

BIOMETRIC CRYPTOSYSTEM USING FUZZY VAULT FOR IRIS

ARCHANA K. C.

Abstract

Crypto-biometrics is an emerging architecture where cryptography and biometrics are merged to achieve high level security systems. Cryptographic construction called fuzzy vault is used to store digital signature based on iris pseudo textures. Iris pseudo textures such as nodes and end points does not change throughout the life period of user and can be used to extract minutiae to lock and unlock the fuzzy vault. The proposed algorithm aims to create a fuzzy vault to store secret key, based on iris pseudo textures. The algorithm has two phases: The first is to extract binary key (digital signature) from iris textures, and the second is to generate fuzzy vault by using Lagrange interpolating polynomial projections.

Keywords: Crypto-biometric, fuzzy vault, polynomial projection, chaff points, unlock complexity.