International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(20s) 2026 pp. 144-160
https://doi.org/10.70917/ijcisim-2026-5155
Article

Performance Analysis of Handcrafted Features for Iris Recognition Using the IITD Dataset

Sunil Sharma[1], G. Uma Devi[2], Rahul Kumar Garg[3]

[1] Department of Computer Science and Engineering, University of Engineering and Management, Jaipur, Rajasthan, India.
Email: bohra.sunil1@gmail.com
[2] Department of Computer Science and Engineering, University of Engineering and Management, Jaipur, Rajasthan, India.
Email: guma.devi@uem.edu.in
[3] Department of Computer Science and Engineering, University of Engineering and Management, Jaipur, Rajasthan, India.
Email: rahulkumargarg08@gmail.com

Abstract: Biometric authentication has become an important part of modern cybersecurity systems because it provides a convenient and reliable means of verifying user identity. Among different biometric modalities, iris recognition is particularly attractive due to the distinct and stable characteristics of the iris. This study evaluates six widely used feature extraction techniques for iris recognition: Local Binary Patterns (LBP), Gabor Filters, Histogram of Oriented Gradients (HOG), Discrete Wavelet Transform (DWT), Scale-Invariant Feature Transform (SIFT), and a hybrid LBP–SIFT method. Experiments were conducted using the IITD Iris Image Database to assess the suitability of these techniques for secure biometric authentication. After normalization, iris images were processed using each feature descriptor, and the resulting features were compared using cosine distance. Performance was assessed through Receiver Operating Characteristic (ROC) curves, Area Under the Curve (AUC), and Equal Error Rate (EER). The results showed that LBP achieved the highest AUC, whereas SIFT produced the lowest EER, indicating strong recognition performance. In contrast, Gabor Filters showed comparatively weaker results, while HOG and DWT provided a reasonable balance between computational complexity and recognition accuracy. The hybrid LBP–SIFT approach produced only a marginal improvement over the individual descriptors. Overall, the findings suggest that handcrafted features can still provide practical solutions for biometric security, particularly in lightweight access-control applications where computational resources are limited and the use of deep learning models may not be practical...
Keywords: iris recognition, cybersecurity, biometric authentication, handcrafted features, LBP, SIFT, secure access, biometric security systems

1. Introduction

The rapid growth of digital technologies has made cybersecurity increasingly important for individuals, government institutions, and organizations, particularly as large amounts of sensitive information are stored and exchanged electronically [1]. At the same time, cyber threats such as identity theft, data breaches, and unauthorized access are becoming more frequent and sophisticated. Traditional authentication methods, including passwords and PINs, continue to be widely used, but they are increasingly vulnerable to phishing, credential theft, social engineering, and brute-force attacks. These limitations have created a growing need for authentication techniques that can provide stronger security while remaining convenient for users and protecting their privacy.

Amongst many, biometric authentication is the most promising solution to solve this problem. The underlying biometric access control systems form a basis for a system in which administrators pay no heed, and access is extremely difficult to steal or share rightly impossible to leave at home. Unlike other biometric modalities namely fingerprint, facial recognition, voice, and gait the modality of iris recognition is in its ability to protect against spoofing, great retention, and high distinctiveness [2]. The patterns in the human iris, which are highly intricate and remain stable from infancy through adulthood and from one individual twin to another, have been proven extremely robust to be used in secure identity verification problems as iris data.

The growing adoption of iris recognition for biometric authentication in areas such as banking, border management, healthcare, and mobile devices has increased its potential as a reliable component of cybersecurity systems. Iris scanners are also being used in high-security environments, including military facilities, research laboratories, and financial institutions, and their integration into smartphones and laptops is gradually expanding. Despite these developments, selecting an appropriate feature extraction and matching technique remains a significant challenge for biometric systems used in cybersecurity applications. An effective method must provide a suitable balance between recognition accuracy, computational efficiency, robustness to variations in environmental conditions, and resistance to spoofing attempts. This balance becomes especially important in resource-constrained environments, such as edge devices, IoT platforms, and low-power embedded systems, where computational resources may not be sufficient to support complex deep-learning-based approaches.

Concerning that, handcrafted feature extraction methods are still very helpful. Typical deep learning models that use large datasets, deep training, and consider suitable GPUs on the other hand provide lightweight, interpretable, and easily customizable methods, which are suitable for optimization but at the expense of specific operational environments. For several years, several descriptors [3] for iris recognition have been proposed that reflect unique traits of the iris texture and structure. Some of them are Local Binary Patterns (LBP) [4] that encode the micro-level texture changes, Gabor filters [5] masking on human visual perception through frequency and orientation information, Histogram of Oriented Gradients (HOG) [6] representing the edge directions, the Discrete Wavelet Transform (DWT) [6] that performs well on frequency domain handed out, and Scale Invariant Feature Transform (SIFT) [7] which has shown to do very well in retrieving the key points against scale and rotation changes. In the cybersecurity framework, depending on the target application and the threat model, a particular technique can be chosen based on the complexity of these techniques, which can be high or low, depending on the dimensionality of features which can be high or low, and depending on discriminative power of the techniques which can be high, medium or low.

While handcrafted methods have been used in many areas of iris biometrics in earlier eras and are still being used in specific security domains, very few recent studies can be found, that propose a comparison of certain performance-based standardized metrics from the point of view of system security. To design secure and user-acceptable biometric authentication systems, it is necessary to know which descriptors are the most effective, not simply in terms of raw accuracy, but also in terms of an acceptable tradeoff between false acceptance and rejection rates. Also, hybrid approaches using several feature kinds can foster resistance, but by doing so simplicity may be sacrificed.

This research provides a comparative performance evaluation between a set of six handcrafted features' extraction techniques such as LBP [4], Gabor [5], HOG [6], DWT [6], SIFT [7], and the combination of LBP and SIFT's (LBP+SIFT) [8] using the IITD Iris image dataset [9]. We study the usefulness of similarity techniques based on cosine distance on similarity computation and evaluate these techniques in the application of the requirements in terms of ROC curves, AUC, and EER [10]. The results from this thesis show practitioners and researchers building on secure biometric authentication systems attempting to achieve low latencies while being resource-aware for such applications as mobile security, secure terminals, and embedded systems.

In this paper, the batch of various handcrafted descriptors is inspected on these attributes of both biometric image analysis and system performance, to provide insight useful for practical iris recognition system design for security purposes, and ultimately contributes to the cybersecurity field with the specific performance of the handcrafted descriptors, to provide insight into the construction of efficient, trustable, and reasonably cost-effective iris recognition system suitable for real-world security purpose where both performance and trust are important.

2. Related Work

Biometric authentication has emerged as a reliable and user-friendly approach for strengthening modern cybersecurity systems. Among the available biometric modalities, iris recognition is considered particularly suitable for secure identity verification because of the uniqueness and relative stability of iris patterns. The choice of feature extraction technique plays an important role in determining the overall performance of an iris recognition system. Therefore, achieving an appropriate balance between recognition accuracy and computational cost is especially important in resource-constrained environments, where complex deep-learning models may not be practical.

In this study, we focus on the evaluation of several prominent handcrafted feature descriptors (HCFDs) using the IITD iris dataset. The relevance of handcrafted techniques has also been highlighted in previous research. Winston and Hemanth (2019) presented a foundational analysis of Local Binary Patterns (LBP), Discrete Wavelet Transform (DWT), and Gabor filters, reporting that LBP and DWT offered useful discriminative capabilities while maintaining relatively low computational requirements for iris recognition [11]. Similarly, Ariffin et al. (2022) examined LBP, HOG, DWT, and Gabor filters, including their use in multimodal fusion. Their findings suggested that combining multiple features can improve recognition performance, although the associated increase in computational complexity remains an important consideration for practical deployment [12].

LBP is regained all over again in numerous works as a reliable texture descriptor. The approach proposed by Podder (2021) for iris feature vector reduction was Haar + LBP, which was efficient and comparable in performance to the constrained environment [13]. On the other hand, while Gabor filters were motivated by the human visual system, they are known for their computational overhead and low robustness in variable lighting environments. Adaptive Gabor filtering was applied by Vejjanugraha (2025) who also observed limited gains in AUC and EER which is consistent with the findings of this study [14]. Edge and frequency-domain information for example are useful features which is useful across biometric modalities such as HOG and DWT. It was presented by Wulandari et al. (2024) when palm vein recognition worked on a CNN framework with the application of a hybrid DWT-HOG pipeline where balanced accuracy and computational cost were achieved [15]. A hybrid model using HOG, LBP, and Gabor and reduced using LLTSA was proposed by Gopinath and Shivakumar (2024) and gives near-perfect accuracy in vein recognition jobs [16].

Based on warnings that have appeared in the past related to fusion where useful information is diluted by useless data, this study explores the relative utility of hybrid descriptors (LBP + SIFT). According to two recent studies, Winston & Hemanth (2019) and Ariffin et. al. (2022), such hybrids only give incremental performance improvement, and may also increase the system complexity [11, 12]. Vangara (2018) also further advocated for lightweight architectures when used for periocular recognition and utilized transfer learning citing the applications of CNN's, while conceding their impracticability on embedded systems [17]. Mehboob and Dawood (2022) demonstrated that hybrid pipelines can process encoded fingerprint descriptors out of a local database to perform liveness detection and that nondeep approaches can be useful in real-time for security purposes [18].

The advantages of multimodal biometric systems are also the advantages of robustness. Ansari and Aljuaid (2022) developed an ATM authentication system fusing face, fingerprint, and retina using deep models. Although able to work, such systems are generally too complex to be used in constrained environments [19]. In the same spirit of hybridization, Nassar (2018) merged deep learning and handcrafted methods for the identification of faces and irises in real deployment systems [20]. Rehman et al. (2020) gave broader insights into biometric modeling through the review of machine learning methods for signature authentication specifically on the angle of (i) interpretability and (ii) generalization [21]. Meanwhile, Yang et al. (2020) proposed FVRAS-Net which was a CNN-based anti-spoofing system for finger vein recognition with high accuracy but heavy reliance on GPU support which was the key aspect of your focus [22].

Feghhi and Esmaeili (2024) [23] provided a technical exploration of many deep architectures in that they proposed a 3-stream 3D CNN design with GLBPD used to achieve very good performance on cyberspace authentication tasks, but like most other vision methods incur the computational price of handcrafted algorithms. Moreover, Divate and Ali (2018) examined multiple identity factors in data about trait-level variability, e.g., to find which biometric modality is most appropriate to perform gender classification based on this factor [24]. Lastly, a survey on periocular biometrics was given by Bhamare and Patil (2022), discussing its importance when the iris is occluded or partially occluded, thus a use case where the handcrafted descriptors have an advantage because of its robustness to incomplete data [25].

Solanki N. et al. (2019) discussed the significant analysis of wavelet families for invisible image embedding which is one of the supportive factors for the present study with objective three discrete wavelet transformation (DWT) [29]. Gaur S. et al. discussed the process of tracking multiple objects under occlusion detection in image as well in the image and video sequences [30]. S D Degadwala et al. (2016-2018), presented the series of studies with five consecutive research papers on topic preserving the key image property in significance manner with during the various operations applied on the same by utilising various innovative methods including privacy preserving using progressive VCS and RST attacks, Efficient privacy preserving system using VCS, Block DWT-SVD and Modified Zernike moment [31,32]. Further they also express advanced solution in image processing with two-way privacy preserving system using combine approach and 4-share VCS based image watermarking [33-34]. For the colour image their study an efficient privacy preserving system based on RST Attacks on colour Image gives a significant solution, play significant role to improve the quality of present study [35]. M F A Sheikh et al. (2019) produces an important study to evaluate performance of cryptographic algorithm which is powerful inside to assess the performance of algorithms used in the machine and deep learning domain [36].

Table 1 presents a summary of all referenced studies where their techniques and descriptors are listed. A structured summary of all referenced studies, their techniques, and the descriptors used is shown in Table 1.

S.No	**Authors**	**Year**	**Summary**	**Feature Descriptors Used**
1	Winston & Hemanth	2019	Review on iris recognition; LBP and DWT were highlighted as efficient	LBP, DWT, Gabor
2	Ariffin et al.	2022	Multimodal fusion of handcrafted descriptors; warns against complexity	LBP, HOG, DWT, Gabor
3	Podder	2021	Iris feature vector reduction using Haar and LBP	Haar, LBP
4	Vejjanugraha	2025	Adaptive Gabor filter application; showed limited improvement	Gabor
5	Wulandari et al.	2024	Palm vein recognition using hybrid DWT-HOG in CNN framework	DWT, HOG
6	Gopinath & Shivakumar	2024	Hybrid model using HOG, LBP, and Gabor with LLTSA for vein recognition	HOG, LBP, Gabor
7	Vangara	2018	Transfer learning with CNN for periocular; challenges on embedded devices	CNN (Transfer Learning)
8	Mehboob & Dawood	2022	Fingerprint liveness detection with hybrid encoded features	Hybrid Encoded Fingerprint Features
9	Ansari & Aljuaid	2022	Multimodal biometric ATM authentication using deep models	Face, Fingerprint, Retina
10	Nassar	2018	Iris and face recognition with handcrafted and deep fusion	Handcrafted + Deep Features
11	Rehman et al.	2020	ML-based biometric signature authentication; generalization focus	Machine Learning techniques

12	Yang et al.	2020	CNN-based finger-vein anti-spoofing system; high performance but heavy compute	CNN
13	Feghhi & Esmaeili	2024	Three-stream 3D-CNN with GLBPD for client authentication	GLBPD, 3D-CNN
14	Divate & Ali	2018	Gender classification using biometric traits	Traditional biometric features
15	Bhamare & Patil	2022	Survey on periocular biometrics; occlusion and partial capture cases	Periocular biometric descriptors
16	Vejjanugraha	2025	Iris matching with adaptive Gabor filter	Gabor

Both traditional handcraft pastimes extraction and modern deep learning-based approaches are found to be of significant interest as obtained from the literature. However, to the best of our knowledge, there is a shortage of recent comparative evaluations of handcrafted descriptors on standard iris datasets (e.g. IITD) [9]. Also, lots of the cited works highlighted that resource constraints in edge computing environments, like embedded systems, mobile devices, and smart authentication terminals demand the lightweight and interpretable alternative for computationally intensive CNNs.

Other than that, this study aims to fill that gap by systematically benchmarking six popular handcrafted feature descriptors (i.e., LBP, Gabor, HOG, DWT, SIFT, LBP-SIFT)[4][5][6][7][8] through the use of robust evaluation metrics such as AUC, ROC, and EER [10]. The empirical findings are anticipated to drive feasibility for cultivating efficient, accurate, and scalable iris recognition systems in biometric cybersecurity frameworks to meet the broader challenge of achieving performance–usability trade-offs reiterated in the reviewed literature.

3. Methodology

The methodology adopted in this experimental study is designed to provide a systematic and unbiased comparison of different handcrafted feature descriptors. To ensure a fair evaluation, the same preprocessing procedures, feature extraction steps, and performance measures are applied consistently to all descriptors. Each technique is tested on the same dataset under identical experimental conditions, allowing their performance to be compared objectively. The overall implementation process used in the study is organized into the following steps.

3.1 Overview of Experimental Framework

In this work, we make a structured evaluation of six popular handcrafted feature descriptors for iris recognition. The main objective is to determine their discriminative power and computational efficiency in biometric cybersecurity systems that run in constrained environments. The feature descriptors that were evaluated include Local Binary Pattern (LBP) [4], Gabor filter [5], Histogram of Oriented Gradients (HOG) [6], Discrete Wavelet Transform (DWT) [6], Scale Invariant Feature Transform (SIFT) [7], and Hybrid method that combines LBP and SIFT [8]. This is done as these descriptors are already established to have sufficient relevance to, and performance on, image analysis and pattern recognition tasks.

The IITD Iris Database [9], a well-known benchmark in iris recognition research is used for conducting all experiments. All six techniques are evaluated in the same standardized protocol to guarantee consistency and fairness. Iris image normalization is a necessary step in the process, using a simplified rubber sheet model to perform this operation to compensate for iris size and position variations. Feature extraction is applied to each of the normalized iris textures resized to 256×64 pixels with the relative descriptor. Finally, cosine similarity is used to compute how close feature vectors are for a consistent matching and comparison method across descriptors.

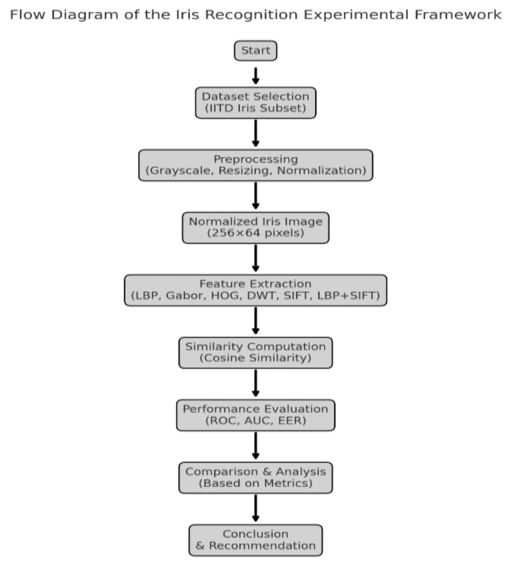

Figure 1: Flow Diagram of the Iris Recognition Experimental Framework

The evaluation metrics for the study of Recognition performance include the use of Receiver Operating Characteristic (ROC) curves, the Area Under the Curve (AUC), and the Equal Error Rate (EER) [10]. These are all useful metrics that give a viewer, a comprehensive view of both accuracy and reliability. To make sure that each descriptor is benchmarked in the same experimental conditions and therefore ensure reproducibility and dataset-specific insights. The intended aim of the framework is to guide to design and implementation of lightweight, high-performance iris recognition systems for real-world applications (i.e. secure access control, embedded systems, and privacy-aware authentication solutions). Figure 1 gives us a complete visual representation of the whole pipeline from the dataset selection to performances and their recommendations.

3.2 Experimental Setup

Google Colab Pro (Paid Version) was used to run all these experiments as it provides access to its powerful computing resources (NVIDIA A100 GPUs & high-performance CPUs). The design of this platform was based on its scalability, to efficiently perform computationally intensive tasks such as image preprocessing, feature extraction, and pairwise similarity computation.

The A100 GPUs helped to accelerate the feature extraction piece, the SIFT keypoint detection [7], and Gabor filter [5] applications in particular. Computing these tasks was known to be computationally intensive, the GPU acceleration greatly shortened the time taken for these operations. Moreover, the high performance of CPUs made sure that the dataset can be processed without memory limitations and thus forms a good working environment to deal with lots of image data from the IITD Iris Database [9].

The experiments were implemented using a modular architecture in which each stage, including image loading, preprocessing, feature extraction, similarity calculation, and performance evaluation, was handled as a separate component. This structure helped maintain consistency throughout the experiments and made the overall workflow easier to manage and reproduce. The use of batch processing and parallel execution also helped reduce processing time when working with a large number of iris images, allowing feature extraction and similarity calculations to be completed efficiently.

The complete iris recognition pipeline was developed in Python using a combination of libraries suited to different stages of the experiment. OpenCV was used for image-processing operations such as resizing and normalization, while NumPy supported array manipulation and mathematical computations. Matplotlib was used to visualize the experimental results, including ROC curves and other performance measures. Scikit-learn was employed for similarity-based evaluation, ROC curve generation, and calculation of the Area Under the Curve (AUC). For frequency-domain feature extraction, the Discrete Wavelet Transform (DWT) was implemented using the PyWavelets (PyWT) library [6]. In addition, the TQDM library was used to monitor the progress of computationally intensive tasks and provide real-time processing updates while running the experiments on Google Colab.

All in all, Google Colab Pro with A100 GPUs is powerful enough for the workload involved with the extraction of features and performance evaluation, making the setup a good platform for reproducible and scalable experiments on iris recognition. The setup was quick so that the results could be achieved quickly without losing the accuracy or reliability of the experiments

3.3 Dataset and Preprocessing

This study uses the IITD Iris Database (Indian Institute of Technology Delhi) [9] which has been widely adopted in the field of biometric research due to its rigorous and consistent nature of depicting iris pattern. Near-infrared images of human irises are included in this dataset, making it suitable for testing and validation of the iris recognition systems due to the better contrast and clarity of the iris features within this spectral range compared to under varying light conditions. It includes 10 images per subject, captured from 224 subjects, which makes it a very diverse and representative set of iris images. A subset of the IITD Iris Database is chosen for this study, which includes 300 iris images of 30 subjects (10 images per person) and is curated. This subset was chosen to achieve data diversity while retaining computational feasibility to maintain all experiments within hardware resources and allow for the capture of intra-class variability as well as inter-class separation. A variety of iris appearances make up the chosen images including many eye shapes and colors, different pupil sizes, and gaze direction. A sample of the iris images in the IITD dataset is shown below in Figure 2, to help one visually better understand the diversity of the images in the dataset.

Figure 2: Sample Images from the IITD Iris Dataset

Preprocessing is given primary importance in standardizing the dataset and preventing unwanted artifacts because of the variability in the iris images. Key Steps in the above preprocessing pipeline are as follows:

(a) **Grayscale Conversion:** First of all, all images are converted into grayscale to eliminate the influence of color. This removes the influence of color difference and ensures that the feature extraction process is limited to extracting the structural pattern of the iris i.e. texture, ridges, and fine details. Secondly, grayscale images also simplify the ensuing step of image processing i.e., segmentation and feature extraction.

(b) **Resizing:** Each image is resized to a fixed dimensions of 128×128 pixels. It is a step, which aims at making the resolutions of the images consistent throughout them and eliminating the discontent arising from different resolutions of different images. It is also the sizing that guarantees compatibility with the feature extraction modules that feed with standardized input dimensions. The work of resizing to 128×128 pixels is simplified, but it retains sufficient resolution for important iris details to still be present.

(c) **Iris Recognition (dropping eyelashes, noise):** The Iris region needs to be isolated from the surrounding regions (by segmentation and normalization). To do this, a segmentation step seeks to first locate the iris in the eye image. The segmentation process is crucial since an error in iris isolation would significantly impair the performance of the feature extraction and recognition process afterward. First, the iris texture is normalized through the application of the rubber sheet model (a simplified version of Daugman's model) after segmentation [26]. This method converts iris to a polar coordinate system and radius and angle stand for iris texture. In both the developed applications, the polar unwrapping standardizes the iris region by flattening the curvature of the iris, such that the output image remains consistent for any subject's iris, representing their radial texture.

The output of this normalization process is a standard input size, (256×64 pixels) used for subsequent feature extraction steps. Removing the geometric variation including but not limited to changes in iris size due to pupil dilation and changes in eye orientation (e.g. left or right gaze, etc.) ensures that a standardized representation of the iris texture is built. Below are the images of this preprocessing step. The first set is original iris images and the second one shows the same images after normalization using the rubber sheet model.

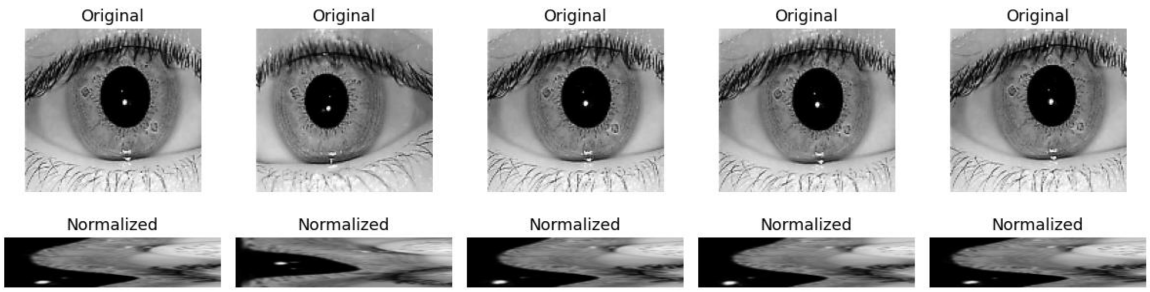

Figure 3: Original and Normalized Iris Images

(d) Noise Removal and Masking: Manual masking is used to remove the noises caused by eyelids and eyelashes. The mask removes or masks any regions outside of the normalized iris area including artifacts from the surrounding tissue. In this way, the iris features do not get contaminated with irrelevant structures, which will improve the accuracy and reliability of the following feature extraction.

3.4 Feature Extraction Techniques

Six different techniques of handcrafted feature extraction in iris recognition are evaluated in this study. They chose these methods based on their relevance in biometric applications, the ability of these methods to generate various representations of texture and structure and their computational feasibility. These techniques are applied to the normalized 256×64 iris textures and assessed in the same setting.

3.4.1 Local Binary Pattern (LBP): Local Binary Pattern (LBP) [4] is a popular and effective texture descriptor and has been successfully applied to the face, iris recognition, etc. It scans each pixel of the image and compares it to its neighbouring pixels of a defined radius. If the intensity of the neighbouring pixel is at least equal to the intensity of the central pixel, it is given the value 1, otherwise 0. Finally, these binary values are interpreted as a decimal number to generate a unique label for this particular pixel, and all of those pixels form a histogram encoding the frequency of different texture patterns present in the image. For this study, 8 neighbours and a radius of 1 uniform LBP are used where rotational invariance is provided. The reason for this is that LBP is of low computational complexity and robust to illumination changes, thus making it an excellent candidate for real-time, embedded biometric systems.

3.4.2 Gabor filters: Gabor filters [5] are biologically inspired descriptors that mimic the spatial response in the human visual cortex. Especially they are good at getting information concerning the orientation and frequency of textures. Applying a bank of four Gabor filters on the normalized iris image, with four different orientations viz. 0, 45, 90, and 135 degrees are done in this study. In this way, the global mean and standard deviation are calculated for each filter response, and these statistical features are concatenated to form a compact descriptor. Iris textures have radial and concentric structures and consequently, Gabor filters are well-suited for highlighting them. Though more computationally costly than LBP [4] or HOG [6], they provide good discriminative power in cases where fine granularity of texture is necessary.

3.4.3 Histogram of Oriented Gradients (HOG): The Histogram of Oriented Gradients (HOG) [6] descriptor makes use of the distribution of edge direction information of localized regions to capture shape and edge information. For each pixel in the normalized iris image, we compute gradient orientations of its small cell (typically 8×8 pixels in size). They are aggregated into histograms in each cell and normalized over larger blocks to improve contrast invariance. The last one is to concatenate all local histograms into one feature vector. HOG is an effective technique for detecting curved and radial structures in iris patterns, and as such, it provides a good compromise between accuracy and computational efficiency.

3.4.4 Discrete Wavelet Transform (DWT): The Discrete Wavelet Transform (DWT [6]) is a multi-resolution analysis technique that analyses the image at different frequency bands and different resolutions. It is capable of capturing both coarse and fine-scaled details. For this study, the applied Haar wavelet decompositions are single-level Haar wavelet decompositions, with the iris image decomposed into four sub-bands which are referred to as: LL (approximation, LH (Horizontal details), HL (Vertical details), and HH (diagonal details) details. The final feature vector is then obtained by flattening and dimensionally reducing these subbands. Due to its efficiency, DWT is known for emphasizing texture changes at different scales and being computationally easy, so it is advisable to be used for applications where speed is relevant.

3.4.5 Scale Invariant Feature Transform (SIFT): The Scale Invariant Feature Transform (SIFT) [7] is an invariance to scale, rotation, and illumination keypoint-based descriptor. For each of them, SIFT detects stable key points across different scales and computes 128-dimensional descriptors. Because there is a variable number of key points in each image, a traditional SIFT implementation yields vectors of varying length. In this work, we summarize the SIFT matches between image pairs with statistical measures (i.e. mean and standard deviation of keypoint match distances computed through brute force matching with Lowe's ratio test) to achieve standardization of the comparisons. This retains SIFT's power to match while providing descriptors small enough to be used in distance scoring.

3.4.6 Hybrid: We create a hybrid descriptor to incorporate a good of local texture (LBP) and structural key points (SIFT) [8]. In this method just like usual LBP histogram is computed but this time it captures it using pixel-level texture variations. Then, it is concatenated with the statistical descriptors of SIFT keypoint matching (mean and standard deviation of pairwise distances). This feature vector combines fine-grained texture and globally salient features in a balanced fashion in a single feature vector for the iris image. The proposed approach aims to increase the recognition accuracy at essentially no additional computational cost and therefore makes it a good candidate for real-time biometric applications.

3.5 Evaluation Metrics

This study then employs a framework for the comprehensive evaluation of each of the handcrafted feature extraction techniques based on statistical similarity measures and biometric system accuracy criteria to assess the performance of each of the techniques. Three criteria (Cosine Similarity, Receiver Operating Characteristic (ROC) Curve with Area Under Curve (AUC), and Equal Error Rate (EER)) [10] are used to evaluate the result. These provide a collective understanding of the discriminative ability of the extracted features and overall recognition reliability for each method.

3.5.1 Cosine Similarity: Given the feature vectors extracted for every iris image, pairwise similarity scores are calculated using the cosine similarity metric. The angular distance between two non-zero vectors is defined as cosine similarity [27]:

$$Cosine\ Similarity\ = \frac{A \cdot B}{\|A\|\|B\|}$$

This is equivalent to the norm of the difference between two feature vectors A and B of two iris images. In other words, the cosine similarity is higher (closer to 1) the better the match and lower otherwise. This metric is quite good for normalized feature vectors is invariant to changes in vector magnitude, and is good for image descriptors where only direction (not scale) matters.

For each method, we compute cosine similarity scores for:

Images from the same subject, that is Genuine pairs,

Images from different subjects, that is imposter pairs.

The ROC curve and AUC as well as EER are derived from these scores.

3.5.2 Receiver Operating Characteristic (ROC) Curve and AUC: An illustration of the trade-off between the True Positive Rate (TPR), and False Positive Rate (FPR) about different similarity thresholds is given using the Receiver Operating Characteristic (ROC) curve. It plots the result of sweeping over a decision threshold in the cosine similarity scores .

- Sensitivity or TPR = Proportion of genuine pairs that are correctly identified.
- FPR (1− Specificity): fraction of impostor pairs wrongly marked as genuine.

Here the ROC curve is an intuitive tool to visualize at what threshold the system performs well.

The ROC curve is then computed and the Area Under the Curve (AUC) is derived [28]. It is a continuous feature for quantifying the overall separability of genuine and imposter pairs. An AUC of 1.0 would be perfect and 0.5 would be for a random classifier. Hence, the higher the AUC, the better the feature descriptor is in separating identities from each other.

3.5.3 Equal Error Rate (EER): The Equal Error Rate (EER) [10] is the scalar at which the False Acceptance Rate (FAR) equals the False Rejection Rate (FRR). But, this is especially important in the case of biometric systems as this operating condition where Type I and Type II errors are equally likely is the point of this system.

Mathematically:

FAR: The imposter pairs that are falsely accepted at this rate.

FRR: Customers will learn the false rejection rate (FRR) of the genuine pairs by FPR; the rate at which genuine pairs are falsely rejected.

A lower EER value represents a higher balance and accuracy of a recognition system. In practice, EER is favored due to its single-value summary of the performance, independent of the threshold.

4. Experimental Results and Analysis

Cosine similarity was used as a distance metric and applied to normalized iris images with all handcrafted feature extraction techniques evaluated. They include three key biometric performance indicators of AUC, EER, and average similarity scores for genuine and imposter image pairs. Similarity score histograms and ROC curves, which are shown in Figures 2 through 7, are presented for performance visualization.

4.1 Local Binary Pattern (LBP):

Local Binary Pattern (LBP) [4] achieves the highest AUC score (0.7780) with the lowest EER (0.3195) in all the results of this project, implying that LBP offers a very good separability of matched and non-matched classes. Using Figure 4, we note that the scores for actual similarities are tightly clustered near 1.0, while for imposters, the scores are less dispersed and lower which indicates good discrimination. This is consistent with LBP being a suitable lightweight, embedded biometric system.

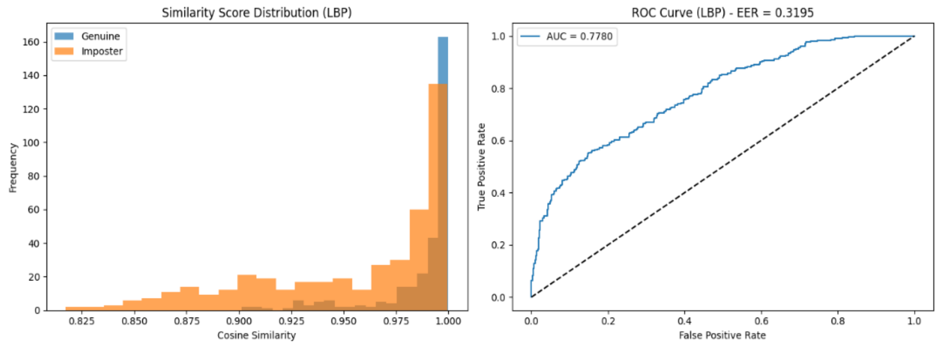

Figure 4: LBP Similarity Distribution and ROC Curve

4.2 Gabor Filters:

Gabor Filters [5] achieved the highest genuine score mean (0:9930), but also has the highest imposter score (0.9804), which accounts for its low AUC (0.6735) and high EER (0.3908). As depicted in Figure 5, the overlap between genuine and imposter distributions is heavy. The reason for the high false acceptance rate is this overlap, and while theoretically very good in frequency domain analysis, Gabor filters are unsuitable for high-security systems.

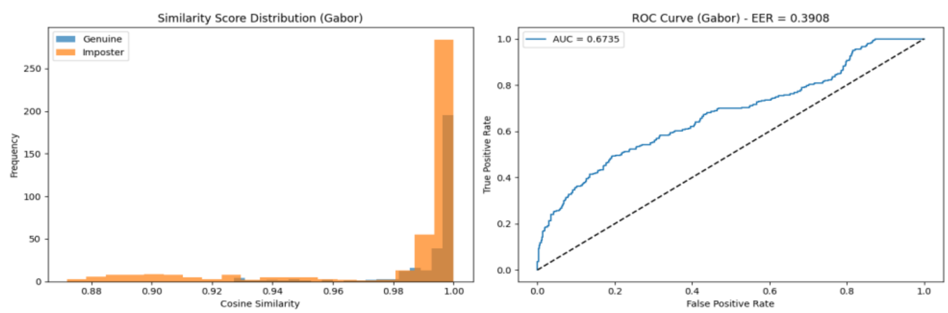

Figure 5: Gabor Filter Similarity Distribution and ROC Curve

4.3 Histogram of Oriented Gradients (HOG):

Like all the methods, the HOG method [6] had a balanced performance. In particular, the AUC and EER for the HOG method were 0.7289 and 0.3356, respectively. As shown in Figure 6, distinguishable histogram curves of genuine (0.7471) and imposter (0.6793) similarity between histograms were maintained by it. In addition, the ROC curve corroborates its potential use in mid-security applications, like personal authentication in constrained access systems.

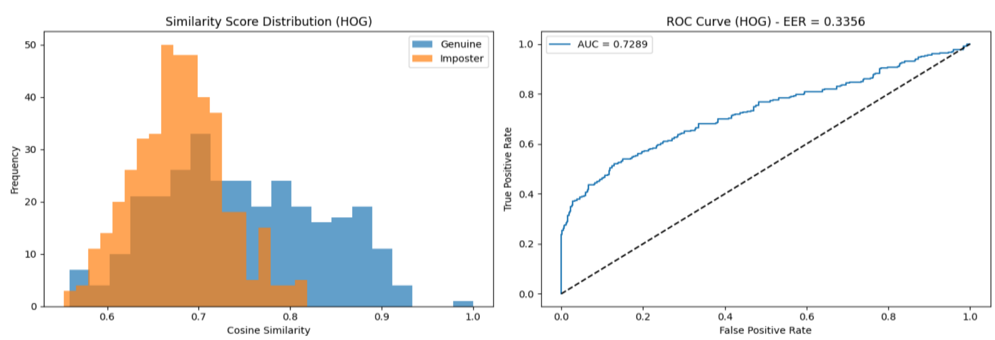

Figure 6: HOG Similarity Distribution and ROC Curve

4.4 Discrete Wavelet Transform (DWT):

DWT [6] yielded almost similar results as HOG with AUC of 0.71506 and EER of 0.3356. Observing Figure 7, in the histogram and ROC curve, moderate discriminability is suggested, in which genuine scores most concentrate in values above 0.93 and impostors tend to concentrate just below. This is because DWT is frequency decomposing in nature and compact which makes it more appropriate for usage in cloud-based and encrypted biometric systems in which data compression is important.

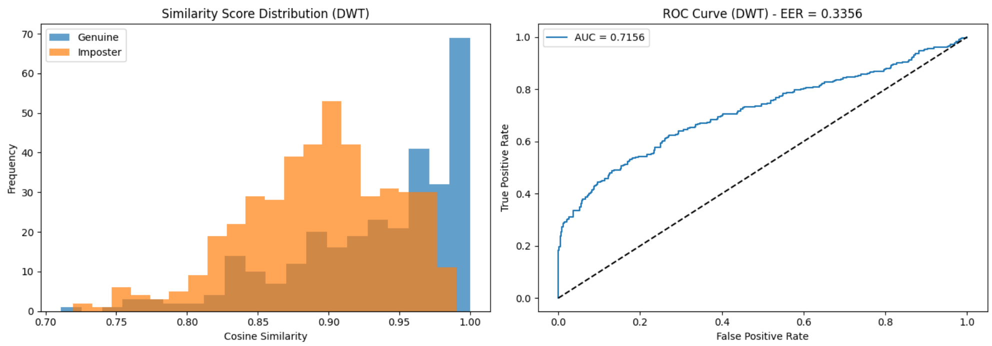

Figure 7: DWT Similarity Distribution and ROC Curve

4.5 Scale-Invariant Feature Transform (SIFT):

Scale Invariant Feature Transform (SIFT) [7] gives the lowest EER of 0.3172 and good AUC of .7578, hence excellent separation between genuine and imposter matches. Figure 8 illustrates the distribution of genuine and imposter scores, as imposter scores concentrate around zero, whereas genuine scores spread out. The broadness of this performance margin sets SIFT forth as a great candidate for high-security applications, such as border control and secure vault access.

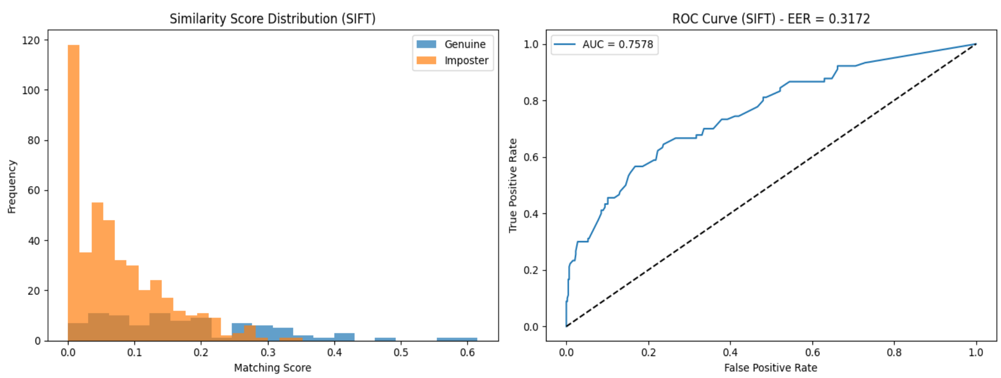

Figure 8: SIFT Similarity Distribution and ROC Curve

4.6 Hybrid Descriptor (LBP + SIFT):

Unfortunately, the hybrid approach [8] did not perform as well as LBP or SIFT separately with an AUC of 0.7040 and EER of 0.3471. Figure 9 shows that the distributions of the two classes overlap, hence the simple feature concatenation only added redundancy rather than increased the separability. Instead, this indicates that learned embeddings or dimensionality reduction is needed for hybrid descriptors to be effective.

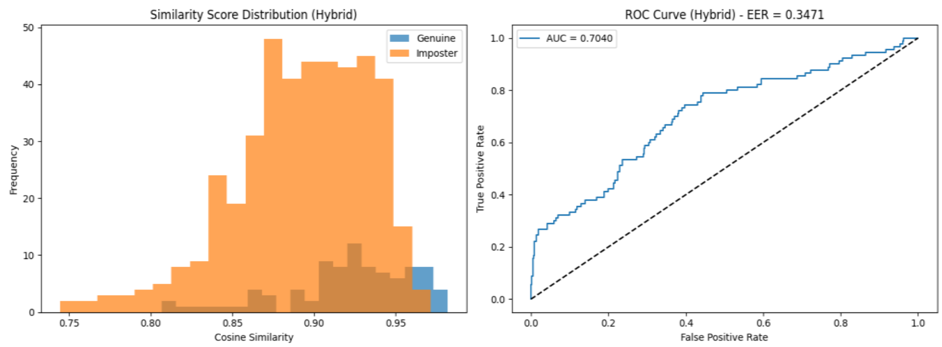

Figure 9: Hybrid LBP + SIFT Similarity Distribution and ROC Curve

4.7 Performance Comparison and Summary Analysis

In the following table, the key performance metrics: AUC, EER, average genuine similarity, and average imposter similarity for all six handcrafted feature extraction methods on iris recognition are tabulated:

Table 2: Summary Table

Method	AUC	EER	GenuineAvg	ImposterAvg
LBP	0.778	0.3195	0.987	0.9546
Gabor	0.6735	0.3908	0.993	0.9804
HOG	0.7289	0.3356	0.7471	0.6793
DWT	0.7156	0.3356	0.9333	0.8934
SIFT	0.7578	0.3172	0.1761	0.0733
Hybrid	0.704	0.3471	0.9214	0.8924

It is seen from the AUC comparison (Figure 10) that LBP has the greatest capability of recognition and is closely followed by SIFT. The poorest separation between genuine and imposter scores was obtained by Gabor in terms of AUC.

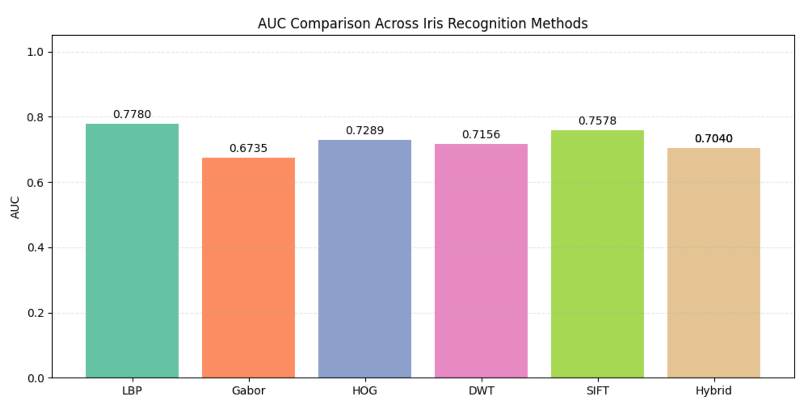

Figure 10: AUC Comparison Across Methods

From the comparison of EER (Figure 11), it is seen that SIFT makes the lowest error rate and hence is the most reliable for use with security-sensitive systems. On the other hand, Gabor had the lowest EER indicating a larger chance for false matches.

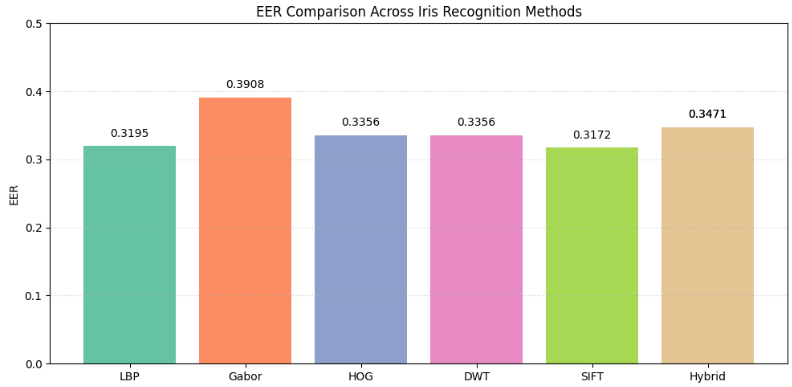

Figure 11: EER Comparison Across Methods

The average genuine match scores are shown in Figure 12. Here Gabor and LBP both work great, which means there is a high similarity between intra-class samples. Despite these poor measures, SIFT gains in terms of a greater separation margin as well as a very low imposter average.

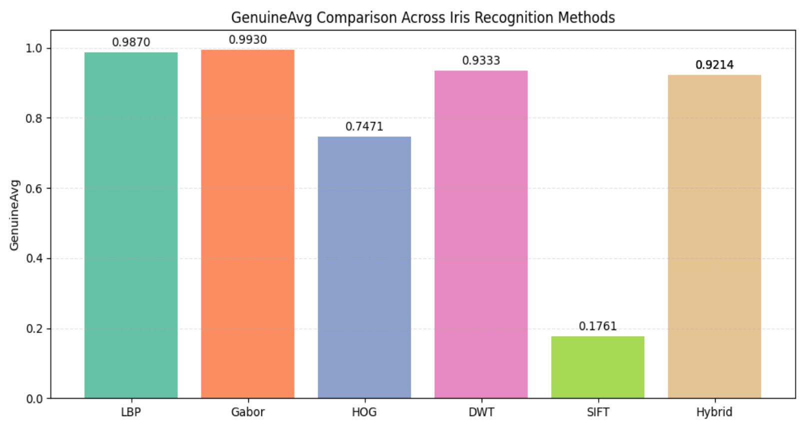

Figure 12: Genuine Similarity Score Comparison

Finally, the average similarity of the imposter pairs is presented in Figure 13. The lowest score was secured by SIFT, proving to be able to reject an illegal identity. Even though the genuine scores are good, high imposter averages raise Gabor and LBP for high-security environments.

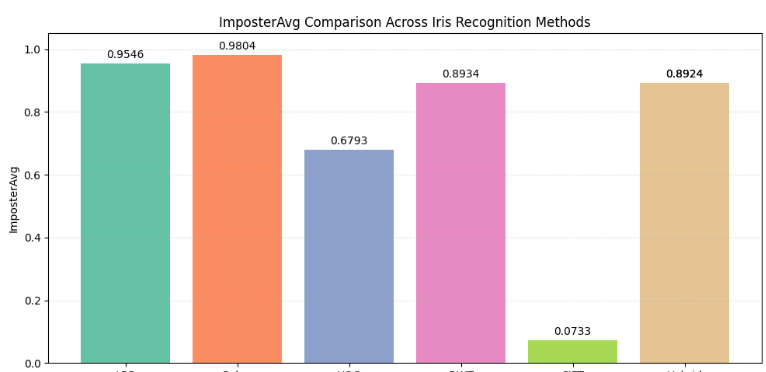

Figure 13: Imposter Similarity Score Comparison

4.8 Analysis

Six manual feature extraction methods receive analysis regarding their capability to perform iris identification applications. LBP delivered the best results because its AUC value reached 0.7780 indicating good generalization capabilities along with high intra-class similarity. This method delivered good computational efficiency and showed compatibility with low-resource environments for mobile authentication systems.

The SIFT algorithm reached sub-optimal results including EER (0.3172) and average imposter similarity (0.0733) but maintained fewer genuine similarity scores than SURF, HSESIFT, and HSELBP. The limited number of matches demonstrates superior discrimination abilities that yield excellent imposter rejection. The security requirements of high-security applications call for SIFT due to its superior ability to reduce false acceptances. Although Gabor filters had the highest genuine similarity scores they delivered the highest false rejection scores (from imposters) which led to an EER of 0.3908. The system needs to integrate this approach with stronger classifier models because it demonstrates unsuitable performance in real-world environments. DWT combined with HOG offered a favorable accuracy-complexity ratio because they generated AUC and EER scores which were not too high or low. Despite meeting certain criteria, they lacked sufficient discriminatory ability for application deployment in hostile or spoof-vulnerable environments. The combination technique between LBP and SIFT failed to produce better results than when used separately. It appears that basic feature fusion methods fall short of achieving effective use of complementary strengths therefore adaptive learned fusion techniques must be employed.

The evaluation of handmade descriptors concludes with accuracy, robustness, and scalability weaknesses that appear when inter-class similarities and environmental changes grow high. The error rate performance leaders LBP and SIFT demonstrate both detectable errors in addition to threshold variations sensitivity. The proposed combination scheme failed to outperform its basic building blocks since manmade features restricted its performance at achieving higher results. Modern security requirements demand the replacement of handcrafted techniques because handcrafted methods fall short of delivering the necessary standards for an advanced biometric system. The research explores logical stages that begin with previous work and advance toward deep learning techniques for end-to-end feature learning along with generalization enhancement and better deployment adaptations.

5. Conclusion and Future Work

Biometric cybersecurity systems for iris recognition were evaluated with an evaluation of six handcrafted feature extraction algorithms, that is LBP and Gabor Filters, HOG and DWT or SIFT, and their combined LBP + SIFT. Cosine similarity scoring of normalized images was applied, using the Iris IITD database through the six feature methods, for all feature methods, and these were evaluated using EER and AUC biometric metrics for the standardized evaluation methodology. Despite having better imposter rejection at 0.3172 EER, SIFT had a lower maximum recorded AUC of 0.7780 compared to LBP. However, the competitive match data produced by Gabor filters was unproductive to the Error Equalization Rate with high Error Equalization Rate measurements as well as the best real match ratings produced by them. HOG and DWT had the best results and affordable computing costs in the processing performance and accuracy levels. The basic handcrafted features themselves were unable to demonstrate any superiority of their hybrid model which showed that the combination of simple elements only added redundant information rather than providing graphical object discrimination power.

Findings from experiments show that handcrafted descriptions are useful for providing input to basic processing systems but prove incapable of working in the presence of performance differences due to spoofing or occlusions requiring a more flexible system. However, the manual generation of features fails to have the requisite abstraction capacity together with the required flexibility to create effective generalizations across customers in differing user groups operating under different operating conditions.

Studies have been focused lately on designing frameworks of deep networks exclusively for the iris recognition system implementation. The fact that the system can learn recognition features automatically out of raw image data without losing spatial information is thanks to the use of convolutional and deep neural networks. These modern models are far better than traditional methods of orienting and extracting complex iris pattern elements. For the upcoming stage, the research team will use established network versions of ResNet and MobileNet as CNN designs which will be utilized to develop more efficient generalized development systems. When building better multilevel nonlinear techniques, the team will also devise antispoofing security frameworks that can unite high-level characteristics with low-level information descriptors. A combination of the pruning, quantization, and model distillation deployment methods will be used to evaluate how well deep model deployments work for real-time biometric authentication systems in resource-constrained environments.

REFERENCES

1. E. A. Debas, R. S. Alajlan and M. M. Hafizur Rahman, "Biometric in Cyber Security: A Mini Review," 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), Bali, Indonesia, 2023, pp. 570-574, doi: 10.1109/ICAIIC57133.2023.10067017
2. Hsieh, S., Li, Y., Wang, W., & Tien, C. (2018). A novel Anti-Spoofing Solution for iris Recognition toward cosmetic contact lens attack using spectral ICA analysis. Sensors, 18(3), 795. https://doi.org/10.3390/s18030795
3. R. Vyas, T. Kanumuri, G. Sheoran and V. Kumari, "Local pattern-based descriptors for iris recognition: A comparative analysis," 2018 IEEE 13th International Conference on Industrial and Information Systems (ICIIS), Rupnagar, India, 2018, pp. 36-41, doi: 10.1109/ICIINFS.2018.8721368
4. Song, K., Yan, Y., Chen, W., & Zhang, X. (2013). Research and perspective on local binary pattern. Acta Automatica Sinica, 39(6), 730–744. https://doi.org/10.1016/s1874-1029(13)60051-8
5. Minhas, S., & Javed, M. Y. (2009). Iris feature extraction using gabor filter. International Conference on Emerging Technologies, 252–255. https://doi.org/10.1109/icet.2009.5353166
6. J, A. S., & S, A. P. (2016). Performance analysis of iris recognition system using DWT, CT and HOG. IOSR Journal of Electronics and Communication Engineering, 11(05), 28–33. https://doi.org/10.9790/2834-1105012833
7. W. Zhao, X. Chen, J. Cheng and L. Jiang, "An application of scale-invariant feature transform in iris recognition," 2013 IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS), Niigata, Japan, 2013, pp. 219-222, doi: 10.1109/ICIS.2013.6607844
8. B. Kaur, "Iris and Periocular Recognition using Shape Descriptors and Local Invariant Features," 2023 2nd Edition of IEEE Delhi Section Flagship Conference (DELCON), Rajpura, India, 2023, pp. 1-5, doi: 10.1109/DELCON57910.2023.10127462
9. Omelina, L., Goga, J., Pavlovicova, J., Oravec, M., & Jansen, B. (2021). A survey of iris datasets. Image and Vision Computing, 108, 104109. https://doi.org/10.1016/j.imavis.2021.104109
10. Tronci, R., Giacinto, G., & Roli, F. (2009). Dynamic score combination: A supervised and unsupervised score combination method. In Lecture notes in computer science (pp. 163–177). https://doi.org/10.1007/978-3-642-03070-3_13
11. Winston, J. J., & Hemanth, D. J. (2019). A comprehensive review on iris image-based biometric system. Soft Computing, 23(23), 11975–11995. https://doi.org/10.1007/s00500-018-3497-y
12. Ariffin, S. M. Z. S. Z., et al. (2022). Image fusion for single-trait multimodal biometrics: A brief review. In 2022 IEEE SCSE (pp. 30–35). https://doi.org/10.1109/SCSE53726.2022.9974027
13. Podder, P. (2021). IRIS feature vector reduction using Haar wavelet transform and local binary pattern [Master's thesis, BUET]. BUET Institutional Repository. http://lib.buet.ac.bd:8080/xmlui/handle/123456789/6077
14. Vejjanugraha, P. (2025). A biometric iris matching system for reliable person identification using adaptive Gabor filter. SPIE Proceedings. https://doi.org/10.1117/12.3057996
15. Wulandari, M., et al. (2024). Hybrid feature extractor using DWT and HOG on CNN-based palm vein recognition. Sensors, 24(2), 341. https://doi.org/10.3390/s24020341
16. Gopinath, P., & Shivakumar, R. (2024). Hybrid feature extraction and LLTSA-based dimension reduction for vein pattern recognition. Biocybernetics and Biomedical Engineering. https://doi.org/10.1080/13682199.2023.2257539
17. Vangara, K. (2018). Transfer learning with convolutional neural networks applied to periocular biometrics [Master's thesis, Florida Institute of Technology]. FIT Repository. https://repository.fit.edu/etd/771/
18. Mehboob, R., & Dawood, H. (2022). DEHFF – A hybrid approach based on distinctively encoded fingerprint features for live fingerprint detection. Biomedical Signal Processing and Control, 75, 103572. https://doi.org/10.1016/j.bspc.2022.103572
19. Ansari, A. S., & Aljuaid, S. M. (2022). Automated teller machine authentication using biometric. Computer Systems Science and Engineering. https://doi.org/10.32604/csse.2022.020785
20. Nassar, A. S. N. (2018). A computer system for the identification of humans by integrating facial and iris features using localization, feature extraction, handcrafted and deep learning approaches [Doctoral dissertation, University of Bradford]. Bradford Scholars. https://bradscholars.brad.ac.uk/handle/10454/16917
21. Rehman, A., Bibi, K., & Naz, S. (2020). Biometric signature authentication using machine learning techniques: Current trends, challenges and opportunities. Multimedia Tools and Applications, 79, 23635–23660. https://doi.org/10.1007/s11042-019-08022-0
22. Yang, W., Luo, W., Kang, W., Huang, Z., & Deng, Z. (2020). FVRAS-Net: An embedded finger-vein recognition and anti-spoofing system using a unified CNN. IEEE Transactions on Information Forensics and Security, 15, 2947–2960. https://doi.org/10.1109/TIM.2020.3001410

23. Feghhi, M. M., & Esmaeili, V. (2024). Real-time client authentication in cyberspace using the GLBPD and three-stream 3D-CNNs with the LSTM. IEEE Access, 12, 151261–151274. https://doi.org/10.1109/ACCESS.2024.3479718
24. Divate, C. P., & Ali, S. Z. (2018). Study of different biometric-based gender classification systems. In 2018 International Conference on Inventive Research in Computing Applications (ICIRCA) (pp. 347–353). IEEE. https://doi.org/10.1109/icirca.2018.8597340
25. Bhamare, D. R., & Patil, P. S. (2022). A review on person identification using periocular biometrics. In Proceedings of the International Conference on Data, Engineering and Applications (pp. 393–402). Springer. https://doi.org/10.1007/978-981-97-0037-0_34
26. A. Mohammed and M. F. Al-Gailani, "Developing Iris Recognition System Based on Enhanced Normalization," 2019 2nd Scientific Conference of Computer Sciences (SCCS), Baghdad, Iraq, 2019, pp. 167-170, doi: 10.1109/SCCS.2019.8852622.
27. Sandhya, S., Balasundaram, A., & Shaik, A. (2022). Deep learning-based face detection and identification of criminal suspects. Computers, Materials & Continua/Computers, Materials & Continua (Print), 74(2), 2331–2343. https://doi.org/10.32604/cmc.2023.032715
28. Nahm, F. S. (2022). Receiver operating characteristic curve: overview and practical use for clinicians. Korean Journal of Anesthesiology, 75(1), 25–36. https://doi.org/10.4097/kja.21209
29. Neha Solanki, Sarika Khandelwal, Sanjay Gaur, Diwakar Gautam (2019), A Comparative Analysis of Wavelet Families for Invisible Image Embedding, Emerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018, AISC Vol.-841,219-227, doi.org/10.1007/978-981-13-2285-3_27
30. Sanjay Gaur, S D Degadwala, Arpana Mahajan (2019), Multiple Objects Tracking Under Occlusion Detection in Video Sequences, Emerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018, AISC Vol.-841,189-196, Springer Nature Singapore, doi.org/10.1007/978-981-13-2285-3_23.
31. S. D. Degadwala and S. Gaur, (2016), A study of privacy preserving system based on progressive VCS and RST attacks, 2016 International Conference on Global Trends in Signal Processing, Information Computing and Communication (ICGTSPICC), Jalgaon, India, 2016, pp. 138-142, doi: 10.1109/ICGTSPICC.2016.7955285
32. S. D. Degadwala and S. Gaur, (2017), An Efficient privacy preserving system using VCS, Block DWT-SVD and Modified Zernike moment on RST attack, International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET) Chennai-India (2017), 1-4, IEEE Explore doi: 10.1109/ ICAMMAET.2017.8186685
33. S. D. Degadwala and S. Gaur, (2017), Two-way privacy preserving system using combine approach: QR-code & VCS, 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Vellore, India, 2017, 01-05, IEEE Explore, doi: 10.1109/IPACT.2017.8245120
34. S. D. Degadwala and S. Gaur, (2017), 4-Share VCS Based Image Watermarking for Dual RST Attacks, Computational Vision and Bio Inspired Computing. Lecture Notes in Computational Vision and Biomechanics, 28. Springer, Cham. doi.org/10.1007/978-3-319-71767-8_77
35. S. D. Degadwala and S. Gaur, (2018), An Efficient Privacy Preserving System Based on RST Attacks on Color Image, Future Internet Technologies and Trends. ICFITT 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 220. Springer, Cham. https://doi.org/10.1007/978-3-319-73712-6_2
36. M F A Sheikh, Sanjay Gaur, Hiral Desai, SK Sharma (2019), A study of Performance Evaluation of Cryptographic Algorithm, Emerging Trends in Expert Applications and Security: Proceedings of ICETEAS 2018, AISC Vol.-841, 379-384, Springer Nature Singapore, doi.org/10.1007/978-981-13-2285-3_44.