Palmprint and Iris based Authentication and Secure Key Exchange against Dictionary Attacks

Abstract

The Multimodal Biometric based user authentication systems are highly secured and efficient to use and place total trust on the authentication server where biometric verification data are stored in a central database. Such systems are prone to dictionary attacks initiated at the server side. In this paper, we propose an efficient approach based on multimodal biometrics (Palmprint and Iris) based user authentication and key exchange system. In this system, texture properties are extracted from the palmprint and iris images are stored as encrypted binary template in the server’s database, to overcome the dictionary attacks mounted by the server. The image processing techniques are used to extract a biometric measurement from the palmprint and iris. During login procedure the mutual authentication is done between the server and user and a symmetric key is generated on both sides, which could be used for further secure communication between them. Thus meet-in-the-middle attack that happens between the user
and the server can also be overcome. This system can be directly applied to strengthen existing password or biometric based systems without requiring additional computation.

Reference

- David Zhang, “Palmprint Idetification using Feature-level Fusion”, Pattern Recognition society, Published by Elseiver Ltd, 2005.

Index Terms

Computer Science Biometrics
### Key words

<table>
<thead>
<tr>
<th>Authentication</th>
<th>Dictionary Attack</th>
<th>Palmprint</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fusion</td>
<td>Iris</td>
<td>Key Exchange</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Minutiae points</td>
</tr>
</tbody>
</table>