Journal of Applied Informatics and Computing (JAIC)
Vol.8, No.1, July 2024, pp. 86~90
e-ISSN: 2548-6861

Text Insertion and Encryption Using The Bit-Swapping Method in Digital Images

Kiswara Agung Santoso [1]*, Muhammad Fahmil Fakih [2]*, Ahmad Kamsyakawuni [3]*
* Jurusan Matematika, Fakultas MIPA, Universitas Jember, Jl. Kalimantan 37 Jember 68121, Indonesia
kiswara.fmipa@unej.ac.id [1], 201810101053@mail.unej.ac.id [2], kamsyakawuni.fmipa@unej.ac.id [3]

Article Info

Article history:

Received 2024-03-21
Revised 2024-05-29
Accepted 2024-05-31

Keyword:

Communication,
Security,
Cryptography,
Steganography,
Bit swapping.

ABSTRACT

Communication is an essential aspect of everyday life, involving the transmission of information through various media. Technological advances have made communication easier but have also increased privacy and data security risks. Several efforts are made to maintain the security of digital information, including coding information (cryptography) and hiding information (steganography). In this article, the author secures information through a combination of cryptography and steganography. To secure text data, we encrypt by exchanging bits between adjacent characters. Subsequently, the encrypted text is hidden within an image. The security analysis results show the successful reconstruction of the message from the stego image and the successful restoration of the message to its original form. The use of the bit swapping method in the text message encryption process has been proven to enhance the security level of the ciphertext, as indicated by the lower TPK calculation value of 0.33 compared to the TPK value in previous studies. Additionally, embedding the ciphertext into digital images has been demonstrated to further increase the security level of the message, evidenced by the NPCR calculation value of 0.0000109% and the UACI calculation value of 0.000000555%. These very small values indicate no significant changes.

I. PENDAHULUAN

Dalam kehidupan sehari-hari, interaksi antarindividu tak dapat terhindarkan. Dari obrolan santai hingga percakapan mendalam, setiap komunikasi menjadi lebih hidup ketika kita dapat menyampaikan gagasan dengan cara yang penuh warna. Komunikasi itu sendiri adalah suatu proses penyampaian informasi, baik melalui kata-kata maupun media lain seperti teks, audio, foto dan video. Komunikasi terjadi secara terus-menerus untuk bertukar informasi, yang bisa berupa pesan umum atau informasi rahasia yang perlu dijaga kerahasiannya. Selain menggunakan media tertulis atau lisan, komunikasi juga dapat terjadi melalui ekspresi tubuh, penampilan personal, dan elemen-elemen sekitar yang menggambarkan suatu pesan atau media komunikasi [1].

Semakin berkembangnya teknologi telah membuat komunikasi menjadi lebih mudah, namun juga meningkatkan kerentanan terhadap pelanggaran privasi dan keamanan data. Perlindungan keamanan data menjadi sangat penting untuk mencegah akses oleh pihak yang tidak berwenang, yang dapat merugikan pengirim dan penerima pesan. Salah satu cara yang efektif untuk menjaga kerahasiaan data adalah dengan menerapkan proses kriptografi dan steganografi, kriptografi telah menjadi komponen integral dalam menjaga privasi dan keamanan informasi di dunia digital saat ini. Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk mengamankan komunikasi dengan cara mengenkripsi pesan dan kemudian mendekripsinya di pihak penerima. Melalui proses enkripsi dan dekripsi, pesan dapat disampaikan dengan a man sehingga hanya pihak yang memiliki kunci yang dapat membaca isinya [2]. Beberapa penelitian yang melakukan pertukaran bit untuk menyembunyikan informasi baik berupa teks maupun image kedalam image lain [3]. Kemudian melakukan pertukaran bit untuk mengkodekan image, Adapun bit yang diturkarkan menggunakan transposisi cipher [4]. Lalu menyisipkan pesan terenkripsi menggunakan algoritma Caesar cipher, Dimana bit yang ditukarkan merupakan pergeseran dari kunci [5]. Selain itu

menyembunyikan teks kedalam image, dimana posisi teks disembunyikan menurut aturan aljabar max-plus [6]. Dan menganalisa bit piksel pada image untuk mengetahui apakah terdapat perubahan signifikan diantara piksel tetangganya [7]. Lalu melakukan pertukaran bit untuk enkripsi dari pesan teks dan petukaran bit LSB untuk menyembunyikan kedalam image. Pebedaannya pada artikel ini system konversi bilangan biner mengacu pada seven segment display [8]. Jika dilihat dari beberapa penelitian sebelumnya, metode bit swaping umumnya digunakan pada steganografi yaitu menyembunyikan teks kedalam image atau mengkodekan image agar tidak dapat diinterpretasikan.

Pada artikel kali ini penulis akan menggunakan metode bit swaping untuk mengkodekan teks, dimana dalam pengkodeannya, tiap karakter dalam plainteks dibuat saling berhubungan satu dengan yang lainnya sehingga perubahan salah satu karakter akan mempengaruhi karakter lainnya dan inilah yang merupakan novelty dari penelitian ini. Setelah itu bit swaping diterapkan lagi pada cipherteks hasil pengkodean dengan piksel dari image guna menyembunyikan ciphertext kedalam image.

II. METODE PENELITIAN

Pada penelitian ini menggunakan data berupa pesan teks yang akan dienkripsi dengan metode *bit swapping*. Selain itu juga menggunakan data berupa citra RGB seperti Gambar a sebagai citra penampung (cover) dan Gambar b citra kunci dengan format jpg.

(a) (b)

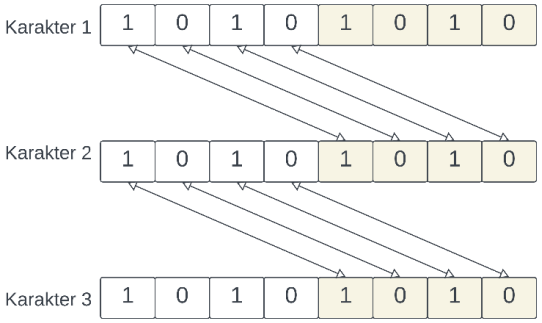
Gambar 1. (a) Citra RGB buah (b) Citra RGB Lena

Penerapan aplikasi ini melibatkan dua langkah utama yang menggabungkan proses kriptografi dan steganografi [2]. Proses kriptografi terdiri dari enkripsi dan dekripsi pesan teks, sedangkan steganografi melibatkan penyisipan dan ekstraksi pesan teks pada citra. Langkah-langkah implementasinya sebagai berikut:

A. Tahap Enkripsi dan Penyisipan Pesan

Proses enkripsi pesan menggunakan algoritma *bit swapping* dan proses penyisipan pesan pada citra menggunakan algoritma *Least Siginificant Bit* [9-11]. Tahap ini dibagi menjadi dua proses yaitu, Proses enkripsi dan proses penyisipan pesan. Langkah dalam enkripsi adalah sebagai berikut:

1) Input teks asli (Plainteks) yang akan dienkripsi.
2) Setiap karakter plainteks direpresentasi biner dengan panjang 8 bit (ASCII).
3) Tukar bit 5-8 karakter pertama dengan bit 1-4 dari karakter kedua. kemudian tukar bit 5-8 dari karakter kedua dengan bit 1-4 dari karakter berikutnya sesuai dengan ilustrasi pada Gambar 2. (Perlu diketahui bahwa dalam teori bilangan urutan bit selalu dimulai dari kanan).
4) Ulangi Langkah 3 hingga semua karakter terkodekan.

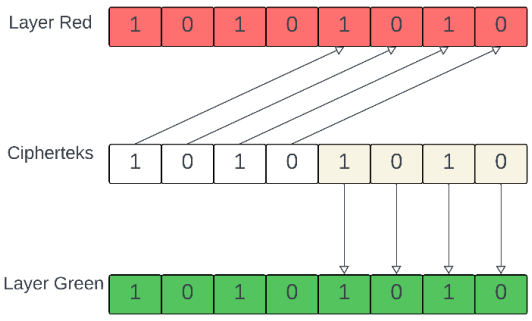


Gambar 2. Proses enkripsi

5) Hasil akhir adalah cipherteks dalam bentuk biner.

Setelah proses enkripsi selesai dilanjut proses penyisipan pesan, langkah dalam penyisipan sebagai berikut:

1) Input: Citra cover (tempat pesan akan disisipkan) dan citra kunci (digunakan untuk proses enkripsi dan dekripsi), dan cipherteks.
2) Tukar bit 1-4 piksel (1,1) dari *layer red* pada citra cover dengan bit 5-8 dari karakter pertama cipherteks
3) Tukar bit 1-4 piksel (1,1) dari *layer green* pada citra cover dengan bit 1-4 dari karakter pertama cipherteks.
4) Ulangi langkah 2 dan 3 untuk menukarkan bit cipherteks karakter kedua dengan piksel (1,2) sesuai ilustrasi pada Gambar . Begitu seterusnya hingga semua karakter cipherteks disembunyikan dalam cover image



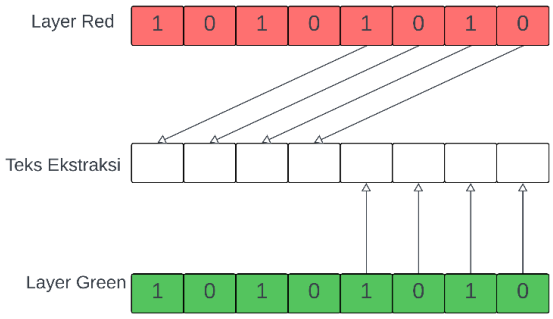
Gambar 3. Proses penyisipan

5) Konversi citra kunci menjadi grayscale
   - Ganti nilai piksel(1,1) layer *blue* dari citra cover dengan rerata nilai piksel citra kunci yang telah diubah menjadi grayscale.
   - Ganti nilai piksel (1,2) layer *blue* dari citra cover dengan jumlah karakter cipherteks. Hal ini berguna untuk mengetahui berapa jumlah piksel yang harus diekstraksi saat proses dekripsi

B. Tahap Ekstraksi Pesan dan Tahap Dekripsi

Tahap ekstraksi pesan dan dekripsi merupakan langkah kritis untuk mengembalikan pesan teks ke bentuk semula setelah melalui proses enkripsi dan penyisipan [12-16]. Tahap ini dibagi menjadi dua proses yaitu, proses ekstraksi dan dekripsi pesan. Langkah dalam ekstraksi sebagai berikut.

1) Input: Citra stego yang berisi pesan terenkripsi dan citra kunci yang digunakan untuk proses otentikasi
2) Konversi citra kunci menjadi grayscale
3) Lakukan verifikasi apakah nilai piksel(1,1) layer *blue* dari citra cover sama dengan rerata nilai piksel citra kunci yang telah dikonversi menjadi grayscale. Jika bernilai sama maka proses berlanjut, sedangkan bila tidak maka proses akan dihentikan.
4) Gabungkan bit 1-4 piksel(1,1) layer *red* dengan bit 1-4 piksel(1,1) layer green sesuai ilustrasi pada Gambar . Hasil penggabungan ini akan menjadi karakter pertama cipherteks
5) Ulangi Langkah 4 untuk posisi piksel selanjutnya sebanyak jumlah karakter cipherteks. Adapun jumlah karakter cipherteks sama dengan nilai piksel(1,2) layer *blue* citra cover.



Gambar 4. Proses ekstraksi

Setelah proses ekstraksi selesai, dilanjutkan dengan proses dekripsi pesan. Langkah dalam dekripsi sebagai berikut:

1) Lakukan pertukaran bit seperti pada proses enkripsi, yaitu bit 5-8 karakter pertama ditukar dengan bit 1-4 dari karakter kedua.
2) Lakukan pertukaran bit 5-8 karakter kedua ditukar dengan bit 1-4 dari karakter ketiga.
3) Ulangi Langkah 1 dan 2 hingga semua karakter dapat didekripsi
4) Rekonstruksi Plainteks: mengubah setiap 8 bit yang telah mengalami pertukaran ke dalam bentuk karakter menggunakan tabel ASCII.

III. HASIL DAN PEMBAHASAN

Penelitian ini dibagi menjadi 2 tahapan utama yaitu.

A. Proses Enkripsi dan Penyisipan

Berdasarkan urauian sebelumnya, langkah-langkah dalam proses ini adalah sebagai berikut.

1) Menginput pesan rahasia.
Misalkan:

`matematika`

2) Setiap karakter plainteks direpresentasikan biner dengan panjang 8 bit, kemudian lanjutkan proses enkripsi dengan metode *bit swapping*

TABEL 1
PROSES ENKRIPSI

Karakter	Sebelum Enkripsi	Setelah Enkripsi
m	01101101	00011101
a	01100001	01000110
t	01110100	01010110
e	01100101	11010111
m	01101101	00010110
a	01100001	01000110
t	01110100	10010110
i	01101001	10110111
k	01101011	00010110
a	01100001	01100110

3) Cipherteks yang dihasilkan dalam bentuk biner selanjutnya disisipkan pada Gambar a dengan ukuran 683x1024x3 pixel dan citra kunci pada Gambar b dengan ukuran 256x256x3 pixel dengan rata-rata nilai pixel adalah 180 untuk layer red, 99 untuk layer green, dan 105 untuk layer blue. Sebagai contoh ambil 1x11 pixel citra penampung seperti berikut.

Nilai RGB 1x11 pixel citra penampung

R	55	79	80	74	97	119	138	158	180	120	112
G	78	101	97	88	106	128	143	162	180	116	106
B	0	19	17	0	1	3	0	7	30	0	0

4) Ganti nilai RGB pada baris dan kolom pertama dengan nilai rata rata dari citra kunci. Dilanjutkan dengan proses penyisipan pada Tabel 2.

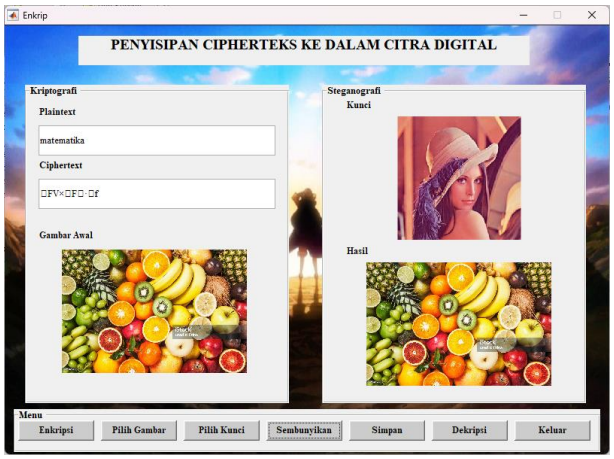
TABEL 2
REPRESENTASI BINER CITRA PADA PROSES PENYISIPAN

Sebelum Penyisipan		**Teks**	**Setelah Penyisipan**	
Layer Red	Layer Green		Layer Red	Layer Green
01001111	01100101	**00011101**	0100**0001**	0110**1101**
01010000	01100001	**01000110**	0101**0100**	0110**0110**
01001010	01011000	**01010110**	0100**0101**	0101**0110**
01100001	01101010	**11010111**	0110**1101**	0110**0111**
01110111	10000000	**00010110**	0111**0001**	1000**0110**
10001010	10001111	**01000110**	1000**0100**	1000**0110**
10011110	10100010	**10010110**	1001**1001**	1010**0110**
10110100	10110100	**10110111**	1011**1011**	1011**0111**
01111000	01110100	**00010110**	0111**0001**	0111**0110**
01110000	01101010	**01100110**	0111**0110**	0110**0110**

5) Dari proses penyisipan diperoleh citra stego dengan nilai desimal seperti berikut.

Nilai RGB 1x11 pixel citra stego

R	180	65	84	69	109	113	132	153	187	113	118
G	99	109	102	86	103	134	134	166	183	118	102
B	105	19	17	0	1	3	0	7	30	0	0



Gambar 5. Tampilan GUI setelah proses enkripsi dan penyisipan

Tampilan program setelah dilakukan proses seperti pada Gambar 5. Proses enkripsi dan penyisipan dimulai dengan menginput pesan ke kolom plainteks, kemudian klik tombol enkripsi untuk melakukan proses enkripsi dan menampilkan cipherteks. Selanjutnya menginputkan citra penampung dan citra kunci dengan klik tombol pilih gambar dan pilih kunci, dilanjutkan dengan klik tombol sembunyikan untuk melakukan proses penyisipan dan menampilkan citra stego yang kemudian dapat di simpan dengan klik tombol simpan.

B. Proses Ekstraksi dan Dekripsi

Berdasarkan uraian sebelumnya, langkah-langkah dalam proses ini adalah sebagai berikut.

1) Proses ini sama dengan proses enkripsi dan penyisipan. Pertama menginput citra stego dan citra kunci, kemudian dicek apakah nilai dari baris dan kolom pertama citra stego sama dengan nilai rata rata RGB dari citra kunci.

TABEL 3
NILAI BINER DARI CITRA STEGO

Layer Red	Layer Green
0100**0001**	0110**1101**
0101**0100**	0110**0110**
0100**0101**	0101**0110**
0110**1101**	0110**0111**
0111**0001**	1000**0110**
1000**0100**	1000**0110**
1001**1001**	1010**0110**
1011**1011**	1011**0111**
0111**0001**	0111**0110**
0111**0110**	0110**0110**

Dari proses ekstraksi diperoleh hasil yaitu

00011101 01000110 01010110 11010111 00010110
01000110 10010110 10110111 00010110 01100110

2) Selanjutnya dilakukan proses dekripsi menggunakan metode *bit swapping* yang menghasilkan nilai biner berikut.

01101101 01100001 01110100 01100101 01101101
01100001 01110100 01101001 01101011 01100001

Dari nilai biner diatas diperoleh hasil dekripsi yaitu.

`matematika`

Gambar 6. Tampilan GUI setelah proses ekstrak dan dekripsi

Tampilan program setelah dilakukan proses seperti pada Gambar 6. Proses ekstraksi dan dekripsi dimulai dengan menginput citra stego dan citra kunci dengan klik tombol pilih gambar dan pilih kunci, kemudian klik tombol ekstrak untuk melakukan proses ekstraksi pesan dan menampilkan pesan tersebut pada kolom teks stego. Selanjutnya klik tombol dekripsi untuk mengembalikan pesan stego menjadi pesan rahasia dan menampilkan pesan tersebut pada kolom hasil.

IV. KESIMPULAN

Berdasarkan penelitian yang dilakukan, diperoleh kesimpulan sebagai berikut. Penggunaan metode bit swapping dalam proses enkripsi pesan teks terbukti meningkatkan tingkat keamanan cipherteks, karena nilai perhitungan TPK yang lebih rendah, yaitu 0,33, dibandingkan dengan nilai TPK pada penelitian sebelumnya. Selain itu, penyisipan cipherteks ke dalam citra digital terbukti menambahkan tingkat keamanan pesan, dibuktikan dengan nilai perhitungan NPCR sebesar 0,0000109% dan nilai perhitungan UACI sebesar 0,000000555%. Nilai-nilai ini sangat kecil, yang menandakan tidak adanya perubahan yang signifikan.

DAFTAR PUSTAKA

[1] E. Setyaningsih, *Kriptografi dan Implementasinya Menggunakan Matlab*, 1 ed., vol. 1. Andi Yogyakarta, 2015.

[2] R. Munir, "Kriptografi / Rinaldi Munir | OPAC Perpustakaan Nasional RI.," Book. Diakses: 7 Agustus 2023. [Daring]. Tersedia pada: https://opac.perpusnas.go.id/DetailOpac.aspx?id=1240782#

[3] K. A. Santoso, Fatmawati, dan H. Suprajitno, "On Max-Plus Algebra and Its Application on Image Steganography," *Scientific World Journal*, vol. 2018, 2018, doi: 10.1155/2018/6718653.

[4] K. Agung, Fatmawati, dan H. Suprajitno, "Image encryption based on pixel bit modification," *J Phys Conf Ser*, vol. 1008, hlm. 012016, Apr 2018, doi: 10.1088/1742-6596/1008/1/012016.

[5] J. Sekip, S. Sikambing, dan N. Sumatera, "Penyisipan Pesan Dengan Algoritma Pixel Value Differencing Dengan Algoritma Caesar Cipher Pada Proses Steganografi," vol. V, no. 1, hlm. 6–11, 2016.

[6] K. A. Santoso, A. Kamsyakawuni, dan A. Riski, "Hiding the Text into An Image by Max-Plus Algebra," dalam *Proceedings - 2019 International Conference on Computer Science, Information Technology, and Electrical Engineering, ICOMITEE 2019*, 2019. doi: 10.1109/ICOMITEE.2019.8921210.

[7] A. L. Tungadi dan E. A. Lisangan, "Kajian Penerapan Semi-Automated Evaluation Based on Similarity pada Investigasi Digital Image Forensics," vol. 1, no. 2, hlm. 7–12, 2016.

[8] K. A. Santoso, A. Pradjaningsih, dan E. Delenia, "Pengaman Teks dengan Kombinasi Metode <i>Electronic Code Book </i>(ECB) dan Kode <i>Seven Segment Display</i>," *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 11, no. 1, hlm. 85–94, Feb 2024, doi: 10.25126/jtiik.20241117448.

[9] T. Musri dan A. Pradana, "Perancangan Enkripsi Keamanan Data Menggunakan Metode Least Significant Bit Dengan Teknik Modifikasi Random Data Encrypt Algorithm Untuk Audio Steganography," *Jurnal: Elektrika Borneo (JEB)*, vol. 6, no. 2, hlm. 48–53, 2020.

[10] A. A. Wahyudi, "Implementasi Steganografi Berkas File Mp3 Menggunakan Metode LSB (Least Significant Bit) Pada Perangkat Mobile Android," Universitas Islam Negara Sunan Kalijaga, Yogyakarta, 2014.

[11] 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.

[12] Kiswara Santoso, Syarif Hidayatulloh, dan Ahmad Kamsyakawuni, "Image Security System Using Playfair Cipher and Modification of Electronic Code Book (ECB) Algorithm," *REFILKOM : Journal of Technology and Information Systems*, vol. 1, no. 1, hlm. 12–20, Jul 2023, Diakses: 27 Oktober 2023. [Daring]. Tersedia pada: https://ejournal.katersipublisher.com/index.php/REFILKOM/article/view/11

[13] K. A. Santoso, R. A. Sukmawati, dan A. Pradjaningsih, "Image security development using 3D playfair cipher combination and bit shift," dalam *AIP Conference Proceeding*, Djogyakarta: AIP Conference Proceedings , Mar 2022, hlm. 020013. doi: 10.1063/5.0079220.

[14] K. Santoso, F. Fatmawati, dan S. Herry, "Image Encryption Technique Based on Pixel Exchange and XOR Operation," *International Basic Science*, vol. 01, no. 1, hlm. 286–288, Agu 2017.

[15] L. Andriani, R. Rihartanto, dan A. B. W. Putra, "Optimasi Vigenere Cipher Menggunakan Bitswap dan Transposisi Acak pada Citra RGB," *Techno.Com*, vol. 19, no. 2, 2020, doi: 10.33633/tc.v19i2.3322.

[16] K. Agung Santoso, A. Tanto Wiraga, A. Riski, J. Matematika, F. Mipa, dan U. Jember, "Penyembunyian Pesan Terenkripsi pada Citra menggunakan Algoritma LSB dan Transposisi Kolom," 2022. [Daring]. Tersedia pada: http://jurnal.polibatam.ac.id/index.php/JAIC