WATERMARKING PADA CITRA DIGITAL DENGAN MENGGUNAKAN *METODE SPREAD SPECTRUM*

Liskedame Yanti Sipayung[1)] dan Rasmi Sitohang[2)]

Dosen Fakultas Teknologi Industri
Institut Sains dan Teknologi TD Pardede Medan

[1)]Liskedamesipayung@gmail.com
[2)]rasmisitohang@istp.ac.id

ABSTRAK

Watermark (tanda air) dapat ditambahkan pada citra digital untuk menunjukkan identitas kepemilikan dari pembuat citra. Namun, *watermark* konvensional, yaitu *visible watermark* atau *watermark* yang terlihat dapat dibuang oleh orang yang ingin menggunakan citra tanpa ijin dari penciptanya.

Salah satu metode nyayaitu Metode*SpreadSpectrum*, adalahsebuahteknik pentransmisian dengan menggunakan *pseudonoise code*, yang independen terhadap data informasi, sebagai modulator bentuk gelombang untukmenyebarkanenergisinyaldalamsebuahjalur komunikasi(*bandwidth*) yang lebih besar daripada sinyal jalur komunikasiinformasi. Olehpenerima, sinyal dikumpulkankembali menggunakanreplika*pseudonoisecode* tersinkronisasi.Metode *Spread Spectrum*akanmenambahkan derau semu (*pseudonoise*) ke dalam *cover-object*.

Aplikasi dapat digunakan untuk menyembunyikan pesan pada citra digital, tanpa menimbulkan kecurigaan.Pesan tidak akan berhasil diekstrak apabila proses ekstraksi menggunakan kunci yang salah atau kunci yang berbeda dengan kunci yang digunakan pada saat proses penyisipan.

Kata Kunci : Citra Digital

ABSTRACT

A watermark can be added to a digital image to show the proprietary identity of the image maker. However, conventional watermarks, namely visible watermarks or visible watermarks can be removed by people who want to use the image without the permission of the creator.

One of the methods, namely the Spread Spectrum Method, is a transmission technique using a pseudonoise code, which is independent of the information data, as a waveform modulator to spread signal energy in a communication line (bandwidth) that is greater than the information communication line signal. By the receiver, the signal is re-collected using a synchronized replica of the pseudonoisecode. The Spread Spectrum method will add pseudonoise to the cover-object.

Applications can be used to hide messages in digital images, without raising suspicion. Messages will not be successfully extracted if the extraction process uses the wrong key or a different key from the key used during the insertion process.

Keywords: Digital Image

I.1 Latar Belakang

Watermark (tanda air) dapat ditambahkan pada citra digital untuk menunjukkan identitas kepemilikan dari pembuat citra. Namun, *watermark* konvensional, yaitu *visible watermark* atau *watermark* yang terlihat dapat dibuang oleh orang yang ingin menggunakan citra tanpa ijin dari penciptanya. Pemecahan dari masalah ini adalah menambahkan *invisible watermark* atau *watermark* yang tak terlihat pada citra digital. Dengan menggunakan *invisible watermark*, pencipta dapat menyisipkan informasi pada citra digital yang menunjukkan bahwa citra tersebut memang dibuat olehnya.*Watermaking* diperlukan untuk melindungi karya intelektual digital seperti gambar,teks,musik,video,dan termasuk perangkat lunak.

Spread Spectrum dapat digunakan untuk menambah *invinsible watermark* ke suatu citra digital. *Spread Spectrum* adalah teknik pentransmisian dengan menggunakan *pseudonoise code*, yang independen terhadap data informasi,

sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*). Oleh penerima, sinyal dikumpulkan kembali dengan menggunakan replika *pseudonoisecode* tersinkronisasi. Dalam kasus *watermarking*, *Spread Spectrum* akan menambahkan derau semu (*pseudonoise*) yang tak terlihat ke *cover-image* (citra yang ditambahkan *watermarking*). Proses penyisipan *watermarking* terdiri dari tiga proses, yaitu *spreading*, modulasi dan penyisipan *watermark* ke citra. Lakukan proses sebaliknya untuk melakukan proses ekstraksi *watermark* dari citra.

Menerapkan metode *SpreadSpectrum*dalam *Watermark*pada citra dalam penyisipan teks agar menghasilkan suatu aplikasi yang berfungsi sebagai alat bantu dalam melindungi hak cipta sebagai bukti otentik atas hak kepemilikan pencipta yang dibuat atau diproduksinya, Agar pihak-pihak dimudahkan dalam melakukan proses *Watermarking* pada citra.

Dalam penulisan skripsi ini, ada beberapa istilah mengenai *watermark* dan *Spread Spectrum* yang dikemukakan oleh beberapa penulis dalam bentuk jurnal antara lain:

Dalam Jurnal Teknik Informatika Universitas Katolik St. Thomas tahun 2018 oleh Isninda Situmorang, *Watermaking* merupakan sebuah proses penambahan kode secara permanen kedalam citra digital.

Dalam Jurnal Teknik Informatika Universitas Islam Negeri Syarif Kasim Riau Pekanbaru, *Spread Spectrum* adalah teknik mentransmisikan sebuah sinyal pita sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi.

I.2 Rumusan Masalah

Berdasarkan latar belakang, maka yang menjadi permasalahan adalah bagaimana menyisipkan informasi *watermark* pada citra digital dengan menggunakan metode *Spread Spectrum*.

I.3 Batasan Masalah

Adapun pembatasan masalah terhadap perangkat lunak yang akan dibangun adalah sebagai berikut:

1. Batasan ukuran dari citra adalah maksimal 1024 x 768 piksel.
2. Dalam menginput aplikasi ini hanya *extension*yang berupa *.bmp, *.jpg.
3. Informasi *watermark* yang dapat disisipkan dibatasi maksimal 100 karakter (teks,huruf,angka dan karakter lain)
4. Aplikasi dapat menampilkan perhitungan singkat dari proses yang dilakukan.

I.4 Tujuan Penulisan

Tujuandari penulisan skripsi ini adalah untuk merancang aplikasi yang dapatmenyisipkan informasi *watermark* pada citra digital dengan menggunakan metode *Spread Spectrum* dan untuk mengetahui cara kerja *watermark* pada pesan.

II. Landasan Teori

2.1 Citra

Citra atau gambar dapat didefenisikan sebagai sebuah fungsi dua dimensi, $f(x, y)$, dimana x dan y adalah koordinat bidang datar, dan harga fungsi f di setiap pasangan koordinat (x, y) disebut intensitas atau level keabuan (*gray level*) dari gambar di titik itu.

Citra digital yang berukuran M x N lazim dinyatakan dengan matriks yang berukuran M baris dan N kolom sebagai berikut:

$$f(x,y) = \begin{bmatrix} f(0,0) & f(0,1) & \cdots & f(0,N-1) \\ f(1,0) & f(1,1) & \cdots & f(1,N-1) \\ \vdots & \vdots & \vdots & \vdots \\ f(M-1,0) & f(M-1,1) & \cdots & f(M-1,N-1) \end{bmatrix}$$

Nilai pada suatu irisan antara baris dan kolom pada posisi (x, y) disebut dengan *picture elements*, *image elements*, *pels*, atau *pixels*. Istilah terakhir (*pixel*) paling sering digunakan pada citra digital.

Citra digital merupakan representatif dari citra yang diambil oleh mesin (citra analog) dengan bentuk pendekatan berdasarkan *sampling* dan kuantisasi. *Sampling* menyatakan besarnya kotak-kotak yang disusun dalam baris dan kolom. Dengan kata lain, *sampling* pada citra menyatakan besar kecilnya ukuran piksel (titik) pada citra, dan kuantisasi menyatakan besarnya nilai tingkat kecerahan yang dinyatakan dalam nilai tingkat keabuan (*gray scale*) sesuai dengan jumlah bit biner yang digunakan oleh mesin. Dengan kata lain, kuantisasi pada citra menyatakan jumlah warna yang ada pada citra.

2.2 Digital Watermarking

Digital Watermarking adalah salah satu bagian dari bidang ilmu steganografi, yaitu suatu bidang ilmu yang mempelajari bagaimana menyisipkan suatu informasi ke dalam informasi lainnya. Pada ide awal kemunculannya, *watermarking* digunakan untuk dapat menyisipkan suatu informasi untuk menunjukkan kepemilikan, tujuan, atau data lain, pada suatu media tanpa mempengaruhi kualitasnya.

Watermarking merupakan hasil penggabungan dari dua teknik, yaitu kriptografi dan steganografi. Steganografi adalah teknik untuk menyembunyikan informasi ke dalam suatu data

tanpa menampakkan keberadaan informasi tersebut dan tanpa menimbulkan kecurigaan bahwa data yang disisipi dengan informasi tersebut telah berubah. Perbedaan mendasar antara steganografi dan kriptografi adalah pada hasil keluarannya. Hasil dari kriptografi adalah data yang berbeda dari aslinya sehingga data tersebut seolah-olah menjadi berantakan, sedangkan hasil dari steganografi memiliki bentuk persepsi yang sama dengan bentuk data awalnya.

2.2.1 Karakteristik *Watermarking*

Ada beberapa karakteristik atau sifat khusus tertentu yang harus dimiliki oleh sebuah *watermark*. Sifat-sifat tersebut sangat bergantung kepada aplikasi *watermarking* yang akan dibuat, atau dengan kata lain tidak ada sekelompok sifat tertentu yang harus dipenuhi oleh semua teknik *watermarking*. Meskipun demikian ada beberapa sifat yang secara umum dipunyai aplikasi *watermarking*. Sebuah *watermark* yang baik dan efektif idealnya akan memiliki karakteristik sebagai berikut:

1. *Perceptual transparency*
   Sebagian besar aplikasi *watermarking* mengharuskan algoritma*watermarking digital* menanamkan watermark sedemikian hingga ia tidak mempengaruhi kualitas media yang disisipi watermark. Media yang telah ditanami *watermark* haruslah sulit dibedakan dengan media aslinya oleh indera manusia, dengan kata lain penanaman *watermark* pada citra haruslah tidak terdeteksi oleh indera penglihatan manusia dan penanaman *watermark* pada audio haruslah tidak dikenali oleh indera pendengaran.
2. *Unobtrusiveness* (tak teramati)
   Watermark yang baik harus tidak teramati atau tidak terlihat oleh manusia.Jadi antara *image* yang memiliki *watermark* dan yang tidak, secara umum tidak akan terlihat bedanya.
3. *Robustness* (kekuatan/ketahanan)
   Sebuah *watermark* haruslah sulit, diharapkan mustahil untuk dihapus. Seandainya ada usaha-usaha untuk menghapus sebuah *watermark*, maka kualitas data *digital* akan mengalami penurunan, bahkan rusak. Ketahanan/r*obustness* suatu *watermark* yang dibutuhkan adalah ketahanan terhadap rekayasa untuk menghapus *watermark.* Ketahanan *watermark* juga harus tinggi terhadap usaha usaha rekayasa untuk menghapus *watermark.* Ada dua rekayasa yang biasa dilakukan yaitu penyatuan dan pemalsuan. Rekayasa dengan penyatuan misalnya adalah penggabungan beberapa salinan dari data digital dengan tujuan menghilangkan watermark. Demikian pula dengan pemalsuan yaitu dengan cara kombinasi data digital, sehingga dapat menghasilkan *watermark* yang berbeda. Kadang-kadang sebuah *watermark* hanya tahan terhadap sebuah proses tetapi rentan terhadap proses yang lain. Tetapi untungnya dalam banyak aplikasi, ketahanan *watermark* terhadap semua proses yang mungkin tidak diperlukan dan dianggap terlalu berlebihan. Biasanya *watermark* harus tahan terhadap pemrosesan sinyal yang terjadi hanya antara proses *embedding* (penyembunyian *watermarking* dalam data) dan deteksi. Contohnya aplikasi *watermarking* pada televisi, jadi yang ditekankan disini adalah proses *kompresi lossy*, *transmisi analog*, dan sebagainya. Sedangkan aplikasi *watermarking* pada suara yang melalui kanal telepon berarti batasan bandwidth sekitar 4000 Hz, tipe data analog, dan *sampling* atau *resampling* pada beberapa *central telepon office* (CTO). Tetapi untuk aplikasi *autenthication*, justru *watermark* diharapkan serentan mungkin terhadap proses pengolahan sinyal digital yang mungkin terjadi atau hampir seluruh proses pengolahan sinyal digital yang dapat dilakukan. Jadi ukuran *robustness* terhadap proses tertentu yang diperlukan untuk aplikasi tertentu mungkin tidak diperlukan dalam aplikasi yang lain. Untuk menentukan ukuran *robustness* harus terlebih dahulu dipikirkan aplikasi apa yang akan menggunakan sistem *watermarking*. Ketahanan terhadap proses-proses pengolahan lainnya, itu tergantung pada metoda *watermarking* yang digunakan. Tetapi dari berbagai penelitian yang sudah dilakukan belum ada suatu metoda *watermarking* ideal yang bisa tahan terhadap semua proses pengolahan *digital* yang mungkin. Biasanya masing-masing penelitian menfokuskan pada hal-hal tertentu yang dianggap penting.
4. *Tamper resistance*
   Yang dimaksud dengan *tamper resistance* adalah ketahanan sistem*watermarking* terhadap kemungkinan adanya serangan *(attack)* atau usaha untuk menghilangkan, merubah bahkan untuk memberikan *watermark* palsu terhadap suatu *host* data.
5. *Fidelity*
   yaitu perbandingan antara kualitas arsip penampung setelah penyisipan*watermark* dengan kualitas arsip semula. Pada penyisipan yang baik, perubahannya tidak dapat dikenali oleh manusia. Untuk *host* data yang berkualitas tinggi maka *fidelity* dituntut setinggi mungkin sehingga tidak merusak data aslinya, sedangkan *host* data yang memiliki *noise* (kualitas kurang) maka *fidelitynya* bisa rendah seperti pada suara pada siaran radio, suara pada telepon ataupun *broadcast* acara televisi.

6. *Computational Cost*
   Ada beberapa aplikasi yang menuntut proses *watermarking* baik*embedding* maupun *extracting* bekerja secara *real time*, ada juga yang mengharapkan salah satu baik *extracting* atau *embedding* saja yang *real time* ataupun duanya boleh tidak *real time*. Contohnya untuk aplikasi *owner identification* atau *proof of ownership*, proses *watermarking* baik *embedding* maupun *extracting* tidak perlu *real time*, sedangkan untuk aplikasi *fingerprinting* pada service *video on demand*, maka proses harus dilakukan secara *real time*.
7. *Recovery*
   yaitu pengungkapan terhadap data yang disembunyikan. *Watermark* yangdisisipkan harus dapat di deteksi kembali.

2.2.2 Proses dan *FrameworkWatermarking*

Jika *watermark* merupakan sesuatu yang ditanamkan, maka watermarking merupakan proses penanaman *watermark* tersebut. Secara umum proses dan *framework*pada *watermarking* tersusun atas dua bagian, yaitu:

1. Penyisipan *watermark (encoder)*
   Penyisipan *watermark* menangani bagaimana sebuah *watermark* ditanamkan pada media induknya. Dibawah ini penggambaran dari proses *encoding.*
   Pada proses penyisipan *watermark*ke citra disebut *encoding*, proses *encoding* bisa saja membutuhkan sebuah kunci,bisa saja tidak karena kegunaan sebuah kunci dalam proses *watermaking*adalah supaya watermaking hanya dapat di ekstraksi oleh pihak yang sah.
2. Pendeteksian watermark (*decoder*),
   Deteksi *watermark* dilakukan untuk membuktikan status kepemilikan citra digital. Verifikasi *watermark* terdiri atas ekstraksi *watermark*.Proses ekstraksi *watermark* disebut juga *decoding*, bertujuan mengungkap *watermark* dari dalam citra. Algoritma pendeteksian *watermark* menentukan apakah didalam sebuah media *digital* terdeteksi *watermark* yang sesuai atau tidak.

Watermark dapat berupa representasi identitas kepemilikan media *digital*, maupun informasi lain yang dipandang perlu untuk ditanamkan kedalam media yang bersangkutan. Algoritma penyisipan *watermark* menangani bagaimana sebuah *watermark* ditanamkan pada media induknya. Algoritma pendeteksian *watermark* menentukan apakah didalam sebuah media *digital* terdeteksi *watermark* atau tidak. Label *watermark* adalah sesuatu data/informasi yang akan kita masukkan ke dalam data digital yang ingin di-*watermark*. Ada 2 jenis label yang dapat digunakan :

1. *Text* biasa : Label *watermark* dari *text* biasanya menggunakan nilai-nilai ASCII dari masing-masing karakter dalam *text* yang kemudian dipecahkan atas bit-perbit, kelemahan dari label ini adalah, kesalahan pada satu bit saja akan menghasilkan hasil yang berbeda dengan *text* sebenarnya.
3. Logo atau Citra atau Suara : Berbeda dengan *text*, kesalahan pada beberapa bit masih dapat memberikan persepsi yang sama dengan aslinya oleh pendengaran maupun penglihatan kita, tetapi kerugiannya adalah jumlah data yang cukup besar.

2.3 Kode ASCII

Kode Standar Amerika untuk Pertukaran Informasi atau ASCII (American Standard Code for Information Interchange) merupakan suatu standar internasional dalam kode huruf dan simbol seperti Hex dan Unicode tetapi ASCII lebih bersifat universal, contohnya 124 adalah untuk karakter "|". Ia selalu digunakan oleh komputer dan alat komunikasi lain untuk menunjukkan teks. Kode ASCII sebenarnya memiliki komposisi bilangan biner sebanyak 7 bit. Namun, ASCII disimpan sebagai sandi 8 bit dengan menambakan satu angka 0 sebagai bit significant paling tinggi.

2.4 Landasan Matematika Kriptografi

Subbab ini akan membahas lebih *detail* mengenai operasi matematika yang digunakan pada metode *Spread Spectrum.*

2.5 Metode Spread Spectrum

Metode spread spectrum adalah sebuah teknik pentransmisian dengan menggunakanpseudonoise code, yang independen terhadap data informasi, sebagai modulator bentuk gelombangmenyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwith*) yang lebih besar dari padasinyal jalur komunikasi informasi, oleh penerima, sinyal kumpulkan kembali menggunakan replikasi psedonoise code tersinkronisasi. Berdasakan defenisi diatas, dapat dikatakan bahwa stenografimenggunakan 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*spreading*,modulasi, dan penyisipan pesan ke citra.Berikut gambaran mengenaiperhitungan yang terjadi di dalam metode spread spectrum. Kemudian melakukan pengecekan ukuran gambar. Jika syarat semua spread spectrum digunakan untuk menyisipkan datawatermark ke dalam citra yang tidak terkompresi. Data watermark dianggap sebagai

sinyalgelombang sempit dan citra dianggap sebagai sinyal gelombang Iebar. Sinyal gelombang sempitmenyebar untuk meningkatkan redudansi dan kemudian dimodulasi dengan urutan binary pseudonoise. Modulasi ini dinamakan *watermark spread spectrum* yang ditambahkan secara linear kedata citra. Alasan penambahan pseudo-noise adalah untuk mencegah pendeteksian danpenyerangan ke data watermark sudah terpenuhi dilanjutkan ke dalam proses penyisipan. Sebelum penyisipan dilakukan, fungsi akan membaca gambar dan mengambil header dari gambarJPEG atau Bitmap 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.Langkahberikutnya yaitu Perhitungan pembangkitan bilangan acak sesuai rumus pembangkitan bilangan acak LCG adalah seperti berikut :

Xn+1 = (aXn+ c) mod Fungsi Linear Congruent Generator(LCG)

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

1. Aplikasi yang akan dibangun harus dapat digunakan untuk melindungi data teks yang disisipkan dalam citra digital.

Teknik *watermarking* yang digunakan adalah dengan metode Spread Spectrum untuk melindungidata teks dalam citra digital.

III. Pembahasan

3.1 Pembahasan

Pembahasan akan mencakup proses penyisipan *watermark* dan proses ekstraksi *watermark* dengan menggunakan metode *Spread Spectrum*.

3.1.1 Proses Penyisipan Watermark dengan menggunakan metode *Spread Spectrum*

Sebagai contoh, misalkan *watermark* yang hendak disisipkan ke citra adalah “CITRA ” dan kunci yang digunakan adalah “1234”, maka proses penyisipan *watermark* adalah sebagai berikut:

1. Proses *Spreading*
   a. Ubah *watermark* “CITRA” ke dalam bentuk biner:
      Karakter Watermark-1 = 'E', kode ascii = 69, biner = 01000101
      Karakter Watermark-2 = 'L', kode ascii =76, biner = 01001100
      Karakter Watermark-3 = 'S', kode ascii = 83, biner = 01010011
      Karakter Watermark-4 = 'I', kode ascii = 73, biner = 01001001
      Karakter Watermark-5 = 'S', kode ascii = 83, biner = 01010011
      Karakter Watermark-5 = '', kode ascii = 32, biner = 00100000
      Karakter Watermark-6 = 'F ', kode ascii = 70, biner = 01000110
      Karakter Watermark-7 = 'R', kode ascii = 82, biner = 01010010
      Karakter Watermark-8 = 'I', kode ascii = 73, biner = 01001001
      Karakter Watermark-9 = 'A', kode ascii = 65, biner = 01000001
      Karakter Watermark-10 = 'N', kode ascii = 78, biner = 01001110
      karakter Watermark-11 =’I’, kode accii = 73, biner = 01001001
   b. Ubah pesan ke bentuk biner:
      01000101010011000101001101001001010
      10011001000000100011001010010010010
      01010000010100111001001001
   c. Konversikan gambar dalam bentuk matriks

$$\begin{pmatrix} 74 & 76 & 92 & 70 \\ 92 & 32 & 185 & 82 \\ 70 & 78 & 78 & 182 \\ 74 & 76 & 163 & 70 \end{pmatrix}$$

      Mengubah matriks kebilangan biner
      01001010001001100010111000100011
      01011100001000001011100101010010
      01000110010011100100111010110110
      010010100
      01001100101000110100011
   d. Proses *Spreading* akan menyebarkan bit dengan menggandakan bit Watermark sesuai dengan jumlah *spreading* yang digunakan. Misalkan Biner pesan disebar dengan skala pengali 4, sehingga menghasilkan bit pesan baru yaitu:
      00001111000000000000111100001111
      00001111000000001111111100000000
      00001111000011110000000011111111
      00001111000000000111100000000111
      00001111000011110000000011111111
      00000000111100000000000000000000
      00001111000000000000111111110000
      00001111000011110000000011110000
      00001111000000000111100000000111
      00001111000000000000000000000111
      00001111000000001111111111110000
      00001111 00000000 11110000 00001111
2. Proses Modulasi
   a.Pembangkitan pseudonoise dari kunci '1234':
      Awalnya BitKunci = 0

BitKunci = BitKunci xor Ascii('1') = 0 xor 49 = 49
BitKunci = BitKunci xor Ascii('2') = 49 xor 50 = 3
BitKunci = BitKunci xor Ascii('3') = 3 xor 51 = 48
BitKunci = BitKunci xor Ascii('4') = 48xor 52 = 4

b. BitKunci 4 digunakan sebagai nilai awal pembangkitan bilangan acak dengan LCG:
X(0) = 4
X(1) = (17* 4) + 7) mod 84 = 75
X(2) = (17* 75) + 7) mod 84 = 22
X(3) = (17* 22) + 7) mod 84 = 45
X(4) = (17* 45) + 7) mod 84 = 16
X(5) = (17* 16) + 7) mod 84 = 27
Ubah semua X ke biner:
0100101100010110001011010001000000011011
Pseudonoise yang dihasilkan adalah " 75 22 45 16 27" Ubah ke bentuk biner "0100101100010110001011010001000000011011".

c. Hasil dari proses modulasi adalah XOR antara bit Watermark dan bit pseudonoise:
BitPesan XOR BitKunci:
01000100000101100010001000011111
00010100010010111110100100101101
00011111000101000100101111101001
00100010000100001110101101000100
00011001001000100001000011100100
01001011111001100010110100010000
00010100010010110001100111011101
00011111000101000100101111100110
00100010000100001110101101000100
00011001001011010001000000010100
01000100000101101101001011100000
00010100 01001011 11100110 00100010

3.1.2 Proses Ekstraksi Watermark

Tahapan dari proses ekstraksi *watermark* terbalik dari proses penyisipan, yaitu: proses ekstraksi hasil modulasi, proses demodulasi dan proses *de-spreading*.

1. Proses Demodulasi

a. Pembangkitan *pseudonoise* dari kunci '1234':
Awalnya BitKunci = 0
BitKunci = BitKunci xor Ascii('1') = 0 xor 49 = 49
BitKunci = BitKunci xor Ascii('2') = 49 xor 50 = 3
BitKunci = BitKunci xor Ascii('3') = 3 xor 51 = 48
BitKunci = BitKunci xor Ascii('4') = 48 xor 52 = 4

b. BitKunci 4 digunakan sebagai nilai awal pembangkitan bilangan acakdengan LCG:
X(0) = 4
X(1) = (17* 4) + 7) mod 84 = 75
X(2) = (17* 75) + 7) mod 84 = 22
X(3) = (17* 22) + 7) mod 84 = 45
X(4) = (17* 45) + 7) mod 84 = 16
X(5) = (17* 16) + 7) mod 84 = 27

c. *Pseudonoise* yang dihasilkan adalah " 75 22 45 16 27" Ubah ke bentukbiner "0100101100010110001011010001000000011011 ".

d. Bit modulasi hasil ekstraksi dari citra:
01000100111001100010001000011111
00010100101110111110100100101101
00011111 11100100 01001011 11101001
00100010 1110000011101011 01000100
00011001 11010010000100001110010
01001011111001100010110100010000
00010100101110110001100111011101
00011111111001000100101111100110
00100010111000001110101101000100
00011001110111010001000000010100
01000100111001101101001 11100000
00010100 10111011 11100110 00100010

2. Proses *De-spreading*

a. Proses *De-Spreading* akan menyusutkan bit Watermark sesuai dengan jumlah *spreading* yang digunakan. Misalkan dilakukan sebanyak 4 (empat) kali *spreading* pada penyisipan, maka pada ekstraksi dilakukan penyusutan dengan mengambil 4 bit dan diganti menjadi 1 bit Watermark. Dengan demikian, hasil demodulasi berikut:
BitPesan XOR BitKunci:
00001111111100000000111100001111
00001111111100001111111100000000
00001111111111110000000011111111
00001111111100001111000000001111
00001111111111110000000011111111
00000000111100000000000000000000
00001111111100000000111111110000
00001111111111110000000011110000
00001111111100001111000000001111
00001111111100000000000000001111
00001111 11110000 11111111 11110000
00001111 00000000 11110000 00001111

IV. Algoritma Dan Implementasi

4.1 Algoritma

Algoritma dari aplikasi *watermarking* ini dibagi menjadi 2 bagian, yaitu algoritma penyisipan watermark dan algoritma ekstraksi watermark.

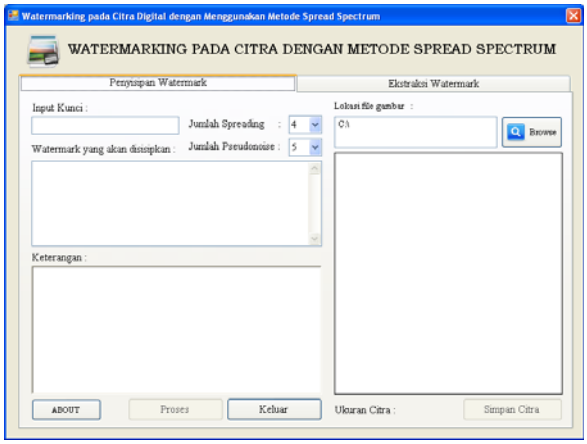
4.1.1 Algoritma Penyisipan Watermark

Algoritma ini berfungsi untuk menyisipkan bit-bit watermark pada citra digital dengan menggunakan metode Spread Spectrum. Berikut adalah algoritma dari proses penyisipan watermark:

1. Ubah pesan ke bentuk biner,
```
BitPesan = ""
For I = 1 To Len(Pesan)
   A = Asc(Mid(Pesan, I, 1))
   BitPesan &= DecToBiner(A, 8)
Next I
```
2. Proses Spreading
```
cTmp = ""
For I = 1 To Len(BitPesan)
   cTmp &= Strings.StrDup(nSpreading, Mid(BitPesan, I, 1))
Next
BitPesan = cTmp
```
3. Ubah kunci ke bentuk biner.
```
A=0For I = 1 To Len(Kunci)
   A = A Xor Asc(Mid(Kunci, I, 1))
Next I
nKunci = A
```
4. Pembangkitan Bilangan Acak,
```
BitKunci = ""
For I = 1 To nModulasi
   A = ((17 * A) + 7) Mod 84
   BitKunci &= DecToBiner(A, 8)
Next
```
5. Proses Modulasi.
```
iCount = -1
HasilXOR = ""
For I = 1 To Len(BitPesan)
   iCount = (iCount + 1) Mod Len(BitKunci)
   HasilXOR &= (Mid(BitPesan, I, 1) Xor Mid(BitKunci, iCount + 1, 1))
Next
BitPesan = HasilXOR
```
6. Sisipkan watermark yang tersimpan pada BitPesan ke citra, melalui bit terakhir dari setiap piksel.

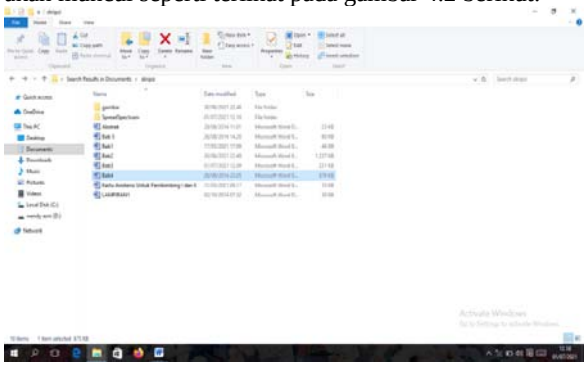
4.2 Implementasi

Saat*file* "SpreadSpectrum.exe" dijalankan, *form* Utama akan tampil seperti terlihat pada gambar 4.1 berikut. Form ini berisi *tab* untuk menyisipkan *watermark* pada citra digital dan tab untuk melakukan proses ekstraksi *watermark* dari citra digital.



Gambar 4.1 Form Utama
(Tab Penyisipan Watermark)

Tekan tombol 'Browse' untuk membuka *file* citra sebagai media *watermark*. Kotak dialog Open akan muncul seperti terlihat pada gambar 4.2 berikut.



Gambar 4.2Kotak Dialog Open File

REFRENSI

[BAS05] Basuki, dkk, Pengolahan Citra Digital, Penerbit Graha Ilmu, Yogyakarta, 2005.

[JIA04] Jiancheng Zou, Rabab K. Ward dan Dongxu Qi. *The Generalized Fibonacci Tranformations and Application to Image Scrambling*. IEEE, 2004.

ispl.korea.ac.kr/conference/ICASSP2004/pdfs/0300385.pdf

[KAD13] Kadir, A. dan Susanto, A. Teori dan Aplikasi Pengolahan Citra, Penerbit Andi, Yogyakarta, 2013.

[MUN04] Munir, R., Pengolahan Citra Digital, Penerbit Informatika, Bandung, 2004.

[PUR00] Purcell, E., J., Varberg, D., Kalkulus dan Geometri Analitis, Jilid Penerbit Erlangga, Jakarta, 2000.

[PUT10] Putra, D., Pengolahan Citra Digital, Penerbit Andi, Yogyakarta, 2010.

[SIM06] Simarmata, J, Teknologi Komputer dan Informasi, Penerbit Andi, Yogyakarta, 2006.

[SUT09] Sutoyo, T, Teori Pengolahan Citra Digital, Penerbit Andi, Yogyakarta, 2009.

Situmorang, Isninda. " Implementasi Watermark pada Cita Menggunakan Metode Spread Spectum". *Jurnal Teknik Informatika Unika Santo Thomas*. Vol.3,no 2018 pp.83-89.