Abstract

Information exchange across the Internet and the storage of sensitive data on open networks, cryptography is becoming an increasingly important feature of computer security. Existing asymmetric encryption algorithms require the storage of the secret private key. Stored keys are often protected by poorly selected user passwords that can be either guessed or obtained through brute force attacks. Combining biometrics with cryptography is seen as a possible solution. Biometric cryptography is a technique using biometric features to encrypt data. This technique has proved to be more secure. This thesis proposes cryptosystem based on palmprints. Here encryption/decryption of data is directly performed by using the palmprint as a key. Due to complexity of palm print information it is not possible, to crack the system. In the encrypting phase, 1024 bits binary string is extracted from the palmprints using differential operations. Here the string is translated to a 128 bits encrypting key using a Hash function, Hence at the same time, an error-correct-code (ECC) is generated. Generally, encryption algorithms use the 128 bits encrypting key to encrypt the data. In decrypting phase, the 1024 bits binary string extracted from the input palmprint is first corrected using the ECC. Again, by the using of same hash function corrected string is translated to decrypting key. The data is finally decrypted by using the decrypting key corresponding general decryption algorithms.