

Fingerprint Image Encryption Using a 2D Chaotic Map and Elliptic Curve Cryptography

Authors : D. M. S. Bandara, Yunqi Lei, Ye Luo

Abstract : Fingerprints are suitable as long-term markers of human identity since they provide detailed and unique individual features which are difficult to alter and durable over life time. In this paper, we propose an algorithm to encrypt and decrypt fingerprint images by using a specially designed Elliptic Curve Cryptography (ECC) procedure based on block ciphers. In addition, to increase the confusing effect of fingerprint encryption, we also utilize a chaotic-behaved method called Arnold Cat Map (ACM) for a 2D scrambling of pixel locations in our method. Experimental results are carried out with various types of efficiency and security analyses. As a result, we demonstrate that the proposed fingerprint encryption/decryption algorithm is advantageous in several different aspects including efficiency, security and flexibility. In particular, using this algorithm, we achieve a margin of about 0.1% in the test of Number of Pixel Changing Rate (NPCR) values comparing to the-state-of-the-art performances.

Keywords : arnold cat map, biometric encryption, block cipher, elliptic curve cryptography, fingerprint encryption, Koblitz's encoding

Conference Title : ICIAP 2018 : International Conference on Image Analysis and Processing

Conference Location : Paris, France

Conference Dates : October 29-30, 2018