., Shekar, Gragnaniello, Verdoliva, L., Marcel, S.: The 1st Competition on Counter Measures to Finger Vein Spoofing Attacks. In: ICB 2015 : proceedings of 2015 International Conference on Biometrics (ICB) : May 19-22, 2015, Phuket, Thailand. pp. 535–540 (2015)
18. Wang, Y., Fang, P.: A Finger-Vein Image Quality Assessment Algorithm Combined with Improved SMOTE and Convolutional Neural Network. Proc. IEEE Int. Conf. Softw. Eng. Serv. Sci. ICSESS. 2020-Octob 138–141 (2020)
19. Win, K.N., Li, K., Chen, J., Viger, P.F., Li, K.: Fingerprint classification and identification algorithms for criminal investigation: A survey. Futur. Gener. Comput. Syst. 110 758–771 (2020)
20. Yang, W., Luo, W., Kang, W., Huang, Z., Wu, Q.: FVRAS-Net: An Embedded Finger-Vein Recognition and AntiSpoofing System Using a Unified CNN. IEEE Trans. Instrum. Meas. 69 (11), 8690–8701 (2020)
21. Zhang, L., Sun, L., Li, W., Zhang, J., Cai, W., Cheng, C., Ning, X.: A Joint Bayesian Framework Based on Partial Least Squares Discriminant Analysis for Finger Vein Recognition. IEEE Sens. J. 22 (1), 785–794 (2022)
22. Zhang, Y., Li, W., Zhang, L., Ning, X., Sun, L., Lu, Y.: Adaptive Learning Gabor Filter for Finger-Vein Recognition. IEEE Access. 7 159821–159830 (2019)
23. Zidan, K.A., Jumaa, S.S.: Finger Vein Recognition using Two Parallel Enhancement Approachs based Fuzzy Histogram Equalization. Period. Eng. Nat. Sci. Vol. 7 (1), 514–529 (2019)
24. GitHub - BIP-Lab/SCUT-SFVD: SCUT-SFVD: A Finger Vein Spoofing/Presentation Attack Database, https://github.com/BIP-Lab/SCUT-SFVD, Accessed: October 13, 2022
25. VERA Finger Vein Presentation Attack Datasets, https://www.idiap.ch/en/dataset/vera-fingervein, Accessed: November 09, 2023