Abstract

As modern means of communication increase in their potential and receptiveness, they instigate additional demands in terms of security. Therefore, communication between users via social network becomes complicated, that increases possibility of threats with respect to user authentication. With the objective of ensuring security in social networks, different user authentication and cryptographic mechanism were designed. But, with different heuristic and computational algorithm, user authentication through single modal biometric is easily broken and vulnerabilities of multimodal approaches in social network still remain unexplored. This paper proposes a novel Fusion based Multimodal Biometric Security (FMBS) method utilizing Face and Fingerprint features of human individuals on social networks. Feature extraction for FMBS is performed utilizing combination of Binomial Feature Distribution Algorithm and Neighborhood Dominant Attribute Identification for both face and fingerprint features. Then, dominant attributes are stored in spatial vector for both the modalities to form biometric fusion template. Finally, Structural Biometric Fusion Template Matching algorithm designed to compute matching accuracy of test data to available training data. Experimental evaluation with
Biometric Research Repositories is conducted. Performance evaluation show that the method significantly improve matching accuracy of human biometric samples, compared to conventional biometrics user authentication that only make use of single modal biometrics. The result shows that the method has low social network authentication time and network space complexity suited for deployment in real time social network sites.

References


Index Terms

Computer Science  Networks

Keywords

Social Network System, Cryptographic Security, Multimodal Biometric, Neighborhood Dominant Attribute, Spatial vector, Template matching