Indonesian Journal of Data and Science ISSN: 2715-9930
Vol 1, No 1, Maret 2020, pp. 19-22

Penerapan Metode Digital Watermarking dan Privilege pada Dokumen Skripsi

Hidayani Nursan[a,1], Muslim[a,2]

[a] *Universitas Muslim Indonesia, Jln. UripSumoharjo Km.5 , Makassar 90231, Indonesia*
[1] *hidayaninursan097@gmail.com;* [2] *Muslim@umi.ac.id*

INFORMASI ARTIKEL

Diterima : 13 Januari 2020
Direvisi : 21 Februari 2020
Diterbitkan : 31 MAret 2020

Kata Kunci:
watermarking
privelege
disable copy and print
dokumen skripsi
keamanan data

ABSTRAK

Dengan perkembangan perangkat komputer dan internet yang semakin pesat menjadikan pertukaran data dan informasi secara digital semakin banyak digunakan. Namun sebagian dari data tersebut harusnya tidak dapat didistribusi atau dimodifikasi secara bebas (tanpa izin), karena mengandung hak kekayaan intelektual penciptanya. Secara garis besar sistem ini memiliki dua inputan yaitu dokumen dan gambar yang mana gambar dijadikan sebagai watermark pada dokumen, kemudian dilanjutkan dengan melakukan proses privilege/disable copy print. Hasil dari penelitian ini adalah sistem berhasil menerapkan layanan watermarking dan disable copy print terhadap file dokumen skripsi di semua flatfoam, kecuali disable copy print belum berhasil di terapkan pada priview di sistem operasi linux.

I. Pendahuluan

Seiring perkembangan teknologi komputer ada beberapa faktor yang membuat data digital seperti audio, citra, dan video banyak digunakan, antara lain karena mudah diduplikasikan, disimpan,diolah lebih lanjut, serta didistribusikan baikdenganmedia disk maupun melalui internet.Denganadanya internet sebagai sistemjaringan terluas membuat hampir segala jenis data dan informasi dapat diperoleh. Sayangnya, sebagian data dan informasi yang dipertukarkan seharusnya tidak boleh dimodifikasi tanpa izin karena mengandung hak cipta pemiliknya. Maka dari itu keamanan data sangat penting untuk diterapkan [1][2].

Watermarking merupakan suatu bentuk aplikasi dari Steganography yang merupakan ilmu yang mempelajari bagaimana menyembunyikan suatu data pada data yang lain. Prinsip dasar watermarking bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan, atau data lain, pada materi multimedia tanpa mempengaruhi kualitasnya. Watermarking ini dapat diterapkan pada berbagai media digital. Jadi watermarking merupakan suatu cara untuk penyembunyian atau penanaman data/informasi tertentu (baik hanya berupa catatan umum maupun rahasia) ke dalam suatu data digital lainnya, teknologi watermarking merupakan suatu solusi dalam melindungi hak cipta kepemilikan terhadap data-data digital. [3]

Bagi kalangan mahasiswa kebiasaan copy paste (menjiplak) tidak lagi menjadi sesuatu yang asing. Sebab sekarang ini, kebiasaan menjiplak telahmenjadi satu-satunya jalan pintas untuk dapat mengerjakan tugas kuliah tanpa harus banyak berpikir. Praktek menjiplak dikalangan mahasiswa umumnya sudah biasa terjadi.. Kebebasan mengakses informasi mendapatkan referensi bahan kuliah di internet, dengan sistem itu mahasiswa menjiplak, print skripsi dan merubah hak ciptanya.

Kebijakan hak cipta adalah pemberian toleransi dari produk hukum yang berupa aturan disiplin dan sanksi yang tegas (misalnya UU hak cipta) terhadap suatu kegiatan aktivitas lembaga tertentu dalam melaksanakan tugas dan fungsinya dengan sebatas ranah kewajaran. Bagi perpustakaan, harus memperhatikan layanan proses pengolahan maupun pangalih-mediaan dokumen. Dalam konteks ini, UU tersebut sudah memberikan batasan dan syarat secara jelas dan tegas terhadap lembaga perpustakaan untuk melindungi setiap koleksi yang didigitalkan terhadap pelanggaran hak cipta. Dalam UU Hak Cipta No.19 Tahun 2002, koleksi digital diartikan sebagai karya cipta hasil pengalihwujudan yang dilindungi oleh hukum hak cipta. Pernyataan ini diatur dalam UU Hak Cipta bahwa: "dalam undang-undang ini ciptaan yang dilindungi adalah ciptaan dalam bidang ilmu pengetahuan, seni, dan sastra yang mencakup: karya terjemahan, tafsir, saduran, bunga rampe, database, dan karya lain dari hasil pengalihwujudan" [4].

Setiap ide, gagasan, maupun pikiran yang sudah tertuang dalam bentuk karya intelektual koleksi adalah dilindungi hak cipta, baik itu berbentuk koleksi cetak (printed) maupun elektronik (digital). Agar aman dalam pelanggran hak cipta, perpustakaan harus menyiapkan perangkat atau peraturan tertulis yang memuat

kesepakatan dan lisensi diantara kedua belah pihak. Dengan pernyataan bahwa setiap koleksi/informasi yang sudah diterimaperpustakaan itu adalah hak prerogatif perpustakaan untuk mengalihmediakan koleksinya ke bentuk apapun tanpa adanya komplain/protes dari si penulis karya (Hutagalung, 2012).

Skripsi merupakan salah satu data digital yang mudah diakses oleh siapa saja, penyebaran dokumen tidak dapat dijamin keamanannya, beberapa kasus pencurian data skripsi contohnya penggandaan, plagiat, mengubah informasi (manipulasi) yang dilakukan dengan cara tidak sah (*illegal*), dan pelanggaran hak cipta (*copyright*).

Privilege adalah hak, imunitas atau manfaat yang hanya dapat dirasakan oleh kelompok tertentu. Atau dapat juga bermakna keuntungan yang hanya seorang atau segelintir orang yang memilikinya, biasanya karena posisi atau karena aturan lainnya. Privilege terkadang diterapkan pada sebuah sistem sebagai pembatasan akses sesuai otoritas pengguna [5][6].

Saat ini di perpustakaan Utsman Bin Affan UMI hak akses soft file skripsi terbuka atau dapat diakses oleh siapa saja, sehingga keamanan dari skripsi tersebut tidak dapat dijamin, oleh karena itu peneliti berinisiatif membuat sebuah rancangan perangkat lunak aplikasi sebagai salah satu cara untuk memberi penanda kepemilikan serta memberi layanan privilege/membatasi akses user melakukan proses copy dan print(disablecopy dan print),judul yang diangkat sesuai dengan permasalahan di atas yakni "Penerapan Metode Digital Watermarking dan Privilege Pada Dokumen Skripsi".

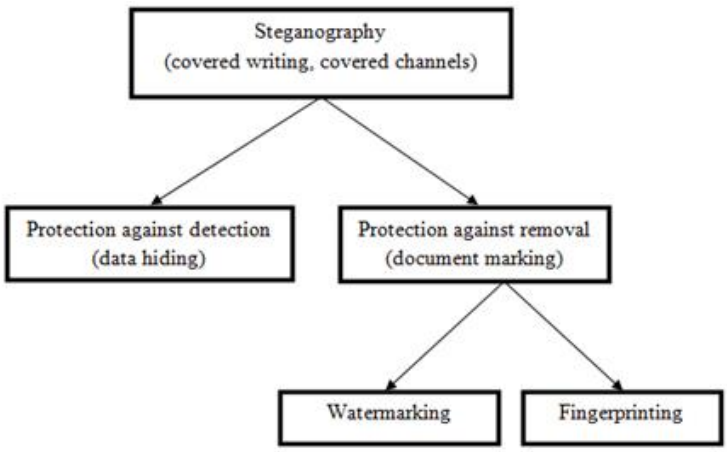
II. Metode

A. *Privileges*

Privilege adalah hak, imunitas atau manfaat yang hanya dapat di rasakan oleh kelompok tertentu. Atau dapat juga bermakna keuntungan yang hanya seorang atau segelintir orang yang memilikinya, biasanya karena posisi atau karena aturan lainnya. Privilege terkadang di terapkan pada sebuah sistem sebagai pembatasan akses sesuai otoritas pengguna. Dalam keamanan sebuah basis data, *Privileges* diterapkan untuk keperluan autorisasi pengguna dalam akses table atau tindakan yang dapat dilakukannya. *Disable copy-print* merupakan salah satu bentuk batasan hak atas *user* dalam melakukan penggandaan dokumen baik dalam bentuk *softcopy* maupun *hardcopy.*

B. *Steganografi*

Sejarah Steganografi merupakan seni penyembunyian pesan kedalam pesan lainnya sedemikian rupa sehingga orang lain tidak menyadari ada sesuatu di dalam pesan tersebut. Katasteganografi *(steganography)* berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung dan *graphein*, yang artinya menulis, sehingga kurang lebih artinya adalah "menulis tulisan yang tersembunyi atau terselubung". *Steganography* dapat dibagi menjadi 2 (dua) bagian yaitu *protectionagainst detection(datahiding)*dan *protection against removal(document marking)*.



Gambar 1. Pembagian Steganografi

Watermarking merupakan salah satu jenis dari document marking. Pembagian *steganography* dapat terlihat dalam Gambar 2.1 Pada gambar dapat dilihat bahwa proteksi dalam steganografi terbagi menjadi dua jenis/model yaitu

1) Protection aginst detection

Model proteksi ini banyak digunakan dalam dunia maya sebagai security tools dalam suatu pengiriman data atau dokumen melalui internet atau media lainnya. Proteksi ini mempunyai metode agar suatu file/media sampul yang telah disisipi data tidak dapat dideteksi oleh *steganalisis*, sehingga data yang dikirimkan aman sampai orang yang ditujukan[7]

2) Protection against removal

Model proteksi ini banyak digunakan dalam media *digital security*. Biasanya model ini berfungsi sebagai penanda hak cipta *(copyright)* agar tidak dapat dihilangkan maupun diganti oleh pihak-pihak lain yang tidak bertanggung jawab. Pada metode ini terdapat dua metode yang dapat digunakan, yaitu *watermarking* dan *fingerprinting*. *Watermarking* merupakan satu bentuk metode dari steganografi dalam mempelajari teknik-teknik bagaimana penyimpanan suatu data digital kedalam data sampul digital yang lain.

C. Watermarking

Watermarking merupakan cara menyisipkan atau proses penambahan kode secara permanen kedalam *citra* digital yang ingin dilindungi hak ciptanya dengan tidak merusak *citra* aslinya dan tahan terhadap serangan. Secara garis besar *watermark* terbagi menjadi dua tipe, yaitu *visible watermark* (nampak) dan *invisiblewatermark* (tidak nampak). *Watermarking* juga dapat diklasifikasikan berdasarkan tipe dokumen yang akan diberi *watermark*. Klasifikasi adalah *Image Watermarking*, *Video Watermarking*, *Audio Watermarking*, *Text Watermarking.*

1) Visible seal

Visible Seal, atau segel yang terlihat. Merupakan salah satu jenis dari algoritma text watermarking, dalam hal ini, objekseperti teks, grafik atau gambar dimasukkan sebagai latar belakang di semua halaman dokumen. Prototipe yang dikembangkan memungkinkan untuk dapat diterapkan pada setiap dokumen dengan segel grafis. *Watermarking* jenis ini terlihat dengan mata telanjang dan diberi fitur keamanan tambahan untuk melindungi dokumen, melalui fitur yang ditawarkan berupa membuat dokumen "read only", yaitu dapat dilihat tetapi tidak dapat dimodifikasi.

2) Watermark embedding

Algoritma yang digunakan untuk menanamkan *watermark* seperti pada penjelasan di bawah ini.

a) InputDokumen
b) Membaca jumlah halaman
c) input Gambar
d) Menentukan ukuran gambar dan transparansi
e) Perulangan :
- *perulangan 1 sampai banyaknya halaman*
- *mencari ukuran kertas*
- *menambahkan layer*

f) Selesai.

III. Hasil dan Pembahasan

Pengujian dilakukan pada duabagian yaitu uji proses sistem dan uji output sistem

Tabel 1. Pengujian Proses sistem

No	Nama File	Ukuran Awal file	Nama File Gambar	Ukuran Awal Gambar	Output			Ukuran Akhir file	Durasi (detik)
					Watermark	Disable copy & Print	Enable		
1	1. Pdf	1,501 kb	Png	78.7 kb	OK	OK	OK	1,791 kb	5,900
2	2. Pdf	789 kb	Png	78.7 kb	OK	OK	OK	963 kb	1,713
3	3. Pdf	366 kb	Png	78.7 kb	OK	OK	OK	472 kb	1,416
4	1. Pdf	1,501 kb	Jpg	28.9 kb	OK	OK	OK	1,761 kb	4,474
5	2. Pdf	789 kb	Jpg	28.9 kb	OK	OK	OK	934 kb	2,228
6	3. Pdf	366 kb	Jpg	28.9 kb	OK	OK	OK	442 kb	1,972

Setelah dilakukan pengujian proses sistem semua *file* pdf berhasil diproses dengan baik, *file* pdf yang diproses dengan gambar yang bertipe *png* atau *jpg* memiliki ukuran *file* yang berbeda-beda. *File* yang

memiliki kapasitas yang lebih besar membutuhkan waktu proses yang lebih lama dibandingkan dengan *file* yang memiliki kapasitas yang lebih kecil.

Tabel 2. Tabel uji output sistem

No	Nama File	Windows		Linux	Mac	Browser	
		Foxit	Adobe reader	Doc. viewer	Preview	Mozilla	Chrome
1	1.Pdf	OK	OK	X	OK	OK	OK
2	2.Pdf	OK	OK	X	OK	OK	OK
3	3.Pdf	OK	OK	X	OK	OK	OK

Berdasarkan hasil uji *output*sistem seperti yang digambarkan pada Tabel 5.10 dimana seluruh *file* telah di lakukan pengujian di berbagai pdf *reader* diberbagai *platfoam*baik di *windows*, *linux, mac os* dan *browser* dapat ditarik kesimpulan bahwa sistem yang dirancang menggunakan metode *digital watermarking*mampu bekerja dengan baik di semua *platfoam*, berbeda layanan *disable copy print.* Layanan *disable copy print* hanya dapat bekerja di *foxit, adobe reader*, dan *prewiew* yang berada di sistem operasi windows dan mac, kecuali pada dokumen *viewer di linux.*

IV. Kesimpulan

Berdasarkan hasil penelitian ini maka penulis dapat menarik beberapa kesimpulan, yaitu:

1. Penerapan metode digital watermarking pada dokumen skripsi berhasil dibuat dengan menguji tiga file skripsi yang memiliki kapasitas yang berbeda-beda.
2. Penerapan layanan disable copy print pada dokumen skripsi berhasil di buat dan diterapkan di lima file reader yaitu foxit, adobe reader, priview, Mozilla dan chrome. Pengujian pada viewer di linux tidak bekerja dengan baik..

Daftar Pustaka

[1] H. Azis, "Network steganography system using covert channel for LSBS stego data on VOIP communication," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 5, pp. 1448–1449, 2019.

[2] H. Azis and F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," *Ilk. J. Ilm.*, vol. 11, no. 2, p. 167, 2019.

[3] H. Azis and R. Wardoyo, "Penerapan Network Steganography Menggunakan Metode Modifikasi LACK Dan Layanan Message Authentication Code Pada Voip Network Steganography System with modification of LACK and Message Authentication Code on VoIP," *Semin. Nas. Komun. dan Inform.*, pp. 13–19, 2015.

[4] Y. Salim and H. Azis, "Metode Digital Watermark Pada File Penelitian Dosen," *Ilk. J. Ilm.*, vol. 9, no. 2, pp. 161–166, 2017.

[5] M. Nazeri, A. Rezai, and H. Azis, "An Efficient Architecture for Golay Code Encoder," *Proc. - 2nd East Indones. Conf. Comput. Inf. Technol. Internet Things Ind. EIConCIT 2018*, pp. 114–117, 2018.

[6] F. Muharram, H. Azis, and A. R. Manga, "Analisis Algoritma pada Proses Enkripsi dan Dekripsi File Menggunakan Advanced Encryption Standard (AES)," *Pros. Semin. Nas. Ilmu Komput. dan Teknol. Inf.*, vol. 3, no. 2, pp. 112–115, 2018.

[7] A. Djamalilleil, M. Muslim, Y. Salim, E. I. Alwi, H. Azis, and Herman, "Modified Transposition Cipher Algorithm for Images Encryption," *Proc. - 2nd East Indones. Conf. Comput. Inf. Technol. Internet Things Ind. EIConCIT 2018*, pp. 1–4, 2018.