Abstract

Biometric Authentication systems adopt a suitable image processing technique to manipulate the biometric images. It refers to verifying a person using their biometric traits that includes physiological, biological and/or behavioral traits like iris, face, fingerprint, voice, hand writing etc. A biometric characteristic should be unique, universal, permanent and acceptable. In this work, the texture feature of palm and finger print extracted using Gabor filter and fusion is done by concatenation. The high dimensionality of fused features are reduced using ant colony
Latent Palm Fused with Fingerprint to Improve Authentication Performance

optimization (ACO) algorithm and finally only the most significant features are used for classification of genuine and imposter users. Any two-class classifier can be used for classification. Three classifiers namely a SVM classifier with Linear and RBF kernels and NC (Normalized Correlation) are used for classification and the results were compared. A classification accuracy of 98.6% is discussed in literature for high resolution scanner images. The least Total Error ever reported in literature is 7.94% [12] This work aims at improving the accuracy of classification of the authentication system with noisy samples, while reducing the Total Error (TE), False Acceptance Rate (FAR), False Rejection Rate (FRR) and Equal Error Rate (EER). For evaluation of the system a real time database was constructed with a finger and palm print scanner. The database consists of four samples each for an individual.

References

- C. J. C. Burges, "A Tutorial on Support Vector Machines for Pattern
- Chang-Chun Lin, Lu-Chan Tseng, Website reorganization using an ant colony system, Expert System with Applications, Vol. 37, 2010, pp. 7598-7605,

Index Terms

Computer Science
Security

Keywords

Multi Biometric Fusion Palm And Fingerprint Ant Colony Optimization Svm Classifier
Gabor Filter
Texture Features.