Abstract

Digital image is a result of someone's work. Therefore, the status of ownership of the image should be protected. Also if it is has been tampered, must be able to detected quickly. Digital watermarking provides the perfect solution to both problems. In the watermarking system in this final project, the system not only able to embed a watermark into an image, but also able to detect the tampered part so that the authenticity of the image is maintained.

The watermark is generated from the host image using ICA algorithm. Therefore, this technique also can be called Self-Embedding Watermarking. Previously, matrix from the host image is segmented into several blocks in order to simplify the calculation process, then obtain the mixing matrix from each block using ICA. After that, Frobenius norm is computed in order to produce single non-negative number. This number, combined with numbers obtained from a similar operation of other blocks, forms a string of watermark that will be embedded. Watermark embedding performed using quantized DCT by replacing the middle coefficient from each block with a number of watermark that has been obtained. The system is tested by introducing several attacks on the watermarked image with expectations that the system able to detect a defected part. In addition, the quality of watermarked image will also be compared with the host image. A good watermark does not degrade much quality of the host image.

The experiments show that the system generates a good quality watermarked image (PSNR > 40 dB). ICA and DCT technique used is also generates watermarks that are robust to certain attacks. Thus, it can be concluded that merging ICA and DCT for watermarking can provide a solution to the image authentication problem.

Keyword : digital watermarking, watermark, ICA, DCT, robust