**ABSTRACT**

The increasing popularity of biometrics and cryptography is driven by the widespread stipulation on information security. Abundant efforts have been made in developing successful methods in these areas in order to accomplish an enhanced level of information security. There are two dominant issues in information security enhancement. One is to defend the user ownership and control the access to information by authenticating an individual’s identity. The other is to make sure the privacy and integrity of information and to secure communication. Cryptography is the science of writing in secret code. Secret-key cryptography and public-key cryptography are the two most important cryptographic architectures. The security of a cryptographic system is reliant on the secrecy of the cryptographic key. Biometric authentication or simply biometrics refers to establishing automatic personal recognition based on the physical and behavioral characteristics of an individual (e.g. face, voice, fingerprint, gait, hand geometry, iris, gene, etc.). Biometrics offers superior security and easier than traditional identity authentication systems (based on passwords and cryptographic keys).Since biometrics characteristics are naturally related with a particular individual, making them insusceptible to being stolen, forgotten, lost or attached. This paper presents a survey on various techniques proposed earlier in developing an authentication system for ensuring individual’s information security by combining biometric characteristics of that particular individual and the cryptographic techniques. In addition, it provides some fundamental idea for future research that may help in eliminating the problems associated with the present authentication systems