ROBUSTNESS CITRA DIGITAL BERWATERMARK DENGAN METODA SHAMIR'S SECRET SHARING SCHEME

Mardianto Chandra[1], Fazmah Arief Yulianto[2], Adiwijaya[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Digital watermarking merupakan metoda untuk menyisipkan suatu informasi, yang biasanya disebut sebagai watermark, pada suatu data digital penampung. Watermarking umumnya hanya digunakan untuk melindungi hak cipta pada satu orang tertentu saja. Bagaimana menangani jika pemilik hak cipta ternyata lebih dari seorang? Solusinya dengan menggunakan metoda secret sharing scheme pada citra digital watermarking. Tugas Akhir ini akan menjelaskan bagaimana bentuk penerapan penyisipan watermark dan pendeteksian kepemilikannya. Serta bagaimana robustness citra digital berwatermark pada proses manipulasi citra digital seperti perubahan brightness, kontras, scaling, flipping dan rotasi.

Kata Kunci : Hak Cipta, Shamir’s Secret Sharing Scheme, Watermarking,

Abstract

Digital watermarking is a method to embed information that we called watermark, in digital data. Generally, watermarking only used for protected copyright of one human. How it works if more than one has copyright? The solutions is using secret sharing scheme in image watermarking. This TA will explain how to embed and detect the watermark. Also, how robust image watermarking in process manipulation image, like brightness, contrast, scaling, flipping and rotation.

BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan teknologi digital semakin meningkat, ini mengakibatkan mudahnya user dalam melakukan proses penggandaan dan pertukaran data seperti pada text, citra, audio maupun video. Pada sistem digital, penggandaan data dapat menghasilkan data baru yang hampir menyerupai data asli, untuk itu di perlukan suatu sistem perlindungan hak cipta terhadap data tersebut.

Pengguna citra digital seringkali melakukan manipulasi pada suatu citra digital untuk mendapatkan tampilan citra digital baru sesuai dengan keinginannya. Karena itu, pemilik menginginkan citra digitalnya tidak di manipulasi oleh orang lain. Jika pun terjadi manipulasi terhadap citra digitalnya, pemilik mempunyai bukti bahwa citra tersebut tetap miliknya. Misal, ada wartawan mempunyai sebuah citra digital yang akan dimuatnya kedalam suatu majalah. Ketika akan diberitakan ternyata yang menjadi pemilik citra digital bukan wartawan tersebut. Untuk menjaga bukti kepemilikan tersebut bisa kita gunakan teknik watermarking. Watermarking yaitu teknik menyisipkan suatu informasi ke dalam data multimedia. Informasi tersebut dapat berupa data citra, audio, atau text yang menggambarkan kepemilikan suatu pihak. Informasi yang disisipkan tersebut disebut *watermark*. *Watermark* dapat dianggap sebagai sidik digital dari pemilik data multimedia tersebut, dalam hal ini berupa citra digital.

Karena hak cipta suatu citra digital tidak hanya dimiliki seorang saja. Maka diterapkanlah suatu metoda untuk melakukan pembagian suatu secret, biasanya berupa kunci, menjadi beberapa bagian yang disebut share, kepada sejumlah pihak (pemilik citra digital) yang disebut participant, dengan kondisi-kondisi tertentu. Metoda tersebut disebut dengan *Secret Sharing Scheme*. Dewasa ini, *Secret Sharing Scheme* telah digunakan pada bidang-bidang aplikasi yang beragam, misalnya kontrol akses, peluncuran senjata atau proyektil, membuka kotak deposito, dan lain-lain. Digital watermarking merupakan salah satu bentuk pengembangan metoda penyembunyian data, yang sebenarnya lebih ditekankan pada fungsionalitas dari data digital yang disisipkan, maupun data digital yang digunakan sebagai penampung. Digital watermarking telah banyak diterapkan dalam berbagai bentuk aplikasi dengan fungsionalitas yang beragam. Penerapan *Secret Sharing Scheme* pada citra digital tentu saja membutuhkan protokol-protokol dan metoda-metoda untuk proses penyisipan (*embedding*) *watermark* serta protokol-protokol untuk proses pendeteksian kepemilikan (*detection*) *watermark*.

Watermark yang disisipkan tentu harus memiliki tingkat ketahanan terhadap manipulasi citra. Karena domain spasial rentan terhadap perubahan yang mengakibatkan kerusakan *watermark* yang disisipi. Untuk itu perlu dilakukan pemilihan pixel-pixel citra yang tepat untuk disisipi agar *watermark* yang disisipi terjamin keakuratannya.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang dikemukakan diatas, maka masalah yang akan diteliti adalah :

1. Bagaimana menyisipkan data ke dalam citra digital dan membentuk *secret* didalam citra digital tersebut.
2. Bagaimana menyisipkan watermark kedalam citra digital dengan menggunakan pendekatan metoda *Shamir's Secret Sharing Scheme.*
3. Bagaimana ketahanan citra digital sesudah penyisipan *watermark.*

1.3 Tujuan Penelitian

Secara umum tujuan penulisan yang ingin dicapai dalam tugas akhir ini adalah:

1. Merancang dan mengimplementasikan citra digital menggunakan perangkat lunak yang dapat menyisipkan watermark dengan pendekatan metoda *Shamir's Secret Sharing Scheme*.
2. Membandingkan kualitas citra digital sebelum dan sesudah proses watermarking dengan pendekatan *Peak Signal to Noise Ratio.*
3. Menguji keakuratan *watermark* dengan pendekatan *Bit Error Rate* sebelum dan sesudah proses manipulasi citra berupa rotasi, flip, invert, zoom, brigthness dan contrast.

1.4 Metoda Penelitian

Metodologi yang dilakukan dalam tugas akhir ini mencakup hal-hal sebagai berikut:

1. Mengumpulkan bahan-bahan referensi yang akan menunjang proses penelitian, seperti jurnal-jurnal tentang penyisipan watermark di domain spasial dan frekuensi. Serta, semua yang berkaitan dengan watermarking. Selain dari jurnal-jurnal tersebut, penulis juga mengumpulkan bahan dari TA terdahulu yang membahas watermarking.
2. Identifikasi permasalahan yang akan muncul pada saat melakukan penelitian ini, seperti pembentukan dan pembagian *secret* dalam pemrograman dan kesulitan menerapkan teori-teori dalam proses penelitian nantinya.
3. Membuat rancangan sistem untuk melakukan proses watermarking dengan metoda *Shamir's Secret Sharing Scheme*.
4. Menyusun algoritma program yang digunakan pada proses penyisipan watermark dengan metoda *Shamir's Secret Sharing Scheme*, kemudian mendeteksi kembali data watermark tersebut.
5. Merancang program berdasarkan algoritma yang telah dibuat dan mengimplementasikannya kedalam bahasa pemrograman Delphi.

6. Melakukan analisa hasil implementasi watermarking dengan metoda *Shamir's Secret Sharing Scheme*, untuk mengetahui tingkat ketahanannya (*robustness*).
7. Membuat kesimpulan dari hasil penelitian watermarking dengan metoda *Shamir's Secret Sharing Scheme*.

BAB V
KESIMPULAN dan SARAN

5.1 Kesimpulan

Dari pembahasan diatas dan hasil pengujian program didapat beberapa kesimpulan, antara lain :

1. Sistem watermarking di domain spasial tidak sepenuhnya fragile watermarking (mudah rusak).
2. Sistem manipulasi yang dapat diatasi di domain spasial hanya berupa sistem manipulasi sederhana dan mengubah ke semua pixel. Selama sistem manipulasi dilakukan di semua pixel citra dan tanpa mengubah ukuran citra, bisa dilakukan suatu sistem untuk meningkatkan ketahanannya hal ini terlihat dari manipulasi citra *contrast* dan *zoom out.*
3. Ukuran citra sangat mempengaruhi besarnya maksimum data yang dapat diterima citra.
4. Pembentukan persamaan polinomial akan sangat mempengaruhi hasil ekstraksi. Hal ini disebabkan karena sistem akan membentuk 7 persamaan polinomial lain dari persamaan tersebut, sehingga penyisipan dilakukan sebanyak 8 kali dengan 8 persamaan polinomial.

5.2 Saran

Untuk mendapatkan performansi yang lebih baik lagi, terdapat beberapa saran yaitu :

1. Pengorganisiran pembentukan persamaan polinomial untuk pembentukan jalur sistem watermarking dilakukan dengan cermat, supaya tidak terjadi penyisipan ganda pada 1 pixel.
2. Dengan sedikitnya jalur yang dilalui diharapkan sistem ini bisa dikembangkan untuk penyisipan ganda (watermark ganda) dengan persamaan polinomial yang berbeda.

DAFTAR PUSTAKA

1. Beimel, Amos and Yuval Ishai, "*On the Power of Nonlinear Secret-Sharing*", http://www.cs.bgu.ac.il/~beimel/Papers/Nonlinear.pdf,
2. Burrus, Sidney C. Wavelet and Wavelet Transform, Prentice-Hall International,Inc.1998.
3. Chen, Pei-chun, Yung-sheng Cheny, and Wen-hsing Hsu, Adaptive-Rate Image Watermarking Based On Spread Spectrum Communication Technique, *http://amp.ece.cmu.edu/publication/Trista/cscc1999_trista.pdf*.
4. Fajri. Desain dan Implementasi Sistem Komputasi Terdistribusi Untuk Kompresi Citra Medis Sinar X Menggunakan JPEG 2000, *http://fajri.freebsd.or.id/tugas_akhir/bab3.pdf*
5. Guo, Huiping and Nicolas D. Georganas, "*A Novel Approach to Digital Image Watermarking based on A Generalized Secret Sharing Scheme*", Multimedia Systems 9, 2003
6. Hung-Min, Sun and Shiuh-Pyng Shieh, "*Constructing Perfect Secret Sharing Schemes for General And Uniform Access Structures*", Journal of Information Science and Engineering 15, 679-689, 1999, http:// www.iis.sinica.edu.tw/JISE/1999/199909_04.pdf,
7. Law, M, Averill and W. David Kelton, "*Simulation Modeling and Analysis*",Third Edition, Mc Graw Hill, 2000
8. Mohr, Alex. "*CSE391 Introduction to Data Compression Lecture 15 Wavelet Transform Coding*", http://www.cs.sunysb.edu/~amohr/cse391/2003-spring/lectures/cse391-lecture13.pdf, 2003,
9. RSA Security, "*What are some secret sharing schemes ?*", http://www.rsasecurity.com/rsalabs/faq/3-6-12.html,
10. Suhono, H, Supangkat, Juanda, dan Kuspriyanto, Watermarking sebagai Teknik Penyembunyian Label Hak Cipta pada Data Digital, ITB, 2000.
11. Teolis, Anthony. Computational Signal Processing with Wavelet, Birkhauser, 1998.