DOI: 10.24996/ijs.2020.61.10.29

Iraqi Journal of Science

ISSN: 0067-2904

Robust Blind Watermarking Technique Against Geometric Attacks for Fingerprint Image Using DTCWT-DCT

Mohamed Lebcir[1], Suryanti Awang*[1], Ali Benziane[2]

[1]Soft Computing & Intelligent System Research Group (SPINT), Faculty of Computing, Universiti Malaysia Pahang, Lebuhraya Tun Razak, 26300, Kuantan, Pahang, Malaysia

[2]Faculty of Science and Technology, University of Djelfa, Algeria

Received: 31/10/2019 Accepted: 31/3/2020

Abstract

In this research paper, a new blind and robust fingerprint image watermarking scheme based on a combination of dual-tree complex wavelet transform (DTCWT) and discrete cosine transform (DCT) domains is demonstrated. The major concern is to afford a solution in reducing the consequence of geometric attacks. It is due to the fingerprint features that may be impacted by the incorporated watermark, fingerprint rotations, and displacements that result in multiple feature sets. To integrate the bits of the watermark sequence into a differential process, two DCT-transformed sub-vectors are implemented. The initial sub-vectors were obtained by sub-sampling in the host fingerprint image of both real and imaginary parts of the DTCWT wavelet coefficients. The basic difference between the relevant sub-vectors of the watermarked fingerprint image in the extraction stage directly provides the inserted watermark sequence. It is not necessary to extract watermark data from an original fingerprint image. Therefore, the technique suggested is evaluated using 80 fingerprint images from 10 persons, from both CASIA-V5-DB and FVC2002-DB2 fingerprint database. For each person, eight fingerprints are set as the template and the watermark are inserted in each image. A comparison between the obtained results with other geometric robust techniques results is performed afterwards. The comparison results show that the proposed technique has stronger robustness against common image processing processes and geometric attacks such as cropping, resizing, and rotation.

Keywords: Fingerprint, Fingerprint image watermarking, DTCWT, DCT, Geometric robust.

Introduction

A fingerprint is demonstrated on the surface of a fingertip by the interpretation of the ridge and valley pattern. The combination of their minutiae points determines the exclusivity of a fingerprint [1, 2]. Because of their distinctiveness, fingerprint images are generally used for user authentication purposes. Thus, it is essential to protect the fingerprint's authenticity. Digital watermarking can be used to verify the authenticity of a fingerprint sample [3]. The basic idea of the digital watermarking approach lies in embedding watermark data into the original fingerprint image in order to maintain fingerprint ownership security. In addition, the watermark data can be encrypted before entrenching the watermark as a second layer of protection [4]. A secret key is used to determine the locations where the watermark would also be inserted in the fingerprint image. If the user wants to check the fingerprint images that could have been corrupted or skewed, the embedded watermark sequence can be retrieved on the basis of the secret key used to encode the watermark. Thus, the operator's key role is preventing attackers from gaining access to the watermark data.

*Email: suryanti@ump.edu.my