JAIC

JOURNAL OF APPLIED INFORMATICS AND COMPUTING

Online ISSN : 2548-6861

Website: https://jurnal.polibatam.ac.id/index.php/JAIC/
Pusat Penelitian dan Pengabdian Masyarakat (P3M) Politeknik Negeri Batam
Jl. Ahmad Yani Parkway Batam Center, Batam 29461

Editor in Chief

Managing Editor

Scientific Board

DOI: https://doi.org/10.30871/jaic.v6i1

PUBLISHED: 2022-07-14

ARTICLES

Journal of Applied Informatics and Computing (JAIC)
Vol.6, No.1, Juli 2022, pp. 25~30
e-ISSN: 2548-6861

Penyembunyian Pesan Terenkripsi pada Citra menggunakan Algoritma LSB dan Transposisi Kolom

Kiswara Agung Santoso [1]* Ahmad Tanto Wiraga [2], Abduh Riski [3]
[1,2,3] Jurusan Matematika, Fakultas MIPA, Universitas Jember
kiswaras@gmail.com [1], ahmadtantowiraga@gmail.com[2], riski.fmipa@unej.ac.id [3]

Article Info

Article history:

Received 2022-01-07
Revised 2022-03-14
Accepted 2022-03-17

Keyword:

Column transposition,
Cryptography,
LSB,
Steganography,
Vigenere cipher.

ABSTRACT

Data security is a very important thing to do so that the message or information sent to someone is not known by an uninterested person. Data security techniques that are often used today are cryptography and steganography. In this study, the data will be used in the form of text. This text message will be hidden into a container in the form of an image (*cover image*). Text messages will be hidden in the image using the LSB algorithm and column transposition. To strenghthen security, the text message will be encrypted first using the vigenere cipher algorithm and column transposition. The results showed that the stego image produced in plain sight is very similar to the original image (*cover image*), this can be seen from the PSNR value which is more than 50 even some experiments have a PSNR value of more than 60. Based on the results of MSE and PSNR analysis, it can be known that the quality of images generated by the proposed method can be categorized well. This can be seen from the value of PSNR above 50 dB and there is even above 60 dB. Based on the results of the LSB enhanced analysis, irregularities in the stego image are not visible so it will not be suspected by unauthorised people for hidden messages.

I. PENDAHULUAN

Pengamanan data merupakan hal yang perlu dilakukan agar data yang dikirim kepada seseorang tidak diketahui oleh pihak ketiga yang tidak berkepentingan. Teknik pengamanan data yang saat ini sering digunakan adalah kriptografi dan steganografi. Kriptografi merupakan teknik mengubah data (*plaintext*) kedalam bentuk lain (*ciphertext*) agar maknanya tidak diketahui oleh orang yang tidak berkepentingan. Sedangkan teknik steganografi merupakan teknik menyembunyikan data (*plaintext*) pada data lain (*cover*) agar keberadaannya tidak diketahui oleh orang yang tidak berkepentingan.

Salah satu algoritma kriptografi yang dapat digunakan adalah *vigenere cipher*, [1] telah melakukan pengamanan pesan teks dengan menggunakan algoritma *vigenere cipher*. Pesan teks hasil enkripsi menjadi samar dan tidak diketahui maknanya oleh orang yang tidak berkepentingan. Namun, hasil enkripsi dengan algoritma vigenere cipher memiliki pola-pola karakter yang berulang sehingga berpeluang dapat dipecahkan enkripsi tersebut.

Algoritma lain yang dapat digunakan dalam kriptografi yaitu transposisi kolom [2] melakukan analisis pada algoritma transposisi kolom. Dari analisis tersebut diketahui bahwa hasil enkripsi transposisi kolom berpeluang dapat dipecahkan dengan melihat jumlah frekuensinya. Oleh karena itu, transposisi kolom akan Kusumaningtyas lebih baik dikombinasikan dengan algoritma lain untuk menambah kekuatan dan kerumitan dalam mengenkripsi.

Selain kriptografi, teknik pengamanan data yang popular digunakan pada saat ini yaitu teknik steganografi. Salah satu algoritma yang dapat digunakan pada steganografi adalah *Least Significant Bit* (LSB) [3] [4], telah melakukan penelitian penyembunyian informasi berupa pesan teks (*plaintext*) pada media gambar (*coverimage*) dengan menggunakan algoritma LSB. Setelah gambar disisipi pesan (*stegoimage*), kualitas gambar tersebut (*stegoimage*) hampir sama dengan gambar sebelum disisipi pesan (*coverimage*). Namun, penyembunyian menggunakan algoritma LSB tergolong mudah dipecahkan.

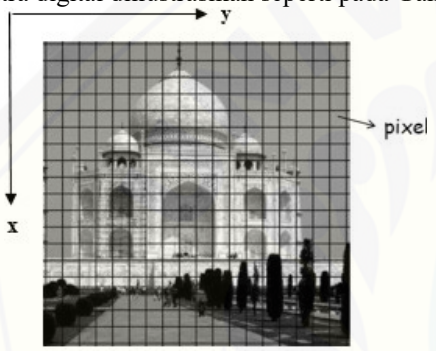
Pada penelitian ini akan melakukan pengamanan pesan berupa teks (*plaintext*) menggunakan algoritma LSB. Untuk

mengatasi kelemahan algoritma LSB, maka urutan penyisipan bit-bit *plaintext* pada piksel citra akan diacak menggunakan algoritma transposisi kolom. Untuk memperlapis keamanan, pesan teks tersebut akan dienkripsi terlebih dahulu dengan menggunakan algoritma *vigenere cipher* dan transposisi kolom sebelum disembunyikan kedalam citra.

II. TINJAUAN PUSTAKA

A. Citra Digital

Citra digital merupakan sekumpulan piksel-piksel yang tersusun dalam bentuk matriks. Setiap piksel dinyatakan sebagai matriks $f(x,y)$ dimana x dan y merupakan suatu koordinat pada bidang dua dimensi. Pada citra digital peletakan titik asal koordinat berada disebelah kiri atas matrik. Nilai $f(x,y)$ merupakan nilai intensitas cahaya atau derajat keabuan pada titik (x,y). Nilai intensitas cahaya pada piksel-piksel memberikan informasi berupa warna citra [5]. Ilustrasi citra digital diilustrasikan seperti pada Gambar 1.



Gambar 1. Ilustrasi citra digital

B. ASCII (American Standard Code for Information Interchage)

ASCII (*American Standard Code for Information Interchage*) merupakan standar internasional berupa kode huruf dan simbol yang digunakan pada komputer untuk menunjukan suatu teks. Kode ASCII memiliki 256 karakter yang dimulai dari 0 sampai 25. ASCII dibagi menjadi tiga bagian, yaitu *ASCII Control Character* (kode karakter ke 0 - 31),kode ini biasanya digunakan untuk mengontrol beberapa hardware seperti code nomor 7 yang bisa digunakan untuk membunyikan suara "beep" dari speaker. *ASCII Printables Character* (kode karakter ke 32 - 128), kode ini merupakan kode dari semua karakter yang ada pada keyboard. T*he Extended ASCII Codes* (kode karakter ke 129 – 255) digunakan untuk tombol tambahan keyboard seperti tombol F1, ctrl, shift, beserta kombinasinya seperti ctrl+V, ctrl+alt+del.

C. Kriptografi

Kriptografi merupakan salah satu teknik pengamanan data. Kata kriptografi berasal dari bahasa Yunani, yaitu *cryptos* yang artinya rahasia dan graphein yang artinya tulisan. Oleh karena itu, kriptografi dapat diartikan sebagai ilmu yang mempelajari tentang tulisan atau pesan rahasia. Kriptografi merupakan teknik pengkodean untuk mengamankan sebuah pesan atau informasi dengan cara mengkodekan pesan tersebut sehingga hanya orang yang diberi akses sajalah yang mengerti maknanya [6].

D. Vigenere cipher

Vigenere Cipher merupakan salah satu algoritma pengamanan data pada kriptografi. Karakter huruf yang digunakan pada algoritma *vigenere cipher* yaitu A, B, C, …,Z yang disamakan dengan nilai 0, 1, 2, …,25. Proses enkripsi algoritma *vigenere cipher* yaitu dengan menggeser huruf pada *plaintext* sejauh nilai kunci pada deret alphabet. Jika jumlah kunci kurang dari *plaintext*, maka kunci diulang hingga setiap karakter *plaintext* memiliki pasangan dengan karakter dari kunci [6]. Dalam implementasi format ASCII, karakter yang digunakan terdapat pada bilangan ASCII ke 32 – 127. Sehingga rumus enkripsi yang digunakan untuk menghitungnya sebagai berikut:

$$C_i = P_i + K_i \ (mod\ 95) \quad (1)$$

Sedangkan untuk mendapatkan kembali *plaintext* yang terenkripsi dirumuskan sebagai berikut:

$$P_i = C_i - K_i \ (mod\ 95) \quad (2)$$

Keterangan:
P_i : Nilai desimal ASCII karakter *plaintext* ke-i
C_i : Nilai desimal ASCII karakter *ciphertext* ke-i
K_i: Nilai desimal ASCII karakter kunci ke-i

E. Transposisi Kolom

Teknik transposisi merupakan teknik memindahkan posisi karakter *plaintext* ke posisi lain tanpa mengubah karakter *plaintext* tersebut. Salah satu algoritma kriptografi menggunakan teknik transposisi adalah transposisi *columnar* atau transposisi kolom. Proses enkripsi algoritma transposisi kolom yaitu dengan menulis *plaintext* secara berderet dengan panjang yang telah ditetapkan, kemudian dibaca kolom demi kolom dengan urutan pembacaan sesuai kata kunci yang digunakan [6]. Panjang deret sesuai dengan panjang kunci yang digunakan. Sedangkan urutan pembacaan kolom berdasarkan urutan abjad kata kunci seperti pada Gambar 2.

Plaintext : SEMOGA DIPERMUDAH SKRIPSI
Kunci : AMIN
Urutan Kunci Sesuai Abjad : AMIN → 1 3 2 4

1	3	2	4
S	E	M	O
G	A		D
I	P	E	R
M	U	D	A
H		S	K
R	I	P	S
I	#	#	#

Ciphertext : SGIMHRIM EDSPEAPU IODRAKS

Gambar 2. Proses transposisi kolom

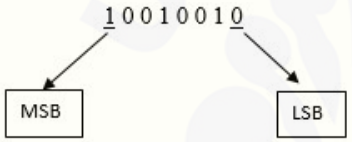
F. *Steganografi*

Steganografi berasal dari bahasa yunani yaitu "*stegos*" yang artinya tersembunyi dan "*graphein*" yang artinya tulisan. Jadi, steganografi merupakan ilmu dan seni menyembunyikan sebuah pesan pada suatu media sehingga keberadaannya tidak diketahui oleh orang yang tidak berkepentingan [6], Misalnya menyembunyikan teks kedalam gambar atau menyembunyikan gambar di dalam gambar [7].

Jadi berbeda dengan kriptografi yang mengamankan pesan dengan cara dikodekan tetapi jika steganografi mengamankan pesan dengan cara menyembunyikan pesan tersebut dalam media lain, dalam penelitian ini pesan teks disembunyikan dalam media gambar/foto.

G. *Least Significant Bit (LSB)*

Least significant bit atau LSB merupakan salah satu algoritma pengamanan data pada steganografi. Algoritma LSB memanfaatkan ketidakmampuan mata manusia dalam membedakan gambar asli (*cover image*) dan gambar yang telah disisipi pesan (*stego image*). Pada susunan bit di dalam sebuah *byte* (1 *byte* = 8 bit), terdapat bit yang paling berarti (*most significant bit* atau MSB) dan bit yang paling kurang berarti (*least significant bit* atau LSB seperti pada Gambar 3.



Gambar 3. MSB dan LSB

Penyisipan dengan algoritma LSB dilakukan pada setiap *byte* piksel *cover image* pada bit yang terletak paling akhir (bit LSB). Bit LSB cocok diganti karena perubahan pada gambar tidak memiliki efek yang berarti yang terlihat oleh mata manusia [5].

H. *Mean Squared Error (MSE) dan Peak Signal to Noise Ratio (PSNR)*

Mean Squared Error (MSE) merupakan salah satu parameter dalam mengukur kualitas metode steganografi [8] dengan membandingkan citra asli (*cover image*) dengan citra setelah disisipkan pesan (*stego image*). Perhitungan nilai MSE dapat dilakukan dengan persamaan berikut:

$$MSE = \frac{1}{NM}\sum_{x=1}^{N}\sum_{y=1}^{M}(p(x,y) - q(x,y))^2 \qquad (3)$$

Keterangan:
$p(x,y)$: Nilai piksel citra asli koordinat (x,y)
$q(x,y)$: Nilai piksel *stego image* pada koordinat (x,y)
M : Jumlah baris piksel (panjang citra)
N : Jumlah kolom piksel (lebar citra)

Peak Signal to Noise Ratio (PSNR) [11] merupakan perbandingan nilai maksimum dari sinyal yang diukur dengan nilai *noise* yang berpengaruh pada sinyal tersebut dalam satuan desibel (dB). Perhitungan nilai PSNR dapat dilakukan dengan persamaan berikut:

$$PSNR = 10.log\frac{M^2}{MSE} \qquad (4)$$

Keterangan:
M : Nilai piksel maksimum
MSE : *Mean Squared Error*

Menurut Hidayat dan Hastuti [9] kriteria kualitas *stego image* dapat dilihat dari nilai PSNR seperti pada Tabel 1 berikut:

TABEL 1
KRITERIA KUALITAS CITRA

PSNR (dB)	Kualitas Citra (*stego image*)
> 60	Sangat Bagus (*excellent*)
$50 - 59$	Bagus (*good*)
$40 - 49$	Layak (*reasonable*)
$30 - 39$	Cukup (*poor*)
< 30	Tidak dapat dipakai (*unusable*)

I. *Enhanced LSB*

Analisis *enhanced* LSB merupakan merupakan metode untuk mendeteksi adanya pesan rahasia pada suatu citra. Metode ini memanfaatkan indera manusia dalam melihat kerusakan pada citra setelah dilakukan *enhanced* LSB. Proses *enhanced* LSB dilakukan dengan mengubah semua bit pada setiap piksel dengan bit LSB pada piksel tersebut [4] [10]. Misalkan suatu piksel bernilai 24, jika dijadikan dalam bentuk bit (binary digit) akan menjadi 11000. Karena bit LSB pada piksel tersebut adalah 1 (bergaris bawah dan dicetak tebal), maka susunan bit-bitnya diubah menjadi 11001.

III. METODE PENELITIAN

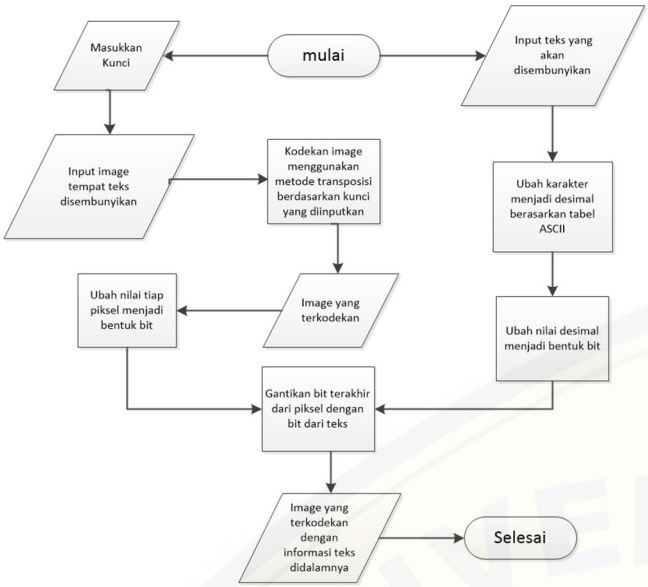
A. *Data Penelitian*

Pesan yang akan digunakan pada penelitian ini berupa teks. Pesan teks (kalimat) yang disembunyikan memiliki tiga variasi panjang karakter yaitu kalimat dengan jumlah karakter 500, 1000, dan 2000 karakter. *Cover image* yang akan digunakan sebagai tempat menyembunyikan kalimat tersebut berupa citra/foto dengan ukuran yaitu 128 x 128 piksel.

B. *Langkah-langkah Penelitian*

Berikut ini adalah flowchart Langkah penelitian dalam menyembunyikan teks kedalam image dimana setiap bit dari karakter teks akan menggantikan bit terakhir dari piksel image. Tetapi sebelum teks disembunyikan kedalam image, image tersebut dikodekan menggunakan metode transposisi kolom, sehingga akan lebih terjamin keamanannya baik teks maupun gambar imagenya. Langkah-langkah penelitian sebagai berikut.

1. Masukkan kunci yang berupa teks untuk mengkodekan image tempat plainteks disembunyikan
2. Masukkan image yang merupakan tempat dimana teks akan disembunyikan
3. Kodekan image menggunakan metode transposisi kolom agar gambar dapat disamarkan



Gambar 4. Langkah-langkah penelitian

4. Ubah nilai desimal tiap piksel menjadi 8 digit biner (bit)
5. Masukkan pesan teks rahasia yang akan disembunyikan dalam gambar
6. Ubah tiap karakter dari teks yang disembunyikan menjadi bentuk desimal berdasarkan table ASCII
7. Ubah bentuk decimal dari karakter pesan menjadi bit
8. Ganti nilai bit terakhir dari tiap piksel dengan bit dari karakter pesan teks
9. Output dari program ini adalah image yang telah terkodekan dimana didalam image tersebut tersimpan pesan rahasia

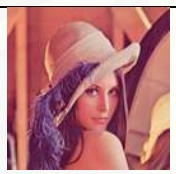
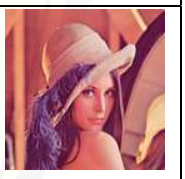
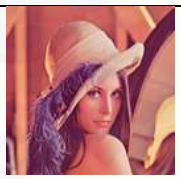
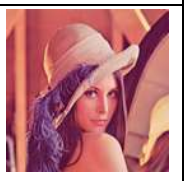
IV. Hasil Dan Pembahasan

Hasil penelitian yang didapatkan dari program sebagai berikut.

A. Hasil Penyembunyian

Pada proses penyembunyian pesan terenkripsi pada citra menggunakan algoritma LSB dan transposisi kolom akan dihasilkan *stego image* seperti pada Tabel 2.

TABEL 2
HASIL *STEGO IMAGE*

No	*Cover Image*	Panjang Teks	*Stego Image*
1	 Citra *peppers*	500	
2	 Citra *peppers*	1000	
3	 Citra *peppers*	2000	
4	 Citra *baboon*	500	
5	 Citra *baboon*	1000	
6	 Citra *baboon*	2000	
7	 Citra *lena*	500	
8	 Citra *lena*	1000	
9	 Citra *lena*	2000	

Proses proses penyembunyian pesan terenkripsi pada citra menggunakan algoritma LSB dan transposisi kolom berhasil dilakukan untuk semua teks dan image yang dibuat contoh, seperti pada Tabel 2. Dan 100% berhasil artinya secara

virtual, *stego image* yang menghasilkan gambar dengan kualitas yang sangat mirip dan tidak dapat dibedakan (untuk semua percobaan).

B. Hasil Ekstraksi

Stego image hasil penyembunyian pesan terenkripsi menggunakan algoritma LSB dan transposisi kolom berhasil diekstraksi. Pesan teks hasil ekstraksi tidak berubah (sama seperti pesan teks yang disembunyikan pada *cover image*). Hal ini menunjukan bahwa program yang dibuat pada Matlab R2015b dapat berfungsi dengan semestinya.

C. Analisis Keamanan

1) Analisis MSE dan PSNR

TABEL 3
HASIL MSE DAN PSNR

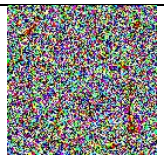
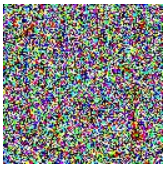
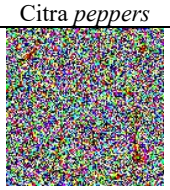
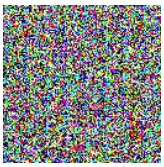
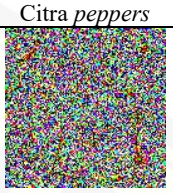
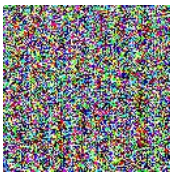
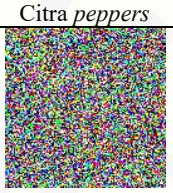
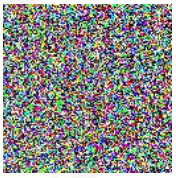
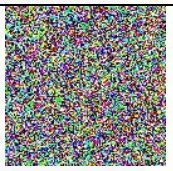
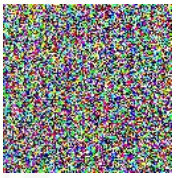
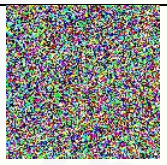
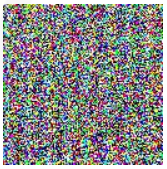
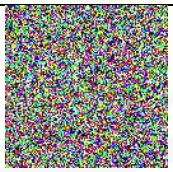
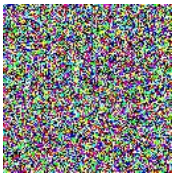
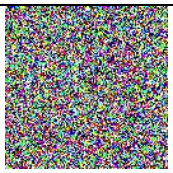
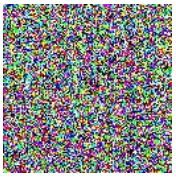
No	Stego Image	Panjang Teks	MSE	PSNR
1	Citra *peppers*	500	0.042725	61.858
2	Citra *peppers*	1000	0.084676	58.8872
3	Citra *peppers*	2000	0.16534	55.9809
4	Citra *baboon*	500	0.042175	61.9142
5	Citra *baboon*	1000	0.083333	58.9566
6	Citra *baboon*	2000	0.16471	55.9975
7	Citra *lena*	500	0.04421	61.7096
8	Citra *lena*	1000	0.08492	58.8747
9	Citra *lena*	2000	0.16339	56.0325

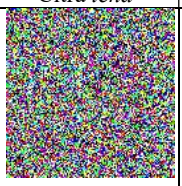
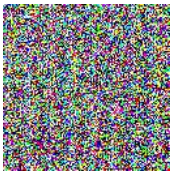
Pada Tabel 3 menunjukan bahwa semakin besar pesan teks yang disisipkan, maka nilai PSNR dari *stego image* semakin kecil dan nilai MSE semakin besar. Hal ini menunjukan bahwa kualitas *stego image* akan semakin berkurang jika pesan yang disisipkan semakin banyak. Nilai PSNR yang dihasilkan dapat dikategorikan baik. Hal ini bisa dilihat dari nilai PSNR diatas 50 dB dan bahkan ada yang diatas 60 dB. Berdasarkan Tabel 2.5, nilai PSNR sebesar ini dikategorikan bagus (diatas 50 dB) dan sangat bagus (diatas 60 dB). Hal ini menunjukan bahwa stego image yang dihasilkan oleh kedua jenis penyisipan ini sama-sama memiliki kualitas yang baik.

2) Analisis *Enhanced* LSB

Tabel berikut ini adalah hasil dari teks yang disembunyikan dalam gambar yang sudah dikodekan

TABEL 4
HASIL ENHANCED LSB

No	*Enhanced Cover Image*	Panjang Teks	*Enhanced Stego image*
1	 Citra *peppers*	500	
2	 Citra *peppers*	1000	
3	 Citra *peppers*	2000	
4	 Citra *baboon*	500	
5	 Citra *baboon*	1000	
6	 Citra *baboon*	2000	
7	 Citra *lena*	500	
8		1000	

	Citra *lena*		
9	 Citra *lena*	2000	

Hasil *stego image* yang telah dilakukan *enhanced* LSB menunjukan bahwa piksel-piksel yang berisi pesan tersembunyi tidak terlihat jelas adanya kejanggalan dan bentuknya hampir sama dengan *cover image* hasil *enhanced* LSB. Hal ini karena pesan disisipkan secara acak pada piksel citra dan membaur dengan piksel lain sehingga piksel yang berisi pesan menjadi terlihat samar dan semakin tidak dicurigai oleh orang yang tidak berkepentingan.

V. KESIMPULAN

Berdasarkan Penelitian yang telah dilakukan dapat disimpulkan bahwa metode yang diajukan dapat berjalan dengan baik. Pada proses penyembunyian pesan rahasia pada *cover image* menghasilkan *stego image* yang secara kasat mata sangat mirip dengan citra asli. Pesan rahasia pada *stego image* dapat diekstraksi dengan baik. Hal ini dibuktikan dengan pesan hasil ekstraksi yang tidak berubah. Pada analisis nilai MSE dan PSNR, kualitas *stego image* yang dihasilkan pada semua percobaan dapat dikategorikan baik karena nilai PSNR diatas 50 dB dan bahkan ada yang diatas 60 dB. Pada analisis *enhanced* LSB, kejanggalan pada *stego image* tidak terlihat jelas sehingga tidak akan dicurigai oleh orang yang tidak berkepentingan akan adanya pesan yang disembunyikan pada *stego image* tersebut.

DAFTAR PUSTAKA

[1] Hamdani, "Penerapan Metode Vigenere pada Kriptografi Klasik untuk Pesan Rahasia," *Informatika Mulawarman*, vol. 7, pp. 26-26, 2012.

[2] J. A. Kusumaningtyas, "Analisa Algoritma Ciphers Transposition: Study Literature," *Multimatrix*, vol. 1, pp. 1-12, 2018.

[3] A. Ardiansyah, M. Kurniasih, "Penyembunyian Pesan Rahasia pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit," *Teknologi Informasi*, vol. 8, pp. 96-101, 2018.

[4] D. E. Kurniawan and N. Narupi, "Teknik Penyembunyian Data Menggunakan Kombinasi Kriptografi Rijndael dan Steganografi Least Significant Bit (LSB)," Jurnal Teknik Informatika dan Sistem Informasi, vol. 2, no. 3, Art. no. 3, Dec. 2016, doi: 10.28932/jutisi.v2i3.630.

[5] D. Putra, "Pengolahan Citra Digital," *ANDI*, 2010.

[6] R. Munir, "Diktat Kuliah IF5054 Kriptografi," *Departemen Teknik Informatika ITB*, 2006.

[7] D. E. Kurniawan, N. R. Hartadi, and P. Prasetyawan, "Analisis Hasil Teknik Penyembunyian Hak Cipta Menggunakan Transformasi DCT dan RSPPMC pada Jejaring Sosial," Jurnal Teknologi Informasi dan Ilmu Komputer, vol. 5, no. 3, Art. no. 3, Aug. 2018, doi: 10.25126/jtiik.201853692.

[8] A. Solichin and S. Kom, "Mengukur Kualitas Citra Hasil Steganografi," Mengukur Kualitas Citra Has. Steganografi, no. April, pp. 1–4, 2015.

[9] E. Y. Hidayat, K. Hastuti, "Analisis Steganografi Metode Least Significant Bit (LSB) dengan Penyisipan Sekuensial dan Acak Secara Kuantitatif dan Visual," Techno.COM, vol. 12, pp. 157-167, 2013

[10] R. Sadikin, "Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java," *ANDI*, 2012.

[11] U. Sara, M. Akter, and M. S. Uddin, "Image Quality Assessment through FSIM, SSIM, MSE and PSNR—A Comparative Study," Journal of Computer and Communications, vol. 7, no. 3, Art. no. 3, Mar. 2019, doi: 10.4236/jcc.2019.73002.