

## Abstrak

Citra medis digital mempunyai dua hal penting yang perlu diperhatikan yaitu autentikasi kepemilikan dan keaslian citra. Kepemilikan citra harus dinyatakan dengan benar dan modifikasi pada citra harus dapat dideteksi. Solusi dari kedua permasalahan tersebut adalah dengan *multiple watermarking*. Pada Tugas Akhir ini *multiple watermark* terdiri dari dua jenis yaitu *signature watermark* dan *reference watermark*. *Signature Watermark* berupa teks, digunakan untuk menyatakan kepemilikan dari citra medis. Sedangkan *reference watermark* berupa citra, digunakan untuk mendeteksi modifikasi yang mungkin terjadi pada citra medis digital.

Penyisipan kedua *watermark* dilakukan pada domain *wavelet* dengan melakukan dekomposisi 2 level dan kuantisasi pada koefisien transformasi. Sesuai dengan adanya batasan yang tegas yang diterapkan pada citra medis, pada proses penyisipannya dimungkinkan melakukan pendefinisian terhadap *Region of Interest* (ROI) yang mana nilai diagnostiknya dilindungi karena informasi yang disisipkan disana hanya bertujuan untuk *integrity control*. Selain itu, untuk meningkatkan ketahanan dari *signature watermark* digunakanlah *hybrid coding*, yaitu penyisipan BCH *encoded watermarks* secara berulang. Pengujian dilakukan dengan mensimulasikan sejumlah serangan terhadap citra yaitu *sharpening*, *white Gaussian noise* dan *kompresi JPEG*. Yang akan dianalisis adalah kualitas citra terwatermark dan ketahanan teks *signature* serta kerentanan citra *reference*.

Hasil pengujian antara lain teknik *multiple watermarking* menunjukkan kinerja *imperceptibility* yang baik. *Sharpening* merupakan serangan yang keras dan penggunaan *hybrid coding* tidak mampu meningkatkan ketahanan *signature watermark* terhadap serangan ini. Sedangkan untuk pemberian *noise* dan kompresi JPEG, penggunaan *hybrid coding* menunjukkan performa yang baik dengan peningkatan *robustness* setelah level serangan mencapai tingkat tertentu. Sementara itu, *reference watermark* memiliki tingkat fragilitas yang tinggi dan mampu mendeteksi serangan yang terjadi bahkan untuk level serangan terkecil sekalipun.

**Kata kunci** : *multiple watermarking, wavelet decomposition, repetitive BCH encoding*