IMPLEMENTASI PENYISIPAN DIGITAL SIGNATURE PADA CITRA DIGITAL DENGAN METODE DISCRETE WAVELET TRANSFORMS

Sapta Anggi Purwaning Sari[1], Maman Abdurohman[2], Fazmah Arif Yulianto[3]

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

Abstrak

Penghargaan terhadap hak cipta menjadi topik yang sedang hangat dibicarakan di masyarakat akhir-akhir ini. Hal ini terkait dengan motivasi bagi para pencipta karya untuk dapat terus berkreasi. Banyak pembajak karya yang tidak menyadari kerja keras para pencipta karya. Para pembajak karya dengan sengaja memperbanyak karya asli seseorang atau bahkan mengaku sebagai pencipta karya yang sah.

Tugas akhir ini mengangkat solusi untuk mengatasi pembajakan karya seseorang. Solusi ini menggunakan teknik digital signature dan steganografi secara bersama-sama. Digital signature adalah suatu teknik kriptografi yang betujuan untuk menjamin kepemilikan suatu data. Ada tiga alasan yang mendasari penggunaan digital signature, yaitu authentication, integrity dan non-repudiation. Keabsahan pengirim (authentication) yang berkaitan dengan masalah kebenaran identitas pengirim. Keaslian informasi (integrity) berkaitan dengan keutuhan informasi. Anti penyangkalan (non-repudiation) mengandung arti agar pengirim tidak dapat menyangkal tentang isi informasi yang dikirim. Steganografi adalah seni dan teknik menyembunyikan informasi ke dalam suatu media agar tidak diketahui oleh seseorang kecuali penerima.

Dalam Tugas Akhir ini dibuat sebuah aplikasi yang dapat menyembunyikan informasi rahasia ke dalam suatu media. Informasi rahasia yang akan disembunyikan adalah digital signature dari sebuah media. Media yang digunakan sebagai tempat menyisipkan digital signature adalah sebuah citra digital.

Dalam teknik kriptografi, digital signature dikirimkan bersama dengan media pembentuk signature dalam bentuk yang terpisah. Dalam aplikasi ini, sebagai penanda keaslian sebuah citra, maka digital signature dan media harus dibentuk menjadi satu kesatuan menggunakan teknik steganografi. Penggunaan digital signature sebagai informasi rahasia dan penanda keaslian diambil untuk lebih memperkuat bukti keaslian media tersebut.

Kata Kunci : digital signature, steganografi.

Abstract

Nowadays, appreciation of copyrights has become a hot topic in public. This is related with motivation of the creator to keep producing something. Many piracy of copyrights do not realize the hard work of the creator. The pirates of copyrights really means to make alot of copies from someone's products or creations even they claime the products as their official rights.

This final project gives solution to deal with piracy of someones products. The solution here uses both digital signature technique and steganography. Digital signature is a cryptography technique which goals is to guaranty the originality of data. There are three reasons of the digital signature usability. They are authentication, integrity and non-repudiation. The sender authentication relates with sender identity verification. The originality of information (integrity) relates with the whole content of the information. Non-repudiation means a lot so that the sender can not deny the information sent. Steganography is an art and technique that hides information in a medium so that anybody else would never know the content of information but the receiver. In this final project, an application would be made to hide the secret information in a medium. The secret information that will be hiden is digital signature of a medium. The medium used as hiden place of digital signature is digital image.

In cryptography technique, digital signature is sent simultaneously with signature former medium in a separated form. In this application, as an indication of image originality, a digital signature and medium should be formed as a united that uses steganography technique. The usability of digital signature as a secret information and an indicator is taken to strengthen the evidence of medium originality.

Keywords : digital signature, steganography.

1. Pendahuluan

1.1 Latar belakang

Hak atas kekayaan intelektual seharusnya menjadi perhatian penting bagi kita. Kreatifitas seseorang akan selalu berkembang jika karyanya dihargai oleh orang lain. Pembajakan karya seseorang oleh orang lain merupakan bentuk tindakan yang tidak menghargai karya orang lain.

Menandai sebuah karya merupakan suatu usaha untuk menjaga keaslian karya tersebut. Sebagai contoh, seseorang membubuhkan tanda tangan kedalam surat yang dibuatnya untuk menandakan bahwa surat itu benar-benar dibuat olehnya. Jika belum puas hanya dengan membubuhkan tanda tangan, bisa ditambahkan stempel untuk memperkuat bukti keasliannya.

Jika permasalahannya ada pada dokumen digital, maka solusi tanda tangan dan stempel dapat kita adaptasi ke bentuk digital. Dalam dunia digital, dikenal teknik kriptografi dengan cara *digital signature*. *Digital signature* fungsinya mirip seperti tanda tangan yaitu sebagai penanda sebuah dokumen. Fungsi stempel dapat diganti dengan teknik steganografi atau *watermarking*. Jika diinginkan dokumen yang memiliki tanda namun tidak dapat terdeteksi oleh orang lain, dapat digunakan teknik steganografi. Sebaliknya, jika tanda yang dibubuhkan ingin ditampilkan bisa digunakan teknik *watermarking*.

Dalam teori *digital signature*, dokumen bersama-sama dengan *signature*-nya dikirimkan ke penerima. Dengan sistem seperti ini, seorang *hacker* masih mempunyai kesempatan untuk memecahkan *digital signature*. Seorang *hacker* dapat dengan mudah mengambil dokumen dan *signature*-nya lalu mencoba melakukan *brute force attack* untuk mengubah *digital signature* dari dokumen tersebut.

Untuk memperkecil kemungkinan pengambilan *digital signature*, maka diperlukan solusi yang lebih efektif. Salah satu caranya yaitu dengan menyisipkan *digital signature* ke dalam dokumen. Proses penyisipan dokumen juga harus menggunakan teknik steganografi, agar seorang hacker tidak menyadari bahwa dalam dokumen tersebut terdapat *signature*.

Dokumen yang akan dijadikan media penyisipan harus mempunyai bit-bit redundan yang dapat dimodifikasi. *Digital signature* disispkan kedalam bit-bit redundan tersebut. Karena sifatnya yang redundan, maka perubahan terhadap bit-bit tersebut diharapkan tidak mengubah kualitas dokumen secara signifikan. Perubahan yang tidak terlalu signifikan ini tidak akan terdeteksi oleh manusia, karena indera visualisasi manusia yang memiliki keterbatasan untuk mendeteksi perubahan dalam skala satuan bit.

Dalam tugas akhir ini akan digunakan algoritma RSA dan SHA-1 sebagai algoritma *digital signature*. Proses penyisipan *digital signature* kedalam dokumen, dalam hal ini citra digital akan dilakukan dengan cara mentransformasikan citra digital. Citra digital yang semula berbentuk domain spasial ditransformasikan kedalam domain skala waktu. Teknik transformasi pada citra digital akan menggunakan DWT (*Discrete Wavelet Transform*), dengan basis *wavelet* Haar.

Latar belakang digunakannya algoritma RSA adalah karena fungsinya yang selain dapat digunakan sebagai algoritma enkripsi, tapi juga untuk autentikasi. Selain itu, keamanan RSA cukup terjamin. Hal ini dikarenakan sulitnya mencari faktor-faktor prima dari bilangan yang besar. Fungsi faktor-faktor prima di sini diperlukan untuk memperoleh kunci *private*.

Fungsi hash SHA-1 digunakan karena dalam penerapan *digital signature*, biasanya algoritma RSA digunakan bersama-sama dengan algoritma *hash function* SHA-1. Selain itu, *Output* yang dihasilkan algoritma SHA-1 adalah 160 bit.

DWT dipilih karena transformasi *wavelet* merupakan perbaikan dari teknik transformasi Fourier. Transformasi *wavelet* dapat memberikan informasi tentang kombinasi skala dan frekuensi, berbeda dengan transformasi Fourier yang hanya memberikan informasi tentang frekuensi. Selain itu transformasi Fourier berbasis pada fungsi *sinus* dan *cosinus* yang bersifat periodik dan kontinu. Hal ini akan berakibat jika akan melakukan perubahan pada suatu posisi, maka akan mempengaruhi posisi-posisi lainnya.

Basis *wavelet* Haar dipilih karena proses komputasinya yang tidak terlalu rumit, mengingat fokus aplikasi yang akan dibuat adalah pada cara pembentukan dan penyisipan *digital signature*. *Wavele*t Haar menggunakan *window rectangular* untuk mengambil sample deretan waktu, sehingga resolusi untuk perubahan pengambilan sample cenderung kasar.

1.2 Perumusan masalah

Dalam tugas akhir ini, terdapat beberapa permasalahan yang timbul yaitu :

1. Bagaimana menjamin suatu informasi adalah milik kita (kebutuhan *identity*).
2. Bagaimana menyimpan informasi (untuk menyisipkan *digital signature* pada citra digital) untuk menjamin bahwa citra digital yang dihasilkan proses invers *Discrete Wavelet Transform* sama dengan citra digital asal.
3. Bagaimana mengekstrak kembali *digital signature* yang telah disisipkan sehingga dapat dilakukan proses verifikasi.

1.3 Tujuan

Tujuan dari Tugas Akhir ini adalah :

1. Mengimplementasikan salah satu teknik kriptografi, yaitu *digital signature* dengan menggunakan fungsi hash SHA-1 dan algoritma RSA.
2. Mengimplementasikan teknik steganografi dengan menggunakan *Discrete Wavelet Transform* basis *wavelet Haar*.
3. Membuat aplikasi untuk proses steganografi antara citra digital dan *digital signature*.
4. Membuat aplikasi untuk verifikasi data hasil pemisahan antara citra steganografi dan *digital signature* untuk menjamin identitas kepemilikan data..

1.4 Metodologi penyelesaian masalah

Metode yang digunakan dalam penyelesaian tugas akhir ini adalah sebagai berikut :

1. Studi Literatur
   Mempelajari konsep kriptografi, steganografi, *digital signature*, algoritma RSA, fungsi hash satu arah SHA1, dan *Discrete Wavelet Transform*.
2. Analisis Sistem
   Mempelajari dan Menganalisis kebutuhan pada implementasi penyisipan *digital signature* pada citra digital. Analisa yang dilakukan meliputi :
   a. algoritma yang digunakan untuk implementasi *digital signature*
   b. metode transformasi yang digunakan untuk implementasi steganografi
   c. cara yang digunakan untuk menjamin citra yang dihasilkan proses invers *Discrete Wavelet Transform* sama dengan citra asal
   d. pemilihan basis *wavelet* untuk *Discrete Wavelet Transform*.
3. Perancangan dan Implementasi
   Melakukan perancangan dan mengimplementasikan implementasi penyisipan *digital signature* pada citra digital dengan metode *Discrete Wavelet Transform*. Perancangan dan Implementasi yang dilakukan terbagi dalam 4 tahap, yaitu :
   a. Mengimplementasikan *digital signature* dengan menggunakan algoritma RSA dan fungsi Hash satu arah SHA1.
   b. Mengimplementasikan steganografi dengan metode *Discrete Wavelet Transform* dengan basis *wavelet* Haar.
   c. Menyimpan informasi untuk menyisipkan *digital signature* pada citra digital.
   d. Melakukan analisa pengaruh beberapa pengolahan citra terhadap ketahanan citra hasil steganografi.
4. Pengambilan Kesimpulan dan Penyusunan Laporan Tugas Akhir

Kesimpulan dan Saran

4.3 Kesimpulan

Kesimpulan yang didapat dari pengerjaan tugas akhir ini antara lain:

1. Metode Discrete Wavelet Transform dapat diterapkan untuk steganografi digital signature pada citra digital bitmap.
2. Semakin besar nilai koefisien bobot penyisipan, maka perbedaan penampakan image sebelum disisipi dan setelah disisipi menjadi semakin besar. Begitu juga sebaliknya.
3. Sistem dapat menjamin identity kepemilikan image berdasarkan deteksi digital signature walaupun image tersebut mengalami perubahan.
4. Image yang telah disisipi digital signature apabila mengalami perubahan, maka tidak akan mempengaruhi digital signature.

4.4 Saran

System yang diimplementasikan pada Tugas Akhir ini merupakan penggabungan antara Digital Signature dengan Steganografi yang diterapkan pada file image. Digital Signature yang diterapkan pada Tugas Akhir ini menggunakan algoritma RSA dan fungsi hash SHA1, sedangkan Steganografi yang diterapkan pada Tugas Akhir ini menggunakan metode Discrete Wavelet Transform. Namun, untuk pengembangan lebih lanjut, metode steganografi DWT dapat diganti dengan metode steganografi yang lain, misalnya Discrete Cosinus Transform.

Daftar Pustaka

1. "Handbook of Applied Chryptography", http://www.cacr.math.uwaterloo.ca/hac/index.html, diakses tanggal 15 November 2006.
2. Kurniawan, Yusuf. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung : Informatika Bandung.
3. Rahardjo, Budi. 2005. *Keamanan Sistem Informasi Berbasis Internet.* Bandung : PT Insan Infonesia.
4. "Digital Signature", http://en.wikipedia.org, diakses tanggal 5 November 2006.
5. "Discrete Wavelet Transform", http://en.wikipedia.org, diakses tanggal 5 November 2006.
6. "Discrete Wavelet Transforms", http://www.quantlet.com/mdstat/scripts/csa/html/node60.html , diakses tanggal 10 November 2006.
7. "Discrete Wavelet Transform", http://www.answers.com , diakses tanggal 10 November 2006.
8. Chen, XL. *Application of the Discrete Wavelet Transform in the Ranging Algorithm of Radio Fuze*. Institute of Physics Publishing, China.
9. "Adaptive Wavelet Coding For Still Images". http://www.stanford.edu . diakses tanggal 10 November 2006.
10. Stollnitz, Eric J. *Wavelet for Computer Graphics*. University of Washington.
11. Nagapadma, Rohini. *Performance Evaluation of Haar Wavelet on Image Compression*. Proceedings of the International Conference on Cognition and Recognition.
12. Polikar, Robi.1996.*The Wavelet Tutorial*, *second edition*.
13. http://www.wavelet.org
14. Jain, A K. *Fundamentals of Image Processing*.
15. Chahyati, Dina. 20 Januari 2003. *Wavelet*. Draft Thesis II.
16. Soehono, Stefanus. 2006. *Audio Steganografi Menggunakan MP3*. Tugas Akhir EC5010 Keamanan Sistem Informasi Departemen Teknik Elektro Institut Teknologi Bandung.
17. Cachin, Christian. 2004. *Digital Steganography*, Switzerland.
18. Tsudik, Gene. ImageDowngrading: A steganographic technique to hide secret messages. Westfeld, Andreas. The Steganographic Algorithm F5, 1999. http://wwwrn.inf.tu-dresden.de/~westfeld/f5.html.