Spread Spectrum Steganography

Yus Gias Vembrina / 13503042
if13042@students.if.itb.ac.id

Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung

Abstrak

Makalah ini berisi mengenai studi steganografi menggunakan metode *spread spectrum*. Metode *spread spectrum* ini tidak hanya tangguh dalam steganografi tetapi juga tangguh dalam *watermarking*, yang merupakan salah satu bidang pengaplikasian dari steganografi yang ditujukan untuk melindungi hak cipta atas produk digital.

Steganografi bukanlah pengganti kriptografi. Keduanya saling melengkapi satu sama lain. Untuk dapat mencapai maksud penggunaannya steganografi harus memenuhi beberapa kriteria tertentu. Lebih jauh lagi, untuk dapat diaplikasikan sebagai *watermarking*, ada kriteria lain yang harus dipenuhi, selain kriteria steganografi.

Salah satu metode yang dapat memfasilitasi tujuan steganografi dan juga *watermarking* adalah *spread spectrum*. Dengan menggunakan metode ini, dapat dihasilkan *watermark* yang mampu memenuhi sebagian besar dari kriteria yang diharuskan. Meskipun bukan merupakan metode yang ideal, metode *spread spectrum* ini dapat menjawab kebutuhan akan steganografi dan *watermarking* yang tangguh terhadap berbagai macam serangan.

Kata kunci: *steganography*, *watermarking*, *spread spectrum*

1. Pendahuluan

Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan di dalam pesan lain sehingga keberadaan pesan yang pertama tidak diketahui. [1] Steganografi berasal dari bahasa Yunani *steganos* yang berarti tulisan tersembunyi. Steganografi sangat kontras dengan kriptografi. Kriptografi merahasiakan makna pesan sementara eksistensi pesan tetap ada, sedangkan steganografi menutupi keberadaan pesan. Steganografi dapat dipandang sebagai kelanjutan dari kriptografi. Dalam prakteknya, pesan dienkripsi terlebih dahulu, kemudian disembunyikan di dalam media lain sehingga pihak ketiga tidak menyadari keberadaan pesan.

Steganografi membutuhkan dua properti, yaitu pesan dan media penampung. Media penampung yang umumnya digunakan sekarang dapat berupa teks, suara, gambar, atau video. Sedangkan pesan yang disembunyikan dapat berupa teks, gambar, atau pesan lainnya.

Keuntungan penggunaan steganografi adalah memungkinkan pengiriman pesan secara rahasia tanpa diketahui bahwa pesan sedang dikirim. Ini membuat pihak ketiga tidak menyadari keberadaan pesan. Sebaliknya, penggunaan kriptografi akan menarik kecurigaan pihak ketiga bahwa ada sesuatu yang disembunyikan dalam pesan yang sedang dikirim.

Steganografi juga memiliki kelemahan. Tidak seperti kriptografi, steganografi memerlukan banyak ruang untuk dapat menyembunyikan beberapa bit pesan. Akan tetapi, kelemahan ini sedikit demi sedikit dapat diatasi seiring dengan perkembangan teknik-teknik dalam melakukan steganografi.

Dalam menyembunyikan pesan, ada beberapa kriteria yang harus dipenuhi. [1]

1. ***Impercepbility***. Keberadaan pesan tidak dapat dipersepsi oleh indrawi. Jika pesan disisipkan ke dalam sebuah citra, citra yang telah disisipi pesan harus tidak dapat dibedakan dengan citra asli oleh mata. Begitu pula dengan suara, telinga haruslah mendapati perbedaan antara suara asli dan suara yang telah disisipi pesan.
2. ***Fidelity***. Mutu media penampung tidak berubah banyak akibat penyisipan. Perubahan yang terjadi harus tidak dapat dipersepsi oleh indrawi.
3. ***Recovery***. Pesan yang disembunyikan harus dapat diungkap kembali. Tujuan steganografi adalah menyembunyikan

informasi, maka sewaktu-waktu informasi yang disembunyikan ini harus dapat diambil kembali untuk dapat digunakan lebih lanjut sesuai keperluan.

2. Sejarah Steganografi

Catatan tertua mengenai penggunaan steganografi tercatat pada masa Yunani kuno. Pada saat itu, penguasa Yunani, Histiaues, sedang ditawan oleh Raja Darius di Susa. Histiaeus ingin mengirim pesan rahasia kepada menantunya, Aristagoras, di Miletus. Untuk itu, Histiaeus mencukur habis rambut budaknya dan menatokan pesan rahasia yang ingin dikirim di kepala budak tersebut. Setelah rambut budak tadi tumbuh cukup lebat, barulah ia dikirim ke Miletus.

Cerita lain masih juga berasal dari zaman Yunani kuno. Medium tulisan pada saat itu adalah papan yang dilapisi lilin dan tulisan ditulisi di papan tersebut. Demeratus, perlu memberitahu Sparta bahwa Xerxes bermaksud untuk menginvasi Yunani. Agar pesan yang dikirimnya tidak diketahui keberadaannya, Demeratus melapisi lagi papan tulisannya dengan lilin. Papan tulisan yang terlihat masih kosong inilah yang dikirim ke Sparta.

Tinta yang tidak nampak merupakan salah satu metode yang populer dalam bidang steganografi. Bangsa Romawi telah menggunakan tinta yang tidak nampak ini untuk menulis pesan di antara baris-baris pesan yang ditulis dengan tinta biasa. Tinta yang tidak nampak ini dapat terbuat dari sari jeruk atau susu. Ketika dipanaskan, warna tinta yang tidak tampak akan menjadi gelap dan tulisannya akan menjadi dapat terbaca. Tinta yang tidak tampak ini juga digunakan dalam Perang Dunia II.

Steganografi terus berkembang selama abad kelima belas dan keenam belas. Pada masa itu, banyak penulis buku yang enggan mencantumkan namanya karena takut akan kekuatan penguasa pada saat itu.

Pengembangan lebih jauh lagi mengenai steganografi terjadi pada tahun 1883 dengan dipublikasikannya kriptografi militer oleh Auguste Kerckhoffs. Meskipun sebagian besar berbicara mengenai kriptografi, Kerckhoffs menjabarkan beberapa deskripsi yang patut dicatat ketika merancang sebuah sistem steganografi. Lebih jauh lagi, Les Filigranes, yang ditulis oleh Charle Briquet di tahun 1907,merupakan sebuah kamus sejarah dari *watermark*, salah satu wujud pengaplikasian steganografi.

Dengan adanya komputer, steganografi memperoleh kemajuan yang sangat pesat. Penyembunyian pesan memasuki era baru berkat adanya komputer.

3. Terminologi dalam Steganografi

Terdapat beberapa istilah yang berkaitan dengan steganografi. [1]

1. *Hiddentext* atau *embedded message*: pesan atau informasi yang disembunyikan.
2. *Covertext* atau *cover-object*: pesan yang digunakan untuk menyembunyikan *embedded message*.
3. *Stegotext* atau *stego-object*: pesan yang sudah berisi *embedded message*.

Dalam steganografi digital, baik *hiddentext* atau *covertext* dapat berupa teks, audio, gambar, maupun video.

4. *Watermarking*

Satu istilah yang sering disebut-sebut adalah *watermarking*. *Watermarking* merupakan aplikasi dari steganografi, namun terdapat perbedaan di antara keduanya. Pada steganografi, media penampung tidak berarti apa-apa. Sedangkan pada *watermarking*, justru media penampung tersebut dilindungi kepemilikannya dengan pemberian label hak cipta (*watermark*). Lebih jauh lagi, *watermarking* berguna untuk membuktikan kepemilikan, *copyright protection*, otentikasi, *fingerprinting*, *tamper profing*, *distribution tracing*, dan sebagainya. Selain melindungi media penampung, pada *watermarking* kekokohan (*robustness*) *watermark* menjadi kriteria utama, tidak seperti pada steganografi. Kekokohan ini menjadi perhatian utama karena *watermark* tidak boleh hilang atau rusak meskipun media penampung dimanipulasi.

Watermarking muncul sebagai jawaban atas keperluan adanya perlindungan terhadap produk digital, misalnya citra hasil seni fotografi, citra hasil pengindraan jauh, musik *mp3*, video peristiwa penting, dan lain sebagainya.

Berikut adalah masalah yang melatarbelakangi munculnya *watermarking*.

1. Masalah kepemilikan. Pemalsuan atas kepemilikan produk digital sering

terjadi. Foto digital, misalnya, tidak memiliki suatu label atau informasi pengidentifikasi yang melekat pada foto tersebut. Apabila ada klaim dari pihak lain yang juga mengaku sebagai pemilik sah atas foto digital tersebut, pemilik foto yang asli tidak dapat memberikan bantahan karena memang ia tidak memiliki bukti otentik yang menandakan kepemilikan.

2. Masalah pelanggaran hak cipta. Penggandaan yang tidak berizin atas produk digital dapat merugikan pemiliknya sebab pemilik produk digital tidak memperoleh royalti apapun terhadap penggandaan ilegal tersebut.
3. Masalah keaslian. Produk digital mudah diubah. Perubahan tersebut dapat berupa rekayasa terhadap produk yang asli, baik perubahan yang dapat dipersepsi maupun tidak. Perubahan yang timbul dapat menyebabkan informasi penting yang terdapat di dalam produk digital hilang.

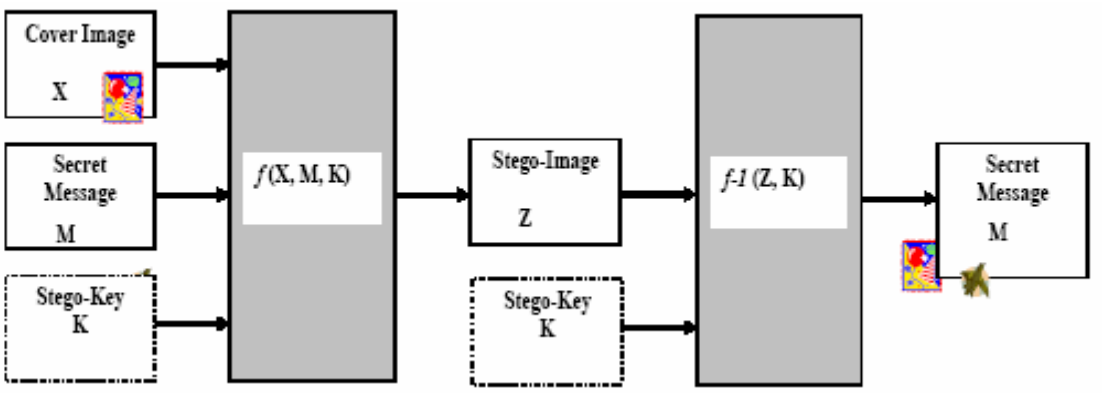
Kriptografi biasa saja tidak dapat menyelesaikan masalah-masalah di atas. Meskipun produk-produk digital dienkripsi, menggunakan algoritma RSA sekalipun, cukup sekali saja diperlukan dekripsi produk-produk digital tersebut. Setelah enkripsi dihilangkan, produk-produk digital tadi dapat langsung diperbanyak dan disebarkan tanpa perlu melakukan dekripsi lagi. Selain itu, tidak terdapat jejak yang dapat menunjukkan bahwa seseorang bertanggung jawab atas penyebaran produk digital ataupun otentikasi mengenai hak seseorang atas produk digital tersebut.

Untuk itu, selain memiliki kriteria yang dimiliki steganografi, *watermarking* harus juga memiliki kriteria berikut. [1] [3] [4]

1. ***Key uniqueness***: Kunci yang berbeda seharusnya menghasilkan *watermark* yang berbeda pula. Ini berarti penggunaan kunci yang salah menyebabkan hasil ekstraksi atau deteksi *watermark* yang salah pula.
2. ***Unambiguous***: Ekstraksi *watermark* harus dapat mengidentifikasi pemilik produk digital tanpa adanya ambiguitas. Lebih jauh lagi, akurasi identifikasi pemilik ini harus dapat bertahan terhadap serangan yang bermaksud merusak *watermark*.
3. ***Noninvertibility***: Secara komputasi, sangat sukar untuk menemukan atau mendapatkan *watermark* bila hanya diketahui produk ber-*watermark* saja.
4. ***Robustness***: *Watermark* haruslah sulit (diharapkan mustahil) untuk dihilangkan. Secara teoritis, *watermark* apapun dapat saja dihilangkan jika penyerang memiliki pengetahuan yang cukup mengenai proses penyisipan *watermark*. Akan tetapi, jika hanya sebagian pengetahuan saja yang dimiliki, misalnya posisi yang tepat dari *watermark* tidak diketahui, usaha penghilangan *watermark*, misalnya dengan menambah derau, akan menurunkan kualitas produk sebelum *watermark* berhasil dihilangkan. *Watermark* harus kokoh terhadap serangan-serangan berikut.
   - ***Common signal processing***: *Watermark* harus tetap dapat diekstraksi meskipun operasi-operasi berkaitan dengan pemrosesan sinyal telah dilakukan terhadap produk. Operasi-operasi ini di antaranya *digital-to-analog* dan *analog-to-digital conversion*, *resampling*, *requantization* (termasuk di dalamnya *dithering* dan *recompression*), dan *common signal enhancements* (misalnya terhadap warna dan tingkat kontras dari gambar, atau *bass* dan *teble* dari audio).
   - ***Common geometric distortions***: *Watermark* juga hendaknya tahan terhadap operasi yang mengubah geometri produk, seperti *rotation*, *translation*, *cropping*, dan *scaling*.
   - ***Subterfurge attacks: collusion and forgery***: *Watermark* diharapkan kokoh terhadap *watermark-watermark* lain yang disisipkan di dalam produk. *Watermark* harus tetap dapat diekstraksi secara induvidual tanpa dipengaruhi oleh *watermark* lain yang disisipkan.
5. ***Secure and reliable***: *Watermark* harus dapat bertahan dari *decoding* dan deteksi yang tidak terotentikasi. *Error rate* yang didapat dari hasil ekstraksi haruslah rendah. Pengubahan *watermark* juga diharapkan sulit untuk dilakukan oleh pihak yang tidak memiliki otoritas.

5. Teknik Steganografi

Tujuan dari teknik-teknik steganografi adalah menyembunyikan keberadaan pesan. Teknik *watermarking*, merupakan bagian dari steganografi yang ditujukan untuk perlindungan hak cipta, tidak hanya



Gambar 1 Model sistem steganografi [6]

dimaksudkan untuk menyembunyikan keberadaan pesan atau informasi, tapi lebih diarahkan untuk menjamin informasi dapat selamat dari beragam serangan yang dimaksudkan untuk menghancurkan *watermark*.

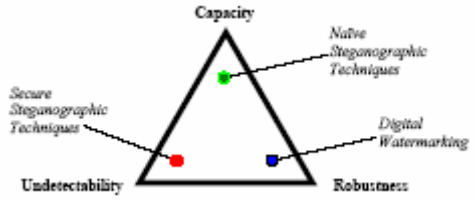
Model yang ditunjukkan pada Gambar 1 menunjukkan sistem steganografi yang umum digunakan pada gambar. Pesan rahasia disisipkan ke dalam medium menggunakan sebuah teknik steganografi tertentu untuk menghasilkan *stego-image* (*stego-object*). Dalam hal ini, medium hanya digunakan sekali saja, namun sebenarnya satu medium yang sama dapat digunakan untuk menghasilkan beberapa *stego-object*. Keamanan dari steganografi ini bergantung pada kunci, yang hanya diketahui oleh pengirim dan penerima pesan. Dalam sistem steganografi yang kuat, hanya pihak yang memiliki kuncilah yang dapat melakukan ekstraksi pesan. Pemanfaatan kunci dalam melakukan penyisipan dan pengekstraksian pesan unik bagi setiap teknik steganografi. Bahkan tanpa kunci, keberadaan pesan tersembunyi haruslah tidak disadari oleh pihak-pihak lain.

Dalam steganografi yang ideal, sebuah *stego-image* haruslah tidak dapat dibedakan dengan -non-*stego-image*, baik secara indrawi (visual) ataupun melalui analisis statistik. Dalam pengiriman pesan steganografi, penting bahwa keberadaan pesan tidak disadari dan tidak dapat dideteksi oleh pihak lain. Dengan kata lain, pihak lain tidak dapat membedakan antara *cover-image* yang belum dimodifikasi dan *cover-image* yang telah disisipi pesan ke dalamnya.

Tidak semua data dalam gambar dapat digunakan untuk keperluan steganografi. Umumnya gambar digital memuat informasi yang redundan dan komponen derau yang berasosiasi dengan detail dari gambar. Kedua hal tersebut merupakan candidat yang dapat dieksploitasi dalam menyisipkan informasi. Prinsip umum yang digunakan dalam steganografi adalah menempatkan informasi ke dalam derau dari gambar. Tujuan lainnya adalah membuat informasi yang disisipkan tidak dapat dibedakan dengan derau-derau acak lain yang ada dalam gambar. Secara umum, gambar yang memiliki lebih banyak detail akan memiliki lebih banyak derau. Contohnya, gambar langit biru yang bersih memiliki derau yang lebih sedikit dibandingkan dengan gambar stadion bola yang dipenuhi penonton.

Untuk meningkatkan pengamanan, penggunaan steganografi dikombinasikan dengan kriptografi. Pesan yang akan disisipkan dienkripsi terlebih dahulu menggunakan metode kriptografi tertentu.

Dalam menyisipkan informasi, ada beberapa faktor yang saling berkompetisi satu sama lain. Gambar 2 menunjukkan tiga faktor yang saling berkompetisi ini: *capacity*, *undetecability*, dan *robustness*.



Gambar 2 Faktor yang berkompetisi dalam steganografi [6]

Kapasitas adalah jumlah informasi (*embedded message*) yang dapat disembunyikan dalam *cover-object* dengan menggunakan teknik steganografi tertentu. Informasi dalam jumlah kecil dapat disembunyikan secara efektif tanpa dapat dideteksi dengan mudah oleh indrawi. Meskipun demikian, analisis statistik terhadap

derau yang ada dapat saja mengungkap keberadaan informasi rahasia. Penyisipan informasi dengan jumlah yang lebih banyak dapat saja mengubah *cover-object* sehingga keberadaan informasi dapat dengan mudah dideteksi.

Anti-deteksi adalah kemampuan untuk menghindari deteksi. Teknik penyembunyian yang tidak dapat dipersepsi oleh indrawi tetap dapat dideteksi dengan menggunakan analisis statistik. Informasi yang disembunyikan mungkin saja tidak dapat diekstraksi, namun pihak lain dapat mendeteksi keberadaan informasi rahasia. Teknik steganografi yang baik hendaknya tidak dapat dideteksi baik oleh indrawi maupun analisis statistik.

Kekokohan adalah ukuran ketahanan teknik steganografi dalam menghadapi berbagai macam manipulasi terhadap medium. *Watermarking* adalah teknik yang memenuhi kriteria ini.

Seringkali ketiga faktor ini saling menghilangkan satu sama lain. Teknik yang mampu menyembunyikan informasi dalam jumlah besar tidak dapat menyembunyikan keberadaan informasi yang dideteksi melalui analisis statistik. Teknik yang kokoh sering mengorbankan kapasitas.

Berikut ini adalah teknik dalam menyisipkan informasi rahasia.

4.1 *Spatial domain technique*

Ranah spasial ini juga dikenal sebagai teknik subtitusi. Subtitusi ini dilakukan sedemikian rupa sehingga medium yang disisipi tidak dapat dipersepsi oleh indrawi perubahannya.

Salah satu metode yang terkenal dalam ranah ini adalah metode *least significant bit*.

Beberapa variasi dalam melakukan metode *least significant bit* adalah sebagai berikut.
- Dari setiap bit yang ada, diisi secara parsial.
- Dari setiap bit yang ada, diisi secara total menggunakan data acak.
- Penggunaan sekuen acak semu.
- Penggunaan permutasi acak semu.
- Penggunaan wilayah dan bit paritas.

4.2 *Transform domain technique*

Ranah *transform* memfokuskan penyisipan pesan ke dalam frekuensi dari *cover-object*. Ranah ini memanfaatkan area *cover-object* yang cenderung tidak akan mengalami pemrosesan digital.

Dalam melakukan hal ini, dapat digunakan beberapa teknik, di antaranya adalah sebagai berikut.
- *Discrete Cosine Transform*
- *Fourier Transform*
- *Wavelet Transform*

5. *Spread Spectrum*

Spread spectrum merupakan bagian dari teknik dalam ranah *transform*.

Definisi *spread spectrum*
Sebuah teknik penransmisian dengan menggunakan *pseudo-noise code*, yang independen terhadap data informasi, sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwidth*) yang lebih besar daripada sinyal jalur komunikasi informasi. Oleh penerima, sinyal dikumpulkan kembali menggunakan replika *pseudo-noise code* tersinkronisasi.

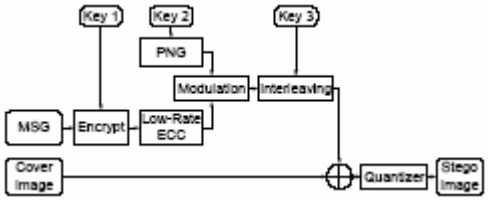
Berdasarkan definisi, dapat dikatakan bahwa steganografi menggunakan metode *spread spectrum* memperlakukan *cover-object* baik sebagai derau (*noise*) ataupun sebagai usaha untuk menambahkan derau semu (*pseudo-noise*) ke dalam *cover-object*.

Cover-object sebagai derau
Sistem yang memperlakukan *cover-object* sebagai derau dapat menambahkan sebuah nilai ke dalam *cover-object*. Nilai ini harus ditransmisikan di bawah tingkat derau yang ditambahkan nilai ke dalamnya. Hal ini berarti kapasitas sangat ditentukan oleh *cover-object*. Sementara nilai yang disisipkan dapat berupa bilangan real, dalam prakteknya, sulit untuk memasukkan dan mengekstraksi nilai real dari satu bit data. Untuk dapat melakukan transmisi lebih dari satu bit, *cover-object* dibagi menjadi bagian-bagian kecil, disebut dengan *sub-cover-object*. Ketika *sub-cover-object* rata (*tile*) metode ini dikatakan menggunakan *direct-sequence spread spectrum steganography*. Ketika *sub-cover-object* terdiri dari titik-titik terpisah yang terdistribusi di seluruh *cover-object*, dalam hal ini *cover-image*, metode ini disebut sebagai *frequency-hopping spread spectrum steganography*. Metode ini memerlukan proses pencarian secara menyeluruh terhadap *cover-object* untuk mendapatkan *carrier* (yang akan disisipi informasi) dan memaksimalkan penggunaan data yang terkandung di dalam *cover-object*.

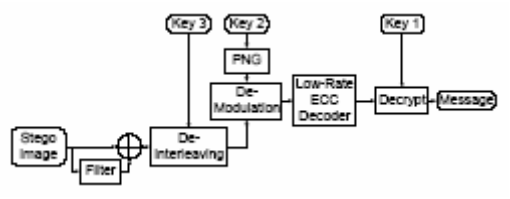
Penggunaan *direct-sequence* memerlukan pemrosesan yang jauh lebih ringan dibandingkan dengan *frequency-hopping*. Di sisi lain, *direct-sequence* tidak dapat mengatasi *cropping*, sementara *frequency-hopping* hanya akan menganggap hal tersebut sebagai sedikit pengurangan energi sinyal. Kapasistas dapat dipertukarkan secara linear dengan kekokohan. Hal ini sebenarnya sangat bergantung pada *cover-object* yang digunakan. Penyaringan spasial dapat menghilangkan informasi dalam *stego-object* jika penggunaan interval cenderung sama dalam setiap *sub-cover-object*. Interval yang acak dapat membantu mengatasi hal ini secara signifikan.

Usaha penambahan derau semu

Metode yang menempatkan informasi di dalam derau semu di keseluruhan *cover-image* disebut sebagai *spread sprectrum image steganography*. Penggunaan metode ini di deskripsikan dalam [2]. Gambar 3 dan Gambar 4 masing-masing menunjukkan langkah-langkah dalam melakukan penyisipan dan pengekstrasian informasi ke dan dari dalam *cover-image*.



Gambar 3 Penyisipan informasi menggunakan metode *spread spectrum image steganography*



Gambar 4 Pengekstrasian informasi menggunakan metode *spread spectrum image steganography*

Untuk melakukan penyisipan, informasi diubah terlebih dahulu menjadi derau semu yang kemudian dimasukkan ke dalam *cover-image* untuk menghasilkan *stego-image*. Untuk melakukan pengekstrasian, *stego-image* disaring untuk mendapatkan derau semu dan kemudian derau semu tadi diekstraksi menjadi informasi. Ada tiga kunci yang digunakan dalam metode ini. Kunci yang pertama digunakan untuk mengenkripsi informasi. Kunci yang kedua digunakan dalam membangkitkan derau semu. Dan, kunci yang ketiga digunakan untuk memasukkan dan menyebarkan informasi yang telah dimodulasi ke dalam *cover-image* sedemikian rupa sehingga penyisipan informasi sesedikit mungkin mempengaruhi *cover-image*.

6. Evaluasi

Dalam [7] terdapat perbandingan antara metode-motode steganografi. Hasil perbandingannya dapat dilihat di **Error! Reference source not found.**.

Metode steganografi yang ideal hendaknya mendapatkan predikat *high* di setiap spesifikasi. Sayangnya, dari metode-metode yang dievaluasi, tidak ada metode yang dapat memenuhi setiap spesifikasi yang ada. Akan

Tabel 1 Perbandingan antara metode-metode steganografi dalam medium gambar

	LSB in BMP	**LSB in GIF**	**JPEG compression**	**Patchwork**	**Spread spectrum**
Invisibility	High*	Medium*	High	High	High
Payload capacity	High	Medium	Medium	Low	Medium
Robustness against statistical attacks	Low	Low	Medium	High	High
Robustness against image manipulation	Low	Low	Medium	High	Medium
Independent of file format	Low	Low	Low	High	High
Unsuspicious files	Low	Low	High	High	High

* tergantung medium yang digunakan

ada spesifikasi yang perlu dikorbankan untuk dapat memenuhi spesifikasi yang lain. Spesifikasi yang diutamakan dapat dipilih sesuai keperluan.

Catatan mengenai *spread spectrum* adalah sebagai berikut. Metode *spread spctrum* memenuhi sebagian besar spesifikasi terutama kokoh terhadap serangan analisis statistik, karena informasi yang disembunyikan disebarkan dalam seluruh gambar tanpa mengganti properti statistik dari gambar yang disisipi informasi rahasia.

Dalam [8] disimpulkan mengenai kelebihan dan kekurangan *spread spectrum* itu sendiri.

Kelebihannya adalah

1. penyembunyian sinyal (kepadatan energi yang rendah, mirip derau),
2. komunikasi yang aman,
3. penolakan multipath, hanya menerima direct path,
4. proteksi terhadap inferensi yang disengaja (jamming),
5. penolakan terhadap inferensi yang tidak disengaja (narrowband),
6. kecil kemungkinan untuk terdeteksi, dan
7. adanya ketersediaan license-free ISM (Industrial, Scientific, and Medical) frequency-bands.

Sedangkan kekurangannya adalah

1. tidak adanya perbaikan performansi melalui penggunaan derau Gaussian,
2. peningkatan *bandwidth* (penggunaan frekuensi, *wideband receiver*), dan
3. peningkatan kompleksitas dalam proses perhitungan.

7. Kesimpulan

Metode *spread spectrum* adalah metode yang mampu menjawab kebutuhan akan steganografi. Lebih jauh lagi, metode ini juga cukup tangguh untuk digunakan dalam *watermarking*. Meskipun bukan merupakan metode yang ideal, *spread spectrum* merupakan metode yang menawarkan hasil terbaik dari metode-metode lainnya.

8. Daftar Pustaka

[1] Munir, Rinaldi. *Diktat Kuliah IF5054 Kriptografi*. 2006. Bandung: Institut Teknologi Bandung.

[2] Marvel, Lisa M., Charles G. Boncelet, dan Charles T. Retter. *Spread Spectrum Image Steganography*. 1999. IEEE Transaction on Image Processing.

[3] Cox, Ingerman J., Joe Kilian, Tom Leighton, dan Talal Shamoon. *Secure Spread Spectrum Watermarking for Multimedia*. ©NEC Research Institute, Technical Report 95 – 10.

[4] Ó Ruanaidh, JJK., WJ. Dowling, dan FM. Boland. *Watermarking Digital Image for Copyright Protection*. 1995. ©IEE.

[5] George, Mercy, Jean-Yves Chouinard, dan Nicolas Georganas. *Spread Spectrum Spatial and Spectral Watermarking for Image and Video*. Ottawa: School of Information Technology and Engineering, University of Ottawa.

[6] Kruus, Peter, Caroline Scace, Michael Heyman, dan Mathew Mundy. *A Survey of Steganographic Techniques for Image Files*. 2002. Advanced Security Research Journal – Network Associates Laboratories, Network Associates, Inc.

[7] Morkel, T., JHP. Eloff, dan MS. Olivier. *An Overview of Image Steganography*. Pretoria: Information and Computer Security Architecture (ICSA) Research Group, Department of Computer Science, University of Pretoria.

[8] Meel, J. *Spread Spectrum (SS)*. 1999. Belgium: De Nayer Instituut.