Implementasi Sistem Keamanan Pesan Text Dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)

Apriansyah[1], Mitra Unik[2], Harun Mukhtar [3]
[1,2,3] Fakultas Ilmu Komputer, Universitas Muhammadiyah Riau (penulis 1)
email : apriansyah@student.umri.ac.id [1], mitraunik@umri.ac.id[2], harunmukhtar@umri.ac.id[3]

Abstract

Indonesia, most cyber incidents reported by respondents relate to loss or leakage of business information such as internal records, information related to customers, employees and intellectuals. This worries the misuse of information held by irresponsible parties. in order to protect information so that it is not misused by unauthorized parties, then an attempt is made to hide the actual information on other information called steganography by using the Least Significant bit (LSB) method and to see the image quality value containing the message using the MSE calculation (Mean Square Error) and PSNR (Peak signal to noise ratio). The process of inserting messages is successfully carried out and produces extraction steganographic images. From testing the picture it can be concluded that the results of the steganography application must be invisible or not visible in plain view, as the purpose of this study is to increase the security sent to arrive at the recipient.

Keywords: *Image, LSB, MSE, PSNR, Steganografy.*

Abstrak

Di Indonesia, sebagian besar insiden siber yang dilaporkan oleh para responden berkaitan dengan kehilangan atau kebocoran informasi bisnis seperti catatan internal, informasi terkait pelanggan, karyawan dan intelektual. Hal ini membuat kekhawatiran dalam penyalahgunaan informasi yang dimiliki oleh pihak-pihak yang tidak bertanggung jawab. demi melindungi informasi agar tidak disalah gunakan oleh pihak yang tidak berkepentingan, maka dilakukanlah satu usaha menyembunyikan informasi yang sebenarnya pada informasi lain yang di sebut steganografi dengan menggunakan metode Least significan bit (LSB) dan Untuk melihat nilai kualitas gambar yang berisi pesan menggunakan perhitungan nilai MSE (Mean Square Error) dan PSNR (Peak signal to noise ratio). Proses penyisipan pesan berhasil dilakukan dan menghasilkan gambar steganografi yang ekstraksi. Dari pengujian gambar dapat disimpulkan bahwa hasil aplikasi steganografi pasti invisible atau tidak terlihat secara kasat mata, seperti tujuan penelitian ini yaitu meningkatkan kemanan yang dikirim agar sampai kepada penerima.

Kata Kunci: *Steganografi, LSB, Image, MSE, PSNR*

PENDAHULUAN

Berkembangnya teknologi informasi melalui jaringan internet membuat pertukaran informasi semakin cepat dan akurat serta terbuka melewati batas-batas negara. Berikut ini adalah trafik penggunaan internet didunia. Berdasarkan Hasil data trafik penggunaan internet pada[1], bahwa Indonesia termasuk dalam 5 besar pengguna internet didunia, yang dapat dilihat pada gambar 1.1 dibawah ini:

TOP 20 COUNTRIES WITH HIGHEST NUMBER OF INTERNET USERS - JUNE 30, 2017

#	Country or Region	Population, 2017 Est.	Internet Users 30 June 2017	Internet Penetration	Growth (*) 2000 - 2017	Facebook 30 June 2017
1	China	1,388,232,693	738,539,792	53.2 %	3,182.4 %	1,800,000
2	India	1,342,512,706	462,124,989	34.4 %	9,142.5 %	241,000,000
3	United States	326,474,013	286,942,362	87.9 %	200.9 %	240,000,000
4	Brazil	211,243,220	139,111,185	65.9 %	2,682.2 %	139,000,000
5	Indonesia	263,510,146	132,700,000	50.4 %	6,535.0 %	126,000,000
6	Japan	126,045,211	118,453,595	94.0 %	151.6 %	26,000,000
7	Russia	143,375,006	109,552,842	76.4 %	3,434.0 %	12,000,000
8	Nigeria	191,835,936	91,598,757	47.7 %	45,699.4 %	16,000,000
9	Mexico	130,222,815	85,000,000	65.3 %	3,033.8 %	85,000,000
10	Bangladesh	164,827,718	73,347,000	44.5 %	73,247.0 %	21,000,000
11	Germany	80,636,124	72,290,285	89.6 %	201.2 %	31,000,000
12	Vietnam	95,414,640	64,000,000	67.1 %	31,900.0 %	64,000,000
13	United Kingdom	65,511,098	62,091,419	94.8 %	303.2 %	44,000,000
14	Philippines	103,796,832	57,607,242	55.5 %	2,780.4 %	69,000,000
15	Thailand	68,297,547	57,000,000	83.5 %	2,378.3 %	57,000,000
16	Iran	80,945,718	56,700,000	70.0 %	22,580.0 %	17,200,000
17	France	64,938,716	56,367,330	86.8 %	563.1 %	33,000,000
18	Turkey	80,417,526	56,000,000	69.6 %	2,700.0 %	56,000,000
19	Italy	59,797,978	51,836,798	86.7 %	292.7 %	30,000,000
20	Korea, South	50,704,971	47,013,649	92.7 %	146.9 %	17,000,000
TOP 20 Countries		5,038,740,614	2,818,277,245	55.9 %	944.1 %	1,326,000,000
Rest of the World		2,480,288,356	1,067,290,374	43.0 %	1,072.2 %	653,703,530
Total World Users		7,519,028,970	3,885,567,619	51.7 %	976.4 %	1,979,703,530

Gambar 1. Trafik Internet Dunia

Di Indonesia, sebagian besar insiden siber yang dilaporkan oleh para responden berkaitan dengan kehilangan atau kebocoran informasi bisnis seperti catatan internal, informasi terkait pelanggan, karyawan dan intelektual. Hal ini membuat kekhawatiran dalam penyalahgunaan informasi yang dimiliki oleh pihak-pihak yang tidak bertanggung jawab. Tetapi kebutuhan memaksa mereka untuk tetap menggunakan fasilitas internet sehingga muncul usaha untuk mengamankan data agar sampai kepada penerima dengan aman. mengindikasikan perlunya memperkuat perlindungan terhadap aset informasi dan privasi. [3].

Demi melindungi informasi agar tidak disalah gunakan oleh pihak yang tidak berkepentingan, maka dilakukanlah satu usaha menyembunyikan informasi yang sebenarnya pada informasi lain yang di sebut steganografi. Teknik steganografi menggunakan dua media yang berbeda secara bersamaan, dimana salah satunya berfungsi sebagai media yang berisikan informasi informasi rahasia (dapat juga disebut *secret file*) dan yang lain berfungsi sebagai media pembawa informasi tersebut (*carrier file*). Dengan menggunkan Metode *least significan bit* (LSB), dimana metode ini digunakan untuk teknik penyisipan pesan. Cara kerja metode LSB yaitu mengubah *bit* redundan *cover image* yang tidak berpengaruh signifikan dengan bit dari pesan rahasia. Dengan menggunakan algoritma LSB (*Least Significant Bit*) *Embedding Process* akan lebih kuat.[4]

LANDASAN TEORI

1. Steganografi

Steganografi (*steganography*) adalah ilmu, teknik atau seni menyembunyikan pesan rahasia (hiding message) atau tulisan rahasia (*covered writing*) sehingga keberadaan pesan tidak terdeteksi orang lain kecuali pengirim dan penerima pesan tersebut. Steganografi berasal dari bahasa Yunani yaitu steganos (tersembunyi/menyembunyikan) dan graphy (tulisan), sehingga secara lengkap bermakna tulisan yang disembunyikan.[5]

Steganografi adalah suatu teknik untuk menyembunyikan informasi pribadi dengan sesuatu yang hasilnya akan tampak seperti informasi normal lainnya. (Arubusman, 2007) Steganografi adalah ilmu dan seni menyembunyikan pesan rahasia (hiding message) sedemikian sehingga keberadaan (eksistensi) pesan yang tidak terdeteksi oleh indera manusia. [6]

Steganografi merupakan cabang ilmu yang mempelajari bagaimana menyimpan informasi rahasia di dalam informasi lainnya.[7]

Kriteria dan Aspek dalam Steganografi

Penyembunyian data rahasia ke dalam media digital mengubah kualitas media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data diantaranya adalah:

a. **Fidelity**. Mutu citra penampung tidak jauh berubah. Setelah penambahan data rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui kalau di dalam citra tersebut terdapat data rahasia.
b. **Robustness**. Data yang disembunyikan harus tahan terhadap manipulasi yang dilakukan pada citra penampung (seperti pengubahan kontras, penajaman, pemampatan, penambahan noise, perbesaran gambar, pemotongan (cropping), enkripsi, dan sebagainya). Bila pada citra dilakukan operasi pengolahan citra, maka data yang disembunyikan tidak rusak.
c. **Recovery**. Data yang disembunyikan harus dapat diungkapkan kembali (recovery). Karena tujuan steganografi adalah data hiding, maka sewaktu-waktu data rahasia di dalam citra penampung harus dapat diambil kembali untuk digunakan lebih lanjut

Steganografi digital menggunakan media digital sebagai wadah penampung, misalnya citra, suara, teks, dan video. Sedangkan data rahasia yang disembunyikan dapat berupa berkas apapun. Media yang telah disisipi data disebut stegomessage. Proses penyembunyian data ke dalam media disebut penyisipan (*embedding*), sedangkan proses sebaliknya disebut ekstraksi. Penambahan kunci yang bersifat opsional dimaksudkan untuk lebih meningkatkan keamanan. [8]

2. Algoritma Hill Chiper

Algoritma Hill Chiper adalah suatu fungsi matematis yang digunakan untuk melakukan enkripsi dan dekripsi.[9] Sejak kekaisaran Romawi, kriptosistem yang lebih rumit dikembangkan oleh orang seperti oleh ahli

Matematika Italia Leon Battista Alberti (lahir pada tahun 1404), Matematikawan Jerman Johannes Trithernius (lahir pada tahun 1492), seorang kriptographer dan diplomat Perancis Blaise de Vigenére (1523−1596), Lester S. Hill, yang menemukan Hill Cipher (Hill Cipher) pada tahun 1929. Hill Cipher merupakan jenis lain dari polygraphic cipher. Sandi ini mengenkripsi suatu string huruf menjadi bentuk string yang lain dengan panjang yang sama. [10]. Hill Cipher menggunakan matriks untuk mentransformasi string berupa blok huruf. Hill Cipher berdasarkan pada aljabar linier dan seperti sandi Vigenére, Hill Cipher merupakan block cipher. Sandi ini dapat dipecahkan dengan known-plaintext attacks tetapi tahan melawan ciphertext-only attack. Cara kerja sandi ini berdasarkan atas perkalian matriks dengan menggunakan sebuah kunci K. Penjelasan mengenai Hill Cipher ini dapat diuraikan sebagai berikut: Misalkan m adalah bilangan bulat positif dan P = C = (Z26)m dan misalkan K = {m x m meripakan matriks yang nilai elemenya terdiri dari Z26| maka untuk suatu kunci K, dapat didefenisikan sebagai ek (x) Mod 26 dan dk (y) = k-1 y Mod 26 dimana semua operasi dilakukan dalam matrix Z¬26.

a. Rumus enkripsi

$C = K.P$

C = Ciphertext
K = Kunci
P = Plaintext

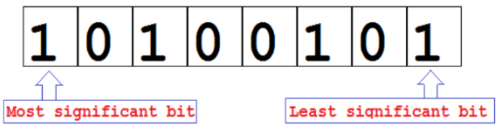
b. Rumus dekripsi

$P = K^{-1}.C$

3. LSB (Least Significant Bit)

Metode LSB *(Least Significant Bit)* dipergunakan untuk menyembunyikan data dengan mengganti bit-bit data yang paling tidak berarti di dalam *cover* dengan bit-bit data rahasia [11]. Konsep kerja metode *Least Significant Bit* (LSB) dalam melakukan penyisipan pesan ke dalam media citra adalah melakukan modifikasi terhadap bit-bit setiap piksel citra yang menjadi *cover* (citra penampung pesan). Bit paling akhir *(least)* dari setiap piksel akan digantikan dengan bit - bit dari pesan yang akan disembunyikan. Proses pengungkapan atau pengambilan pesan dari dalam citra penampung dilakukan dengan mengambil bit-bit piksel citra hasil yang berada pada posisi akhir, kemudian dikonversikan menjadi karakter. Proses utama dalam metode LSB adalah proses *embedding* dan proses *ekstraction* [12].

Pada penelitian ini, akan digunakan metode LSB (Least Significant Bit) yang merupakan teknik penyembunyian data yang bekerja pada domain spatial atau waktu. Untuk menjelaskan teknik penyembunyian LSB yang dipakai ini kita menggunakan citra digital sebagai covertext. Setiap pixel yang ada di dalam file citra berukuran 1 sampai 3 byte. Pada susunan bit dalam setiap byte (1 byte = 8 bit) , ada bit yang paling berarti (most significant bit atau MSB) dan bit yang paling kurang berarti (least significant bit atau LSB).



Gambar 2. Contoh LSB dan MSB

HASIL DAN PEMBAHASAN

1. **Langkah Perhitungan Algoritma Hill Cipher**

Proses pertama adalah mengubah plain text (pesan) menjadi deretan angka sesuai dengan tabel di bawah ini :

Tabel 1. Merubah Plain Text (Pesan) Menjadi Deretan Angka

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Sebagai contoh : plain text TIF UMRI menjadi : 19, 8, 5, 20, 12, 17, 8.

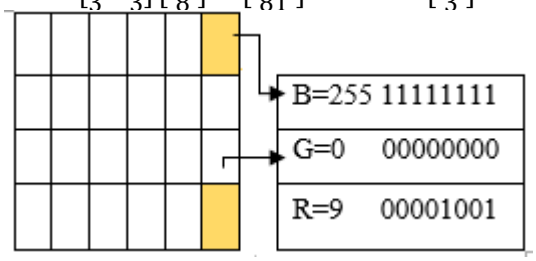
Langkah selanjutnya adalah membagi deretan angka tadi menjadi blok matriks yang sesuai dengan jumlah kolom matriks kunci (2).

Pembagian blok

TI = 19 / 8 FU = 5 / 20 MR = 12 / 17 I = 8

Memulai proses enkripsi (Matriks kunci * blok matriks(Plain text)) C(TI) :

$$\begin{bmatrix}4 & 3\\ 3 & 3\end{bmatrix}\begin{bmatrix}19\\ 8\end{bmatrix} = \begin{bmatrix}100\\ 81\end{bmatrix} mod 26 = \begin{bmatrix}22\\ 3\end{bmatrix}$$



C(FU):

$$\begin{bmatrix}4 & 3\\ 3 & 3\end{bmatrix}\begin{bmatrix}5\\ 20\end{bmatrix} = \begin{bmatrix}80\\ 75\end{bmatrix} mod26 = \begin{bmatrix}2\\ 23\end{bmatrix}$$

C(MR):

$$\begin{bmatrix}4 & 3\\ 3 & 3\end{bmatrix}\begin{bmatrix}12\\ 17\end{bmatrix} = \begin{bmatrix}99\\ 87\end{bmatrix} mod26 = \begin{bmatrix}21\\ 9\end{bmatrix}$$

C(I):

$$\begin{bmatrix}4 & 3\\ 3 & 3\end{bmatrix}\begin{bmatrix}8\\ 25\end{bmatrix} = \begin{bmatrix}107\\ 99\end{bmatrix} mod26 = \begin{bmatrix}3\\ 21\end{bmatrix}$$

Maka cipher text = 22, 3, 2, 23, 21, 9, 3, 21 = WDCXVJD

2. Langkah Perhitungan LSB

Proses penggantian nilai piksel gambar dengan metode LSB, baca nilai RGB gambar yang digunakan, kemudian ubah nilai gambar tersebut kedalam nilai biner, kemudian gabungkan nilai pesan, kunci dan ubah menjadi nilai biner. Berikut adalah langkah perhitungan LSB dari hasil *mixcolumns*.

A0	7D	63	9A
1	22	D0	1A
11	6C	F1	D5
59	78	65	DD

A0	A = 65	100000001
	0 = 0	000000000

Pesan yang akan disembunyikan adalah A0 dengan merubah pesan ke nilai desimal kemudian dirubah kedalam nilai 8 bit. Tiga bit paling yang akan dimasuk kedalam bit piksel gambar. Gambar mengunakan RGB 6 x 4 piksel, dengan simulasi gambar berwarna biru dengan nilai R = 9, G = 0, B =255 pada kolom bit piksel yang akan digunkan.

Tablet 2. Perubahan Nilai RBG

	B	**G**	**R**
Piksel	11111111	00000000	00001001
A	1111111**1**	0000000**0**	0000100**0**
	1111111**0**	0000000**0**	0000100**0**
	1111111**0**	0000000**1**	

Tabel diatas memperlihatkan perubahan nilai bit piksel warna yang dimasukan pesan, terdapat perubahan nilai akhir bit pikselwarna. Perubahan nilai bit yang terjadi tidak signifikan, hingga masih terlihat sama dengan nilai bit piksel warna sebelum dirubah.

KESIMPULAN DAN SARAN

Berdasarkan hasil peneitan yang dilakukan system keamanan pesan dengan teknik steganografi dengan menggunakan metode LSB diperoleh kesimpulan sebagai berikut :

1. Pesan berhasil disisip kedalam citra gambar dengan metode least significant bit (LSB) dan algoritma hill cipher.
2. Dari pengujian gambar dapat disimpulkan bahwa hasil aplikasi steganografi pasti invisible atau tidak terlihat secara kasat mata, seperti tujuan penelitian ini yaitu meningkatkan kemanan yang dikirim agar sampai kepada penerima.
3. Dari pengujian MSE dan PSNR dapat disimpulkan bahwa ukuran pixel sangat mempengaruhi banyak text yang dapat disisip ke dalam citra gambar.

Saran

Aplikasi *steganography* ini masih mempunyai banyak kekurangan, sehingga perlu dikembangkan lagi agar aplikasi ini dapat lebih sempurna. Untuk meningkatkan kualitas dan fungsionalitas dari aplikasi *steganography* ini, maka penulis menyampaikan saran-saran sebagai berikut :

1. Media penampung pesannya tidak hanya menggunakan citra .BMP saja, tetapi menggunakan citra yang lain dan juga dapat menggunakan file audio atau video.
2. Jumlah pesan yang disisipkan kedalam citra tidak hanya satu atau dua pesan saja, tetapi dapat disesuaikan jumlahnya oleh pengguna.
3. Dibutuhkan metode steganography lain yang lebih tahan terhadap manipulasi citra.

DAFTAR PUSTAKA

[1] www.internetworldstats.com, “top 20 countries with the highest number of internet users,” 2018.

[2] E. S. Wijaya and Y. Prayudi, “Konsep Hidden Message Menggunakan Teknik,” *Media Inform.*, vol. 2, no. 1, pp. 23–38, 2004.

[3] www.pwc.com, “Menurut Survei PwC, Para Eksekutif di Indonesia Manfaatkan Teknologi Baru untuk Mengelola Ancaman Siber dan Mencapai Keunggulan Kompetitif,” 2017. [Online]. Available: https://www.pwc.com/id/en/media-

centre/press-release/2017/indonesian/menurut-survei-pwc--para-eksekutif-di-indonesia-manfaatkan-tekno.html.

[4] Michael Sitorus, "Teknik Steganography Dengan Metode Least Significant Bit (Lsb)," Vol. 11, No. 2, Pp. 14–15, 2015.

[5] D. Darwis, "Teknik Steganografi Untuk Penyembunyian Pesan Text Menggunakan Algoritma Gifshuffle," *J. Teknoinfo*, vol. 11, no. 1, pp. 1–5, 2017.

[6] Z. A. I. Niswati, "Steganografi Berbasis Least Significant Bit (Lsb) Abstrak . Penelitian ini bertujuan untuk menerapkan metode LSB untuk menyisipkan pesan gambar ke gambar grayscale . Hal ini diperlukan karena sering terjadi bahwa pesan gambar dikirim adalah pesan rahasi," vol. 5, no. 2, pp. 181–191, 2008.

[7] Muchlisin Riadi, "Sejarah, Prinsip Kerja dan Teknik Steganografi," 2017. [Online]. Available: https://www.kajianpustaka.com/2017/09/sejarah-prinsip-kerja-teknik-steganografi.html.

[8] A. Susanto, "Studi dan Implementasi Steganografi pada Berkas MIDI," 2010.

[9] muamalkhoerdin, "Algoritma Hill Cipher (Sandi Hill)," 2015. [Online]. Available: https://muamalkhoerudin.com/2015/03/22/algoritma-hill-cipher-sandi-hill/.

[10] T. S. Alasi, "Penerapan Hill Chiper pada Keamanan Pesan Teks," pp. 1–5, 2007.

[11] Bonifacius Vicky Indriyono, "Penerapan Keamanan Penyampaian Informasi Melalui Citra dengan Kriptografi Rijndael dan Steganografi LSB Information Security Through Imagery with Rijndael Cryptography," pp. 228–241, 2016.

[12] T. S. Pandapotan and T. Zebua, "Analisa Perbandingan Least Significant Bit dan End Of File Untuk Steganografi Citra Digital Menggunakan Matlab," no. November, pp. 11–12, 2016.