Abstract

Network security has become a great threat to the network accessible resources that consists of policies to prevent, monitor unauthorized access, modification, and misuse of computer network. Several algorithms and techniques were proposed for the secure transmission of data and to protect user’s privacy. Secret-key cryptography and public-key cryptography are the techniques used for the protection of security issues. However, such a key needs to be stored in a protected place or it should be transported by a shared communication line. So generation of cryptographic key using biometric traits of both sender and receiver during communication avoids key storing and improves security strength. The proposed approach for detecting the quality of fingerprint by using the method called orientation certainty level (OCL). If the image has good quality then feature extraction will be done using Scale Invariant Feature Transform, otherwise poor quality image will get ignored. By using cover image the obtained cancellable template will get hidden. Then the hidden image will be transmitted from sender to receiver and receiver to receiver to sender by using Variable Least Significant Bit techniques. Finally the performance metrics like FAR (False Acceptance Rate), FRR (False Rejection Rate), and
Fingerprint bio-Crypto key generation using Scale Invariant Feature Transform (SIFT)

Accuracy of the proposed work is compared with the existing system.

**References**


Index Terms

Computer Science Security

Keywords

Cryptography key, Orientation Certainty Level, Scale Invariant Feature Transform, Variable Least Significant Bit