Abstract

Moustafa Hussein Aly

Optical PTFT Asymmetric Cryptosystem Based Secure and Efficient Cancelable Biometric Recognition System

Recently, biometric systems are extensively and commonly utilized for authentication and verification applications. The security issue and the dependence on a specific biometric for the biometric verification process are the main challenges confronted in biometric systems. The security issue comes due to the exploitation of the original biometrics in stored servers. Therefore, if any attacks have been introduced to the stored biometrics, they will be missed indefinitely. Consequently, the stored original biometrics must be secured through maintaining and storing these templates away from exploitation in their servers. So, there is a need for designing a cancelable biometric recognition system (CBRS) that is a promising protection trend in biometric verification and authentication fields. The CBRS is based on the conversion of biometric data into a different arrangement. In this article, a novel CBRS based on the suggested optical PTFT (Phase Truncated Fourier Transform) asymmetric encryption algorithm is introduced. In the proposed algorithm, two different distributions of phases in the output and Fourier planes are maintained as deciphering keys, and thus, the encryption keys will not be utilized for the decryption process. This leads to the advantage that the two ciphering keys may be utilized as public secret keys to encrypt distinct biometric images. Consequently, the suggested PTFT cryptosystem is an asymmetric encryption/decryption technique compared to the preceding related optical encryption techniques that are symmetric techniques such as Optical Scanning Holography (OSH) and Double Random Phase Encoding (DRPE). The suggested PTFT asymmetric encryption algorithm also has a wonderful practical performance in security applications. One of the main contributions of the proposed optical PTFT asymmetric encryption algorithm is that it removes the linearity features of the optical OSH and DRPE symmetric encryption algorithms through its great features of the phase truncation nonlinear operation. Subsequently, this produces an encrypted biometric template with two public keys, and the authenticated user can retrieve the original biometric template utilizing two private keys with achieving a high security and cancelability performance for the stored biometrics. To conrm the efcacy of the suggested optical encryption algorithm for developing a secure CBRS, various biometric datasets of face, ear, palmprint, ngerprint, and iris images are examined and analyzed. Extensive comparative analyses are performed amongst the suggested algorithm and the optical OSH and DRPE encryption algorithms. The experimental outcomes achieved for performance quality assessment assure that the suggested CBRS is reliable, robust, and realistic. It has great security and cancelability prociency that expose excellent cancelable biometric recognition performance even in the existence of noise. Moreover, the performed experiments declare that the suggested CBRS guarantee an average FRR (False Reject Rate) of 0.0012, EER (Equal Error Rate) of 0.0019, and FAR (False Accept Rate) of 0.0030, and an average AROC (Areas under the Receiver Operating Characteristic) of 0.9996.