Penerapan Steganografi pada *Corporate Internet Reporting* (CIR)

Imamah
Universitas Trunojoyo Madura
Jl. Raya Telang Po Box 02 Kamal Bangkalan
e-mail: i2m@trunojoyo.ac.id

Abstrak

Corporate Internet reporting (CIR) adalah proses komunikasi yang berkaitan dengan informasi keuangan dan non keuangan meliputi sumber daya dan kinerja perusahaan melalui internet . CIR mempercepat distribusi pelaporan perusahaan, sehingga perusahaan dapat melakukan berbagai tindakan yang diperlukan tanpa mengenal jarak, waktu dan tempat. Namun dari sisi lain, keamanan dari laporan yang dikirimkan melalui internet sangat rentan, terutama jika berkaitan dengan laporan keuangan perusahaan. Pada penelitian ini diusulkan penerapan steganografi pada CIR untuk melindungi data perusahaan dari pihak-pihak yang tidak berhak mengaksesnya. Hasil dari penelitian ini membuktikan bahwa untuk menyisipkan 10 kB ≤ data ≤ 60 kB cover image harus memiliki ukuran piksel minimal 512x512 piksel. Nilai PSNR tertinggi didapatkan pada cover image berukuran 1024x1024 piksel yaitu 35,6 dB saat disisipkan data berukuran 55 kB dan 39,7 dB saat disisipkan data berukuran 27 kB. Nilai PSNR terendah didapatkan pada cover image berukuran 128x128 piksel. Berdasarkan hasil penelitian dapat disimpulkan bahwa metode steganografi dengan menggunakan algoritma DCT dapat diterapkan pada CIR dengan ukuran dan kapasitas data tertentu.

Kata kunci: *Keamanan data, steganografi, cloud computing, stego-file.*

1. Pendahuluan

Ketepatan waktu dalam penyampaian laporan sangat penting bagi tingkat manfaat dan nilai laporan. Tepat waktu dapat diartikan sebagai ketersediaan informasi kepada para pengambil keputusan sebelum informasi tersebut kehilangan kapasitasnya dalam mempengaruhi keputusan. Pelaporan perusahaan melalui internet atau *Corporate Internet Reporting* (CIR) dilakukan dalam rangka menjamin distribusi informasi tepat waktu kepada yang berhak mendapatkan informasi [1]. Permasalahan yang muncul dalam penggunaan CIR ini adalah dari segi *privacy*.

Aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses[2]. *Privacy* mengarah pada data-data yang sifatnya *private* sedangkan *confidentiality* biasanya berkaitan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pengguna tidak boleh dibaca oleh administrator. Contoh *confidential information* adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. CIR termasuk contoh lain dari *confidentiality*. Jika CIR sampai tersebar luas atau diakses oleh orang yang tidak berhak maka akan menimbulkan resiko tertentu bagi perusahaan. Pengamanan data terhadap CIR yang akan didistribusikan melalui internet perlu dilakukan demi menjaga aspek *confidentiality* dari perusahaan.

Dalam bidang keamanan data, ada banyak teknik yang digunakan diantaranya adalah watermaking, enkripsi dan steganografi. Watermaking adalah penyisipan informasi pada media dengan tujuan untuk memberikan sidik digital dari pemilik yang sah atas produk multimedia tersebut. Watermaking yang digunakan untuk memberikan *signature* pada multimedia harus dilakukan sedemikian rupa sehingga tidak merusak data digital yang dilindungi. Teknik yang berikutnya adalah enkripsi, yang merupakan proses *encoding* atau penyandian sebuah pesan dengan menggunakan algoritma tertentu untuk mengacak data di dalamnya sehingga sulit dipahami dan dibutuhkan waktu untuk memecahkan kunci rahasia yang ditambahkan dalam proses enkripsi. Teknik keamanan yang terakhir adalah steganografi. Steganografi (steganography) adalah teknik menyembunyikan data rahasia di dalam media digital sehingga keberadaan data rahasia tersebut tidak diketahui [3]. Steganografi membutuhkan dua *property*: media penampung (*cover image*) dan pesan rahasia yang akan disembunyikan. Steganografi digital menggunakan media

digital sebagai media penampung, misalnya citra, suara (audio), teks, dan video. Data rahasia yang disembunyikan juga dapat berupa citra, suara, teks, atau video[4].

Penggunaan steganografi antara lain bertujuan untuk menyamarkan keberadaan data rahasia sehingga sulit dideteksi , dan melindungi hak cipta suatu produk. Perbedaan antara steganografi dan enkripsi terletak pada tampak atau tidaknya data rahasia. Jika pada enkripsi atau disebut juga kriptografi, data yang telah disandikan tetap tersedia atau tampak, maka dengan steganografi data rahasia disembunyikan dalam media tertentu sehingga tidak tampak [5]. Data rahasia yang disembunyikan dapat diekstraksi kembali persis sama seperti keadaan aslinya dengan menggunakan kunci yang tepat.

Pada penelitian ini steganografi dipilih sebagai metode pengamanan yang diusulkan. Hal ini berdasar pada proses pengamanan dilakukan dengan menyembunyikan data laporan dalam media gambar, sehingga tidak akan terlihat secara kasat mata bahwa dalam gambar tersebut terdapat data penting yang disembunyikan. selain itu, untuk melakukan ekstraksi data dari cover image juga dibutuhkan kunci yang sesuai. Keamanan yang berlapis ini merupakan kelebihan dari steganografi dibandingkan dengan enkripsi.

2. Metode Penelitian

Penelitian ini mengusulkan penerapan steganografi menggunakan algoritma *Discrete Cossin Transform* (DCT) untuk melindungi data laporan perusahaan yang dikirimkan melalui internet. Data akan disembunyikan dengan menggunakan media gambar atau citra. Citra yang digunakan sebagai *cover image* dapat memiliki format apa saja, namun pada penelitian ini digunakan format .jpg. File yang akan disisipkan dalam citra *cover image* memiliki format .xls dan .doc yang diduga format file yang umum digunakan dalam pembuatan laporan.

2.1. Steganografi Menggunakan Algoritma DCT

Discrete Cosine Transform(DCT) merepresentasikan sebuah citra dari penjumlahan sinusoida dari magnitude dan frekuensi yang berubah-ubah. Sifat dari DCT adalah mengubah informasi citra yang signifikan dikonsentrasikan hanya pada beberapa koefisien DCT. DCT menghitung kuantitas bit-bit *image* dimana pesan tersebut disembunyikan didalamnya. Steganografi menggunakan DCT dilakukan dengan melakukan transformasi piksel-piksel pada citra dari satu tempat (*domain*) ke tempat yang lain. Langkah awal adalah dengan mencari koefisien transformasi dari citra JPEG kemudian citra akan mengalami kompresi berdasarkan pada dimensi dari citra tersebut. Pada penelitian ini digunakan citra *grayscale* atau citra dua dimensi. DCT dua dimensi memetakan sebuah citra atau sebuah segmen gambar ke dalam komponen frekeunsi dua dimensi (2D). DCT menyusun sinyal tersebut ke frekeunsi spasial yang disebut dengan koefisien DCT. Frekeunsi koefisien DCT yang lebih rendah muncul pada kiri atas dari sebuah matriks DCT, dan frekeunsi koefisien DCT yang lebih tinggi berada pada kanan bawah dari matriks DCT [6]. Sistem penglihatan manusia tidak begitu *sensitive* dengan error yang ada pada frekenusi tinggi disbanding dengan yang ada pada frekuensi rendah. Karena itu, maka frekuensi yang lebih tinggi tersebut dapat di kuantisasi. Suatu matriks dua dimensi S(x,y) dimana x=0,,…n-1 dan y=0,1,….m-1 dapat ditransformasikan ke dalam ranah frekuensi dengan menggunakan persamaan DCT berikut:

$$S(u,v)= C(u)\,C(v) \sum_{x=0}^{n-1}\sum_{y=0}^{m-1} S(x,y)\cos\left[\frac{\pi(2x+1)u}{2n}\right]\cos\left[\frac{\pi(2y+1)v}{2m}\right] \quad (1)$$

Dengan :

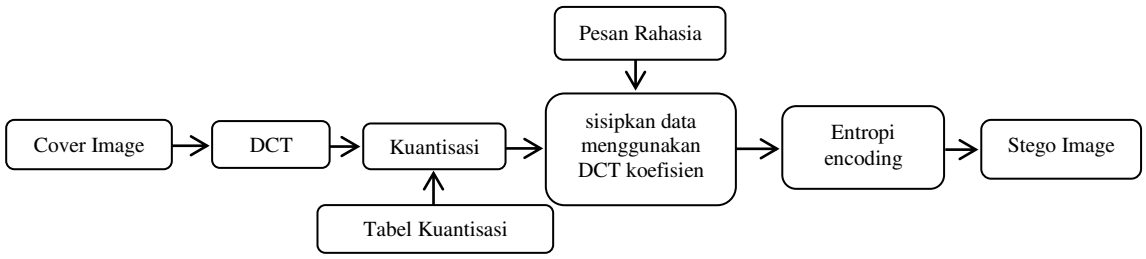
u=0,1,…n-1 dan v=0,1,…m-1

$$C(u)=C(v)=\begin{cases}\sqrt{\frac{1}{n}} & \text{Untuk } u=v=0\\ \sqrt{\frac{2}{n}} & \text{Untuk } u=v=1,2,..n-1\end{cases}$$

Untuk proses steganografi menggunakan DCT ditunjukkan oleh gambar 1 dengan langkah-langkah sebagai berikut:

1. *Cover image* akan dibagi menjadi 8x8 blok, jika *cover image* berukuran 256x256 maka akan terbentuk blok sejumlah N=1024 yang memiliki indeks N=0 sampai dengan N-1.
2. Untuk setiap satu blok *cover image*, ubah ke dalam ranah frekuensi menggunakan transformasi DCT-2D 8x8.
3. DCT koefisien akan dikuantisasi berdasarkan tabel kuantisasi untuk gambar jpeg.

4. Kemudian sisipkan setiap bit data rahasia pada setiap koefisien frekuensi tengah DCT secara merata pada semua blok *cover image*. Setiap bit dari pesan rahasia akan disisipkan pada koefisien DCT yang dikuantisasi menggunakan algoritma *Huffman/ entropi encoding*.
5. Lakukan transformasi balik IDCT (Inverse Discrete Cosine Transform) untuk setiap blok *cover image* dan kemudian tempatkan kembali blok-blok *cover image* pada tempat atau lokasi semula sebelum dilakukan pengacakan blok sehingga didapatkan *stego image* dengan bentuk yang hampir sama dengan *cover image* semula.



Gambar 1. Algoritma DCT untuk *embedding secret data.*

Sedangkan untuk transformasi baliknya dapat diperoleh dengan persamaan *inverse Discrete Cosine Transform* (IDCT) sebagai berikut:

$$S(x,y)= \sum_{u=0}^{n-1}\sum_{v=0}^{m-1} S(u,v)C(u)C(v)cos\left[\frac{\pi(2x+1)u}{2n}\right] cos\left[\frac{\pi(2y+1)v}{2m}\right] \quad (2)$$

Dengan :

u=0,1,…n-1 dan v=0,1,…m-1

$$C(u)=C(v)=\begin{cases}\sqrt{\frac{1}{n}} & \text{Untuk } u=v=0\\ \sqrt{\frac{2}{n}} & \text{Untuk } u=v=1,2,..n-1\end{cases}$$

2.2. Evaluasi Hasil

Pada penelitian ini, akan dilakukan uji coba untuk membuktikan apakah data CIR yang disembunyikan dapat diketahui keberadaannya atau tidak. Hal ini dilakukan dengan melakukan pengujian nilai PSNR. PSNR adalah pengukuran dari perbandingan *noise* dalam sinyal, semakin kecil nilainya menunjukkan semakin tinggi *noise* yang dihasilkan. Sebaliknya nilai PSNR yang tinggi menunjukkan bahwa *noise* semakin sedikit dan ini juga berarti bahwa kualitas gambar yang dihasilkan bagus. Nilai PSNR yang melebih nilai 30 dB menunjukkan *stego image* aman dan tahan terhadap serangan steganalisis [7]. Rumus untuk menghitung PSNR ditunjukkan persamaan 3 dan 4.

$$PSNR=10 \times \log_{10}\frac{255^2}{MSE} \quad (3)$$

$$MSE=\frac{1}{MN}\sum_{i=1}^{M}\sum_{j=1}^{N}(a_{ij}-b_{ij})^2 \quad (4)$$

Dengan a_{ij} dan b_{ij} adalah nilai dari setiap piksel pada citra, sedangkan M dan N adalah nilai tinggi dan lebar piksel pada *cover image*.

3. Hasil dan Pembahasan

Penelitian ini akan membuktikan apakah *stego image* yang dihasilkan layak diterapkan pada CIR atau tidak. Ukuran kelayakan ditentukan berdasarkan nilai PSNR yang dihasilkan. Semakin tinggi nilai PSNR yang dihasilkan maka semakin bagus kualitas *stego image* dan juga berarti aman dari serangan steganalisis. CIR biasanya merupakan file yang berukuran besar dengan minimal ukuran 10 Kb untuk tipe file .doc dan .xls, sehingga pada penelitian ini juga akan diteliti mengenai ukuran piksel yang tepat untuk menyisipkan data diatas 10 kB.

3.1. Data Uji

Data yang digunakan dalam penelitian ini adalah citra *grayscale* yang berformat .jpg. Jumlah data yang diuji sebanyak 4 citra dan ditunjukkan oleh tabel 1. Sedangkan pesan yang disisipkan memiliki format file .xls dan .doc ditunjukkan pada tabel 2.

Tabel 1. Data citra yang akan dijadikan *cover image*

Nama Citra	Mountain.jpg	Tower.jpg	Nature.jpg	Castle.jpg
Cover image				
Ukuran Citra (piksel)	128x128	256x256	512x512	1024x1024

Tabel 2. Pesan rahasia yang akan disisipkan pada *cover image*

Nama File	Keuangan.doc	LaporanUsaha.xls
File		
Ukuran File	55 Kb	27 Kb

PT. ABADI JAYA, Tbk
LAPORAN LABA RUGI
Untuk Tahun yang Berakhir 31 Desember 2014

Pendapatan :		
Penjualan		Rp. 20.000.000
Retur Penjualan	Rp. 1.000.000	
Potongan Penjualan	Rp. 2.000.000	
		Rp. 17.000.000
Penjualan Bersih		**Rp. 17.000.000**
Harga Pokok Penjualan		
Persediaan 1 Jan 2014	Rp. 5.000.000	
Pembelian	Rp. 3.000.000	
Barang Tersedia Untuk dijual	Rp. 8.000.000	
Persediaan 31 Des 2014	(Rp. 1.000.000)	
Harga Pokok Penjualan		**(Rp. 9.000.000)**

FORMAT LAPORAN KEUANGAN BULANAN

No.	Uraian	Debet	Kredit
1	Gas LPG	Rp 612,000	
2	Bayar Rekening Listrik	Rp 390,534	
3	Bayar Rekening Air	Rp 100,000	
4	Kimia Laundry	Rp 417,000	
5	Plastik dan Kresek	Rp 351,800	
6	Gaji Karyawan	Rp 2,760,000	
7	Uang Makan Karyawan	Rp 213,000	
8	Pulsa	Rp 38,000	
9	Uang keamanan dan kebersihan	Rp 30,000	
10	ATK	Rp 32,000	
11	Service Mesin dan Peralatan	Rp 100,000	
12	Depresiasi Mesin dan Peralatan	Rp 150,000	
13	Sewa tempat	Rp 800,000	
	Sub Total	**Rp 5,994,334**	

3.2. Hasil Uji Coba

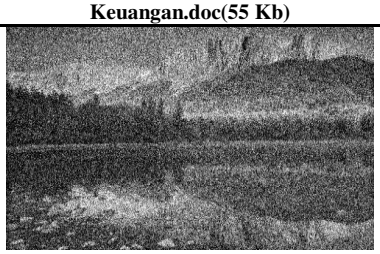
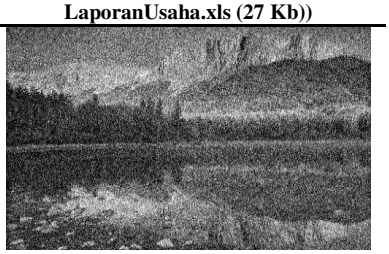
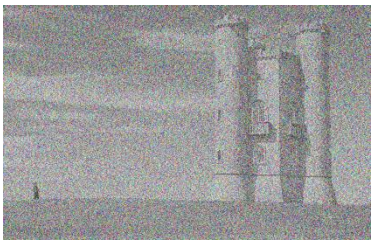
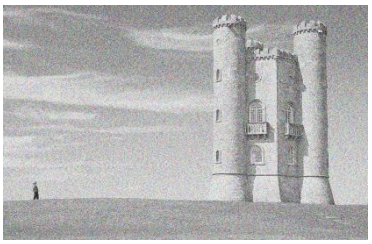
Pada penelitian ini, *cover image* pada tabel 1 masing-masing akan disisipkan data keuangan.doc dan data laporanusaha.xls. Proses penyisipan ditunjukkan pada gambar 1. *Cover image* akan dibagi menjadi blok piksel, kemudian akan dikuantisasi. Pada saat penyisipan data, algoritma akan meminta pengguna untuk memasukkan *stego key* yang akan digunakan untuk melakukan ekstraksi data. Ekstrasi data ini adalah proses pemisahan *stego image* menjadi *cover image* dan pesan. Tabel 4 menunjukkan hasil *stego image* dari DCT. Gambar dari *cover image* mountain.jpg dan tower.jpg saat disisipi file dengan ukuran 55 Kb (450560 bit) dan 27 Kb (221184 bit) mengalami banyak *noise* sehingga gambar asli tidak tampak. Hal ini disebabkan karena ukuran file yang disisipkan melebihi kapasitas yang seharusnya. Berdasarkan penelitian dari chang, dkk didapatkan bahwa pada algoritma DCT, penyisipan hanya bisa dilakukan maksimum 9n/64 bits untuk setiap 8x8 blok. D_k ($1 \leq k \leq 9$) dimana untuk setiap D_k hanya dapat disisipkan 1 bit. Sehingga dengan menggunakan perhitungan telah didapatkan data kapasitas maksimum penyisipan ditunjukkan tabel 3, sedangkan perbandingan besarnya kapasitas *embedding* dengan besarnya kapasitas data keuangan.doc dan data laporanusaha.xls dapat diamati pada gambar 2.

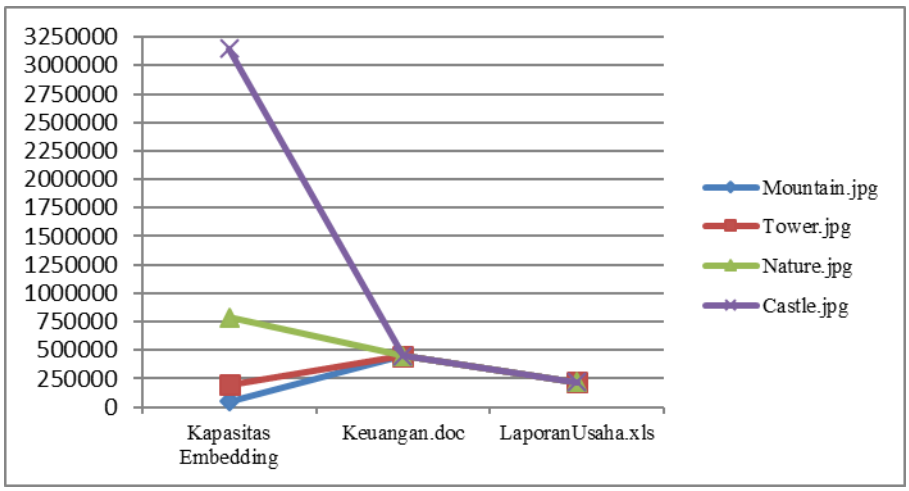
Dari penelitian ini dapat disimpulkan bahwa piksel ukuran 128x128 dan 256x256 dapat dijadikan *cover image* untuk menampung data yang kapasitasnya 6-10 Kb saja. Sedangkan piksel 512x512 dan 1024x1024 dapat digunakan untuk menampung data yang kapasitasnya >20 kB.

Tabel 3. Kapasitas maksimum embedding pada cover image

Nama Citra	**Ukuran Piksel**	**Kapasitas Embedding(bit)**
Mountain.jpg	128 x128	49064
Tower.jpg	256 x256	196520
Nature.jpg	512 x512	786344
Castle.jpg	1024x1024	3145640

Tabel 4. Perbandingan *Cover image* dengan *Stego Image*

Cover Image	Stego Image (Cover Image+ Keuangan.doc(55 Kb)	Stego Image(Cover Image+ LaporanUsaha.xls (27 Kb))
		
		
		
		



Gambar 2. Grafik perbandingan kapasitas embedding dengan kapasitas pesan rahasia

Sedangkan nilai PSNR yang didapatkan dari penelitian menggunakan *cover image* ditunjukkan pada table 5. Nilai PSNR tertinggi ditunjukkan saat menggunakan *cover image* castle.jpg yang memiliki ukuran piksel terbesar yaitu 1024x1024 piksel. Nilai PSNR terendah ditunjukkan oleh *cover image* mountain.jpg dengan ukuran piksel juga rendah yaitu 128x128 piksel. Nilai PSNR di bawah 30 dB menunjukkan kualitas citra dari *cover image* mengalami perubahan dan rentan terhadap serangan steganalisis[7].

Tabel 5. PSNR dari *cover image* dan *stego image*

Cover Image	Keuangan.doc (dB)	LaporanUsaha.xls (dB)
Mountain.jpg	05.5	08.8
Tower.jpg	08.4	09.5
Nature.jpg	32.4	38.4
Castle.jpg	35.6	39.7

4. Simpulan

CIR merupakan data laporan yang biasanya memiliki format .doc ataupun .xls. file kosong dari format .doc dan .xls rata-rata berukuran 6-15 kB. Hal inilah yang menjadi latar belakang dipilihnya ukuran citra dari mulai 128x128 piksel sampai dengan 1024x1024 piksel. Penelitian ini membuktikan bahwa untuk menyisipkan 10 kB $\leq$ data $\leq$ 60 kB *cover image* harus memiliki ukuran piksel minimal 512x512 piksel.

Nilai PSNR tertinggi didapatkan pada *cover image* berukuran 1024x1024 piksel yaitu 35,6 dB saat disisipkan data berukuran 55 kB dan 39,7 dB saat disisipkan data berukuran 27 kB. Nilai PSNR terendah didapatkan pada *cover image* berukuran 128x128 piksel. Berdasarkan hasil penelitian dapat disimpulkan bahwa metode steganografi dengan menggunakan algoritma DCT dapat diterapkan pada CIR dengan ukuran dan kapasitas data tertentu.

Daftar Pustaka

[1] Widaryanti. Analisis faktor-faktor yang mempengaruhi ketepatan waktu Corporate Internet Reporting yang terdaftar di BEI. *Jurnal Ilmu Manajemen dan AkuntansiTerapan*. 2011;Vol.2, No.2.

[2] Merkow, Mark S., and Breithaupt J. Information security: Principles and practices. Pearson Education. 2014.

[3] Kumar, Pramendra, and Sharma VK. Information Security Based on Steganography & Cryptography Techniques: A Review. *International Journal*.2014; Vol 4, No 10.

[4] Cheddad A, Condell J, Curran K, Kevitt PM. Digital image steganography: Survey and analysis of current methods. *Signal Processing*.2010; Vol. 90, pp 727–752.

[5] Filler T and Fridrich J Gibbs. Contruction in steganography. *IEEE Trans on Info Forensics and Security.*2010; Vol 5, pp 705-720.

[6] Sakr AS,Ibrahem, et all. A steganographic method based on DCT and new quantization technique. 22nd International Conference on Computer Theory and Applications (ICCTA). Alexandria. 2012; pp. 187-191

[7] Chen PY, Lin H. A DWT Based Approach for Image Steganography. *International Journal of Applied Science and Engineering*. 2006;Vol 4, pp.275-290.