

ABSTRACT OF THE DISCLOSURE

WIRELESS BIOMETRIC AUTHENTICATION SYSTEM AND METHOD

Embodiments of the invention involve using biometric templates to wirelessly authenticate individuals. In one embodiment, a mobile device may generate a first biometric template and a first public value from a first biometric sample of a user and generate a first cryptographic key by passing the first biometric template to a fuzzy extractor's generate function. An access device may generate a second biometric template from a second biometric sample of the user, generate a second secret cryptographic key by passing the second biometric template and the first public value to the fuzzy extractor's reproduce function, encrypt the second biometric template with the second secret cryptographic key, and broadcast the encrypted template to a plurality of nearby mobile devices including the mobile device. If the mobile device is able to decrypt the encrypted template with the first cryptographic key, the access device can associate the user with the mobile device.

FIG. 1