Peningkatan Least Significant Bit (LSB) pada Citra dengan Formasi 2-3-3 dan Bilangan Acak Linear Congruential Number Generator (LCG)

Pahala Sirait[1], Irpan Adiputra Pardosi[2]
Program Studi Teknik Informatika
STMIK Mikroskil
Medan, Indonesia
Email: pahala@mikroskil.ac.id, irpan@mikroskil.ac.id

Abstrak— Steganografi merupakan seni dan ilmu untuk menyamarkan pesan dan termasuk teknik yang kuat untuk menyisipkan pesan rahasia di dalam citra. Tedapat banyak metode implementasi LSB diantaranya formasi 2-3-3 dan Linear Congruential Generator (LCG). Penelitian ini membandingkan kedua metode tersebut berdasarkan kapasitas penyisipan, waktu eksekusi dan ketahanan terhadap noise yang akan diukur menggunakan MSE dan PSNR. Hasil dari penelitian ini mendapatkan secara keseluruhan metode formasi 2-3-3 lebih baik.

Kata Kunci— ***Formasi 2-3-3; LCG; Metode Steganografi***

I. PENDAHULUAN

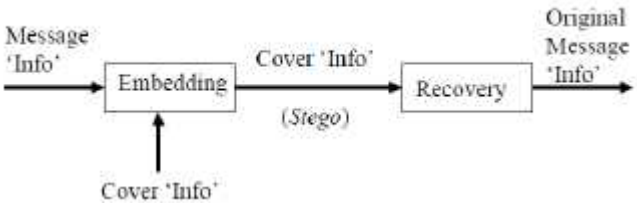
Steganografi merupakan seni untuk menyamarkan komunikasi dengan cara menyisipkan informasi dalam citra [1]. Algoritma *Least Significant Bit*(LSB) merupakan salah satu metode sederhana yang digunakan dalam steganografi, dengan metode ini kapasitas penyisipan pesan relatif kecil disebabkan jumlah pesan yang banyak dalam citra akan mempengaruhi tampilan citra, sementara kebutuhan akan hal itu semakin meningkat [1][4][5][6]. Beberapa penelitian sudah dikembangkan untuk mengatasi masalah ini diantaranya dengan menggunakan metode Linear Congruential Number Generator (LCG) [1][3][7] ataupun metode formasi 2-3-3 [8][9][10]. Adanya kebutuhan akan peningkatan penyisipan pesan dalam citra dengan metode steganografi[5][4][6], menyebabkan perlunya hasil dari kedua penelitian diuji untuk mendapatkan metode yang paling baik ditinjau dari segi jumlah pesan yang disisip maupun kualitas citra hasil yang didapatkan. Untuk mendapatkan hasil yang tepat perlu dilakukan kajian dan penelitian mendalam untuk membandingkan keduanya baik dari segi data, cara menguji hingga teknik ujicoba ketahanan citra hasil steganografi. Tujuan utama dalam penelitian ini adalah membandingkan perfomansi dari kedua metode ditinjau dari segi (1) waktu eksekusi proses penyisipan dan ektraksi, (2) kapasitas muatan (*imperceptibility*) menggunakan nilai MSE dan PSNR, dan (3) ketangguhan (*robustness*) yakni tingkat pengembalian citra hasil diberikan pengolahan citra berupa kontras dan noise *salt.*

II. STEGANOGRAFI

Steganografi merupakan seni dan ilmu untuk menyembunyikan pesan sehingga tidak diketahui orang lain, memiliki perbedaan yang sangat kontras dengan kriptografi karena keberadaan pesan tidak disamarkan tapi isinya dikaburkan, keuntungannya pengiriman pesan tidak menarik perhatian penerima ataupun orang lain [7].

A. Metode LSB (Least Significant Bit)

Teknik Steganografi dengan menggunakan metode *Least Significant Bit* (LSB) adalah teknik yang paling sederhana dan sering digunakan untuk memasukkan informasi pada *coverfile*[4]. LSB menggunakan bit terendah dalam bilangan biner, hal ini merupakan hal penting dalam konsep penyimpanan data komputer dan pemrograman yang berlaku untuk urutan dimana data tersebut akan disusun, disimpan dan dikirimkan[5]. Biasanya, tiga bit dari setiap pixel dapat menyembunyikan pesan dalam gambar dengan LSB untuk setiap *byte* pada gambar 24 bit.



Gambar 1. Blok diagram dari steganografi

Menggunakan LSB untuk meyembunyikan sebuah data rahasia ke dalam gambar dapat mengoptimalkan kapasitas dari jumlah data rahasia yang dapat disembunyikan dan dari gambar yang sudah disisipkan data rahasia tersebut tidak terlihat perbedaan hasil yang jelas ketika di lihat dengan indra visual manusia, karena LSB bekerja dengan cara menyisipkan data rahasia pada satu atau lebih bit terendah atau bit yang paling kanan pada salah satu atau ketiga byte warna dari warna RGB pada satu piksel gambar [6]. Jika menggunakan gambar 24-bit, setiap bit warna merah (Red), hijau (Green) dan biru (Blue) dapat digunakan, yang merepresenteasikan 1.

byte. Dengan kata lain, satu pixel dapat menyimpan 3 bit pesan. Sebuah gambar dengan ukuran 800 × 600 pixel, dapat menampung pesan rahasia sebanyak 1,440,000 bits atau 180,000 byte data penyisipan [7]. Misalnya 3 pixels dari gambar 24-bit seperti terlihat di bawah ini:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

Jika data 200 diubah menjadi biner 11001000, akan disisipkan ke dalam gambar dengan LSB, maka hasil penyisipan seperti berikut ini:

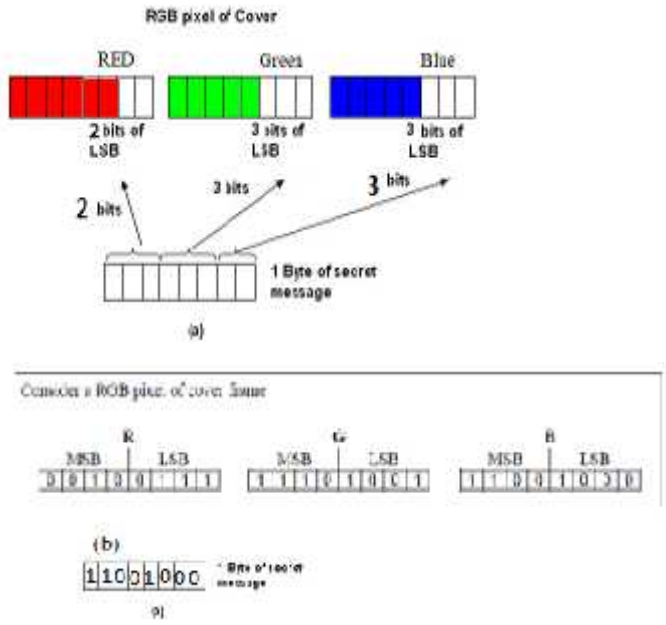
(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

B. Metode LSB Formasi 2-3-3

Tidak jauh berbeda dengan LSB, pada Enhanced Least Significant Bit (Enhanced LSB) dilakukan peningkatan dalam penyembunyian pesan yang awalnya hanya penyisipan pada 1 digit paling kanan, kini ditingkatkan dengan formasi 2-3-3 substitusi. Dengan menggunakan Enhanced LSB, keberadaan data yang disembunyikan lebih sulit untuk di deteksi dan dibutuhkan tidak hanya satu warna untuk menyembunyikannya. Sebagai contoh bit data rahasia yang pertama dan kedua di sembunyikan pada byte warna merah pada warna RGB, kemudian byte warna hijau menyembunyikan bit data rahasia yang ketiga, keempat dan kelima, selanjutnya bit data rahasia keenam, ketujuh dan kedelapan disembunyikan pada byte warna biru. Dengan formasi 2-3-3 substitusi ini maka setiap 1 pixel dari citra penampung dapat menampung 1 karakter pesan [9]. Misalnya 8 bit pesan akan disisipkan 2 bit ke R, 3 bit ke G dan 3 bit ke B. Secara detail akan dijelaskan pada gambar 2 (a) dan (b)[10].



Gambar 2(a) dan (b) Penyisipan Bit ke dalam Gambar

C. Metode LSB Linear Congruential Generator (LCG)

Standar minimal metode linear Congruential Generator (LCG) [1] biasanya digunakan untuk men-generate bilangan acak yang digunakan untuk mencocokan lokasi bit tertentu dalam gambar dimana bit data rahasia tersimpan. Metode ini merupakan salah satu pembangkit bilangan acak paling baik terutama untuk penggunaan memori komputer.

Formulasinya dijelaskan dibawah ini.

$$\mathbf{X_{n+1} = (aX_n + c) \bmod m}$$

Dimana:
X_0 adalah nilai awal, batasan nilai ; $0 <= X_0 < m$
a adalah pengali (*multiplier)*; $a \geq 0$
c adalah penbamahan (*increment*); $c \geq 0$
m adalah modulus ; $m > X_0$, $m > a$, $m > c$
Urutan bilangan acak yang muncul < Xn > diperolah dari pengaturan
$X_{n+1} = (aX_n + c) \bmod m$, $n \geq 0$
X_n memilih antara [0, m-1], $n \geq 0$
Bilangan acak sebelumnya X_i, maka bilangan acak berikutnya X_{i+1} yang dibangkitkan dengan;
$X_{i+1} = f(X_i, X_{i-1,\ldots,} X_{i-n+1}) (\text{mod } m) = (a_i x_i + a_2 x_{i-1} + \ldots + a_n x_{i-n+1} + c) (\text{mod } m)$ [1][6]
Urutan bilangan acak linier didefenisikan oleh *m, a, c* dan X_0 yang memiliki periode penuh, jika dan hanya jika memenuhi persyaratan berikut ini;

- Bilangan positif yang dibagi *m* dan *c* adalah 1
- Jika *q* bilangan prima yang membagi m, maka q membagi a -1
- Jika 4 membagi *m*, maka 4 membagi *a* -1

Tambahan, nilai m harus lebih besar sehingga periode tidak lebih dari m element. Nilai dari *m* mengharuskan komputeasi yang cepat dari (aXn+c) misalnya, kecepatan men-generate bilangan random.

D. Metode Pengukuran

Teknik Steganografi diukura berdasarkan dua atribut yaitu *impercepbility* dan kapasitas, yang akan diukur menggunakan Mean squared Error (MSE) dan Peak Signal to Noise Ratio (PSNR) diantara gambar asli dan gambar stego yang sudah disisipkan pesan rahasia. [10]. Persamaan yang digunakan dalam metode PSNR terlihat seperti dibawah ini (2).

$$PSNR = 10\log_{10} L^2/MSE \qquad (2)$$

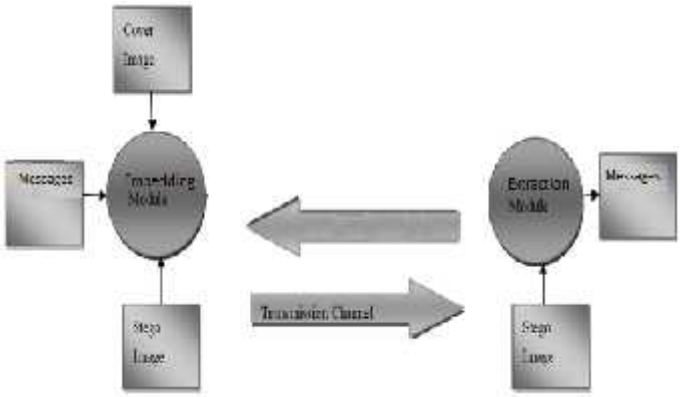
Dimana L adalah puncak level sinyal untuk gambar. Nilai dari MSE dihiutung berdasarkan(3).

$$MSE = \frac{1}{HW} \sum_{i=1}^{H} \sum_{j=1}^{W} (P(i,j) - S(i,j))^2 \qquad (3)$$

III. METODOLOGI

Penelitian ini mengadopsi metode eksperimen untuk mengetahui dampak menggunakan seleksi pixel bervariasi dan acak selama proses penyisipan dari segi *imperceptibiliy* dan kapastias penyimpanan. Metode ini menunjukkan standarisasi

prakek yang digunakan untuk memanipulasi variabel bebas yang digunakan untuk menganalisa data yang dibangkitkan.



Gambar 3. Framework dari sistem

Pengujian akan dilakukan untuk mendapatkan data perbandingan untuk kedua metode yang akan menggunakan dataset dengan tipe data BMP, JPG dan PNG berdasarkan;

a) Waktu eksekusi penyisipan dan ekstraksi.

b) Kecepatan penyisipan dan kapasitas dari kedua metode.

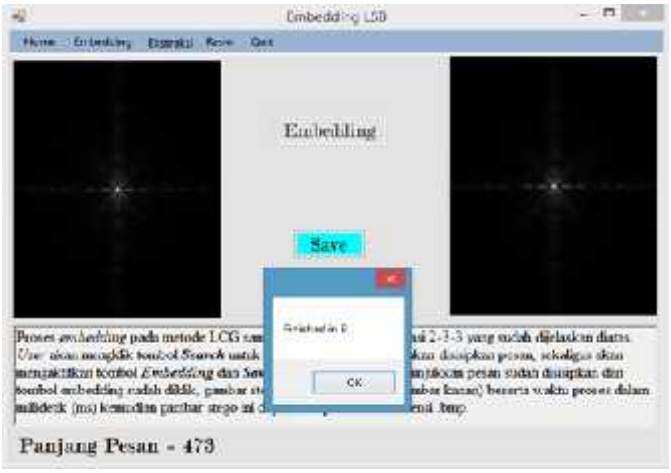
c) Ketahanan dari setiap metode dari proses pengolahan citra berupa peningkatan kontras dan penmbahan noise *salt* menggunakan aplikasi photoshop.

IV. HASIL PENGUJIAN

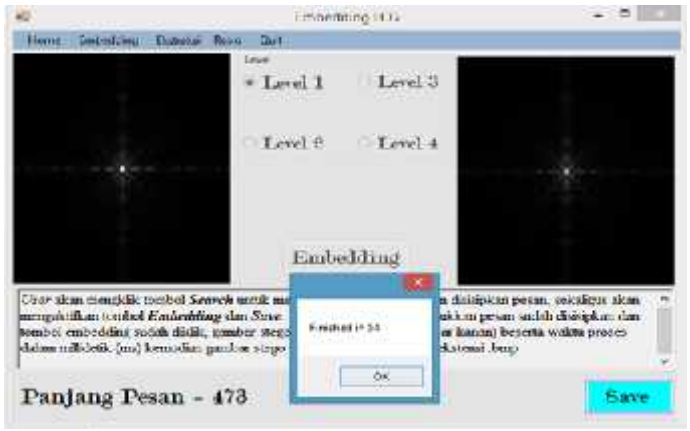
Implementasi dari kedua metode dalam penelitian ini menggunakan pemrograman c# dan akan menguji gambar sebanyak 20 buah terdiri dari 10 BMP, 5 JPG dan 5 PNG.

A. Hasil

Pada Gambar 4(a) dibawah memperlihatkan proses penyisipan pesan dengan formasi 2-3-3 dan Gambar 4(b) untuk metode LCG yang terdiri dari 4 level (level1, level2, level3 dan level4). Level ini merepresentasekan jumlah bit yang disisipkan.



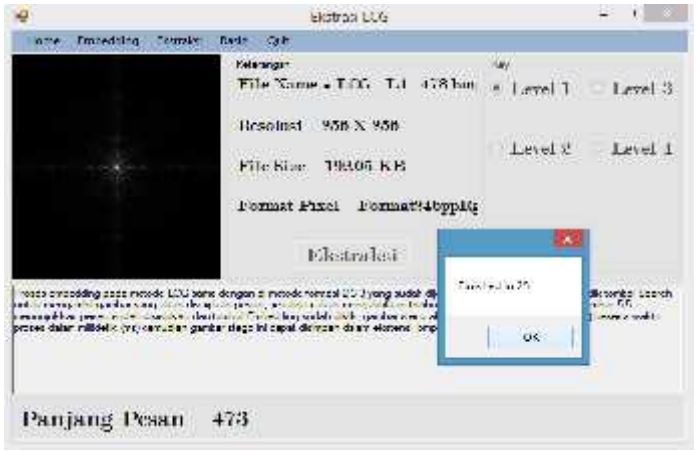
(a)



Gambar 4 (a) dan (b) Contoh Penyisipan Kedua Metode

Proses ekstraksi pesan khusus untuk LCG akan benar (kembali ke data awal) jika level yang dipilih saat ektraksi sama dengan level saat penyisipan. Gambar 5(a) memperlihatkan proses ektrasksi pesan dengan formasi 2-3-3 dan Gambar 5(b) untuk metode LCG, dimana levelnya (level1) sudah dipilih sebelum proses ekstraksi.

(a)



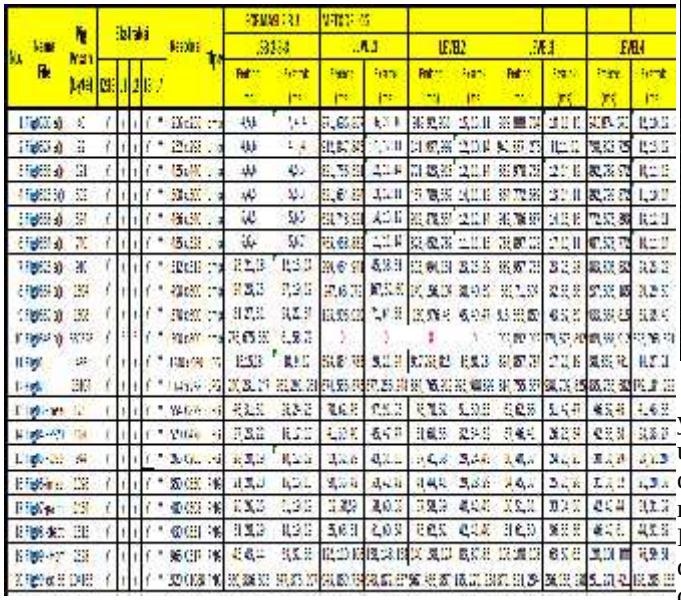
Gambar 5 (a) dan (b) Contoh Ektraksi Kedua Metode

B. Hasil Pengujian Efisiensi Waktu Terbaik

Proses penyisipan dan ekstraksi menghasilkan waktu yang berbeda untuk setiap prosesnya, sehingga untuk mendapatkan

hasil yang lebih baik maka setiap proses akan dilakukan sebanyak 3 kali. Tabel I dibawah ini adalah hasil penyisipan dan ekstraksi kedua metode dengan 20 dataset.

TABEL I. WAKTU PENYISIPAN DAN EKSTRAKSI



Keterangan.

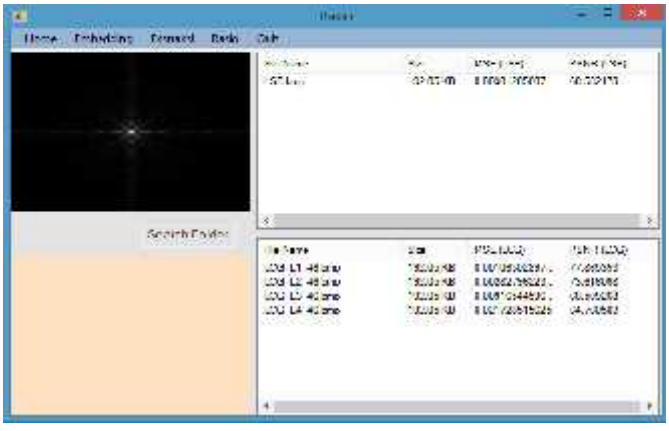
Y = Yes (Ekstraksi berhasil sesuai data awal).

F = Fail (Embedding dan Ekstraki gagal, program tidak melanjutkan proses)

Dari tabel 1 diatas dapat dilihat bahwa waktu penyisipan dan ekstraksi formasi 2-3-3 jauh lebih efisien dibandingkan dengan dengan metode LCG.

C. Hasil Pengujian Maksimum Penyisipan Pesan

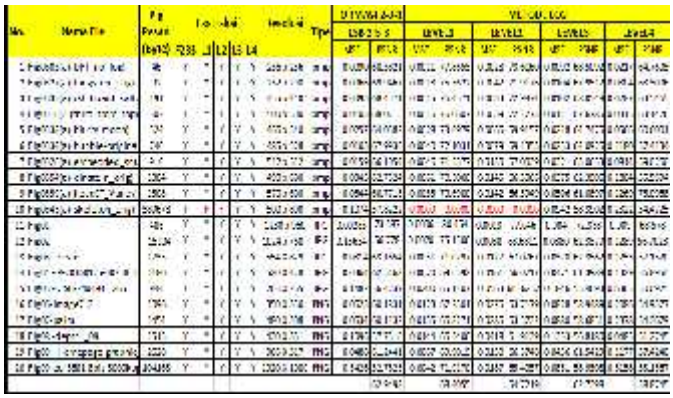
Pengujian ini untuk mendapatkan dampak kapasitas penyisipan dengan kualitas dari gambar stego yang akan diukur dengan MSE dan PSNR dengan citra asli, prsesnya terlihat pada gambar 6 dibawah ini.



Gambar 6. Form Pengjujian MSE dan PSNR Gambar Stego

Tabel 2 dibawah ini merupakan hasil dari keseluruhan dataset yang telah di uji, untuk menentukan kapasitas dari metode yang lebih baik untuk proses penyisipan ke dalam gambar.

TABEL II. HASIL PENGUJIAN KAPASITAS PENYISIPAN



Dari Tabel II diatas didapatkan untuk ketiga tipe gambar yaitu BMP, JPG dan BMP, dengan metode Formasi 2-3-3 untuk semua gambar proses penyisipan dan ekstraksi berhasil dilakukan dengan rata-rata PSNR = 62,9496; sedangkan untuk metode LCG Level 1 rata-rata PSNR = 68,4055; rata-rata PSNR Level 2 = 64,7219; rata-rata PSNR Level 3 = 62,7398; dan rata-rata PSNR Level 4 = 58,8745 tapi proses penyisipan dan ekstraksi tidak berhasil untuk semua data, terjadi kegagalan (F) pada gambar BMP karena tidak dapat diproses diakibatkan ketidaksesuaian antara jumlah pesan dengan aturan dalam pemrosesannya. Jika ditinjau dari segi keberhasilan penyisipan dan ekstraksi pada dataset yang digunakan, maka secara keseluruhan metode formasi 2-3-3 lebih baik dari segi jumlah penyisipan pesan. Jika dibandingkan dengan LCG, kualitas PSNR formasi 2-3-3 lebih baik daripada LCG Level 3 dan 4 tapi tidak untuk Level 1 dan 2.

D. Hasil Pengujian Ketahanan Data

Pengujian ini dilakukan untuk mengetahui ketangguhan (*robustness*) kedua metode untuk tetap menjaga pesan yang ada di dalam gambar stego meskipun sudah ditambahkan noise contrast dan salt dengan aplikasi photoshop. Tabel 3 dibawah ini merupakan hasil pengujian ketangguhan gambar stego terhadap noise.

TABEL III. HASIL PENGUJIAN KETAHANAN DATA

Dari Tabel III diatas, penambahan noise yang dilakukan dengan photoshop untuk peningkatan *constrast* dimulai dari 1, 5, 10 dan 11 peningkatan *contrast* tidak dilanjutkan lagi karena kedua metode sudah gagal melakukan ektraksi ke data awal. Dari hasil pengujian peningkatan contrast hanya metode LCG Level 2 yang dapat mengesktraksi data sesuai data awal dan lebih baik dibandingkan metode Formasi 2-3-3 tapi secara

keseluruhan Formasi 2-3-3 lebih baik dibanding LCG Level 1, 3 dan 4. Sedangkan untuk pemberian noise salt dengan penambahan noise sebesar 0.1 kedua metode dinyatakan gagal mengekstraksi data sesuai data awal, metode Formasi 2-3-3 mampu mengektraksi tapi tidak sesuai data awal sedangkan metode LCG gagal karena program tidak mampu menyelesaikan proses.

V. Kesimpulan Dan Saran

A. KESIMPULAN

Setelah melihat hasil dan kinerja kedua metode LSB berdasarkan waktu eksekusi, *imperceptiblity*, dan ketahanan data, kesimpulan yang didapatkan bahwa formasi 2-3-3 lebih efisien dibandingkan dengan LCG dan *Imperceptibility* formasi 2-3-3 lebih baik dibandingkan LCG Level 3 dan 4 tetapi tidak untuk Level 1 dan 2.

B. SARAN

Untuk meningkatkan hasil perbandingan dari kedua metode tersebut, beberapa kemungkinan perbaikan yang dapat dilakukan, seperti melakukan penyisipan dan ekstraksi kedua metode secara bersamaan (paralel) untuk mendapatkan waktu eksekusi yang lebih baik dan melakukan pengujian terhadap noise yang ditambahkan dengan aplikasi yang lebih baik misalnya matlab sehingga hasil pengujian ketangguhan kedua metode akan lebih tepat.

Referensi

[1] G. M. Kamau, S. Kimani and M. Mwangi, "An Enhanced Least Significant Bit Steganographic Method For Information Hiding," *Journal of Information Engineering and Aplications,* vol. 2, 2012.

[2] B. Dunbar, "A Detailed look at Steganographic Techniques and their use in an Open-Systems Environment," *SANS Institute,* 2002.

[3] G. M. Kamau, S. Kimani and W. Mwangi, "A general Purpose Image-Based Electors Smart Card Using an Enhanced Least Significant Bit Steganographic Method for Information Hiding : A case study of the Kenyan Electoral Process," *International Journal of Computer Science,* vol. 10, no. 2, 2013.

[4] H. B. Kekre, A. Athalawale and P. N. Halarnkar, "Increased Capacity of Information Hiding in LSB's Method for Text and Image," *World Academy of Science, Engineering and Technology,* vol. 02, 2008.

[5] S. Bajpai and D. K. Saxena, "Enhancing Embedding Capacity by Compartmentalizing Pixel Using LSB Techniques in Steganography," *An International Journal of Engineering Sciences,* vol. 10, 2014.

[6] H. Gupta, P. R. Kumar and D. S. Changlani, "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method," *International Journal of Emerging Technology and Advanced Engineering,* vol. 03, no. 06, 2013.

[7] I. Susanti, "Penerapan Steganografi Gambar Pada Least Significant Bit (LSB) Dengan Penggunaan PRNG (Pseudo Random Number Generator)," Departemen Ilmu Komputer Institut Pertanian Bogor, Bogor, 2007.

[8] M. Juneja and P. S. Sandhu, "Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images," *Indian Journal of Applied Research,* vol. 03, no. 05, 2013.

[9] I. A. Pardosi, S. Megawan, N. P. Sembiring and S. L. Purba, "Aplikasi Penyembunyian Pesan pada Citra dengan Metode AES Kriptografi dan Enhanced LSB Steganografi," *JSM STMIK Mikroskil,* vol. 16, 2015.

[10] G. R. Manjula and A. Danti, "A Novel Hash Based Least Significant Bit (2-3-3) Image Steganography In Spatial Domain," *International Journal of Security, Privacy and Trust Management (IJSPTM),* vol. 04, 2015.

[11] R. Munir, "Algoritma Enkripsi Citra Digital Berbasis Chaos dengan Penggabungan Teknik Permutasi dan Teknik Substitusi Menggunakan Arnold Cat Map dan Logistic Map," in *Prosiding Seminar Nasional Pendidikan Teknik Informatika*, 2012.

[12] B. Beighlie, "Imaging Essentials," *Research Imaging Solutions,* pp. 1-32, 2011.

[13] R. Munir, Pengolahan Citra Digital dengan Pendekatan Algoritmik, Bandung: Penerbit Informatika, 2004.

[14] D. Putra, Pengolahan Citra Digital Edisi 1, Yogyakarta: Penerbit Andy, 2010.

[15] T. Sutoyo, E. Mulyanto, V. Suhartono, O. Nurhayati and Wijanarto, Teori Pengolahan Citra Digital, Yogyakarta: Penerbit Andi, 2009.

[16] C. C. Li and B. Sun, "Using Linear Congruential Generators for Cryptographic Purposes".

[17] L. Y. Por, D. Beh, T. F. Ang and S. Y. Ong, "An Enhanced Mechanism for Image Steganography Using Sequential Color Cycle Algorithm," *The International Arab Journal of Information Technology,* vol. 10, 2013.