STEGANOGRAFI PESAN TERENKRIPSI AFFINE CIPHER MENGGUNAKAN METODA LSB DENGAN POLA GENAP GANJIL

by Herny Februariyanti

Submission date: 19-Mar-2021 12:46PM (UTC+0700)
Submission ID: 1536837122
File name: 2019_SINTAK_Steganografi_Pesan_Terenkripsi_Affine_Cipher.pdf (586.82K)
Word count: 3512
Character count: 20177

STEGANOGRAFI PESAN TERENKRIPSI AFFINE CIPHER MENGGUNAKAN METODA LSB DENGAN POLA GENAP GANJIL

Herny Februariyanti[1], Wahyudi[2], Arief Susanto[3], Rihartanto*[4]
[1]Fakultas Teknologi Informasi, Universitas Stikubank Semarang
[2,3]Jurusan Teknologi Informasi, Politeknik Negeri Samarinda
e-mail: [1]hernyfeb@edu.unisbank.ac.id, [2]wahyudi030596@gmail.com, [3]arief.susanto@umk.ac.id,
[4]rihart.c@gmail.com

ABSTRAK

Kriptografi dan steganografi merupakan dua teknik berbeda yang bertujuan sama, yaitu melindungi informasi dari yang tidak berkepentingan. Kriptografi mengubah pesan asli menjadi sesuatu yang bersifat rahasia, sementara steganografi menuliskan pesan dengan cara tertentu sehingga keberadaannya tidak disadari. Dalam penelitian ini, informasi yang disembunyikan berupa pesan yang sudah terenkripsi dengan Affine cipher. Informasi disembunyikan pada citra RGB menggunakan metoda LSB dengan pola genap ganjil. Ukuran pesan yang disembunyikan berada pada rentang 2% sampai mendekati 100% dari kapasitas yang dapat ditampung. Hasil pengujian menunjukkan bahwa kualitas citra hasil hasil steganografi masih tergolong baik, yang ditunjukkan oleh nilai PNSR terendah yaitu 59.1003dB untuk pesan mendekati 100% dari kapasitas maksimum. Demikian pula, secara visual tidak terlihat perbedaan antara citra asli dengan citra hasil steganografi. Penelitian ini juga membuktikan bahwa dua kriteria steganografi yang baik, yaitu imperceptible dan fidelity dapat terpenuhi.

***Kata Kunci**:Affine Cipher, LSB,* pola genap-ganjil, imperceptible, fidelity

1. PENDAHULUAN

Informasi merupakan aset yang perlu dijaga dan dilindungi. Dilindungi dari pengguna yang tidak berhak dan dijaga keaslian serta kebenarannya. Banyak cara yang dapat digunakan untuk melindungi informasi tersebut. Dua dari banyak metode yang dapat digunakan adalah enkripsi dan steganografi. Enkripsi atau sering juga disebut dengan kriptografi merupakan proses penyandian informasi menjadi bentuk lain yang tidak mudah dipahami[1], sedangkan steganografi merupakan proses menyamarkan informasi sehingga keberadaannya tidak mudah diketahui. Dari banyak teknik enkripsi yang ada, secara garis besar dibedakan menjadi enkripsi klasik dan modern. Teknik enkripsi klasik seperti *Caesar Cipher*[2], *Affine Cipher*[3], *dan Vigenere cipher yang* memiliki algoritma yang relatif sederhana dibandingkan dengan teknik enkripsi modern seperti DES, RSA atau AES.

Demikian pula halnya pada steganografi yang terdiri dari berbagai macam metode, diantaranya adalah *Least Significant Bit* (LSB), *Spread Spectrum* [4], *low bit coding* [5], algoritma transformasi, dan *Redundant Pattern Encoding*. MetodeLSB termasuk metode yang paling umum [6]digunakan dalam penyembunyian pesan. Salah satu alasannya adalah karena LSB tidak memerlukan komputasi yang rumit dalam penyembuyian pesan [7]. LSB bekerja dengan cara mengubah nilai bit terakhir data pada *cover* dengan bit-bit pesan yang disembunyikan. Sehingga secara sederhana, jika setiap bit terakhir pada *cover* diambil kembali, maka pesan yang disembunyikan dapat dengan mudah diketahui.

Kriptografi dan steganografi memiliki kelebihan dan kekurangannya masing-masing. Misalnya, hasil enkripsi berupa bentuk acak yang tidak mudah dipahami justru dapat menimbulkan tantangan bagi sebagian orang untuk memecahkan sandi teresebut. Sementara sifat steganografi yang menempelkan informasi pada media lain, rentan untuk dapat diekstraksi. Karena itu dalam penelitian ini dilakukan penyembunyian pesan terenkripsi menggunakan metode LSB. Pesan atau informasi yang disembunyikan adalah berupa teks, sementara yang digunakan sebagai cover adalah citra RGB. Sebelum disembunyikan, pesan terlebih dahulu dienkrisi menggunakan affine cipher. Dengan demikian, diharapkan kedua teknik sederhana ini dapat saling menutupi kekurangannya masing-masing.

2. METODE PENELITIAN

2.1 Affine Cipher

Kriptografi adalah ilmu atau teknik dimana pesan asli diacak sedemikian rupa menggunakan suatu kunci tertentu sehingga menjadi sesuatu yang sulit dibaca atau tidak dikenali. Proses mengubahan dari bentuk asli menjadi bentuk teracak disebut sebagai enkripsi sementara proses untuk mengembalikan bentuk teracak menjadi bentuk aslinya kembali disebut dengan dekripsi. Kedua proses ini memerlukan sebuah kunci, yang tergantung dari algoritma yang digunakan, kunci tersebut dapat merupakan kunci simetris ataupun kunci

asimetris. Algoritma untuk melakukan enkripsi dan dekripsi biasanya tidak bersifat rahasia, Yang dirahasiakan adalah kunci atau parameter lainnya yang digunakan dalam melakukan enkripsi dan dekripsi tersebut.

Affine cipher merupakan salah satu teknik enkripsi yang digolongkan sebagai teknik enkripsi klasik. Algoritma ini merupakan perluasan atau pengembangan dari Caesar cipher [8]. Proses enkripsi dilakukan menggunakan Persamaan (1) dan dekripsi menggunakan persamaan (2). P merupakan karakter atau huruf asli dan C adalah karakter atau huruf hasil enkripsi. m dan b merupakan kunci enkripsi, dengan ketentuan bahwa m relatif prima terhadap n, serta m dan b harus berada pada rentang antara satu sampai dengan n. n adalah banyaknya karakter yang dapat diakomodasi. Dalam penelitian ini, jumlah karakter yang digunakan sebagai nilai n adalah 128, yang merupakan jumlah karakter ASCII standar yang mewakili seluruh huruf, angka dan simbol yang ada pada *keyboard*.

$$C \equiv (m \cdot P + b) \bmod n \quad (1)$$

$$P \equiv m^{-1} \cdot (C - b) \bmod n \quad (2)$$

*Affine Cipher*memerlukan sepasang kunci yaitu yaitu *m* dan *b*. Agar hasil enkripsi dapat didekripsi, maka diperlukan m^{-1} yang merupakan nilai invers dari *m*. Syarat yang harus dipenuhi agar m memilki nilai invers adalah *m* harus relatif prima terhadap n. Relatif prima (*coprime*), artinya m dan n hanya memiliki satu faktor persekutuan, yaitu 1. Sebagai contoh jika kunci yang dipilih untuk m dan b adalah 7 dan 12. Angka 7 adalah relatif prima terhadap 128, karena kedua bilangan ini hanya memiliki satu faktor persekutuan, yaitu satu. Nilai m^{-1} dapat dihitung menggunakan fungsi kongruen pada Persamaan (3), sehingga diperoleh nilai m^{-1} yaitu 55.

$$(m^{-1} \times m) \bmod 128 \equiv 1 \quad (3)$$

Misalkan, kata "Multimedia" dienkripsi menggunakan kunci dan nilai invers yang sudah diperoleh tersebut, yaitu m= 7, b= 12, n= 128 dan m^{-1}= 55, maka ilustrasi tahapan perhitungan untuk proses enkripsi dan dekripsi ditunjukkan pada Gambar 1.

Plainteks (P)	M	u	l	t	i	m	e	d	i	a
P_i (ASCII)	77	117	108	116	105	109	101	100	105	97
P_i x m	539	819	756	812	735	763	707	700	735	679
(P_i x m) + b	551	831	768	824	747	775	719	712	747	691
((P_i x m) + b) mod 128	39	63	0	56	107	7	79	72	107	51
Ciphertext (C)	'	?	null	8	k	bell	O	H	k	3

a. Proses enkripsi

Ciphertext (C)	'	?	null	8	k	bell	O	H	k	3
C_i (ASCII)	39	63	0	56	107	7	79	72	107	51
C_i - b	27	51	-12	44	95	-5	67	60	95	39
m^{-1} (C_i-b)	1485	2805	-660	2420	5225	-275	3685	3300	5225	2145
(m^{-1} (C_i-b)) mod 128	77	117	108	116	105	109	101	100	105	97
Plaintext (P)	M	u	l	t	i	m	e	d	i	a

b. Proses dekripsi

Gambar 1. Ilustrasi proses enkripsi dan dekripsi menggunakan Affine cipher

Untuk mengetahui seberapa jauh perubahan hasil enkripsi dibandingkan dengan teks aslinya, atau untuk mengetahui seberapa tepat hasil dekripsi terhadap teks aslinya dapat diuji menggunakan Mean Absolute Error (MAE). MAE merepresentasikan rata–rata kesalahan *(error)* absolut antara hasil enkripsi atau hasil dekripsiterhadap teks asli.Nilai ini dihitung menggunakan Persamaan (4), yang secara matematis didefinisikan sebagai:

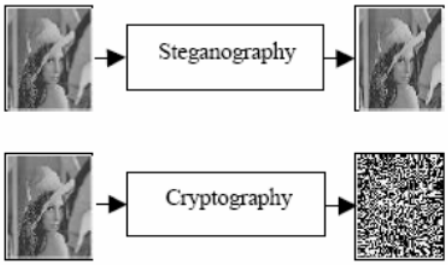
$$MAE = \frac{1}{n}\sum_{i=1}^{n}|f_i - y_i| \quad (4)$$

$f_i$adalah nilai hasil enkripsi/dekripsi sementara y_i adalah nilai karakter teks aslinya, dan n adalah jumlah seluruh karakter yang terdapat teks, dengan asumsi jumlah karakter hasil enkripsi/dekripsi sama dengan jumlah karakter pada teks aslinya.

2.2 Steganografi

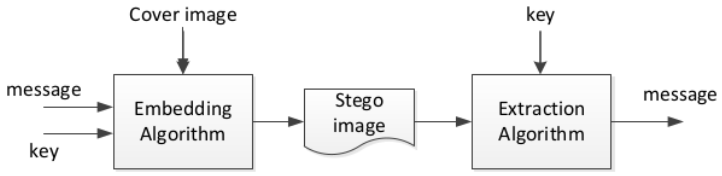
Steganografi berasal dari Bahasa Yunani steganos yang memiliki arti pesan tersembunyi, merupakan ilmu dan seni menyembunyikan pesan rahasia kedalam pesan lainnya sehingga keberadaan pesan rahasia tersebut tidak diketahui atau tidak disadari. Pada prakteknya, dalam pesan lain yang digunakan sebagai media tempat menyembunyikan pesan rahasia disebut sebagai *cover*. Cover ini dapat memiliki bentuk yang sama ataupun berbeda dari pesan yang disembunyikan. Bentuk data yang sering digunakan sebagai cover diantaranya adalah citra dan audio, dan pesan yang disembunyikan dapat berbentuk teks atau citra. Secara sederhana, ukuran cover selalu lebih besar dibanding dengan pesan yang disembunyikan.

Meskipun memiliki tujuan yang sama dengan kriptografi, yaitu untuk melindungi pesan penting atau rahasia, steganografi sangat berbeda dengan kriptografi. Jika kriptografi mengubah pesan sedemikian rupa sehingga tidak diketahui maknanya, pada steganografi pesan dilindungi dengan cara menyamarkannya ke dalam bentuk lain sehingga keberadaannya tidak disadari. Perbedaan antara antara steganografi dan kriptografi secara visual ditunjukkan pada Gambar 2.



Gambar 2. Perbedaan Steganografi dengan Kriptografi [9]

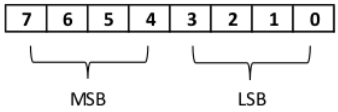
Secara umum, proses steganografi ditunjukkan pada Gambar 3. Pada gambar tersebut diasumsikan bahwa pesan yang akan disembunyikan adalah teks dan yang digunakan sebagai cover adalah citra. Proses embedding untuk menghasilkan stego-media memerlukan masukan berupa pesan yang akan disembunyikan dan cover untuk menampung pesan. Sedangkan pada proses ekstraksi, sebagai masukan adalah stego-media yang dihasilkan pada proses sebelumnya. Kunci bersifat opsional, tergantung teknik atau metoda apa saja yang terlibat pada proses steganografi tersebut.



Gambar 3. Model Steganografi

Metode LSB adalah salah satu algoritma yang banyak digunakan untuk menyembunyikan suatu pesan ke dalam cover. Steganografi dengan metode LSB dilakukan dengan cara memodifikasi bit-bit pada kelompok bit LSB pada setiap piksel yang terdapat pada cover-image. Bit-bit LSB ini dimodifikasi dengan menggantikannya dengan bit-bit pesan yang ingin disembunyikan.

Bit-bit LSB merupakan bit-bit pada posisi kanan pada barisan data biner yang nilainya dianggap kurang atau tidak signifikan. Posisi bit MSB dan LSB Gambar 4. Nilai setiap bit pada barisan data biner 8bit adalah 2 pangkat posisi dari bit tersebut. Misalkan, diketahui urutan bit biner 1001 0001, maka nilai bit pada posisi ke-7 (paling kiri) adalah 2^7, nilai bit pada posisi ke-4 adalah 2^4 dan nilai bit pada posisi ke-0 (paling kanan) adalah 2^0. Sehingga 1001 0001 merupakan representasi dari nilai desimal 145 yang diperoleh dari 128+16+1. Dari sini dapat dilihat bahwa bit-bit pada posisi MSB memiliki pengaruh yang lebih besar dibanding dengan yang berada pada posisi LSB. Bit posisi ke-7 adalah bit yang memiliki pengaruh paling besar, sebaliknya bit posisi ke-0 adakah bit yang memiliki pengaruh paling kecil.



Gambar 4. Posisi bit-bit MSB dan LSB

Perubahan nilai bit pada kelompok LSB ini memberi pengaruh yang relatif tidak signifikan. Steganografi menggunakan metoda LSB hanya memodifikasi nilai bit pada kelompok LSB. Dalam perspektif intensitas warna pada citra, perubahan nilai pada kelompok LSB ini relatif sulit dibedakan secara visual. Sebagai contoh, misalkan huruf A yang memiliki nilai ASCII 65 akan disembunyikan pada piksel-piksel berwarna hitam mulai piksel ke-10 sampai piksel ke-17. Modifikasi hanya dilakukan pada satu bit terakhir setiap piksel, ilustrasi penempatan setiap bit huruf A ke dalam 8 piksel pada cover ditunjukkan pada Gambar 5. Disini terlihat dari 8 piksel yang dimodifikasi, perubahan hanya terjadi pada piksel saja, yaitu piksel ke-11 dan piksel ke-17 karena hanya kedua bit tersebut yang memiliki nilai bit yang berbeda.

Gambar 5.Ilustrasi penyembunyian huruf A ke dalam cover

Penggunaan metoda LSB yang memodifikasi bit terakhir pada citra, secara visual tidak menunjukkan perbedaan dengan citra aslinya. Namun metoda ini memiliki kekurangan diantaranya dari sisi keandalannya. Metoda LSB ini sangat sensitif terhadap proses *filtering*, *scalling*, rotasi atau *cropping* yang dapat mengakibatkan kerusakan pada pesan yang telah sembunyikan.

Pengukuran kualitas citra hasil steganografi dilakukan menggunakan Peak Signal to Noise Ratio (PNSR), dimana untuk mendapatkan nilai PNSR tersebut terlebih dulu dihitung nilai MSE-nya. MSE dihitung menggunakan Persamaan (4) dan PNSR dihitung menggunakan Persamaan (5).

$$MSE = \frac{1}{m \times n} \sum_{i=0}^{m} \sum_{j=0}^{n} \left(X_{ij} - X'_{ij} \right)^2 \quad (4)$$

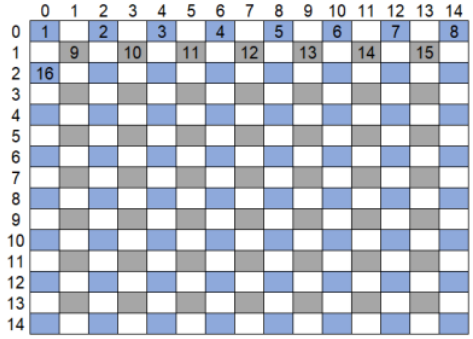
$$PNSR = 10 \log_{10} \frac{I^2}{MSE} \quad (5)$$

X_{ij} adalah intensitas piksel baris ke *i* dan kolom ke *j* dari *cover-image*, X'$_{ij}$ adalah intensitas piksel baris ke *i* dan kolom ke *j* dari *stego-image*, *m* dan *n* adalah ukuran baris dan kolom *cover-image*, dan *I* adalah intensitas piksel maksimum. Untuk citra 8 bit maka *I* = 255. Semakin besar PSNR (semakin kecil MSE) maka kualitas *stego image*akan semakin baik. Nilai PSNR yang diharapkan adalah di atas 50dB lebih tinggi dibanding dengan penelitian yang sudah ada sebelumnya [10], [11].

2.3 LSB dengan pola genap ganjil

Penyembunyian pesan dilakukan dengan cara mengganti satu bit terakhir dari nilai piksel cover dengan satu bit pesan yang disembunyikan. Pesan yang disembunyikan adalah hasil enkripsi menggunakan affine cipher. Posisi piksel yang digunakan untuk penyembunyian pesan mengkuti pola genap ganjil. Yang dimaksud dengan pola genap ganjil ini adalah untuk setiap baris genap, modifikasi hanya dilakukan pada kolom genap. Dan untuk setiap baris ganjil, modifikasi hanya dilakukan pada kolom ganjil juga. Secara visual, pola ini

ditunjukkan pada Gambar 6. Urutan modifikasi dilakukan dari kiri ke kanan dan dari atas ke bawah yang ditunjukkan dengan angka satu sampai 16. Dengan pola genap ganjil ini, jumlah piksel yang dapat digunakan untuk penyembunyian pesan adalah 50% dari jumlah piksel secara keseluruhan.



Gambar 6. Pola posisi piksel tempat peyembunyian pesan

Pada penelitian ini, data yang disembunyikan dibedakan menjadi dua, yaitu panjang pesan dan isi pesan itu sendiri. Panjang pesan disimpan sebagai integer 16 bit dan disembunyikan pada komponen R, sementara setiap karakter pesan disimpan sebagai data 8 bit dan disembunyikan pada komponen B. Komponen R dan B digunakan sebagai tempat penyembunyian pesan, karena perubahan nilai pada kedua komponen ini memberi pengaruh visual yang lebih rendah dibandingkan dengan perubahan pada komponen G.

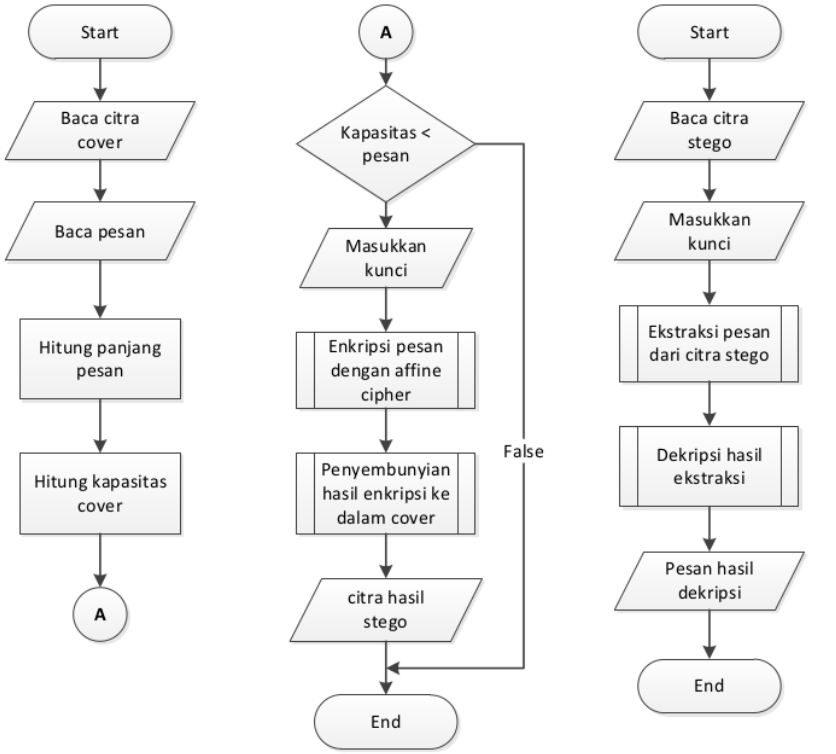
4. HASIL DAN PEMBAHASAN

Proses penyembunyian pesan terenkripsi ke dalam citra dilakukan dengan mengikuti alur yang tunjukkan pada flowchart pada Gambar 7. Dimulai dengan membaca citra yang digunakan sebagai cover dan pesan yang disimpan sebagai file teks. Dilanjutkan dengan menghitung panjang pesan yang akan disembunyikan serta menghitung daya tampung pada cover. Penyembunyian pesan hanya dapat dilakukan jika kapasitas daya tampung lebih besar atau sama dengan panjang pesan yang akan disembunyikan.

Setelah syarat kecukupan kapasitas terpenuhi, kemudian dimasukkan pasangan kunci yang digunakan untuk melakukan proses enkripsi. Pesan asli dienkripsi dengan Affine cipher menggunakan kunci yang diberikan. Hasil enkripsi inilah yang selanjutnya disembunyikan ke dalam cover. Hasil steganografi adalah berupa citra RGB yang sering juga disebut sebagai *stegoimage*.

Dalam penelitian ini, digunakan dua citra yang berukuran sama yaitu 500 x 400 piksel yang memiliki karakteristik warna yang berbeda. Citra pertama memiliki ragam warna yang kaya dibandingkan dengan citra ke dua yang terlihat hampir monoton. Kedua citra mampu menampung sampai 12500 karakter, yang merupakan setengah dari hasil perkalian resolusi piksel dibagi delapan bit.

Data yang akan disembunyikan ke dalam cover, disimpan dalam enam file teks yang berbeda yang masing-masing mewakili jumlah karakter tertentu, yaitu mulai sekitar 2% sampai dengan mendekati 100% dari kapasitas cover. Perbedaan jumlah karakter ini bertujuan untuk mengetahui penurunan kualitas citra terhadap peningkatan jumlah data yang disembunyikan. Pasangan kunci yang digunakan adalah m=7 dan b=12. Contoh hasil enkripsi untuk teks pertama yang teridiri dari 247 karakter ditunjukkan pada Gambar 8.



Gambar 7. Proses penyembunyian (a) dan ekstraksi pesan (b)

Ada teknik lain yang dapat digunakan untuk mengamankan informasi salah satunya adalah steganografi, teknik ini digunakan untuk menyembunyikan informasi rahasia ke dalam suatu media sehingga keberadaan pesan tersebut tidak diketahui oleh orang lain

SH3180y♬ky1 3k♬1[3♬]1H3└381Hk]?♬
3y3♬1?♬8?
y1•O♬]3•3♬y3♬1k♬V┴*•31k113 3d1138?♬
[313H3 3d1180]3♬┴]*3Vk@180y♬ky1k♬k1Hk]
?♬3y3♬1?♬8?y1•O♬[O•:?♬
[ky3♬1k♬V┴*•31k1*3d31k31yO1H3 3•11?38?
1•OHk311Odk♬]]31yO:O*3H33♬1└O13♬180*10
:?818kH3y1HkyO83d?k1┴ Od1┴*3♬]1 3k♬

Gambar 8. Teks asli (kiri) dan hasil enkripsi (kanan)

Pengujian hasil enkripsi mengunakan MAE ditunjukkan pada Tabel 1. Untuk memudahkan pengujian, teks asli dan hasil enkripsi disimpan sebagai file teks. Selisih rata-rata jumlah karakter pada file ke- dan ke-2, ke-2 dan ke-3 dan seterusnya adalah sebanyak 2500 karakter. Hasil pengujian menunjukkan bahwa perubahan hasil enkripsi dari terhadap teks aslinya relatif konstan. Terlihat bahwa peningkatan jumlah karakter yang dienkripsi tidak memiliki pengaruh signifikan terhadap perubahan nilai MAE.

Tabel 1. Hasil pengujian pesan

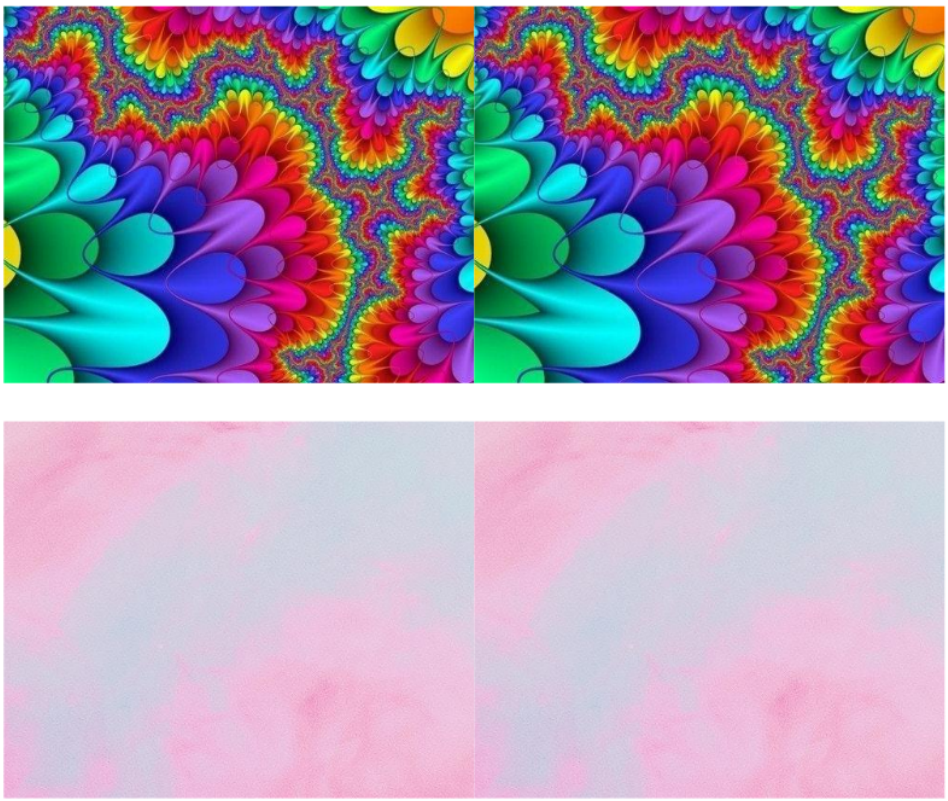
Plainteks	Nama File (cipherteks)	Jumlah Karakter	MAE
Pesan1.txt	Pesan1_e.txt	247	51.3765

Pesan2.txt	Pesan2_e.txt	2500	50.8648
Pesan3.txt	Pesan3_e.txt	5000	51.1736
Pesan4.txt	Pesan4_e.txt	7500	51.1955
Pesan5.txt	Pesan5_e.txt	10000	50.9990
Pesan6.txt	Pesan6_e.txt	12000	51.2622

Hasil pengujian kualitas citra hasil steganografi ditunjukkan pada pada Tabel 2, dan secara visual perbandingan citra sebelum dan sesudah pesan disembunyikan ditunjukkan pada Gambar 9. Data yang disembunyikan ke dalam kedua cover tersebut adalah sebanyak 12000 karakter.Sebagai gambaran, rata-rata jumlah huruf dan karakter pada satu halaman teks ukuran A4 yang diketik dengan font Times New Roman 12pt dengan jarak satu spasi berkisar antara 2700 sampai 2900 karakter.

Tabel 2. Hasil pengujian citra hasil steganografi

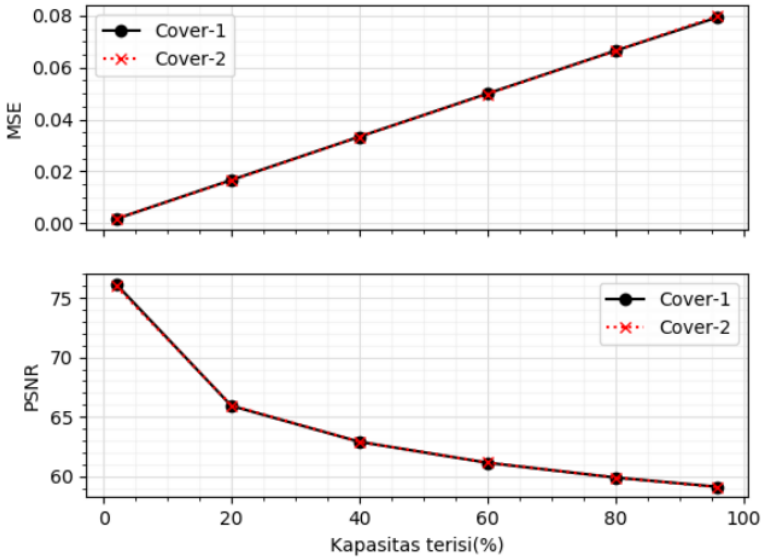
Ciphertext	Jumlah karakter	Kapasitas terisi (%)	Cover-1		Cover-2	
			MSE	PSNR	MSE	PSNR
pesan1_e.txt	247	1.98	0.0016	76.1580	0.0016	75.9824
pesan2_e.txt	2500	20.00	0.0166	65.9241	0.0164	65.9735
pesan3_e.txt	5000	40.00	0.0333	62.9051	0.0333	62.9055
pesan4_e.txt	7500	60.00	0.0500	61.1447	0.0498	61.1582
pesan5_e.txt	10000	80.00	0.0665	59.9024	0.0665	59.9055
pesan6_e.txt	12000	96.00	0.0794	59.1309	0.0800	59.1003



Gambar 9. Citra asli (kiri) dan citra hasil steganografi (kanan)

Secara visual tidak terlihat perbedaan antara citra sebelum dan sesudah dilakukan penyembunyian pesan, meskipun jumlah data yang disembunyikan cukup besar. Jumlah karakter yang disembunyikan pada kedua citra pada Gambar 9 tersebut lebih kurang sebanyak empat halaman teks ukuran A4. Kondisi ini memenuhi salah satu kriteria steganografi yang baik, yaitu imperceptible yang berarti hasil steganografi tidak mudah dikenali dengan menggunakan panca indra, dalam hal ini indra visual.

Perubahan nilai MSE linier dengan peningkatan jumlah data yang disembunyikan ke dalam cover, yang ditunjukkan oleh grafik pada Gambar 10. Peningkatan nilai MSE ini berakibat pada penurunan PNSR yang mewakili kualitas dari citra. Berbeda dengan MSE yang mengalami perubahan linier terhadap perubahan kapasitas data, perubahan nilai PNSR bersifat logaritmik. Untuk kapasitas penyembunyian pesan mendekati 100% dari kapasitas maksimum yang dapat ditampung, nilai PNSR masih jauh lebih tinggi dibanding nilai yang dijadikan sebagai tolok ukur. PNSR terendah untuk kedua cover yang digunakan masih berada pada kisaran 59dB, jauh lebih berada diatas 50dB yang dijadikan sebagai tolok ukur.



Gambar 10. Perubahan nilai MSE dan PSNR karena perubahan kapasitas terisi

Hasil pengujian ini membuktikan bahwa kriteria steganografi berikutnya, yaitu *fidelity* yang berarti tidak terjadi penurunan kualitas yang signifikan pada cover, juga terpenuhi. Kriteria lain dari steganografi adalah recovery. Recovery berarti data yang disembunyikan harus dapat diambil kembali atau diekstraksi. Dalam hal ini, merujuk pada aliran proses pada Gambar 7, kriteria ini dapat dianggap juga terpenuhi. Karena sama halnya pada kriptografi, setiap data yang dienkripsi harus dapat dekripsi dengan tepat. Maka pada steganografi, setiap data yang disembunyikan juga harus dapat ditemukan kembali dengan tepat.

4. KESIMPULAN

Penelitian ini menunjukkan bahwa penyembunyian pesan terenkripsi menggunakan LSB dapat saling menutupi kekurangannya masing-masing. Data acak yang biasanya merupakan hasil engkripsi tersamarkan dalam steganografi, sementara data pada steganografi yang biasanya dalam keadaan 'apa adanya" juga terlindungi karena telah dilakukan enkripsi. Pengujian menunjukkan bahwa tidak terjadi penurunan kualitas citra yang signifikan, baik secara visual maupun dilihat dari nilai PNSR, dimana nilai PNSR terendah masih berada pada kisaran 59 dB. Namun penggunaan pola genap ganjil berpengaruh pada menurunnya jumlah data yang dapat disembunyikan ke dalam cover. Untuk mengatasi kekurangan ini, pada penelitian selanjutnya akan diteliti penggunaan komponen warna lainnya sebagai tempat penyembunyian isi pesan.

DAFTAR PUSTAKA

[1] N. D. Nathasia and A. E. Wicaksono, "Penerapan Teknik Kriptografi Stream - Cipher Untuk Pengamanan Basis Data," *Basis Data, ICT Res. Cent. UNAS*, vol. 6, no. No. 1, p. 22, 2011.

[2] T. Limbong and P. D. P. Silitonga, "Testing the Classic Caesar Cipher Cryptography using of Matlab,"

Int. J. Res. Technol., vol. 6, no. 2, pp. 175–178, 2017.

[3] S. A. Babu, "Modification Affine Ciphers Algorithm For Cryptography Password," *Int. J. Res. Sci. Eng.*, vol. 3, no. 2. April, p. [346-351, 2017.

[4] M. M. Assyahid, R. Rihartanto, and D. S. B. Utomo, "Implementasi Steganografi Pesan Text ke Dalam Audio Dengan Metode Spread Spectrum," in *Prosiding Seminar Nasional Ilmu Komputer dan Teknologi Informasi (SAKTI)*, 2018, vol. 3, no. 2, pp. 27–34.

[5] M. Wakiyama, Y. Hidaka, and K. Nozaki, "An audio steganography by a low-bit coding method with wave files," *Proc. - 2010 6th Int. Conf. Intell. Inf. Hiding Multimed. Signal Process. IIHMSP 2010*, pp. 530–533, 2010.

[6] B. S. Champakamala, K. Padmini, and D. K. Radhika, "Least Significant Bit algorithm for image steganography Overview of Steganography," *Int. J. Adv. Comput. Technol.*, vol. 3, no. 4, pp. 34–38, 2014.

[7] S. A. Patil and K. P. Adhiya, "Hiding Text in Audio Using LSB Based Steganography," *Inf. Knowl. Manag.*, vol. 2, no. 3, pp. 8–15, 2012.

[8] Y. Antika, "Implementasi Algoritma Affine Cipher Dan Tripple DES Dalam Mengamankan File Image," *Maj. Ilmiah INTI*, vol. 14, no. 2, pp. 200–206, 2019.

[9] Y. Aditya, A. Pratama, and A. Nurlifa, "Studi pustaka untuk steganografi dengan beberapa metode," in *Seminar Nasional Aplikasi Teknologi Informasi 2010 (SNATI 2010)*, 2010, pp. 32–35.

[10] Li and A. Lu, "LSB-based Steganography Using Reflected Gray Code for Color Quantum Images," *Int. J. Theor. Phys.*, vol. 57, no. 5, pp. 1516–1548, 2018.

[11] Pandian, "An Image Steganography Algorithm Using Huffman and Interpixel Difference Encoding," *Int. J. Comput. Sci. Secur.*, vol. 8, no. 6, pp. 202–215, 2014.

STEGANOGRAFI PESAN TERENKRIPSI AFFINE CIPHER MENGGUNAKAN METODA LSB DENGAN POLA GENAP GANJIL

ORIGINALITY REPORT

13%	10%	5%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas 17 Agustus 1945 Surabaya Student Paper	2%
2	Submitted to Padjadjaran University Student Paper	1%
3	mti.kominfo.go.id Internet Source	1%
4	Dedy Abdullah, Doni Nugroho Saputro. "IMPLEMENTASI ALGORITMA BLOWFISH DAN METODE LEAST SIGNIFICANT BIT INSERTION PADA VIDEO MP4", Pseudocode, 2017 Publication	1%
5	Muhammad Harith Noor Azam, Farida Ridzuan, M Norazizi Sham Mohd Sayuti, Ahmed A. Alsabhany. "Balancing the Trade-Off Between Capacity and Imperceptibility for Least Significant Bit Audio Steganography Method: A New Parameter", 2019 IEEE Conference on Application, Information and Network Security (AINS), 2019	1%

	Publication	
6	thousands-passed.xyz Internet Source	1 %
7	e-journals.unmul.ac.id Internet Source	1 %
8	media.neliti.com Internet Source	1 %
9	Amna Shifa, Muhammad S. Afgan, Mamoona N. Asghar, Martin Fleury, Imran Memon, Saima Abdullah, Nadia Rasheed. "Joint Crypto-Stego Scheme for Enhanced Image Protection With Nearest-Centroid Clustering", IEEE Access, 2018 Publication	1 %
10	zombiedoc.com Internet Source	<1 %
11	www.unisbank.ac.id Internet Source	<1 %
12	Rama Prameswara Ritonga, Muhammad Zarlis, Erna Budhiarti Nababan. "Modification Affine Cipher Transform Digraph to Squared the value of ‘n’ in Text Security", 2020 4rd International Conference on Electrical, Telecommunication and Computer Engineering (ELTICOM), 2020 Publication	<1 %

13	Submitted to UIN Syarif Hidayatullah Jakarta Student Paper	<1 %
14	Tika Erna Putri, Muhammad Rifqi Al Fauzan, Prima Asmara Sejati. "PERBAIKAN ALGORITMA STEGANOGRAFI TEKNIK LEAST SIGNIFICANT BITS UNTUK APLIKASI KEAMANAN DATA", JOURNAL ONLINE OF PHYSICS, 2018 Publication	<1 %
15	eprints.umg.ac.id Internet Source	<1 %
16	Submitted to Universitas Dian Nuswantoro Student Paper	<1 %
17	Yugendra Chincholkar, Sanjay Ganorkar. "Audio Watermarking Algorithm Implementation using Patchwork Technique", 2019 IEEE 5th International Conference for Convergence in Technology (I2CT), 2019 Publication	<1 %
18	khairunnisanur.wordpress.com Internet Source	<1 %
19	Submitted to CONACYT Student Paper	<1 %
20	docplayer.info Internet Source	<1 %
	ejournal3.undip.ac.id	

21	Internet Source	<1%
22	jurnal.untan.ac.id Internet Source	<1%
23	sintak.unisbank.ac.id Internet Source	<1%
24	M. Anusha, K. N. Bhanu, D. Divyashree. "Secured Communication of Text and Audio using Image Steganography", 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 2020 Publication	<1%
25	ejournal.unida.gontor.ac.id Internet Source	<1%
26	text-id.123dok.com Internet Source	<1%
27	"Authentication Aspects of Dynamic Routing Protocols: Associated Problem & Proposed Solution", International Journal of Recent Technology and Engineering, 2019 Publication	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		