

Analisa Perbandingan LSB Steganografi Random Color pada Operasi Bilangan Bit XOR

Rohsih Hana Sundari^{*1}, Zamah Sari², Sofyan Arifianto³

^{1,2,3}Teknik Informatika/Universitas Muhammadiyah Malang

rhsundari@webmail.umm.ac.id^{*1}, zamahsari@umm.ac.id², sofyar_arifianto@umm.ac.id³

Abstrak

Steganografi merupakan teknik untuk menyembunyikan keberadaan data ke dalam data lain sehingga keberadaannya tidak diketahui. Sehingga selain pengirim dan penerima tidak ada yang mengetahui isi dari pesan tersebut dan tidak mudah untuk dicurigai [1]. Beberapa algoritma yang cocok dengan teknik steganography, salah satunya yaitu algoritma LSB (Least Significant Bit). Algoritma LSB juga dikembangkan di beberapa penelitian seperti LSB Shifting dan LSB Random Color. LSB Random color merupakan algoritma yang menyisipkan nilai bit ke dalam warna pixel (RGB). Penyisipan pesan ke dalam cover image dilakukan dengan cara perkalian XOR pixel pada bit terakhir warna green dan bit terakhir nilai ASCII dari password. Hasil XOR akan menentukan posisi bit secret image dalam menggantikan nilai bit terakhir pada cover image. Penelitian ini bertujuan untuk menganalisa dan membandingkan LSB steganografi random color pada operasi bilangan XOR dan tanpa operasi bilangan XOR. Proses menentukan posisi bit secret image pada LSB tanpa XOR akan dilakukan menggunakan nilai ASCII dari password. Pengujian diukur dengan menghitung nilai MSE dan PSNR pada file stegano image. Penelitian ini menggunakan 3 jenis file cover image berwarna dengan jumlah masing-masing file yang berbeda, dan menggunakan 1 file secret image yang sama. Hasil perbandingan membuktikan algoritma LSB random color tanpa XOR memiliki hasil yang lebih baik daripada random color tanpa XOR dengan nilai MSE sebesar 0,44375 dan PSNR sebesar 51,65945 dB, sedangkan random color dengan XOR bernilai MSE sebesar 0,47955 dan PSNR sebesar 51,32245 dB.

Kata Kunci: Steganografi, LSB Random Color, bit XOR, MSE, PSNR

Abstract

Steganography is a technique to hide the existence of data in other data so that its whereabouts are unknown. So besides the sender and recipient no one knows the contents of the message and is not easy to suspect [1]. Some algorithms that are suitable with steganography techniques, one of them is the LSB (Least Significant Bit) algorithm. The LSB algorithm was also developed in several studies such as LSB Shifting and LSB Random Color. LSB Random color is an algorithm that inserts a bit value into a pixel (RGB) color. The insertion of messages into the cover image is done by multiplying the XOR pixel on the last bit of green and the last bit of the ASCII value of the password. The XOR result will determine the position of the secret image bit in replacing the last bit value on the cover image. This study aims to analyze and compare LSB random color steganography in XOR number operations and without XOR number operations. The process of determining the position of secret bit images on LSB without XOR will be done using the ASCII value of the password. The test is measured by calculating the MSE and PSNR values in the stegano image file. This study uses 3 types of color cover image files with the number of each file that is different, and uses 1 same secret image file. The results of the comparison prove that the random color LSB algorithm without XOR has better results than the random color without XOR with an MSE value of 0,44375 and a PSNR of 51,48447 dB, whereas a random color with XOR of an MSE value of 0,47955 and a PSNR of 51,32245 dB.

Keywords: Steganography, LSB Random Color, MSE, PSNR

1. Pendahuluan

Perkembangan teknologi informasi yang sangat pesat menuntut semua aktivitas untuk menghasilkan sebuah informasi yang berguna bagi setiap orang, termasuk juga semua bidang kehidupan, hal ini ditandai dengan banyaknya pengguna komputer, baik dalam kepentingan perusahaan atau bisnis, pendidikan dan kesehatan, sampai kepada hal-hal yang bersifat hiburan

[2]. Era perkembangan teknologi informasi juga menuntut untuk keamanan sebuah informasi yang memang tidak banyak orang tahu, seperti rahasia perusahaan, rahasia pribadi, dan masih banyak rahasia-rahasia lainnya. Keberagaman data rahasia seperti text, image, dan audio menjadi salah satu alasan berkembangnya teknik keamanan informasi. Banyak metode tentang keamanan informasi yang dapat digunakan dalam menyimpan atau mengamankan sebuah informasi, salah satunya yaitu metode steganography [3].

Steganography merupakan metode untuk menyembunyikan keberadaan data ke dalam data lain sehingga keberadaannya tidak diketahui [4]. Pengirim dan penerima yang mengetahui isi dari pesan tersebut, tidak semua orang dan tidak mudah untuk dicurigai. Steganography tidak jauh beda dengan kriptografi, hanya saja nilai kecurigaan kriptografi lebih mudah dikenali dari pada steganography [5]. Teknik yang digunakan kriptografi yaitu mengubah pesan asli menjadi pesan yang tidak bisa dibaca selain pengirim dan penerima, sedangkan teknik steganografi yaitu menyembunyikan pesan ke dalam file.

Ada banyak algoritma yang sesuai dengan metode steganografi, dan salah satu algoritma yang populer dan sering digunakan untuk menyembunyikan sebuah gambar atau data yaitu Algoritma Least Significant Bit (LSB) [6]. Least Significant Bit (LSB) merupakan teknik pendekatan yang sederhana dimana nilai bit pesan atau bisa disebut dengan nilai bit secret disisipkan ke dalam nilai bit terkecil pada citra yang akan disisipi [7]. Teknik bit paling sedikit atau paling belakang dari cover image akan digunakan untuk menyembunyikan pesan rahasia dengan cara mengganti nilai bit tersebut dengan nilai bit file yang akan disembunyikan. Jenis pesan yang dikirim pun beragam dapat berupa data text, image ataupun audio.

Penelitian yang pernah dilakukan sebelumnya seperti yang dilakukan Kamaldeep joshii dan Rajkumar Yadav jurnal yang berjudul "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication" [8]. Penelitian ini bertujuan untuk mencoba mengkolaborasikan dua metode yaitu kriptografi dan steganografi. Jurnal ini menggunakan dua algoritma yaitu Algoritma Vernam Cipher dimana algoritma ini untuk mengenkripsi pesan yang akan dimasukkan dan disembunyikan, sedangkan algoritma kedua yaitu algoritma LSB Shifting (LSB-S) dimana algoritma ini untuk menyisipkan nilai bit pesan ke dalam nilai bit pixel gambar. Pengujian dari gambar hasil kolaborasi kedua metode tersebut diuji menggunakan parameter berdasarkan nilai hasil PSNR dan MSE.

Penelitian lain seperti yang dilakukan Xinyi Zhou, Wei Gong, Weslong Fu, dan Lian Jingjin mengeluarkan jurnal yang berjudul "An Improved Method for LSB Based Color Image Steganography Combined with Cryptography" [9]. Penelitian ini bertujuan menyembunyikan sebuah pesan ke dalam sebuah gambar, dengan mengombinasikan metode kriptografi. Algoritma yang digunakan pada jurnal tersebut yaitu Algoritma RSA, dimana algoritma ini mengenkripsi sebuah pesan rahasia, lalu algoritma selanjutnya yaitu algoritma LSB Random Color, digunakan untuk menyisipkan nilai bit dari pesan yang akan disisipkan ke dalam cover image. Pengujiannya menggunakan parameter berdasarkan nilai hasil PSNR dan MSE.

Algoritma *LSB Random Color* merupakan algoritma yang menyisipkan nilai bit ke dalam warna *pixel (RGB)* [9]. Warna dari *pixel* tersebut yaitu Red, Green, Blue yang berjumlah 24 bit. Warna *pixel* tersebut masing-masing memiliki 8 bit tiap warna. Penyisipan pesan ke dalam *cover image* dilakukan dengan cara perkalian *XOR* *pixel* pada bit terakhir warna green dan bit terakhir nilai ASCII dari password. Hasil *XOR* akan menentukan posisi bit secret image dalam menggantikan nilai bit terakhir pada *cover image*.

Peak Signal-to-Noise Ratio (PSNR) merupakan rumus untuk mengukur nilai perbandingan antara nilai maksimum gambar dengan nilai *Mean Squared Error (MSE)*. *MSE* merupakan rumus untuk mengukur nilai rata-rata error antara gambar asli (*cover image*) dengan gambar yang mengandung pesan (*stegano image*) [8]. Gambar yang dapat dilihat oleh mata manusia umumnya sebesar 28 dB. Kualitas gambar yang dihasilkan semakin baik jika semakin besar nilai PSNR, sedangkan nilai MSE semakin kecil, maka semakin sedikit perubahan yang dihasilkan [9].

Berdasarkan pembuktian-pembuktian yang telah dijelaskan, penelitian tugas akhir ini akan mencoba membandingkan proses algoritma *LSB Random Color*. Proses yang dibandingkan yaitu antara *LSB Random Color* dengan operasi bilangan *bit XOR* dan *LSB Random Color* tanpa operasi bilangan *bit XOR*. Perbandingan pengujian ini menggunakan parameter dari nilai hasil PSNR dan MSE. Proses pertama *LSB Random Color* dengan operasi bilangan *bit XOR* akan mengacu pada penelitian yang dilakukan oleh Xinyi Zhou,dkk sedangkan proses kedua nya dilakukan sama seperti proses pertama hanya tanpa menggunakan operasi bilangan *bit XOR*.

2. LSB Random Color pada operasi bilangan XOR

Algoritma LSB random color merupakan salah satu algoritma LSB yang sudah dikembangkan lebih baik daripada algoritma sebelumnya. Algoritma LSB Random Color dimana proses nya yaitu dengan menyisipkan nilai bit ke dalam warna pixel (RGB), warna pixel yang dimaksud yaitu Red, Green, Blue[9]. Cara menyisipkan pesan ke dalam cover image yaitu dengan proses XOR pixel warna hijau (Green) dengan nilai ASCII dari password, kemudian hasil XOR akan menentukan posisi bit secret image dalam menggantikan nilai bit terakhir pada cover image.

Algoritma LSB Random Color tanpa bit XOR merupakan salah satu usulan penelitian yang di usulkan oleh dosen UMM bernama Zamah Sari, ST. MT. Algoritma ini akan memanfaatkan binary password ASCII untuk tugas penyisipan file secret image, jika sebelumnya algoritma Random Color hanya menyisipkan di nilai Red jika hasil bit XOR bernilai 1 dan Blue jika bernilai 0, maka algoritma ini akan memanfaatkan semua nilai dalam pixel Red, Green dan Blue. Algoritma LSB Random Color tanpa bit XOR ini menyisipkan pesan secret (rahasia) ke dalam cover image dengan cara mengganti 1 bit terakhir dari nilai Red, Green, Blue pada pixel cover image. Cara menyisipkan pesan ke dalam cover image yaitu dengan proses binary bit password terakhir yang akan menentukan posisi bit file secret yang akan disisipkan, jika binary bit password bernilai 1 maka bit file secret disisipkan ke bit terakhir menggantikan posisi terakhir bit pixel cover image, namun jika bernilai 0 maka bit file secret tidak disisipkan dan beralih ke pixel cover image selanjutnya.

3. Peak Signal-to-Noise Ratio (PSNR) dan Mean Squared Error (MSE)

Peak Signal-to-Noise Ratio (PSNR) merupakan rumus untuk mengukur nilai perbandingan antara nilai maksimum gambar dengan nilai *Mean Squared Error* (MSE). Sedangkan MSE merupakan rumus untuk mengukur nilai rata-rata *error* antara gambar asli (*cover image*) dengan gambar yang mengandung pesan (*stegano image*) [8].

Umumnya gambar dapat dilihat dengan mata manusia jika nilai PSNRnya lebih tinggi dari 28 dB, semakin besar nilai PSNR maka semakin baik kualitas gambar yang dihasilkan. Sedangkan semakin kecil nilai MSE maka semakin sedikit perubahan yang dihasilkan [9]. Rumus MSE dan PSNR bisa dilihat di Persamaan 1.

$$MSE = \frac{1}{N} \sum_{i=1}^n (C_i - S_i) \quad (1)$$

$$PSNR = 10 \log \left(\frac{255^2}{MSE} \right)$$

C_i merupakan nilai *pixel* dari citra *cover image*, kemudia S_i merupakan nilai *pixel* dari *citra secret image*, kemudian N merupakan jumlah dari perkalian panjang dan lebar dari citra *stegano image* (dalam *pixel*)[9]. Setelah mendapatkan nilai *error* pada proses *steganography*, maka bisa dihitung nilai PSNR dari *file stegano image* [9].

4. Data Site

Pengujian yang dilakukan untuk mencoba algoritma LSB Random Color tanpa bit XOR dan membandingkannya dengan algoritma LSB Random Color dengan bit XOR yang dilakukan oleh Bayu Yuda Purnomo, maka dilakukan pengujian pada setiap hasil penyisipan yaitu file *steganography*. File yang digunakan untuk cover image dan secret image yaitu berformat .jpg dan akan menghasilkan file *stegano image* dengan format .png. Berikut adalah Tabel 1 detail *file cover image* dan *file secret image* untuk penelitian ini, dan bisa dilihat di Gambar 1 dan Gambar 2.

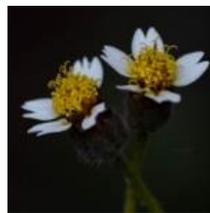
Tabel 1. Detail File Cover Image dan Secret Image

Nama File Stegano	Perhitungan MSE dan PSNR penyisipan file secret 200x200 (32 kb)	
	LSB Random Color dengan bit XOR	LSB Random Color tanpa bit XOR

Stegano 1 500x500 pixel (159 kb)
Stegano 2 700x700 pixel (307 kb)
Stegano 3 900x900 pixel (480kb)



Gambar 1. File Cover Image



Gambar 2. File Secret Image

5. Hasil dan Pembahasan

Pengujian perbandingan ini dilakukan pada dua algoritma yaitu algoritma Random Color dengan bit XOR dan Random Color tanpa bit XOR. Pengujian ini dilakukan dalam satu kali pengujian dengan menggunakan 3 buah file cover image yang memiliki ukuran pixel berbeda, kemudian disisipkan dengan 1 buah file secret image yang memiliki ukuran file sama. File cover image yang dipakai berupa gambar berwarna berukuran 500x500 pixel dengan size file 159 kb, 700x700 pixel dengan size file 307 kb, 900x900 pixel dengan size 480 kb, dan secret image yang memiliki size 32 kb. Hasil penyisipan dapat dilihat pada Gambar 3 dan Gambar 4. Hasil pengujian perbandingan berdasarkan nilai MSE dan PSNR pada kedua algoritma dapat dilihat pada Tabel 2 dan Tabel 3.

Tabel 2. Tabel Perhitungan MSE pada File Stegano

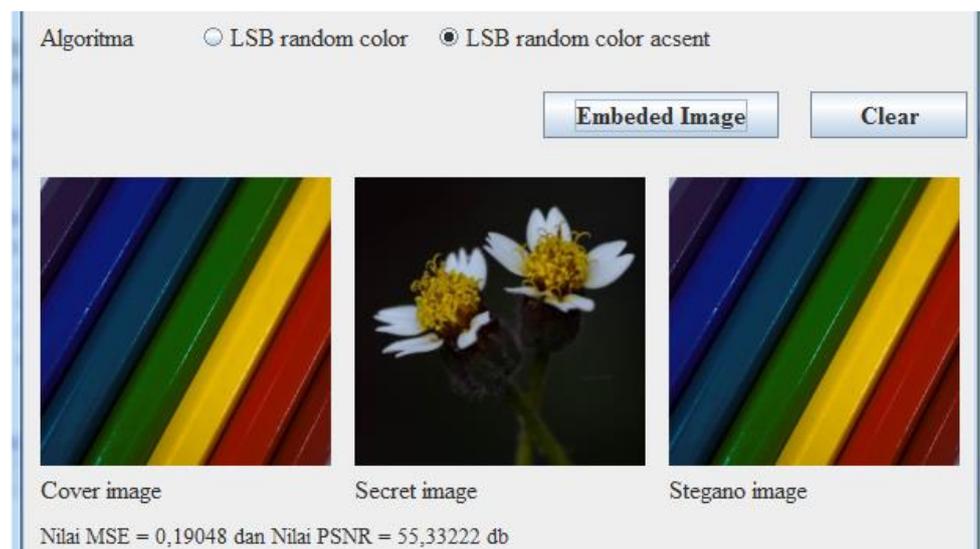
Nama File Stegano	Perhitungan MSE penyisipan file secret 200x200 (32 kb)	
	LSB Random Color dengan bit XOR	LSB Random Color tanpa bit XOR
Stegano 1 500x500 pixel (159 kb)	0,46417	0,15660
Stegano 2 700x700 pixel (307 kb)	0,27128	0,19694
Stegano 3 900x900 pixel (480kb)	0,15660	0,22312

Tabel 3. Tabel perhitungan PSNR pada File Stegano
Perhitungan PSNR penyisipan file secret 200x200 (32 kb)

Nama File Stegano	LSB Random Color dengan bit XOR	LSB Random Color tanpa bit XOR
Stegano 1 500x500 pixel (159 kb)	51,46405 db	55,33222 db
Stegano 2 700x700 pixel (307 kb)	53,79660 db	55,18745 db
Stegano 3 900x900 pixel (480kb)	56,18292 db	54,64540 db



Gambar 3. Hasil Proses Penyisipan Pada Cover Dari Algoritma LSB Random Color

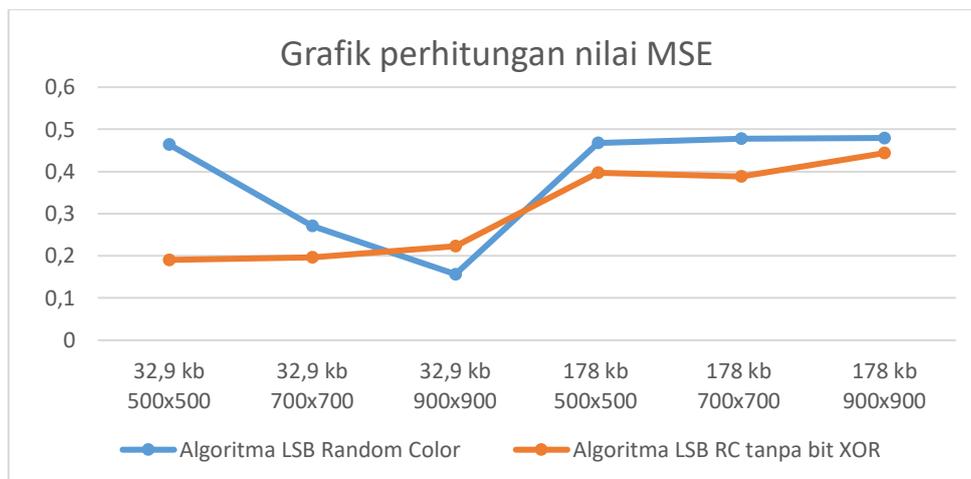


Gambar 4. Hasil Proses Penyisipan Pada Cover 500x500 Pixel Dari Algoritma LSB Random Color Tanpa Bit XOR

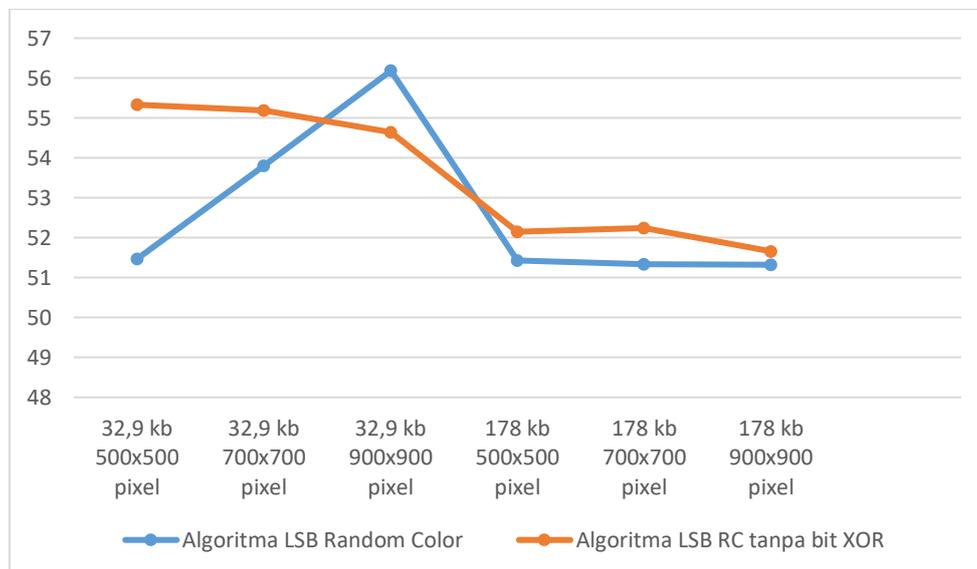
Hasil pengujian pada Tabel 2 dan Tabel 3 menyimpulkan bahwa perhitungan MSE dan PSNR untuk penyisipan file secret image ke dalam file cover image dengan menggunakan algoritma *LSB Random Color tanpa bit XOR* terlihat lebih baik dari pada *LSB Random Color dengan bit XOR* yaitu pada ukuran cover image 500x500 pixel dan juga 700x700 pixel.

5.1 Analisa Perbandingan Nilai MSE dan PSNR

Analisa ini dilakukan untuk membuktikan ketahanan kedua algoritma Random Color dalam proses penyisipan, baik dari cover image ataupun secret image. Analisa yang dilakukan yaitu perbandingan nilai MSE dan PSNR pada proses penyisipan file secret image dengan menambah ukuran file. Ukuran file yang akan disisipkan ke dalam file cover image di setiap algoritmanya masing-masing yaitu file berukuran 32 kb dan 178 kb. Hasil grafik dari nilai MSE dan PSNR pada perbandingan *Algoritma LSB Random Color dengan bit XOR* dan *Algoritma LSB Random Color tanpa bit XOR* ditampilkan pada Gambar 5 dan Gambar 6.



Gambar 5. Grafik Perbandingan Nilai MSE Dari Algoritma LSB Random Color Dengan Bit XOR dan LSB Random Color Tanpa Bit XOR



Gambar 6. Grafik Perbandingan Nilai PSNR Dari Algoritma LSB Random Color Dengan Bit XOR dan LSB Random Color Tanpa Bit XOR

Hasil analisa perbandingan proses penyisipan menggunakan algoritma *LSB Random Color* dengan bit XOR dan algoritma *LSB Random Color tanpa bit XOR* ditentukan dari nilai MSE dan PSNR. Grafik pada gambar 5 menjelaskan nilai error (MSE) dari algoritma *LSB Random color tanpa bit XOR* memiliki nilai error lebih sedikit dari pada algoritma *LSB Random Color dengan bit*

XOR, jika disisipkan file *secret* lebih besar pada semua ukuran *cover image*. Hasil analisa untuk nilai PSNR pada gambar 6 menjelaskan bahwa algoritma *LSB Random Color dengan bit XOR* lebih tinggi dari pada algoritma *Random Color tanpa bit XOR*, jika disisipkan file yang lebih kecil pada ukuran *cover image* yang lebih besar.

6. Kesimpulan dan Saran

Kesimpulan yang dapat diambil dari tahapan penelitian membuktikan bahwa *Algoritma Random Color tanpa bit XOR* yang diusulkan oleh dosen UMM, Zamah sari ST. MT., memberikan hasil yang lebih baik dari pada algoritma *Random Color dengan bit XOR* yang diteliti oleh Xinyi Zhou dkk. Hal ini memunculkan pengembangan algoritma baru dari *Algoritma Random Color* itu sendiri yaitu *Algoritma Binary Key* yang diciptakan oleh Zamah Sari ST. MT. dosen UMM. Algoritma ini memanfaatkan *bit binary password* untuk proses penyisipan file *secret image* pada file *cover image* sehingga *LSB green* dapat dimanfaatkan secara maksimal untuk proses penyisipan.

Saran digunakan agar penelitian dapat dikembangkan dan lebih bermanfaat oleh pembaca. Berikut adalah saran yang bisa disampaikan agar dapat dikembangkan penelitian:

1. Saran untuk penelitian selanjutnya yaitu menyempurnakan kembali proses decode dari *Algoritma Random Color* agar dapat dikembangkan dan digunakan dalam proses pengiriman file rahasia, begitu juga dengan *Algoritma Binary Key* yang memiliki keunggulan lebih besar dibandingkan *Algoritma Random Color*.
2. *Algoritma LSB Binary Key* dapat diteliti dan dibandingkan kembali dengan algoritma LSB lainnya agar dapat mengetahui proses penyisipan *Algoritma Binary Key* secara maksimal.
3. *Algoritma Binary Key* dapat di coba untuk implementasi proses penyisipan file secret image pada cover image dengan nilai warna pixel CMYK (Cyan, Magenta, Yellow, Black).

Daftar Notasi

- MSE : Nilai *Mean Square Error* citra *steganography*
 C_i : Nilai *pixel* dari citra *cover image*
 S_i : Nilai *pixel* dari citra *secret image*
N : Jumlah dari perkalian panjang dan lebar dari citra *stegano image* (dalam *pixel*)
PSNR : Nilai *Peak Signal-to-Noise Ratio* citra pada *stegano image*

Referensi

- [1] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, 2010.
- [2] X. Dong, Q. Liu, and D. Yin, "Business performance, business strategy, and information system strategic alignment: An empirical study on Chinese firms," *Tsinghua Sci. Technol.*, vol. 13, no. 3, pp. 348–354, Jun. 2008.
- [3] M. A. Alia, K. A. Maria, M. A. Alsarayreh, E. A. Maria, and S. Almanasra, "An Improved Video Steganography: Using Random Key-Dependent," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 234–237.
- [4] S. Tan and B. Li, "Targeted steganalysis of edge adaptive image steganography based on LSB matching revisited using B-spline fitting," *IEEE Signal Process. Lett.*, vol. 19, no. 6, pp. 336–339, 2012.
- [5] N. Hopper, L. von Ahn, and J. Langford, "Provably Secure Steganography," *IEEE Trans. Comput.*, vol. 58, no. 5, pp. 662–676, May 2009.
- [6] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Process.*, vol. 90, no. 3, pp. 727–752, 2010.
- [7] K. Thangadurai and G. S. Devi, "An analysis of LSB based image steganography techniques," in *Computer Communication and Informatics (ICCCI), 2014 International Conference on*, 2014, pp. 1–4.
- [8] K. Joshi and R. Yadav, "A new LSB-S image steganography method blend with Cryptography for secret communication," in *Image Information Processing (ICIIP), 2015 Third International Conference on*, 2015, pp. 86–90.
- [9] X. Zhou, W. Gong, W. Fu, and L. Jin, "An improved method for LSB based color image steganography combined with cryptography," in *Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on*, 2016, pp. 1–4.

