OPEN ACCESS
J. OF INISTA, VOL. 3, NO. 1, PP.069-075, NOV 2020

ISSN : 2622-8106 (ONLINE)
DOI: 10.20895/INISTA.V2I2

Journal of Informatics, Information System, Software Engineering and Applications

Analisis Hasil Implementasi Metode *Threefry* Sebagai Pembangkit *Random Number Generator* Pada Proses *Spread Spectrum Image Steganogrhapy*

Radhitya Iman Utama [#1], Ipam Fuaddina Adam [*2], Wahyu Adi Prabowo [#3]

 # Institut Teknologi Telkom Purwokerto
Jl. DI Panjaitan No 128, Purwokerto, Jawa Tengah Indonesia

[1] 15102111@st3tekom.ac.id
[2] ipam@ittelkom-pwt.ac.id
[3]wahyuadi@ittelkom-pwt.ac.id

accepted on 30-11-2020

Abstrak

Pada Era Modern saat ini pertukaran informasi dan cara memperoleh informasi dapat dilakukan dengan mudah dan dengan membutuhkan waktu yang relatif singkat. Perlindungan terhadapap data-data yang sangat penting haruslah kuat sehingga tidak mudah untuk di ambil oleh orang yang tidak memiliki wewenang untuk melakukan akses terhadap data tersebut.Steganografi merupakan seni untuk menyembunyikan pesan rahasia kedalam sebuah media sedemikian rupa sehingga membuat orang lain tidak menyadari adanya sesuatu di dalam media tersebut. Steganografi memiliki begitu banyak metode, salah satunya adalah metode Spread Spectrum. Di dalam metode tersebut memiliki keunggulan dimana adanya penggunaan noise yang di ambil dari pembangkitan angka semu. Angka-angka yang dihasilkan secara baik dapat mempengaruhi keamanan data yang akan disembunyikan. *Pseudo-Random Number Generator* (PRNG) yang akan menggunakan metode *Threefry* dimana metode ini diturunkan dari algoritma kriptografi *Threefish* dengan harapan menaikan tingkat penyamaran dan keamanan data dalam metode Spread Spectrum.

Kata Kunci : Data, PRNG, Steganografi, Spread Spectrum, Threefry.

I. PENDAHULUAN

Dampak negatif dari pesatnya perkembangan teknologi informasi terhadap kegiatan masyarakat, seperti adanya kebocoran data atau terjadinya pencurian data-data rahasia oleh kelompok atau perorangan yang dapat menyebabkan kerugian bagi orang lain yang memiliki hak dalam mengaksesnya

Spread spectrum merupakan salah satu metode steganografi dari ranah transform. Sebuah teknik pentransmisian dengan menggunakan *pseudo-noise code*, yang independen terhadap data informasi, sebagai modulator bentuk gelombang untuk menyebarkan energi sinyal dalam sebuah jalur komunikasi (*bandwith*) yang lebih besar daripada sinyal jalur komunikasi informasi[1].

Threefry adalah *random number generator* yang merupakan adaptasi non-kriptografi dari cipher blok Threefish dari Fungsi Skein Hash. Penggunaan dalam spread spectrum yaitu dengan 20 putaran (secara default), maka akan memiliki margin keselamatan yang cukup besar dibandingkan jumlah putaran minimum tanpa cacat statistik yang diketahui, tetapi masih memiliki kinerja yang sangat baik[2].

Dalam jurnal ini juga akan dibahas mengenai dampak perubahan kualitas dari citra yang dihasilkan setelah penyisipan, yang akan diukur secara subjektif, dan objektif. Pengukuran secara subjektif dilakukan dengan pengamatan menggunakan hasil ELA, sedangkan pengukuran secara objektif dilakukan dengan menggunakan metode Peak Signal Noise Ratio (PSNR) yang mengukur tingkat perbedaan dari citra yang telah disisipkan dengan yang belum tersisipkan.

II. TINJAUAN PUSTAKA

Chaeriah Bin Ali Wael pada tahun 2014 melakukan penelitian dengan judul Analisa Performansi *Spread Spectrum Image Steganography* (SSIS) pada Kanal Mulitpath Rayleigh Fading. Pada penelitiannya analisa yang dilakukan pada performansi teknik SSIS dengan menggunakan adata yang berupa text berekstensi .txt dan penyisipan pada citra 24bit berkestensi .jpg berukuran 256x256 piksel. Hasil yang diperoleh dari penelitian ini yaitu teknik SSIS dipengaruhi oleh jumlah bit pesan yang disisipkan, dimana jumlah bit pesan ini memiliki jumlah maksimum yang ditentukan oleh ukuran *cover*, *code rate*, kode konvolusi dan level kuantisasi. Hasil nilai SNR yang tinggi maka kualitas stego-image yang diterima semakin baik[3].

Achmad Noercholis dan Yohanes Nugraha pada tahun 2016, dengan penelitan yang berjudul Pengamanan Pesan Teks Menggunakan Teknik Steganografi Spread Spectrum Berbasis Android. Pada penelitian ini membahas bagaimana teknik steganografi digunakan pada citra digital dengan bermakasud untuk memberikan pengamanan pada pesan text yang disisipkan didalamnya. Pada penelitian ini teradapat dua proses yaitu proses *embedding* dan proses ekstraksi. Pada kedua proses ini digunakan *Random Number Generator* (RNG) yaitu menggunakan algoritma *Linear Congruential Generator* (LCG). Hasil dari penelitian ini dapat disimpulkan bahwa semakin besar ukuran gambar yang akan disisipkan maka semakin banyak jumlah karakter atau teks yang dapat disisipkan[1].

Wamiliana, Astria Hijriani, dan Pita Utari Ningtyas pada tahun 2017 melakukan penelitian dengan judul Perbandingan Metode Dynamic Cell Spreading (DCS) Dan Spread Spectrum Pada Steganografi Berbasis Aplikasi Web. Pada penelitian ini dilakukan tiga metode pengujian yaitu manipulasi *brightness*, *contrast*, dan *cropping* pada stego-image. Penelitian ini menghasilkan kesimpulan dimana Spread Spectrum memiliki ketahanan yang baik setalah stego-image diujikan, hal ini dikatakan baik apabila pihak lain tidak memiliki wawasan yang cukup dalam melakukan steganalisis, dibandingkan dengan DCS yang melakukan penyisipan text pada tiap pixel secara acak. Pertambahan ukuran pada masing-masing metode tergantung kombinasi warna yang digunakan, gambar dengan dominan hitam akan memiliki ukuran gambar lebih besar sedangkan gambar dengan kombinasi warna dominan putih akan memiliki pertambahan ukuran gambar yang lebih sedikit karena tiap pixelnya didominasi nilai RGB yang lebih kecil[4].

Winda Winanti pada tahun 2017 melakukan penelitan dengan judul Penyembunyian Pesan pada Citra Terkompresi JPEG Menggunakan Metode Spread Spectrum. Pada penelitian ini dilakukan studi mengenai bagaimana steganografi pada media citra digital. Citra digital yang digunakan adalah citra terkompresi dengan format file JPEG. Hasil penelitian ini yaitu kualitas citra terkompresi JPEG yang dihasilkan bergantung dari

besarnya ukuran pesan. Berdasarkan pengamatan yang dilakukan saat pengujian di penelitian ini, citra JPEG yang disisipkan lebih banyak penan akan mengalami perubahan yang lebih besar pada hasil gambarnya[5].

Isninda Situmorang pada tahun 2018 melakukan penelitian dengan judul Implementasi Watermark Pada Citra Menggunakan Metode Spread Spectrum. Tujuan dari penelitian ini adalah untuk mengetahui cara kerja watermark pada pesan, menerapkan metode Spread Spectrum dalam watermark pada citra dalam penyisipan teks. Penelitian ini menghasilkan suatu aplikasi yang memiliki fungsi 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[6].

Dalam penelitian ini akan membahas perubahan yang terjadi pada citra hasil steganografi apabila sebuah *random number generator* yang digunakan sebagai pengacak sinyal pada metode Spread Spectrum menggunakan Threefry *random number generator* yang selama ini menggunakan *random number generator* seperti *Linear Congruential Random Number Generator* dimana sistem pengacak sinyal memiliki banyak kekurangan dimana didalam penmbuatan angka acak dapat di prediksi dengan menggunakan metode tertentu.

Berikut ini merupakan dasar teori yang digunakan :

Steganografi

Steganografi berasal dari bahasa Yunani yaitu Steganós yang berarti menyembunyikan dan Graptos yang artinya tulisan sehingga secara keseluruhan artinya adalah tulisan yang disembunyikan. Steganografi sudah digunakan sejak ribuan tahun yang lalu untuk kepentingan politik, militer, diplomatik, serta untuk kepentingan pribadi sebagai alat komunikasi[7].

Spread Spectrum

Metode *Spread Spectrum* dalam steganografi diawali dari skema komunikasi *Spread Spectrum*, yang mentransmisikan sebuah sinyal pita sempit ke dalam sebuah kanal pita lebar dengan penyebaran frekuensi. *Spread Spectrum* steganografi terpencar pencar sebagai pesan yang diacak (*encrypt*) melalui gambar. Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*. Proses penyisipan pesan menggunakan metode Spread Spectrum terdiri dari tiga proses, yaitu spreading, modulasi, dan penyisipan pesan ke citra[8].

Pseudo-Random number generator (PRNG)

Pseudo-Random number generator (PRNG) adalah fungsi yang, setelah diinisialisasi dengan beberapa nilai acak (yang disebut seed), menampilkan urutan yang tampak acak, dalam arti bahwa pengamat yang tidak mengetahui nilai seed tidak dapat membedakan output. dari generator bit acak[9].

Counter-Based Pseudo-Random Number Generator (CBPRNG)

Sebagian besar pseudorandom number generator (PRNGs) berskala buruk untuk komputasi paralel berkinerja tinggi secara masif karena mereka dirancang sebagai transformasi keadaan berurutan. Dalam hal ini menunjukkan bahwa transformasi independen dari banyak *counter* menghasilkan kelas PRNG alternatif besar dengan sifat statistik yang sangat baik (jangka panjang, tidak ada struktur atau korelasi yang dapat dilihat). PRNG *counter-base* ini cocok untuk CPU multi-core modern, GPU, cluster, dan perangkat keras tujuan khusus karena mereka melakukan vektorisasi dan paralelisasi dengan baik, dan membutuhkan sedikit atau tidak ada memori untuk keadaan[2].

Threefry

Threefry adalah *random number generator* yang merupakan adaptasi non-kriptografi dari cipher blok Threefish dari Fungsi Skein Hash. Threefry adalah salah satu jenis CounterBased Pseudo-Random Number Generator yang dimana didalamnya akan menghasilkan 2 angka sekaligus. Penggunaan dalam spread spectrum yaitu dengan 20 putaran (secara default), maka akan memiliki margin keselamatan yang cukup besar dibandingkan jumlah putaran minimum tanpa cacat statistik yang diketahui, tetapi masih memiliki kinerja yang sangat baik[2].

MSE dan PSNR

PSNR Peak Signal to Noise Ratio (PSNR) merupakan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal tersebut. PSNR biasanya diukur dalam satuan decibel (dB). PSNR digunakan untuk mengetahui perbandingan kualitas citra cover (asli) sebelum dan sesudah disisipkan pesan[7].

Berikut ini merupakan rumus untuk menghitung nilai PSNR.

$$PNSR = 10\ log_{10}(\frac{C_{max}^2}{MSE})$$

MSE (Mean Square Error). MSE adalah nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi (dalam kasus steganografi ; MSE adalah nilai error kuadrat rata-rata antara citra asli (cover-image) dengan citra hasil penyisipan (stego-image)[7].

Berikut ini merupakan rumus untuk menghitung nilai MSE.

$$MSE = \frac{1}{M.N}\sum_{x=1}^{M}\sum_{y=1}^{N}(S_{xy} - C_{xy})^2$$

Dimana :

- C_{max} adalah nilai pixel terbesar pada keseluruhan citra
- X dan Y adalah koordinat suatu titik pada citra
- M dan N adalah dimensi dari citra
- S adalah citra tersisipi (stego-image)
- C adalah citra asli (cover image)

Nilai PSNR jatuh dibawah 30 dB mengindikasikan kualitas yang relative rendah, dimana distorsi yang dikarenakan penyisipan terlihat jelas. Akan tetapi kualitas stego-image yang tinggi berada pada nilai 40dB dan diatasnya[7].

Error Level Analysis (ELA)

Error Level Analysis merupakan salah satu metode forensik yang digunakan untuk mengidentifikasi bagian-bagian dari suatu gambar dengan tingkat yang berbeda dari suatu hasil kompresi. Teknik ini dapat digunakan untuk menentukan hasil gambar telah dimodifikasi secara digital atau merupakan gambar asli. Teknik ELA diperkenalkan oleh Krawetz yang tersedia secara online dari website (https://29a.ch/photo-forensics/#error-level-analysis)[10].

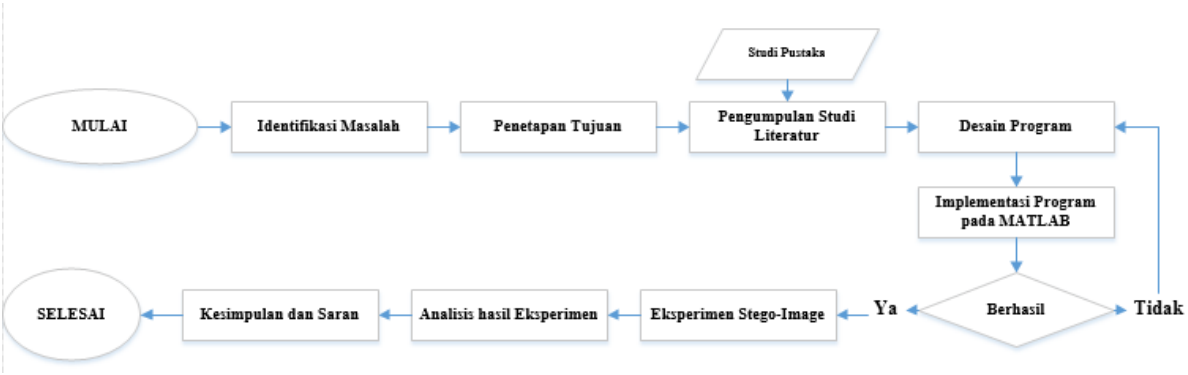
Pada web tersebut memiliki skala default dalam pengaturan untuk Error Level Analysis (ELA) sebagai berikut pada Table 1 Default ELA.

Table 1 Default ELA

Setting	Score
JPEG Quality	90
Error Scale	20
Magnifier Enhancement	None
Opacity	0.95

III. METODE PENELITIAN

Setelah melakukan penulisan uraian pada Latar Belakang, penulis melakukan penggambaran pada tahapan-tahapan yang akan dilakukan pada penelitian ini. Berikut ini merupakan tahapan-tahapan yang penulis lakukan dalam melakukan penelitian yang akan di gambarkan pada Gambar 1 Alir Penelitian.



Gambar 1 Alir Penelitian

Penelitian ini dimulai dengan melalui identifikasi masalah yang ada pada metode spread spectrum, masalah ini di ambil dari adanya kekurangan pada pembangkit angka semu yang bukan merupakan angka semu dimana angka-angka yang dihasilkan berdasarkan suatu rumus tertentu. Dengan hal ini penulis melakukan penetapan tujuan untuk mengubah pembangkit angka semu tersebut dengan pembangkit angka semu yang lain yang memiliki hasil angka-angka acak yang lebih baik dimana angka tersebut dihasilkan dari turunan algoritma kriptografi yang memiliki keamanan lebih. Pengambilan studi pustaka berasal dari buku-buku, makalah, jurnal dan studi lain sejenisnya dengan bukti yang mumpuni sebagai dasar studi literatur pada penelitian ini. Dari studi literatur yang telah ada maka penulis melakukan pembuatan desain program yang dimana akan ditulisan pada aplikasi matlab apabila implementasi tidak berhasil maka penulis akan melakukan pembuatan desain ulang dan apabila telah berhasil maka akan dilakukan proses untuk menghasilkan gambar hasil steganografi. Hasil tersebut akan melalui proses analisis dengan cara melihat ukuran dan resolusinya, perbandingan nilai MSE dan PSNR, serta melihat hasil dengan menggunakan ELA. Pada Akhir penelitian akan ditulis dalam kesimpulan dan saran yang ditarik dari hasil analisis yang telah dilakukan sehingga dapat menjadi hasil akhir untuk pengetahuan penelitian dan untuk menjadi tolak ukur pada penelitian selanjutnya.

IV. HASIL DAN PEMBAHASAN

Berdasarkan dari analisis yang telah dilakukan, aplikasi yang digunakan memiliki fungsi embedding dan extracting pada citra menggunakan metode Spread Spectrum telah berhasil di implementasikan ke dalam MATLAB dengan baik. Selanjutnya pengujian stego-image dari Spread Spectrum tersebut.

Pengujian pengaruh dari stego-image dilakukan dengan 3 cara, yang pertama membandingkan hasil size dan resolusi, yang kedua menggunakan perbandingan hasil nilai MSE dan PSNR, dan yang ketiga membandingkan hasil dari ELA.

4.1 Perbandingan hasil Size dan Resolusi

a. Perbandingan Size

Table 2 Perbandingan Size

Citra	Gambar Asli	SS_LCG	SS_Threefry	Keterangan
Island	1.58 Megabytes	705 Kilobyte	705 Kilobyte	Penyusutan
Black	22.3 Kilobytes	28.3 Kilobyte	28.3 Kilobyte	Pengembangan
Cats	66.4 Kilobytes	705 Kilobyte	705 Kilobyte	Pengembangan
Alif	2.92 Megabytes	5.13 Megabyte	5.13 Megabyte	Pengembangan
Spectrum	54.9 Kilobytes	51.1 Kilobyte	51.1 Kilobyte	Penyusutan

Dalam Tabel 2 Perbandingan Size dapat diambil sebanyak 40% dari hasil eksperimen mengalami penyusutan dan 60% mengalami pengembangan. Perbedaan yang di hasilkan dari penggunaan angka semu LCG dan Threefry tidak terlalu berbeda jauh sehingga angka dari nilai Size yang dihasilkan sama.

b. Perbandingan Resolusi

Table 3 Perbandingan Resolusi

Citra	Gambar Asli	SS_LCG	SS_Threefry	Keterangan
Island	1366 x 768	1366 x 768	1366 x 768	Sama
Black	1330 x 1048	1330 x 1048	1330 x 1048	Sama
Cats	1024 x 512	1024 x 512	1024 x 512	Sama
Alif	1728 x 2592	1728 x 2592	1728 x 2592	Sama
Spectrum	1282 x 867	1282 x 867	1282 x 867	Sama

Dalam Tabel 3 Perbandingan Resolusi dapat disimpulkan bahwa teknik Steganografi Spread Spectrum dengan menggunakan RNG LCG maupun RNG Threefry akan menghasilkan ukuran resolusi yang sama dengan ukuran resolusi dari covernya.

4.2 Perbandingan haasil nilai MSE dan PSNR

Table 4 Nilai MSE dan PSNR

Gambar	Hasil pada SS_LCG		Hasil pada SS_Threefry	
	MSE	PSNR	MSE	PSNR
Island	0.498234339413535	51.1564670409884	0.498384946416951	51.1551544476653
Black	0.0565445101302876	60.6068991492845	0.0563943255084276	60.6184495412498
Cats	0.497826258341471	51.1600256069649	0.497610727945964	51.1619062616764
Alif	0.530170363344955	50.8866491396176	0.53016619572569	50.8866832792317
Spectrum	0.493711766925118	51.1960688272728	0.493821529101072	51.195103409545

Dapat dilihat pada table 4 Nilai MSE dan PSNR dimana hasil dari MSE memiliki keunggulan apabila lebih rendah dan pada PSNR, semakin tinggi nilainya maka akan semakin baik hasilnya. Hasil MSE yang dapat ditarik dari table 4 yaitu terdapat 2 gambar dengan hasil pada LCG yang lebih tinggi dibandingkan dengan Threefry sedangkan 3 gambar lainnya Threefry memiliki keunggulan dibandingkan LCG. Hal ini dapat dilihat pada nilai-nilai dalam table 4 Nilai MSE dan PSNR.

4.3 Perbandingan hasil dari ELA

Table 5 Hasil ELA

Gambar	**SS_LCG**	**SS_Threefry**
Island	Tidak terdeteksi	Tidak terdeteksi
Black	Terdeteksi (Kiri Gambar)	Terdeteksi (Kiri Gambar)
Cats	Tidak terdeteksi	Tidak terdeteksi
Alif	Terdeteksi (Atas Gambar)	Terdeteksi (Atas Gambar)
Sprectrum	Tidak Terdeteksi	Tidak Terdeteksi

Hasil yang diperoleh bahwa adanya 2 gambar yang terdeteksi yaitu pada gambar Black dan gambar Alif sedangkan 3 gambar lainnya tidak terdeteksi. Pada kedua *random number generator* tidak menimbulkan perbedaan pada hasil ELA yang didapatkan.

V. KESIMPULAN

Beberapa kesimpulan yang dapat diambil dari penelitian ini adalah sebagai berikut :

1. Dari hasil pengembangan algoritma steganografi Spread Spectrum dengan menggunakan *Random Number Generator* Threefry di peroleh hasil bahwa adanya peningkatan terhadap kemanan data dan lebih memiliki ketahanan terhadap serangan.
2. Gambar yang telah tersisipi pesan (Stego-Image) tidak berbeda jauh dengan gambar aslinya (Cover Image) apabila dilihat dengan menggunakan mata manusia secara langsung karena perubahan yang terjadi tidak terlalu besar sehingga tidak berpengaruh pada kualitas gambar.
3. Penggunaan *Pseudo-Random Number Generator* (PRNG) dengan menggunakan metode Threefry dan metode *Linear Congruential Generator* (LCG) memiliki hasil yang mirip sehingga tidak menimbulkan perubahan kualitas gambar hasil (Stego-Image).
4. Algoritma steganografi Spread Spectrum dapat berfungsi dengan baik menggunakan Pemrogramman MATLAB.

DAFTAR PUSTAKA

[1] J. Antivirus, "STEGANOGRAFI SPREAD SPECTRUM," vol. 10, no. 1, pp. 32–41, 2016.
[2] Sunoru, "Random Number Generator 123 Family," *Random123 Family*, 2018. [Online]. Available: https://sunoru.github.io/RandomNumbers.jl/latest/lib/random123/#RandomNumbers.Random123.Threefry2x. [Accessed: 16-Jan-2019].
[3] C. Bin and A. Wael, "ANALISA PERFORMANSI SPREAD SPECTRUM IMAGE STEGANOGRAPHY (SSIS) PADA KANAL MULTIPATH RAYLEIGH FADING," pp. 1–10, 2014.
[4] J. Komputasi, "PERBANDINGAN METODE DYNAMIC CELL SPREADING (DCS) DAN SPREAD SPECTRUM PADA STEGANOGRAFI BERBASIS APLIKASI," vol. 5, no. 1, pp. 60–68, 2017.
[5] W. Winanti, "Penyembunyian Pesan pada Citra Terkompresi JPEG Menggunakan Metode Spread Spectrum," no. 13505017.
[6] I. Situmorang, "Implementasi Watermark Pada Citra Menggunakan Metode Spread Spectrum," vol. 03, pp. 83–89, 2018.
[7] O. A. Solichin and S. Kom, "Mengukur Kualitas Citra Hasil Steganografi," no. April, pp. 3–6, 2015.
[8] A. G. Salman and T. Nugraha, "Program Aplikasi Steganografi Menggunakan Metode Spread Spectrum Pada Perangkat Mobile Berbasis Android," *ComTech*, vol. 3, no. 2, p. 12, 2012.
[9] H. C. A. van Tilborg and S. Jajodia, Eds., "PRNG," in *Encyclopedia of Cryptography and Security*, Boston, MA: Springer US, 2011, p. 978.
[10] D. Universitas, B. Darma, J. Jenderal, A. Yani, and N. Palembang, "ANALISIS DIGITAL FORENSIK REKAYASA IMAGE," vol. 21, no. 1, pp. 54–63, 2019.