

Implementasi Watermark Pada Citra Menggunakan Metode Spread Spectrum

Isninda Situmorang

STMIK Budi Darma Medan, Medan - Indonesia

Email : isninda.situmorang@gmail.com

Abstrak

Watermarking merupakan sebuah proses penambahan kode secara permanen ke dalam citra digital. Penyisipan kode ini harus memiliki ketahanan (*robustness*) yang cukup baik dari berbagai manipulasi, seperti perubahan, transformasi, kompresi, maupun enkripsi. Kode yang disisipkan juga tidak merusak citra digital sehingga citra digital terlihat seperti aslinya. Watermarking sangat diperlukan untuk melindungi karya intelektual digital seperti gambar, teks, musik, video, dan termasuk perangkat lunak. Penggandaan atas produk digital yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab semakin meraja lela tanpa ada ikatan hukum yang pasti sehingga merugikan pemegang hak cipta akan produk digital tersebut. Metode *spread spectrum* adalah sebuah teknik pentransmisi dengan menggunakan *pseudonoise code*, yang independen terhadap data informasi, sebagai modulator bentuk gelombang menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar dari pada sinyal jalur komunikasi informasi, oleh penerima, sinyal terkumpul kembali menggunakan replikasi *pseudonoise code* tersinkronisasi.

Kata Kunci : *Watermarking, Spread Spectrum*

Abstract

Watermarking is a process of adding code permanently to a digital image. The insertion of this code must have a fairly good robustness from various manipulations, such as conversion, transformation, compression, and encryption. The inserted code also does not damage the digital image so that the digital image looks like the original. Watermarking is needed to protect digital intellectual works such as images, text, music, videos, and including software. The doubling of digital products carried out by irresponsible parties is increasingly rampant without any definite legal ties that harm the copyright holders of these digital products. Spread spectrum method is a transmission technique using pseudonoise code, which is independent of information data, as a modulator waveforms propagate signal energy in a communication path (*bandwidth*) that is greater than the information communication path signal, by the receiver, the reconnect signal uses replication pseudonoise code synchronized.

Keywords: *Watermarking, Spread Spectrum*

1. PENDAHULUAN

Istilah *watermarking* ini muncul dari salah satu cabang ilmu yang disebut dengan steganography, yaitu merupakan cabang ilmu yang mempelajari tentang bagaimana menyembunyikan suatu informasi rahasia di dalam informasi lainnya. Aplikasi *watermarking* sebagai data hiding sangat diperlukan untuk pengiriman data informasi yang sifatnya rahasia (*covert communication*), misalnya untuk pengiriman data informasi pada intelijen. Agar data informasi rahasia yang di sisipkan tidak mudah diketahui dan terjaga keamanannya maka teknik *watermarking* yang dilakukan harus memiliki sifat invisible atau inaudible yaitu tidak tampak (untuk data digital seperti citra, video, text) atau tidak kedengarannya (untuk jenis audio) oleh pihak lain menggunakan panca indra[1].

Pengolahan citra adalah setiap bentuk pengolahan sinyal dimana *input* adalah gambar, seperti foto atau video bingkai, sedangkan output dari pengolahan gambar dapat berupa gambar atau sejumlah karakteristik atau parameter yang berkaitan dengan gambar[2][3]. Kebanyakan gambar dan teknik pemrosesan melibatkan atau memperlakukan foto sebagai dimensi dua sinyal dan menerapkan standar-teknik pemrosesan sinyal untuk itu, dapat juga digunakan untuk optick dan pengolahan gambar analog. Akuisisi gambar atau yang menghasilkan gambar input di tempat pertama disebut sebagai pencitraan.

Watermaking merupakan sebuah proses penambahan kode secara permanen ke dalam citra digital [4]. Penyisipan kode ini harus memiliki ketahanan (*robustness*) yang cukup baik dari berbagai manipulasi, seperti perubahan, transformasi, kompresi, maupun enkripsi. Kode yang disisipkan juga tidak merusak citra digital sehingga citra digital terlihat seperti aslinya. *Watermarking* sangat diperlukan untuk melindungi karya intelektual digital seperti gambar, teks, musik, video, dan termasuk perangkat lunak. Penggandaan atas produk digital yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab semakin meraja lela tanpa ada ikatan hukum yang pasti sehingga merugikan pemegang hak cipta akan produk digital tersebut. Penyisipan *watermark* memiliki peran yang cukup signifikan untuk mencegah hal ini terjadi.

Masalah yang dihadapi sering kali data yang dikirim dari satu tempat ke tempat lain yang merupakan data rahasia sehingga keamanannya perlu dijamin. Oleh karena itu diperlukan teknik *watermarking* bekerja dengan menyisipkan sedikit informasi yang menunjukkan kepemilikan, tujuan, atau data lain pada media digital tanpa mempengaruhi kualitasnya. Dengan adanya implementasi *watermark* ini diharapkan dapat melindungi penyisipan teks pada citra dengan menggunakan metode *spread spectrum*.

Metode *spread spectrum* adalah sebuah teknik pentransmisian dengan menggunakan pseudonoise code, yang independen terhadap data informasi, sebagai modulator bentuk gelombang menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwith*) yang lebih besar dari pada sinyal jalur komunikasi informasi, oleh penerima, sinyal kumpulan kembali menggunakan replikasi pseudonoise code tersinkronisasi [4].

Adapun yang menjadi tujuan penelitian yang dilakukan oleh penulis adalah Untuk mengetahui cara kerja *watermark* pada pesan, Menerapkan metode *spread spectrum* dalam *watermark* pada citra dalam penyisipan teks. Agar menghasilkan suatu aplikasi yang berfungsi sebagai alat bantu atau sistem dalam melindungi hak cipta sebagai bukti otentik atas hak kepemilikan pencipta atas content yang dibuat atau diproduksinya, Agar pihak-pihak dimudahkan dalam melakukan proses *watermaking* pada citra.

2. LANDASAN TEORI

2.1 Sejarah *Watermarking*

Watermarking sudah ada sejak 700 tahun yang lalu. Pada akhir abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi watermark atau tanda air dengan cara menekan bentuk cetakan gambar atau tulisan pada kertas yang baru setengah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang berwatermark. *Watermarking* merupakan suatu bentuk dari Steganography, yaitu ilmu yang mempelajari bagaimana menyembunyikan suatu data baik itu citra maupun teks pada data yang lain [5].

2.2. Metode *Spread Spectrum*

Metode *spread spectrum* adalah sebuah teknik pentransmisian dengan menggunakan pseudonoise code, yang independen terhadap data informasi, sebagai modulator bentuk gelombang menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwith*) yang lebih besar dari pada sinyal jalur komunikasi informasi, oleh penerima, sinyal kumpulan kembali menggunakan replikasi pseudonoise code tersinkronisasi[1][6]. Berdasarkan definisi diatas, dapat dikatakan bahwa stenografi menggunakan metode *spread spectrum* memperlakukan cover-object. Baik sebagai derau(noise) ataupun sebagai usaha untuk menambah derau semu (*pseudonoise*) ke dalam cover modulasi, dan penyisipan menggunakan metode *spread spectrum* ini terdiri dari tiga proses, yaitu pengambilan pesan dari matriks frekuensi, demodulasi dan de- spreading. Berikut gambaran mengenai perhitungan yang terjadi di dalam metode *spread spectrum*. Pada proses encode dapat digambarkan sebagai berikut. Dengan sebuah gambar dengan mengecek ukuran pesan yang dimasukkan apakah lebih kecil dari ukuran gambar pada yaitu memasukkan ke dalam rumus :

$$\text{PanjangPesan}=(\text{ukuranpesan})+28)*4*8 \dots(1)$$

Angka 28 adalah untuk tag pemberian tanda pada gambar yang sudah disisipkan , angka 4 adalah besar faktor pengali yang berguna untuk penyebaran bit serta angka 8 adalah bit gambar. Setelah mengecek ukuran file. Selesai kemudian pengecekan ukuran gambar, metode stenografi yang

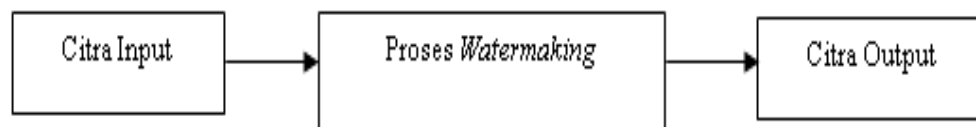
digunakan dan kata kunci, jika syarat semua spread spectrum digunakan untuk menyisipkan data watermark ke dalam citra yang tidak terkompresi[3]. Data watermark dianggap sebagai sinyal gelombang sempit dan citra dianggap sebagai sinyal gelombang lebar. Sinyal gelombang sempit menyebar untuk meningkatkan redudansi dan kemudian dimodulasi dengan urutan binary pseudo noise. Modulasi ini dinamakan *watermark spread spectrum* yang ditambahkan secara linear ke data citra. Alasan penambahan pseudo-noise adalah untuk mencegah pendeteksian dan penyerangan ke data watermark sudah terpenuhi dilanjutkan ke dalam proses penyisipan. Sebelum penyisipan dilakukan, fungsi akan membaca gambar dan mengambil header dari gambar JPEG yang sudah disisipkan sebelumnya, kemudian gambar dari body ini nanti akan disisipi pesan. Sebelum proses-proses penyebaran, yang dilakukan adalah mengubah pesan ke bentuk biner. Langkah berikutnya yaitu Perhitungan pembangkitan bilangan acak sesuai rumus pembangkitan bilangan acak LCG adalah seperti berikut :

$$X_{n+1} = (aX_n + c) \bmod \dots (2)$$

3. PEMBAHASAN

Langkah selanjutnya adalah identifikasi masalah dari hasil analisa terhadap sistem. Maka dapat diidentifikasi masalah, yaitu sebagai berikut :

1. Aplikasi yang akan dibangun harus dapat digunakan untuk melindungi data teks yang disisip dalam citra digital.
2. Teknik *watermarking* yang digunakan adalah dengan metode Spread Spectrum untuk melindungi data teks dalam citra digital. Adapun diagramnya dapat dilihat pada gambar di bawah ini



Gambar 1: Proses Watermaking

3.2.1 Citra Input

a. Gambar

Citra input merupakan citra yang memiliki intensitas warna berkisar antara 0 sebagai nilai minimum sampai 255 yang merupakan nilai maksimum.

Adapun gambar yang digunakan dalam proses ini adalah gambar dengan ukuran 4 x 4 pixel, Dimana gambar ini nantinya akan dikonversikan terlebih dahulu dalam bentuk biner. Adapun gambar yang digunakan dapat dilihat pada gambar di bawah ini.



Gambar 2: Gambar yang akan digunakan

b. Teks yang digunakan adalah teks dengan format txt dan doc

3.2.2 Proses

- Pesan : test
- Kunci : sonny
- Keterangan : Kunci bebas apa saja sonny hanya sebagai contoh.
- Gambar : Cece Kirana.bmp
- Penyelesaian
- Langkah 1 : Konversikan pesan dalam bentuk biner dengan hasil sebagai

berikut :

01110100 01100101 01110011 01110100
 t e s t

Langkah 2 : Konversikan gambar dalam bentuk matriks

$$\begin{pmatrix} 15 & 255 & 15 & 0 \\ 15 & 240 & 15 & 15 \\ 15 & 255 & 0 & 255 \\ 15 & 255 & 15 & 0 \end{pmatrix}$$

Langkah 2 : Konversikan matriks menjadi bilangan biner sehingga diperoleh hasil sebagai berikut :

00001111111111110000111100000000
 00001111111100000000111100001111
 00001111111111110000000011111111
 00001111111111110000111100000000

Langkah 3 : Bangkitkan *pseudonoise* dengan bibit pembangkitan yang ditentukan berdasarkan kunci masukan yaitu "sonny".

s = 01110011
 o = 00110111
 $\frac{\quad}{01000100}$ Xor
 n = 01101110
 $\frac{\quad}{00101010}$ Xor
 n = 01101110
 $\frac{\quad}{01000100}$ Xor
 y = 01111001
 $\frac{\quad}{00111101}$ Xor

Langkah 4 : kemudian nilai akhir ini 01100101 dikonversikan ke desimal nilai 101 : Setelah mendapatkan nilai dari kata kunci (101) kemudian nilai tersebut digunakan sebagai bibit awal pembangkitan bilangan acak. Perhitungan pembangkitan bilangan acak sesuai rumus pembangkitan bilangan acak LCG adalah seperti berikut :

$$X_{n+1} = (aX_n + c) \text{ mod } m$$

$$a = 17$$

$$c = 7$$

$$m = 84$$

X_n = Bilangan bulat ke-n

Perhitungannya adalah sebagai berikut:

$$X_1 = (17 * 101 + 7) \text{ mod } 84 \text{ hasilnya } X_1 = 44$$

$$X_2 = (17 * 44 + 7) \text{ mod } 84 \text{ hasilnya } X_2 = 83$$

$$X_3 = (17 * 83 + 7) \text{ mod } 84 \text{ hasilnya } X_3 = 74$$

$$X_4 = (17 * 74 + 7) \text{ mod } 84 \text{ hasilnya } X_4 = 5$$

$$X_5 = (17 * 5 + 7) \text{ mod } 84 \text{ hasilnya } X_5 = 8$$

Hasil tersebut diatas yaitu "44 83 74 5 8" dirubah dalam bentuk biner sehingga menjadi "00101100 01010011 01001010 00000101 00001000"

Langkah 5 : Pesan akan dimodulasi dengan *pseudonoise signal* dengan fungsi XOR (*Exclusive OR*).

00001111111111110000111100000000
 00001111111100000000111100001111
 00001111111111110000000011111111
 00001111111111110000111100000000

Maka hasil proses modulasi antara segmen pesan dengan pseudonoise signal menggunakan fungsi XOR adalah :

00100011101011000100010100000101
 00000111111100000000111100001111

00001111111111110000000011111111
 00001111111111111000011110000000

Hasil dari proses modulasi inilah yang akan disisipkan ke bit-bit gambar. Sebagai contoh, misalkan mengambil 4 *pixel* pertama dari gambar Cece kirana.bmp dan mengambil 4 bit pertama dari modulasi antara segmen pesan dan *pseudonoise signal*.

Red = 180 186 185 182
 Green = 166 172 174 171
 Blue = 163 169 172 169

Kemudian diubah menjadi biner dan disisipkan hasil proses modulasi antara segmen pesan dengan *pseudonoise signal* menjadi sebagai berikut

Red	Green	Blue
1 0 1 1 0 1 0	1 0 1 0 0 1 1	1 0 1 0 0 0 1
1 0 1 1 0 1 0	1 0 1 0 1 1 0	1 0 1 0 1 0 0
1 0 1 1 1 0 0	1 0 1 0 1 1 1	1 0 1 0 1 1 0
1 0 1 1 0 1 1	1 0 1 0 1 0 1	1 0 1 0 1 0 0

4. PEMBAHASAN

4.1 Algoritma

Algoritma adalah urutan langkah-langkah logis penyelesaian masalah yang disusun secara sistematis dan logis". Kata Logis merupakan kata kunci dalam Algoritma[7].

4.1.1 Algoritma Penyisipan

```

Input      : i ← kunci
            : x ← pesan
            : y ← image
            m, j ← bilangan acak
Output     : xn ← hasil penyisipan
Proses     :
            while (i < x) do
                m ← 0;
                j ← 0;
                while (j < 8) do
                    ts ← x[i];
                    ts ← (ts >> (7-m));
                    ts ← (ts & 1);
                    if (ts=0) then
                        begin
                            i=((x)+28)*4*8
                            ts = y xor y+1
                            Xn+1 = (jXn+ i) mod m
                        elseif
                        begin
                            i=((x)+28)*4*8
                            ts = y xor y+1
                            m ← m+1;
                            n ← n+2;
                            j ← j+1;
                        endwhile
                    xn[i] ← ts1;
    
```

end

4.1.2 Algoritma Ekstraksi

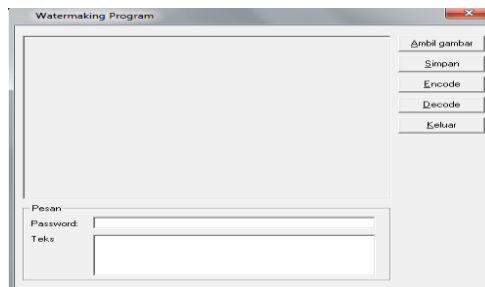
Adapun algoritma yang digunakan dalam proses ekstraksi pesan pada image ini adalah sebagai berikut

```

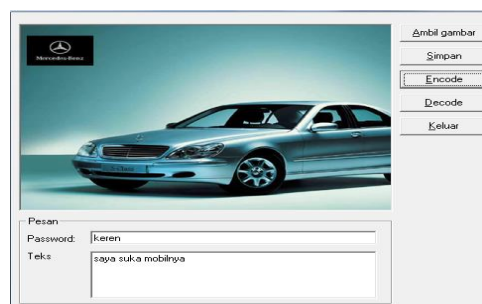
Input      : i ← kunci
           : Xn ← hasil penyisipan
           : m, j ← bilangan acak
Output     : x[i] ← Pesan
Proses     :
           : m ← 0;
           : j ← 0;
           : for i ← 0 to (Panjang_Teks-1) do
           :   m ← 0;
           :   s1 ← 0;
           :   j ← 0;
           while (j<8) do
           :   ts ← (teks[n] & 1);
           :   ts ← (ts << (7-m));
           :   xn+1 = (jXn- tsi) mod m
           :   m ← m+1;
           :   j ← j+1;
           :   n ← n+2;
           endwhile
           :   x[i] ← ts1;
           endfor
end
    
```

4.2 Implementasi

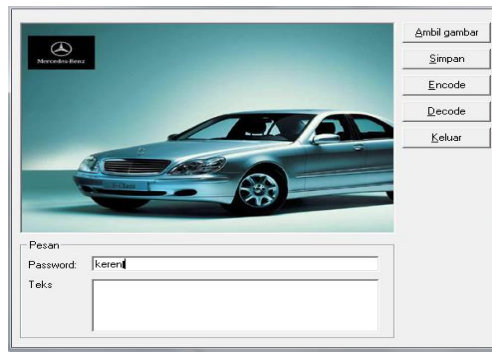
Adapun hasil eksekusi program ketika pertama kal dijalankan adalah sebagai berikut :



Gambar 3: Tampilan Utama



Gambar 4: Tampilan Encode



Gambar 5: Proses Input Password

5. KESIMPULAN

Berdasarkan hasil-hasil pengujian yang diperoleh sebelumnya, maka dapat disimpulkan beberapa hal sebagai berikut :

1. Proses yang dilakukan dengan aplikasi yang akan dibangun harus dapat digunakan untuk melindungi data teks yang disisip dalam citra digital, teknik *watermaking* yang digunakan adalah dengan metode *spread spectrum* untuk melindungi data teks dalam citra digital.
2. *Spread Spectrum* yang diimplementasikan membantu memenuhi kriteria *fidelity* karena penyisipan *watermark* tidak menyebabkan perubahan yang berarti terhadap kualitas citra hasil *watermaking*. Hal ini tentu saja berarti citra hasil *watermaking* sulit dibedakan dengan citra aslinya.

DAFTAR PUSTAKA

- [1] G. Budiman and L. Novamizanti, "Implementasi Teknik Watermarking menggunakan FFT dan Spread Spectrum Watermark pada Data Audio Digital," no. November 2017, 2016.
- [2] T. Sutojo, E. Mulyanto, V. Suhartono, and O. K. I. D. W. I. NURHAYATI, "Teori Pengolahan Citra Digital."
- [3] V. Lusiana, "Teknik Kompresi Citra Digital untuk Penyimpanan File menggunakan Format Data XML," vol. 19, no. 2, pp. 112–119, 2014.
- [4] A. Suheryadi, "PENERAPAN DIGITAL WATERMARK SEBAGAI VALIDASI KEABSAHAN GAMBAR," vol. 3, no. September, pp. 1–6, 2017.
- [5] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.
- [6] M. A. I. Pakereng, Y. R. Beeh, and S. Endrawan, "Perbandingan Steganografi Metode Spread Spectrum dan Least Significant Bit (LSB) Antara Waktu Proses dan Ukuran File Gambar."
- [7] M. Drs, "Lamhot Sitorus, Algoritma Dan Pemrograman, Yogyakarta: CV," *Andi Offset*, 2015.