ABSTRACT

University of Macau

BIOMETRIC WATERMARK EMBEDDING IN
DOCUMENT IMAGES

by Lam Ioi Tun, Victor

Thesis Supervisor: Associate Professor, Prof Pun Chi Man
Master of Science in E-Commerce Technology

In respect to the issues on privacy, security and legal significance of a document, some sorts of security protections should be put on a document to ensure its genuineness and integrity. In this thesis, signatories' digital biometric fingerprint acting as a watermark message will be embedded into a document image by the methods of Flipping, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT).

When Flipping is applied for watermark message embedding and extraction, document image will firstly be adaptively partitioned into fixed size pixel blocks according to the number of bits in the watermark message and the flipping will be performed on the basis of bit to partition. While in applying DCT, both document image and watermark message will firstly be adaptively partitioned into equal numbers of fixed size blocks and message embedding and extraction will be done on the basis of block to block. However in DWT, no partition is applied on images but rather, a two level iterations of DWT have been processed for watermark message embedding and extraction.

Experimental results from the prototype system show that the proposed methods Flipping, DCT and DWT are successfully tested for embedding a fingerprint watermark message in document images and the embedded watermark message can be extracted from the watermarked document images. Further experiments on robustness by introducing some sorts of interferences imitated by Gaussian White

Noise, JPEG compression, Low-Pass Filters, and by their scanned copy against DCT and DWT's watermarked document images were tested. Except for the document images from scanning, the embedded watermark message, with certain degree of tolerance, can be extracted from the watermarked document images even under such various imitated attacks. However, the tolerance may not be acceptable as the interferences become larger. Therefore, further studies on other digital watermarking techniques and improvements on the current studied methods to minimize the degree of tolerance should be continued in the future. Another robustness test whose attack was also imitated by a scanned copy of the Flipping's watermarked document images indicated the failure on extracting a visible embedded fingerprint watermark message.

Using a close degree of imitating interference attack and visibility quality watermarked document images generated from DCT and DWT method, robustness comparison between these two watermarked document images showed that the extracted embedded watermark message on the attacked watermarked document images from DCT method seemed to be more robust than the other one. But the difference is so insignificant that, as a whole, one cannot conclude that DCT method has better performance than DWT method.