Synthesis of Palm Print in Feature Fusion Techniques for Multimodal Biometric Recognition System Online Signature

T. Vijayakumar,
Professor,
Department of ECE,
Guru Nanak Institute of Technology,
Hyderabad, India.
Email: vishal_16278@yahoo.co.in

Abstract: Biometric identification technology is widely utilized in our everyday lives as a result of the rising need for information security and safety laws throughout the world. In this aspect, multimodal biometric recognition (MBR) has gained significant research attention due to its ability to overcome several important constraints in unimodal biometric systems. Henceforth, this research article utilizes multiple features such as an iris, face, finger vein, and palm print for obtaining the highest accuracy to identify the exact person. The utilization of multiple features from the person improves the accuracy of biometric system. In many developed countries, palm print features are employed to provide the most accurate identification of an actual individual as fast as possible. The proposed system can be very suitable for the person who dislikes answering many questions for security authentication. Moreover, the proposed system can also be used to minimize the extra questionnaire by achieving a highest accuracy than other existing multimodal biometric systems. Finally, the results are computed and tabulated in this research article.

Keywords: Biometric recognition, Feature fusion, Palm print

1. INTRODUCTION

A biometric authentication system is a method used to identify a person by using a vector, which has been combined with a quantifiable physical or behavioural feature. Due to considerable research undertaken in the field of forensics, monitoring systems, attendance systems, smartphone unlocking, automatic customer makers, and border and control systems, the
biometric recognition domain has occupied a major part in our everyday applications [1]. The biometrical traits can be explained as a measurement of a person's physiological or behavioural trait.

In general, biometrics is classified into two types:

1. Physiological Biometrics
2. Behavioral Biometrics

Biometric physiology refers to the measuring of different characteristics of a human body such as fantasy, facial, iris, and hand geometry; comportment biometrics refers to measuring the behavior of a person, for example, voice, signature, gait, and keystroke dynamics, while performing certain tasks [2, 3]. The biometrics are comparably more precise and confident. However, the safety of physical biometrics is challenged by their publicity and openness.

![Modern Biometric authentication system](image)

**Figure 1** Modern Biometric authentication system

The human faces and their fingerprints are available to the world and it can be easily recorded by everyone. Once a high-resolution image is taken, anybody may recreate and reuse the face or fingerprint of the real person [4, 5]. While the conduct biometrics is not as exact and dependable as the physical, they are more personalized to the owner and not readily reproduced. The usage of multimodal biometrics is a way to increase the safety of biometric data [6, 7].
More than one biometric feature or method can be utilized to store biometric data in a fused form in a multimodal biometry system, which ensures greater safety because it is impossible to regenerate or replicate one biometric feature from a fused biometrics template [8, 9]. The combination of human face with fingerprint, face, and iris are commonly used in the multimodal biometric system [10, 11]. This combination is also possible. For this reason, one of the physical characteristics and behavioral biometric characteristics are important to assure accuracy and privacy [12, 13].

Moreover, combining physical and behavioral biometric features would improve the precision and decrease spoof assaults in a biometric system. Biometric data are always prone to security threats if kept in an unencrypted form. The "BioStar2" database is one example of such violations. The database has kept data on biometrics in an unencrypted manner, including fingerprints, face identifying information, and user passwords. Recently, a team of security experts found a security violation in the database [14].

Many developing and developed nations in the globe, including the UK, the United States, the UK, Finland, Japan and Germany, and many more, have been using the database services. Security researchers got the data by doing certain procedures only via the web browser. This indicates that the biometric data of users can be affected thus it should not be reused, even if affected, in a fused and encrypted form [15].

Figure 2 Simple Block Diagram of Biometric Verification Process
2. ORGANIZATION OF THE RESEARCH

This research article has contained the following contents in various sections. Section 3 delivered a recent research paper working methodology on multimodal biometric recognition systems. Section 4 discusses feature fusion techniques for multimodal biometric recognition systems. Section 5 contains results discussion for various methods. Section 6 containing future challenges and the conclusion of the research report.

3. PRELIMINARIES

The pade et al integrated identity testing features of human iris and palm print. Firstly, palm print and iris were merged and then different energy distribution transformations have decreased the usefulness and a comparison was made on different techniques of energy transformation. Hartley converted 58.40 percent of the most genuine rate of acceptance (GAR) [16].

Guesmi et al. have offered another fusion approach, which is identified for modifying the curve and selecting appropriate functions, where the features of iris and fingerprint were recovered. The given features were matched to the database and a GAR of 98.3% was achieved [17].

Xing et al showed a novel technique for integrating gait with face particularly with Closed Circuit TV (CCTV) camera. Input images have been obtained and disparities between the values of same individual have been minimized. They combined the features in a subspace of connection with the features of a single person. They created a chemical database of 40 subjects by using 2 open CASIA Gait and ORL face datasets to demonstrate their technique. The nearest rankings were used and their accuracy was 98.7%. Many techniques are proposed to extract biometrics that has been documented by the scientific community [18]. For instance, Sheik et al used DT-DWT transformation to extract functions from the fingerprint. They have used the AdaBoost rating and achieved an accuracy of 99.5% [19]

However, the majority of multimodal systems depend on the combination of physiological features. As most physiological characteristics are publically available, it's worth combining the biometric physiological characteristics and the biometric computational characteristics. The functional fusion of fingerprints with online signatures using deep learning...
approaches have been investigated to the best of our knowledge. In the combination of fingerprints and online signatures was offered but just proposed the fusion process and testing results were not provided [20]. Furthermore, the attachment and online signatures of Imran et al are merged at the feature level. However, no deep learning approaches and conventional algorithms such as kNN and SVM were utilized. The technique indicated was 98.5% accuracy by using the 2006 Fingerprint verification competition dataset, and the MCYT-100 signature dataset. This research article exposes the most common behavioral biometric identification for deep learning is a fingerprint, iris, face and palmprint, which are the most common physiological biometrics with the online signature [21].

4. PROPOSED FRAMEWORK

    The CNN approach is very suitable for best feature extraction procedure in many image classification procedures. The proposed system added the palm print features for training through CNN for multimodal biometric recognition system. It includes three layers as follows;

1. Convolutional Layer
2. Pooling Layer
3. Fully Connected Layer
Figure 3 Feature Extraction through Proposed CNN

The input image passes through the aforementioned three layers to identify various features of the exact person in order to deploy an accurate recognition. The features are retrieved by filtering images from multiple convoluted layers via the input frame for visual information to remain determined by using kernels or meshes. Filters in the early CNN layers identify simple patterns and colors to detect more complicated patterns and colors, when an image is crossed. Filters identify characteristics by using a convolution technique to generate a characteristic output map. When the image passes through the pooling layer, CNN's complexity is reduced [22, 23, 24]. The fully connected layers will combine a one-dimensional vector's properties with a "ReLU" function to leverage classification results. The figure represents the CNN model for feature extraction and classification to identify biometric systems from the online signature.
Verification Phase

The proposed framework includes the verification phase. Besides, this additional verification unit increases the accuracy of proposed system. If an unknown user attempt to log in to any database, the features are extracted and compared with many verification units such as the face, fingerprint, finger vein, iris, and palm print. Nevertheless, the system does not have any feedback to reach back to the user. So the person, who dislikes answering many questions from authentication websites, may appreciate this approach. The final decision can be either login or not authenticated to an unauthorized person. If the person is authorized, log in the credentials without attempting to answer many inquiries [25, 26].

![Additional Verification Process Diagram]

Figure 4 additional verification Process

5. RESULTS & DISCUSSION

This research article has utilized the proposed dataset named as MBR. Palm print, fingerprint, iris, face, and finger vein are included in our training dataset as shown in the figure. To improve the identification accuracy, the palm print is utilized in multimodal biometric recognition system. Figure 5 shows various authenticated palm print samples.
Besides, some of the standard datasets are used for training and testing in order to compute the accuracy of the system. USM and SDUMLA-HMT datasets are used to check the system accuracy [27]. Figure 6 shows the multi-features present in our training dataset.

It is noted that, the multimodal feature fusion with palmprint framework achieves a better identification than any other uni-modal and ridgelet transform methods. Finally, the proposed framework is constructed with “ReLU” activation function to declare the final decision. Table 1 shows the computed values of the proposed biometric recognition system.
Table 1 Comparison Between Unimodal and Multimodal

<table>
<thead>
<tr>
<th>S.No</th>
<th>Biometric Model</th>
<th>Fusion Approach</th>
<th>Identification Accuracy</th>
<th>Recognition error (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Uni-modal</td>
<td>Iris, face</td>
<td>84%</td>
<td>0.051</td>
</tr>
<tr>
<td>2</td>
<td>Image processing by ridgelet transforms</td>
<td>finger print</td>
<td>82%</td>
<td>0.175</td>
</tr>
<tr>
<td>3</td>
<td>Multimodal</td>
<td>Iris, face, finger vein,</td>
<td>89%</td>
<td>0.023</td>
</tr>
<tr>
<td>4</td>
<td>Proposed Multimodal CNN Approach</td>
<td>Iris, face, finger print/vein, palm print</td>
<td>94%</td>
<td>0.008</td>
</tr>
</tbody>
</table>

The ReLU function has received a vector to include the fusion of many features with a set of authorized person through multiple biometric databases. The proposed framework is performed in the user identification to correct the error present in the existing method. The accuracy is one of the evaluating parameters for the proposed system performance, which is defined as,

\[
Accuracy = \frac{No. \text{ of exact classified images}}{Total \text{ numer of images}} \times 100
\]

Figure 7 Performance Measure of Proposed Framework
Figure 7 shows the proposed multimodal fusion biometric recognition system, which has achieved a better accuracy level than existing methods.

6. CONCLUSION

To conclude, this paper has developed a multimodal biometric model for user identification in the existing technologies. To recognize an accurate individual without making a mistake, the system uses the CNN deep learning algorithm for performing feature extraction. Feature level fusion and two distinct methods of score fusion were employed to identify the person from the iris, face, finger vein, and palm print. To our knowledge, this is the first work to explore the use of deep learning techniques for a multimodal biometric model that includes palmprint. Furthermore, as previously said, no work has been done using palmprint on a multimodal biometric identification system, which is one of the most popular in many developed countries, like Switzerland, the United States, and others. As far as additional research is concerned, this research work aims to develop hybrid deep-learning classification techniques from scratches that are suited for each character rather than a pre-trained model. For example, it offers greater precision to create a combination of CNN and a finger vein support vector machine (SVM) for palm-print images. In general, the SVM may be classified for the images in a good manner. Additionally, this research work investigates the more comprehensive variety of identification features such as DNA, signature, or hand shape with deep learning algorithms. The suggested model with multiple level fusion processes and different multimodal datasets would also be interesting to expand the spectra of tests [28, 29].

REFERENCES


**Author’s Biography**

T. Vijayakumar, is currently working as Professor, in Department of ECE, at GNIT, Hyderabad, India. His research includes Computer Vision, Motion Analysis, Stereo Vision, Object Recognition, computer graphics, photo interpretation, image retrieval, Embedded Image Processing and Real-time image and video processing applications.