REPOSITOR, Vol. 3, No. 2, Februari 2021, Pp. 233-242
ISSN : 2714-7975
E-ISSN : 2716-1382

Analisa Perbandingan LSB Steganografi Antara Shifting dan Random Color

Bayu Yudha Purnomo[*1], Agus Eko Minarno[2], Zamah Sari[3]
[1,2,3]Universitas Muhammadiyah Malang
bayu.yudha.purnomo@gmail.com[*1], agoes.minarno@gmail.com[2], zamahsari@umm.ac.id[3]

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. Beberapa algoritma yang cocok dengan teknik steganography, salah satunya yaitu algoritma LSB (Least Significant Bit). Algoritma LSB sendiri sudah dikembangkan oleh beberapa penelitian sebelumnya, yaitu menjadi algoritma LSB Random Color dan algoritma LSB Shifting. Dua algoritma tersebut merupakan algoritma yang terbaru dari algoritma LSB. Beberapa penelitian sebelumnya melakukan pengujian algoritma LSB random color dan algoritma LSB shifting dengan menggunakan data yang berbeda, dan hasil penelitian sebelumnya tidak melakukan perbandingan mana yang lebih baik dari dua algoritma tersebut. Dalam penelitian ini penulis membuat penelitian dengan judul analisa perbandingan LSB steganografi antara shifting dan random color. Pengujian diukur dengan menghitung nilai MSE dan PSNR pada file stegano image. Penelitian ini menggunakan 2 jenis file cover image yaitu berwarna dan hitam putih dengan jumlah masing-masing 3 file yang berbeda, dan menggunakan 1 file secret image yang sama. Sehingga diperoleh hasil perbandingan bahwasannya algoritma LSB random color memiliki performa lebih baik, meskipun mengunakan jenis file berwarna atau hitam putih.

Kata Kunci: *Steganografi, Algoritma LSB Random Color, Algoritma LSB Shifting, MSE, PSNR*

Abstract

Steganography is a technique to hide the existence of data in to another data so that it will be considered as unknown. Moreover, the sender and the recipient cannot be identified as well as the contents of the message which is not easy to suspect. There are some algorithms that are suitable with steganography techniques, one of them is LSB (Least Significant Bit) algorithm. LSB algorithm has been developed by several previous studies, namely LSB Random Color algorithm and LSB Shifting algorithm. These two algorithms are the newest kind of LSB. In addition, several previous studies tested them by using different data but they did not make a comparison towards them. Thus, the writers made this study under the title Comparative Analysis of LSB Steganography between Shifting and Random Color. The test was measured by calculating the MSE and PSNR values in the stegano image file. This study used 2 types of cover image files, such as color and black-white in which each of them had 3 different files, and used 1 same secret image file. Therefore, the comparison results show that LSB random color algorithm has better performance than the shifting one, either by using a color file type or black-white.

Keywords: *Steganography, LSB Random Color Algorithm, LSB Shifting Algorithm, MSE, PSNR*

1. Pendahuluan

Perkembangan teknologi informasi yang sangat pesat menuntut semua aktifitas untuk menghasilkan sebuah informasi yang berguna bagi setiap orang[1], termasuk juga semua bidang kehidupan, hal ini ditandai dengan banyaknya pengguna komputer, baik dalam kepentingan perusahaan atau pribadi[2]. Bukan hanya itu saja, dari era perkembangan teknologi informasi juga menuntut untuk keamanan sebuah informasi[3]. Banyak metode tentang keamanan informasi yang dapat digunakan dalam mengamankan sebuah informasi[4], salah satu metode yang digunakan untuk menyembunyikan informasi yaitu *steganography*[5].

Kata *steganography* berasal dari istilah bahasa Yunani, yaitu *steganos* yang berarti tertutup atau rahasia dan *graphy* yang berarti tulisan [6]. *Steganography* merupakan teknik untuk menyembunyikan keberadaan data ke dalam data lain sehingga keberadaannya tidak

diketahui[7]. *Steganography* tidak jauh beda dengan *cryptography*[8], hanya saja nilai kecurigaan *cryptography* lebih mudah dikenali daripada *steganography*[9], karena teknik yang digunakan *cryptography* yaitu mengubah pesan asli menjadi pesan yang tidak bisa dibaca selain pengirim dan penerima[10], sedangkan teknik yang digunakan *steganography* yaitu menyembunyikan pesan ke dalam file[11].

Ada banyak algoritma yang cocok untuk teknik *steganography*[12], antara lain algoritma untuk *audio steganography*[13], algoritma untuk *video steganography*[14], algporitma *text steganography*[15]*,* dan salah satu algoritma yang sering digunakan untuk menyembunyikan sebuah data menggunakan media gambar yaitu *Algortima Least Significant Bit* (LSB)[16]. *Least Significant Bit* (LSB) merupakan teknik pendekatan yang sederhana dimana nilai bit pesan rahasia disisipkan ke dalam nilai bit terkecil pada citra yang akan disisipi[17]. Dalam teknik ini memanfaatkan bit paling belakang dari *cover image* untuk menyisipkan pesan rahasia[18].

Beberapa penelitian yang sudah dilakukan sebelumnya seperti yang dilakukan oleh Nadeem Akhtar, Pragati Johri, Shahbaaz Khan jurnal yang berjudul "*Enhancing the Security and Quality of LSB based Image Steganography*"[19]. Penelitian tersebut bertujuan untuk meningkatkan keamanan dan kualitas gambar dengan menggunakan teknik *steganography*. Salah satu algoritma yang diterapkan dalam jurnal ini yaitu menggunakan algortima *Least Significant Bit* (LSB). Dan dalam penelitian ini juga menggunakan algoritma RC4 dimana untuk mengacak bit gambar pesan ke dalam *pixel* gambar sampul dengan begitu menggunakan algoritma RC4 dapat meningkatkan ketahanan *steganography*. Metode yang diusulkan medapatkan hasil yang baik menggunakan teknik Least Significant Bit dengan keamanan yang baik dan tidak merusak gambar[19].

Kamaldeep Joshii dan Rajkumar Yadav jurnal berjudul "*A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication*"[20]. Penelitian ini bertujuan untuk mencoba mengkolaborasikan dua metode yaitu *cryptography* dan *steganography*. Kemudian dalam jurnal ini menggunakan dua algoritma yaitu yang pertama algoritma *Vernam Cipher* dimana digunakan untuk mengenkripsi pesan yang akan dimasukkan disembunyikan. Algoritma yang kedua yaitu algoritma *Least Significant Bit Shifting* (LSB-S) dimana digunakan untuk menyisipkan nilai bit pesan ke dalam nilai bit *pixel* gambar. Hasil dari kolaborasi antara *cryptography* dan *steganography* dengan menggunakan parameter berbeda seperti PSNR dan MSE mendapatkan hasil yang bagus[20].

Xinyi Zhou, Wei Gong, Weslong Fu, dan LianJing Jin jurnal yang berjudul "*An Improved Method for LSB Based Color Image Steganography Combined with Cryptography*"[21]. Penelitian ini bertujuan tidak jauh beda dengan penelitian yang ada di atas, yaitu menyembunyikan sebuah pesan ke dalam sebuah gambar, dengan mengkombinasikan metode *cryptography*. Salah satu algoritma yang digunakan pada jurnal tersebut yaitu algoritma RSA, dimana digunakan untuk mengenkripsi sebuah pesan rahasia, kemudian algoritma selanjutnya yaitu algoritma *Least Significant Bit Random Color*, dimana digunakan untuk menyisipkan nilai bit dari pesan yang akan disisipkan ke dalam *cover image*. Pengujiannya menggunakan parameter berdasarkan nilai hasil PSNR dan MSE. Menggunakan kolaborasi antara *cryptography* dengan penyembunyian informasi mendapatkan hasil yang bagus, karna disatu sisi keloborsi tersebut tidak merusak karakteristik *file cover image,* dan disisi lain kolaborasi tersebut tidak mepermudah user lain untuk mengetehu{Citation}i informasi yang disembunyikan[21].

Beberapa penelitian sebelumnya melakukan pengujian algoritma *LSB random color* dan algoritma *LSB shifting* dengan menggunakan data yang berbeda, dan hasil penenlitian sebelumnya tidak melakukan perbandingan mana yang lebih baik dari dua algoritma tersebut dengan menggunakan perhitungan MSE dan PSNR pada setiap *file stegano image*. Penulis mengambil judul analisa perbandingan LSB steganografi antara shifting dan random color. Dari penelitian sebelumnya kedua algoritma memiliki kelebihan dalam teknik penyisipan suatu pesan. Pada penelitian kali ini, peneliti melakukan perbandingan antara algoritma *LSB random color* dengan algoritma *LSB shifting* dengan menggunakan 2 jenis *file cover image* yaitu berwarna dan hitam putih dengan jumlah masing-masing 3 *file* yang berbeda, dan menggunakan 1 *file secret image* yang sama dan mambandingkannya menggunakan perhitungan nilai MSE dan PSNR pada setiap *file stegano image*.

2. LSB Random Color dan LSB Shifting

Algoritma *LSB random color* merupakan salah satu algoritma *Least Significant Bit* yang sudah dikembangkan lebih baik daripada algoritma sebelumnya. Algoritma *LSB random color*

digunakan untuk menyisipkan nilai bit ke dalam warna *pixel* (RGB), warna *pixel* yang dimaksud yaitu *red*, *green*, *blue*[21]. Cara menyisipkan pesan ke dalam *cover image* yaitu dengan proses XOR *pixel* warna *green* dengan nila ASCI dari *password*, kemudian hasil XOR akan menentukan posisi bit *secret image* dalam menggantikan nilai bit terakhir pada *cover image*.

Algoritma *LSB shifting* (LSB-S) merupakan salah satu algoritma *Least Significant Bit* yang sudah dikembang lebih baik daripada algoritma sebelumnya. Algoritma *LSB shifting* digunakan untuk menyisipkan pesan *secret* (rahasia) ke dalam *cover image* dengan cara mengambil 4 bit terakhir pada *pixel cover image* dan bit pertama dari bit terakhir pada *pixel cover image* dipindah kebelakang[20]. Cara menyisipkan pesan ke dalam *cover image* yaitu dengan proses XOR bit terakhir *pixel cover image* dengan bit dari nilai pesan yang akan disisipkan, kemudian hasil dari XOR akan menggantikan posisi terakhir bit *pixel cover image*.

3. Peak Signal-to-Noise Ratio(PSNR)

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*)[20].

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[21]. Rumus MSE dan PSNR bisa dilihat di Persamaan 1.

$$MSE = \frac{1}{N}\sum_{i=1}^{n}(C_i - S_i)$$
$$PSNR = 10log\left(\frac{255^2}{MSE}\right) \quad (1)$$

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*)[21]. Setelah mendapatkan nilai *error* pada proses *steganography*, maka bisa dihitung niilai PSNR dari *file stegano image*[21].

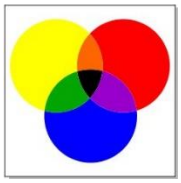
4. Data site

Perancangan sistem pada penelitian ini menggunakan Algoritma *LSB random color* dan LSB shifting. Kedua algoritma tersebut akan diuji bedasarkan hasil nilai perhitungan MSE dan PSNR, kemudian akan dibandingkan mana yang lebih baik dari kedua algoritma tersebut. Penelitian ini menggunakna media berupa gambar berformat JPG, dan media tersebut adalah sebuah *file cover image* dan *file secret image* untuk mengimplementasikan teknik *steganography* menggunakan algoritma LSB *random color* dan algoritma *LSB shifting*, kemudian hasil dari proses *steganography* berupan gambar berformat PNG. Tabel 1 berikut adalah detail *file cover image* dan *file secret image* untuk penelitian ini, dan bisa dilaihat di Gambar 1 dan Gambar 2.

Tabel 1. Detail file cover image dan secret image

Algoritma	Berwarna		Hitam Putih	
	Cover image (pixel)	Secret image (pixel)	Cover image (pixel)	Secret image (pixel)
LSB Random Color	500x500	10x10 (11 kb)	500x500	10x10 (11 kb)
	700x700	10x10 (11 kb)	700x700	10x10 (11 kb)
	900x900	10x10 (11 kb)	900x900	10x10 (11 kb)
LSB Shifting	500x500	10x10 (11 kb)	500x500	10x10 (11 kb)
	700x700	10x10 (11 kb)	700x700	10x10 (11 kb)
	900x900	10x10 (11 kb)	900x900	10x10 (11 kb)

Gambar 1. File cover image



Gambar 2. File secret image

Teknik penyisipan menggunakan algoritma *LSB random color* dengan memanfaatkan warna *red*, *green*, *blue* pada *pixel cover image*, dan proses penyisipan *file secret image* ditentukan dari perkalian XOR *LSB green* dengan *LSB password* yang sudah dirubah dalam bentuk *biner*, jika hasil perkalian XOR menghasilkan bit 1 maka bit pertama dari *secret image* akan menggantikan posisi nilai *biner LSB red* pada *cover image*, akan tetapi jika perkalian menghasilkan bit 0 maka nilai bit pertama dari *secret image* akan menggantikan posisi nilai *biner LSB blue* pada *cover image*. Proses penyisipan akan berhentin jika nilai *biner secret image* sudah tersisipkan.

Sedangkan teknik penyisipan menggunakan algoritma *LSB shifting* hanya memanfaatkan *pixel* warna *blue* pada cover image. Sebelum proses penyisipan *file secret image*, akan dilakukan eksekusi pada *file cover image* terlebih dulu yaitu dengan mengambil 4 bit terakhir dari *pixel* warna *blue*, dan 4 bit tersebut akan melakukan pergeseran posisi, bit pertama berpindah kebagian paling belakang dari 3 bit sesudahnya. Penyisipan *file secret image* ditentukan dari perkalian XOR bit *secret image* dengan LSB 4 bit terakhir yang sudah dirubah posisinya, hingga bit *secret image* habis dikalikan semuanya. Proses perkalian menghasilkan bit yang siap menggantikan posisi bit terakhir pada bit *pixe*l warna *blue cover image*.

5. Hasil dan pembahasan

Setelah proses implementasi sistem maka dilakukan pengujian di setiap hasil penyisipan yaitu *file stegano image* untuk mengetahui mana yang lebih baik antara algoritma *LSB random color* dan algoritma LSB *shifting*. Pengujian dilakukan dengan tiga tahapan. Tahapan pertama menentukan nilai *error* (MSE) di setiap *file stegano image*. Tahapan kedua jika nilai MSE sudah ditemukan, maka akan dilakukan pengujian tampilan di setiap *file stegano image*, yaitu dengan cara menghitung nilai PSNR. Tahapan ketiga menentukan seberapa besar *file secret image* yang dapat disisipkan kedalam *file cover image*.

Setelah melakukan semua skenario pengujian akan didapatkan data berupa *stegano image* yang memilik nilai *error* (MSE) dan PSNR yang dapat dianalisa. Analisis dilakukan untuk mengetahui siapa yang lebih baik antara algoritma *LSB random color* dan algoritma *LSB shifting* pada implementasi teknik *steganography*. Skenario pengujian menggunakan beberapa *file cover image* berwarna dan hitam putih yang berformat JPG, dengan ukuran yang berbeda yaitu 500x500 *pixel*, 700x700 *pixel*, 900x900 *pixel*, dan juga menggunakan satu *file secret image* dengan ukura 10x10 *pixel* (11kb). Batas maksimal ukuran *file secret image* yang bisa digunakan untuk penyisipan pada *file cover image* untuk berwarna yaitu 15 % dari ukuran *size cover image*, dan untuk *file cover image* hitam putih menggunakan *file secret image* dengan ukuran 85 % dari *size cover image*. Hasil pengujian sebagai berikut:

Tabel 2. Hasil Pengujian encode algoritma LSB random color

Color	Cover image	Secret image	LSB Random Color	
			MSE	PSNR
Berwarna	500x500	10x10 (11 kb)	0.17141	55.79039
	700x700	10x10 (11 kb)	0.08671	58.75020
	900x900	10x10 (11 kb)	0.05602	60.64701

Hitam Putih	500x500	10x10 (11 kb)	0.18308	55.50439
	700x700	10x10 (11 kb)	0.09301	58.44559
	900x900	10x10 (11 kb)	0.07430	59.42084

Hasil pengujian pada Tabel 2 menyimpulkan bahwa penyisipan *file secret image* dengan menggunakan algoritma *LSB random color* terlihat baik karna nilai PSNR menunjukkan lebih besar dari nilai minimalnya yaitu 28 dB. *File cover image* yang berwarna dan hitam putih menunjukkan lebih baik mengunakan *file cover image* yang berwarna. Semakin besar ukuran *file cover image* maka semakin bagus proses penyisipannya

Tabel 3. Hasil Pengujian encode algoritma LSB shifting

Color	Cover image	Secret image	LSB shifting	
			MSE	PSNR
Berwarna	500x500	10x10 (11 kb)	5199.82834	10.97091
	700x700	10x10 (11 kb)	1937.05184	15.25939
	900x900	10x10 (11 kb)	1600.38461	16.08856
Hitam Putih	500x500	10x10 (11 kb)	3097.27299	13.22101
	700x700	10x10 (11 kb)	2151.43141	14.80353
	900x900	10x10 (11 kb)	12.94968	37.00821

Hasil pengujian pada Tabel 3 menyimpulkan bahwa penyisipan *file secret image* dengan menggunakan algoritma *LSB shifting* terlihat buruk, karna nilai PSNR menunjukkan lebih rendah dari nilai minimalnya yaitu 28 dB, dan untuk tampilan warna *file stegano image* yang dihasilkan semuanya berubah. Ada satu *file cover image* berukuran 900x900 pixel berwarna hitam putih menunjukkan nilai PSNR yang lebih besar dari nilai minimalnya, dan untuk tampilan *file stegano image* tersebut hampir mirip dengan *file* aslinya. *File cover image* yang berwarna dan hitam putih menunjukkan lebih baik mengunakan *file cover image* yang hitam putih. Semakin besar ukuran *file cover image* maka semakin bagus proses penyisipannya

Tabel 4. Perhitungan nilai MSE dan PSNR menggunakan file secret image maksimal

Algoritma	Jenis	Nama File	MSE	PNSR
LSB Random Color	Berwarna	ST 1	0.48311	51.29032
	Hitam Putih	ST 2	0.50260	51.11861
LSB Shifting	Berwarna	ST 1	11347.77235	7.58170
	Hitam Putih	ST 2	1825.64164	15.51665

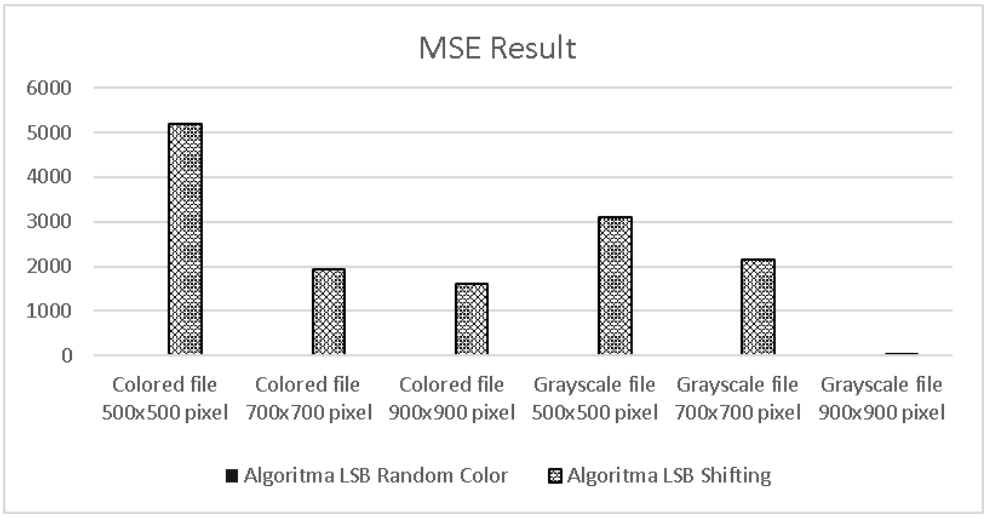
Perhitungan nilai *error* (MSE) dan PSNR pada table 4 masih tetap menunjukkan bahwasannya algoritma *LSB random color* lebih unggul daripada algoritma *LSB shifting*, walaupun itu menggunakan jenis *file* berwarna maupun *file* hitam putih. Hasil dari proses penyisipan dapat dilihat pada Gambar 3 dan Gambar 4.

Gambar 3. Hasil penyisipan menggunakan algoritma LSB random color

Gambar 4. Hasil penyisipan menggunakan algoritma LSB shifting

5.1 Analisa Perbandingan Nila MSE

Perbandingan pertama yang dilakukan yaitu dengan menghitung nilai *error* (MSE) terhadap *file stegano image* yang telah dilakukan proses penyisipan *file secret image* kedalam beberapa *file cover image* dengan warna berbeda dan ukuran yang berbeda. Pengujian dilakukan dengan tiga *file cover image* berwarna dan tiga *file cover image* hitam putih dengan satu *file secret image*. Gambar 5 dibawah ini merupakan hasil analisis perbandingan nilai *error* (MSE).

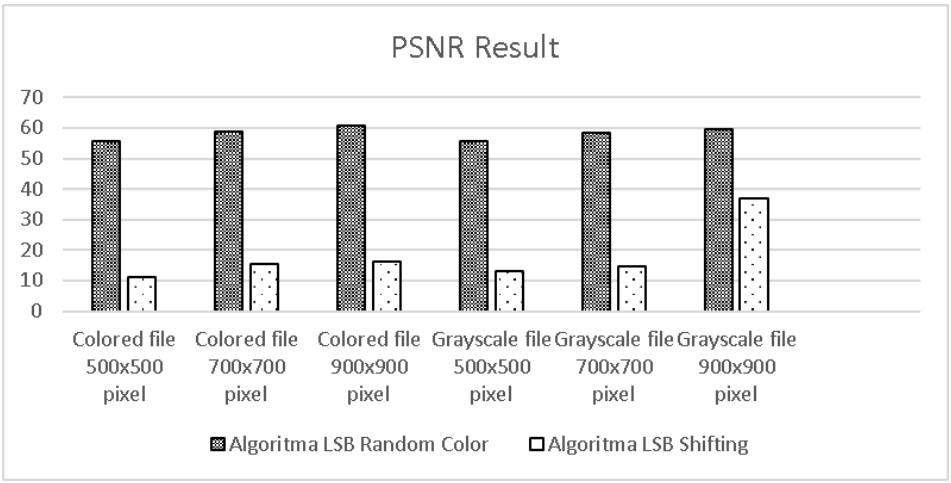


Gambar 5. Hasil analisa perhitungan MSE pada proses penyisipan di setiap algoritmanya

Poin analisa yang dapat diambil dari Gambar 3 yaitu bahwasannya nilai *error* (MSE) pada algoritma *LSB shifting* lebih tinggi dari pada algoritma *LSB random color*. Hal ini terlihat pada Tabel 3 dan 4 dimana setiap algoritmanya masih memiliki nilai *error* (MSE) pada proses penyisipan *file secret image*, akan tetapi proses penyisipan yang menggunakan algoritma *LSB shifti*ng dengan *file cover image* berukuran 900x900 *pixel* yang berwarna hitam putih menunjukkan nilai MSE yang berbeda dari nilai MSE yang terdapat pada *file stegano image* lainnya.

5.2 Analisa Perbandingan Nilai PSNR

Jika nilai MSE sudah ditemukan, maka analisa perbandingan yang kedua bisa dilakukan yaitu dengan menghitung nilai PSNR terhadap *file stegano image* yang telah dilakukan proses penyisipan *file secret image* kedalam beberapa *file cover image* dengan warna berbeda dan ukuran yang berbeda. Pengujian dilakukan dengan tiga *file cover image* berwarna dan tiga *file cover image* hitam putih dengan satu *file secret image*. Gambar 6 dibawah ini merupakan hasil analisi perbandingan nilai PSNR:



Gambar 6. Hasil analisa perhitungan PSNR pada proses penyisipan di setiap algoritmanya

Poin analisa yang dapat diambil dari Gambar 4 yaitu bahwasannya nilai PSNR pada algoritma *LSB shifting* lebih rendah dari pada algoritma *LSB random color*. Hal ini terlihat pada Tabel 3 dan Tabel 4 dimana kecurigaan penglihatan mata manusia pada gambar memiliki batas minimal yaitu 28 dB, jika melebihi dari batas minimal maka gambar tersebut bisa dibilang baik, dan jika kurang dari batas minimal maka gambar tersebut bisa dibilang buruk. Proses penyisipan yang menggunakan algoritma *LSB shifting* dengan *file cover image* berukuran 900x900 *pixel* yang berwarna hitam putih menunjukkan berbeda dari *file stegano image* lainnya, karna *file* ini memiliki nilai yang melebihi batas minimalnya, maka *file* tersebut bisa dibilang bagus.

5.3 Analisa nilai maksimal secret image

Analisa selanjutnya yaitu untuk mengetahui nilai maksimal *file* yang dapat disisipkan kedalam *cover image* dengan menggunakan algoritma *LSB random color* dan algoritma *LSB shifting*. Pengujian kali ini terdapat dua *file cover image* yaitu berwarna dan hitam putih yang berukuran 900x900 *pixel*, kemudia satu *file secret image* dengan ukuran 15% dari *size cover image* untuk berwarna, dan satu *file secret image* dengan ukuran 85% dari *size cover image* untuk hitam putih. Hasil Pengujian dapat dilihat di Gambar 7 dan Gambar 8.

Gambar 7. file secret image sebelum dan setelah proses pengekstrakan menggunakan algoritma LSB random color

Gambar 8. file secret image sebelum dan setelah proses pengekstrakan menggunakan algoritma LSB shifting

Poin analisa yang dapat diambil dari Gambar 5 dan Gambar 6 yaitu *file secret image* dengan ukuran 15% dari *size cover image* untuk berwarna, dan *file secret image* dengan ukuran 85% dari *size cover image* untuk hitam putih menghasilakn *file secret image* yang berbeda dari sebelumnya, meskipun itu menggunakan algoritma *LSB random color* dan *algoritma LSB shifting*. Hasil analisa di atas bahwasannya disarankan untuk menggunakan *file secret image* dengan ukuran dibawahnya untuk mendapatkan hasil yang lebih baik.

6. Kesimpulan

Hasil penyisipan *file* mengunakan *cover image* berwarna lebih baik dari pada menggunakan *cover image* hitam putih pada implementesi algoritma *LSB random color*. Hasil untuk penyisipan *file cover image* menggunakan jenis warna malah menghasilkan kebalikan dari algoritma *LSB random color*, yaitu lebih baik mengunakan *cover image* hitam putih dari pada *file* yang berwarna. Kapasitas penyisipan sebuah *file secret image* ke dalam *cover image*, lebih besar menggunakan *cover image* hitam putih daripada *cover image* yang berwarna, meskipun menggunakan algoritma *LSB random color* atau algoritma *LSB shifting*. Algoritma LSB random color memiliki performa lebih baik dari pada algoritma LSB shifting, meskipun menggunakan jenis file berwarna atau hitam putih.

Daftar Notasi

MSE : Nilai *Mean Square Error* citra *steganograph*y

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] W. Yuntian and Y. Wei, "Information Based on Strengthening the Awareness and Promotion of Information Technology," in *2010 3rd International Conference on Information Management, Innovation Management and Industrial Engineering*, 2010, vol. 4, pp. 88–90.

[2] L. Li, R. Ge, S. Zhou, and R. Valerdi, "Guest EditorialIntegrated Healthcare Information Systems," *IEEE Trans. Inf. Technol. Biomed.*, vol. 16, no. 4, pp. 515–517, Jul. 2012.

[3] 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.

[4] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Comput. Secur.*, vol. 24, no. 2, pp. 147–159, 2005.

[5] 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.

[6] T. Jamil, "Steganography: the art of hiding information in plain sight," *IEEE Potentials*, vol. 18, no. 1, pp. 10–12, Feb. 1999.

[7] 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.

[8] A. Kumar and K. Pooja, "Steganography-A Data Hiding Technique," *Int. J. Comput. Appl.*, vol. 975, p. 8887.

[9] N. Hopper, L. von Ahn, and J. Langford, "Provably Secure Steganography," *IEEE Trans. Comput.*, vol. 58, no. 5, pp. 662–676, May 2009.

[10] A. Ranjan and M. Bhonsle, "Advanced technics to shared amp; protect cloud data using multilayer steganography and cryptography," in *2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT)*, 2016, pp. 35–41.

[11] P. Jayaram, H. Ranganatha, and H. Anupama, "Information hiding using audio steganography–a survey," *Int. J. Multimed. Its Appl. IJMA Vol*, vol. 3, pp. 86–96, 2011.

[12] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed, and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," *J. Syst. Eng. Electron.*, vol. 29, no. 3, pp. 639–649, Jun. 2018.

[13] H. Ghasemzadeh and M. H. Kayvanrad, "Comprehensive review of audio steganalysis methods," *IET Signal Process.*, vol. 12, no. 6, pp. 673–687, 2018.

[14] R. Balaji and G. Naveen, "Secure data transmission using video Steganography," in *2011 IEEE International Conference On Electro/Information Technology*, 2011, pp. 1–5.

[15] M. H. Shirali-Shahreza and Mohammad Shirali-Shahreza, "Text Steganography in chat," in *2007 3rd IEEE/IFIP International Conference in Central Asia on Internet*, 2007, pp. 1–5.

[16] 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.

[17] 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.

[18] S. K. Bandyopadhyay, D. Bhattacharyya, D. Ganguly, S. Mukherjee, and P. Das, "A tutorial review on steganography," in *International conference on contemporary computing*, 2008, vol. 101, pp. 105–114.

[19] N. Akhtar, P. Johri, and S. Khan, "Enhancing the security and quality of LSB based image steganography," in *Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on*, 2013, pp. 385–390.

[20] 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.

[21] 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.

ISSN: 2714-7975; E-ISSN: 2716-1382