

ABSTRAK

Kemudahan penyebaran media digital seperti foto dapat merugikan pemilik hak cipta media tersebut. Pihak-pihak yang tidak bertanggung jawab dapat dengan mudah membajak dan mengakui kepemilikan dari media tersebut. Oleh sebab itu, dibutuhkan cara yang tepat untuk melindungi hak cipta sekaligus menjadi bukti bahwa media tersebut merupakan milik pemegang hak cipta yang sah. Permasalahan tersebut dapat diatasi dengan menggunakan digital *watermarking* menggunakan steganografi *least significant bit* (LSB) dan kriptografi *vigenere cipher*. Steganografi *least significant bit* (LSB) merupakan teknik penyisipan yang digunakan untuk menyisipkan *watermark* yang berisi informasi kepemilikan kedalam citra gambar *bitmap*. Steganografi *least significant bit* (LSB) bekerja dengan cara menyisipkan setiap *bit* dari *watermark* kedalam *bit* terakhir dari setiap warna dasar (*red*, *green* dan *blue*) yang terdapat pada setiap *pixel* gambar *bitmap*. Akan tetapi, Steganografi *least significant bit* (LSB) memiliki kelemahan terhadap modifikasi gambar sehingga dapat merusak atau menghilangkan *watermark* yang terdapat pada gambar sehingga tidak dapat terlihat ketika dilakukannya proses ekstraksi.

Proses penyisipan terdiri dari dua tahap yaitu tahap enkripsi menggunakan kriptografi *vigenere cipher* dan dilanjutkan dengan tahap penyisipan menggunakan steganografi *least significant bit* (LSB). Untuk mencegah rusak atau hilangnya *watermark* yang terdapat pada gambar dapat dilakukan dengan cara memodifikasi posisi penyisipan *watermark* pada gambar. *Watermark* disisipkan pada pojok kiri atas, pojok kanan atas, pojok kiri bawah dan pojok kanan bawah pada gambar secara vertikal. Hal tersebut dilakukan dengan tujuan mencegah rusak atau hilangnya *watermark* karena proses pemotongan pada gambar. Selain itu dilakukan juga modifikasi terhadap proses ekstraksi. Proses ekstraksi dilakukan sebanyak delapan kali yaitu empat kali ekstraksi vertikal dengan posisi pojok kiri atas, pojok kanan atas, pojok kiri bawah dan pojok kanan bawah pada gambar serta empat kali ekstraksi horizontal dengan posisi pojok kiri atas, pojok kanan atas, pojok kiri bawah dan pojok kanan bawah gambar. Proses ekstraksi dilakukan sebanyak delapan kali dimaksudkan untuk mencegah rusak atau hilangnya *watermark* karena proses rotasi dan *flip* pada gambar.

Berdasarkan hasil penelitian yang telah dilakukan, steganografi *least significant bit* (LSB) dan kriptografi *vigenere cipher* dapat digunakan untuk menyisipkan *watermark* kedalam gambar. Selain itu, modifikasi yang dilakukan terhadap posisi penyisipan *watermark* dan ekstraksi *watermark* dapat meningkatkan ketahanan (*robustness*) dari proses modifikasi gambar yang dapat merusak atau menghilangkan *watermark*.

Kata Kunci : *Digital Watermarking, Robustness, Steganografi Least Significant Bit (LSB)*