5th International Conference on Advanced Research in Computing (ICARC) 2025
Graduate Colloquium

Paper ID:243

Privacy-Protected Iris Recognition Using Block-Feature Fusion

Wickramaarachchi W.A.W.U.[1,2*], Zhao D.[1], Zhou J.[1], Xiang J.[1]

[1] Wuhan University of Technology ,Wuhan, China, [2]Rajarata University of Sri Lanka, Mihintale, Sri Lanka
[*]wirajudara@gmail.com

There is a strong correlation between individuals and their iris patterns and those patterns are unchanged throughout human life. Therefore, the iris biometric is regarded as a distinct, reliable biometric that can be utilized as an authentication element. The privacy of users and the security of iris biometric systems can be seriously threatened if attackers gain access to users' enrolled biometric information. The recognition accuracy and privacy of enrolled iris templates of an iris recognition system are two essential aspects required to maintain at a higher level. Information distortion is one of the convenient ways to provide privacy on an iris template. However, this would result in degrading the recognition accuracy of the iris recognition system. When an authentication system tries to provide both concurrently, there is a trade-off between recognition accuracy and privacy aspects. It would be a significant result if the research could make a well-balanced trade-off between the recognition accuracy and privacy of iris templates. Transforming iris features is one strategy to achieve privacy in iris templates. We propose an approach that processes the features of an iris template block-wise. However, the block size is limited to the size of a column to control the degradation of discriminatory information of original iris templates. The XOR operation is applied to three adjacent columns in two steps in the fusion process. In this process, the first XOR operation is applied between a column and its' next adjoining column. The second XOR operation is applied between the previous result and the next adjacent column. This process continues up to the end of the input iris template. Two datasets were used to test the three proposed approaches. The proposed approach achieved higher recognition accuracy meantime keeping privacy at an acceptable status. Based on the results of dataset 1, the proposed approach accepts genuine users at a rate of 99.11% while it accepts 0.01% of imposters. For dataset 2, the Genuine Acceptance Rate (GAR) is depicted as 81.12% while FAR is at 0.01%. As further improvements, the research can be extended to more widespread databases and higher-quality iris samples.

Keywords: *Biometric Authentication, Feature transformation, Irreversibility, Bit Fusion, XOR operation.*