

Implementasi Penyisipan Pesan Teks Terenkripsi Menggunakan Kriptografi ElGamal pada Citra Digital Menggunakan Steganografi LSB

Elpridayanti Saragih¹, Dodi Siregar², Haida Dafitri³

^{1,2,3} Program Studi Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia
Email: ¹ elfridayantisaragih01@gmail.com, ² dodi.729ar@gmail.com, ³ aida.stth@gmail.com
Email Penulis Korespondensi: dodi.729ar@gmail.com

Article History:

Received Jun 12th, 202x

Revised Aug 20th, 2023

Accepted Aug 26th, 2023

Abstrak

Keamanan pesan merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi penting yang isinya hanya boleh diketahui oleh pihak yang berhak saja. Oleh karena itu dibutuhkan keamanan untuk pesan yang bersifat rahasia sehingga pesan tidak dapat disadap oleh orang yang tidak diinginkan dan isi informasi pesan tersebut menjadi lebih aman. Salah satu caranya adalah dengan menerapkan kriptografi metode ElGamal dan LSB untuk dapat memberikan keamanan pada pesan teks dengan cara menyisipkan ke dalam citra digital, algoritma ElGamal menitik beratkan kekuatan kuncinya pada pemecahan masalah logaritma diskrit. Dengan memanfaatkan bilangan prima yang besar serta masalah logaritma diskrit yang cukup menyulitkan dan juga dengan menerapkan metode LSB untuk tempat penyisipan teks maka keamanan kuncinya lebih terjamin. Hasil uji coba terhadap lima objek gambar dengan ekstensi .BMP pada aplikasi yang dibangun berjalan dengan baik dan benar. Gambar yang dimasukkan pada proses enkripsi penyisipan teks pada gambar setelah itu melakukan proses dekripsi dan gambar yang dihasilkan setelah proses enkripsi dan dekripsi tidak berbeda dengan gambar aslinya dan hal yang sama untuk ukuran gambar tidak ada perubahan.

Kata Kunci : Kriptografi, steganograf, ElGamal, Least Significant Bit (LSB), Teks

Abstract

Message security is very important in maintaining the confidentiality of information, especially those containing important information whose contents should only be known by the entitled party. Therefore, security is needed for messages that are confidential so that messages cannot be intercepted by people who do not want them and the information content of the message becomes more secure. One way is to apply ElGamal and LSB cryptography methods to be able to provide security to text messages by inserting into digital images, the ElGamal algorithm focuses on the strength of the key in solving discrete logarithm problems. By utilizing large prime numbers and discrete logarithm problems which are quite difficult and also by applying the LSB method for text insertion, the security of the key is more guaranteed. The test results on five image objects with the .BMP extension on the application that was built were running well and correctly. The image that is inserted in the encryption process is the insertion of text in the image after it is decrypted and the image produced after the encryption and decryption process is no different from the original image and the same thing for the image size does not change.

Keyword : Cryptography, steganography, ElGamal, Least Significant Bit (LSB), Text

1. PENDAHULUAN

Perkembangan teknologi saat ini sangat pesat, hal ini seiring berjalan dengan kejahatan yang ada dalam dunia teknologi itu pula seperti yang sering didengar seperti *hacker*, *cracker*, *carder* dan sebagainya. Pesan atau file rahasia adalah hasil pengolahan data menjadi wujud yang berguna bagi penerima yang menggambarkan sebuah fakta yang digunakan untuk alat bantu dalam suatu pengambilan keputusan. Pentingnya isi pesan menyebabkan pesan hanya boleh diketahui oleh orang-orang tertentu [1]. Jika sebuah pesan yang bersifat rahasia yang bersifat rahasia diketahui atau diambil oleh orang yang tidak berkepentingan, maka sangat berbahaya karena dapat merugikan pemilik pesan tersebut. Pesan yang diketahui tersebut dapat menjadi dikembangkan lagi menjadi informasi yang menguntukan pencuri pesan tersebut. Inilah pentingnya keamanan untuk menjaga pesan yang bersifat rahasia sehingga pesan tidak bisa diketahui oleh orang yang tidak berkepentingan [2].

Media gambar dapat digunakan sebagai suatu pilihan yang tepat untuk menyimpan data rahasia secara mudah dan berkesan estetik. Penerapan steganografi pada media citra adalah dengan menyisipkan pesan. Metode ini paling sederhana akan tersamarkan dengan baik pada citra digital seperti foto yang akan dikirim kepada orang lain, sehingga dengan menyembunyikan data penting ke dalam foto maka cara ini akan mempersulit orang lain untuk membaca secara kasat mata pesan yang disisipkan pada media gambar [3].

Steganografi merupakan seni menyembunyikan pesan teks sedemikian rupa sehingga tak seorang pun mengetahui keberadaan informasi selain pengirim dan penerima pesan tersebut. Steganografi memerlukan dua properti yaitu sebagai media penampung dan pesan rahasia.[4]. Steganografi semakin diperlukan untuk memberikan keamanan yang maksimal untuk dalam proses mengirimkan suatu informasi. Teknik steganografi umum digunakan bersamaan dengan menggunakan dua media yang berbeda, dengan itu salah satunya yang berfungsi untuk media yang berisikan informasi (*carrier file*) dan yang berfungsi untuk sumber informasi tersebut (*secret file*) [5]. Kriptografi merupakan ilmu dan seni dapat untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti artinya[6].

Algoritma ElGamal merupakan salah satu algoritma asimetris dalam kriptografi. Algoritma ini memiliki tingkat keamanan dalam pemecahan masalah logaritma diskret pada group pergandaan bilangan prima yang besar, maka upaya untuk memecahkan pesan yang telah dienkripsi menjadi sangat sulit. Selain tingkat keamanan pada pemecahan logaritma diskret, algoritma ElGamal memiliki kelebihan dalam menghasilkan *ciphertext* (pesan yang telah tersamarkan) yang berbeda untuk *plaintext* (pesan belum disamarkan, masih dapat dibaca dengan jelas) yang sama pada proses enkripsi, tetapi ketika *ciphertext* di dekripsi akan menghasilkan *plaintext* (pesan belum disamarkan, masih dapat dibaca dengan jelas) yang sama pada proses enkripsi, tetapi ketika *ciphertext* di dekripsi akan menghasilkan *plaintext* yang sama. Proses algoritma ElGamal terdiri atas 3 proses yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Setiap proses dalam algoritma ini menggunakan teori bilangan terutama bilangan prima dan *modulo* bilangan[7]. Algoritma kriptografi kunci publik ElGamal merupakan algoritma blok *chipper* yaitu algoritma yang melakukan proses enkripsi pada blok-blok *plaintext* yang kemudian menghasilkan blok-blok *chiphertext*, yang nantinya blok-blok *chiphertext* tersebut akan didekripsi kembali dan hasilnya kemudian digabungkan menjadi *plaintext* semula[8]. *Least Significant Bit (LSB)* merupakan teknik penyisipan pesan yang paling sederhana dan cepat dalam penggunaan metode steganografi. Pesan disembunyikan dengan menyisipkan bit-bit pesan pada bit terendah atau bit yang paling kanan dari 1 *byte pixel cover* dimana 1 *byte* = 8 bit [9]. Pada berkas file gambar yang berektensi bitmap 24-bit dan setiap pixel tersusun dari tiga warna merah, hijau dan biru (*RGB*). Masing- masing susunan terdapat bilangan 8 bit yang dimulai dari 0 sampai 255 yaitu menggunakan bilangan biner 00000000 sampai 11111111. Setiap pixel pada berkas gambar bitmap 24 bit dapat kita lakukan penyisipan 3 bit data[10]. Adapun tujuan penelitian ini adalah untuk membangun suatu aplikasi steganografi dalam menyisipkan pesan teks pada citra digital dengan menerapkan metode ElGamal dan *LSB*.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi merupakan sebuah teknik yang dikenal sebagai yang digunakan untuk mengamankan data atau informasi pribadi atau sensitif dengan mengenkripsi *plaintext* menggunakan kunci tertentu, menciptakan *ciphertext* yang tidak dapat dipahami oleh orang luar. Proses deskripsi algoritma selesai, dan *ciphertext* kemudian diubah kembali menjadi *plaintext*[11]. Algoritma kriptografi sering disebut dengan *cipher* adalah suatu fungsi matematis digunakan untuk melakukan enkripsi dan dekripsi[12].

2.2 Metode ElGamal

Algoritma kriptografi ElGamal merupakan salah satu algoritma kunci asimetris yang didasarkan pada algoritma diskrit. Keamanan dari algoritma ElGamal terletak pada sulitnya perhitungan algoritma diskrit ketika *p* merupakan bilangan prima yang besar[13]. Dalam proses implementasi algoritma ElGamal terdiri dari tiga proses yaitu, pembentukan kunci kriptografi, proses algoritma enkripsi dan dekripsi[14]

2.2.1 Proses Penerapan Metode ElGamal Pembentukan Kunci

Langkah-langkah dalam pembuatan kunci adalah sebagai berikut:

1. Pilih sembarang bilangan prima p , dengan syarat $p > 255$.
2. Pilih bilangan acak g dengan syarat $g < p$.
3. Pilih bilangan acak x dengan syarat $1 < x < p - 2$.
4. Hitung $y = g^x \text{ mod } p$.

Kunci *public* nya adalah y, g, p sedangkan kunci *private* nya adalah x . nilai $y, g,$ dan p tidak dirahasiakan sedangkan nilai x harus dirahasiakan karena merupakan kunci *privat* untuk mendekripsi *plaintext*.

Langkah-langkah dalam mengenkripsi pesan adalah sebagai berikut:

1. Potong *plaintext* menjadi blok-blok $m_1, m_2, m_3, m_4, \dots$, nilai setiap blok di dalam selang $[0, p-1]$.
2. Ubah nilai blok pesan ke dalam nilai *ASCII*.
3. Pilih bilangan acak k , dengan syarat $1 < k < p - 1$ sebanyak m .
4. Setiap blok m dienkripsi dengan rumus sebagai berikut:
$$a = g^{ki} \text{ mod } p$$
$$b = y^{ki} \text{ mod } p$$
5. Susun *chipertext* dengan urutan $a_1, b_1, a_2, b_2, \dots, a_n, b_n$.

Pasangan a dan b adalah *chipertext* untuk blok pesan m . Hasil yang didapat dari proses enkripsi berupa pesan rahasia (*chipertext*).

Langkah-langkah dalam mendekripsi pesan adalah sebagai berikut:

1. Hitung *plaintext* m dengan persamaan rumus sebagai berikut:
$$m_i = b_i \cdot a_i^{p-1-x} \text{ mod } p$$
2. Nilai m_i yang didapat dalam bentuk *ASCII* kemudian diubah menjadi *plaintext*.
3. Susun *plaintext* dengan urutan $m_1, m_2, m_3, \dots, m_n$

Maka hasil yang didapat dari proses dekripsi berupa pesan asli (*Plaintext*)[15].

2.3 Metode LSB (Least Significant Bit)

Metode LSB merupakan teknik penyisipan pesan dalam steganografi dimana penyisipan pesan dilakukan dengan mengganti deretan bit-bit data yang paling belakang dalam segmen citra dengan deretan bit-bit pesan yang akan disisipkan[16]. Pada susunan bit didalam sebuah byte, ada bit yang paling signifikan yang disebut MSB (*Most Significant Bit*) dan bit yang paling kurang signifikan atau LSB (*Least Significant Bit*). Sebagai contoh byte 11010010, angka bit 1 (pertama, digaris-bawahi) adalah bit MSB, dan angka bit 0 (terakhir, digaris-bawahi) adalah bit LSB. Bit yang cocok untuk diganti adalah bit LSB, sebab perubahan tersebut hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya[17].

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini memerlukan beberapa tahapan yang akan digunakan untuk mencapai hasil rancangan sistem yang baik dan benar. Berikut beberapa tahapan yang akan dijelaskan:

3.1 Penerapan Metode ElGamal dan LSB

Penerapan metode ElGamal dan LSB dilakukan agar penelitian yang dilakukan menjadi lebih baik. Masalah utama yang akan diselesaikan dalam penelitian ini adalah bagaimana pesan teks dapat diamankan dengan baik sehingga semua informasi tidak bisa di baca oleh orang yang tidak berkepentingan. Pada algoritma ElGamal ini terdiri dari tiga proses, yaitu proses pembangkitan pasangan kunci, proses enkripsi dan proses dekripsi. Algoritma ini melakukan proses enkripsi pada blok-blok *plaintext* dan kemudian menghasiok-blok *chipertext* yang kemudian dilanjutkan dengan proses dekripsi, sehingga menjadi pesan yang utuh dan mudah dipahami [18]. Adapun cara mengamankan pesan teks menggunakan sebuah algoritma ElGamal karena metode ElGamal mampu membuat pesan teks menjadi lebih aman karena dikombinasi dengan metode LSB, dimana teks yang akan dikirim akan disisipkan pada sebuah citra.

Proses penerapan metode ElGamal penyisipan pesan teks pada citra digital dengan proses enkripsi dan dekripsi. Adapun langkah-langkah yang diperlukan sebagai berikut:

1. Masukan Teks yang akan di enkripsi (*plaintext*)
Plaintext: HARAPANMEDAN
2. Pesan akan dipotong menjadi blok-blok karakter dan dikonversi ke dalam bilangan *ASCII*.

Tabel 1. Konversi Karakter Pesan Ke Kode *ASCII*

I	<i>plaintext</i> m_i	Karakter	<i>plaintext</i> m_i <i>ASCII</i>
1	m_1	H	72
2	m_2	A	65
3	m_3	R	82
4	m_4	A	65
5	m_5	P	80
6	m_6	A	65
7	m_7	N	78
8	m_8	M	77
9	m_9	E	69
10	m_{10}	D	68
11	m_{11}	A	65
12	m_{12}	N	78

Langkah selanjutnya, proses menentukan bilangan acak $p \in (0,1, \dots, 256)$ kemudian nilai *ASCII* tersebut dimasukan ke dalam blok-blok nilai m secara berurutan dan melakukan proses Enkripsi, seperti tabel 2:

Tabel 2. Pembentukan Nilai Kunci

Mn	Nilai	Kunci
m_1	72	12
m_2	65	8
m_3	82	20
m_4	65	70
m_5	80	65
m_6	65	76
m_7	78	104
m_8	77	114
m_9	69	12
m_{10}	68	40
m_{11}	65	50
m_{12}	78	35

Hasil proses Enkripsi pada tabel 2 membentuk *ciphertext* seperti berikut:

193, 133, 16, 192, 4, 27, 128, 209, 15, 247, 193, 245, 179, 16, 179, 32, 193, 181, 16, 189, 32, 254, 34, 39

Di dalam bentuk karakter *ciphertext* tabel 2 menjadi " + '#' = +'"]A'# + %}\$&"

Setelah proses enkripsi selesai langkah selanjutnya melakukan proses dekripsi seperti pada tabel 3:

Tabel 3. Proses Dekripsi

I	Karakter	plaintext m_i	plaintext m_i ASCII
1	M	m_1	77
2	B	m_2	66
3	W	m_3	87
4	N	m_4	78
5	U	m_5	85
6	V	m_6	86
7	A	m_7	65
8	V	m_8	86
9	Y	m_9	89
10	Y	m_{10}	89
11	S	m_{11}	83
12	Q	m_{12}	81

Setelah proses dekripsi selesai maka karakter yang telah dienkripsi sebelumnya kembali menjadi pesan asli yaitu: "HARAPANMEDAN" dan langkah selanjutnya melakukan proses metode LSB seperti pada gambar 1.



Gambar 1. Pixel Regional Citra Lena R,G,B 5 x 5 pixels

Pada citra warna di atas di lakukan transformasi ke *citra grayscale* dengan cara menghitung rata-rata elemen warna *Red, Green, Blue*. Secara matematis perhitungannya adalah sebagai berikut:

$$f_o(X, Y) = \frac{f_i^R(X, Y) + f_i^G(X, Y) + f_i^B(X, Y)}{3}$$

Hasil pixel citra warna *Red, Green* dan *Blue* pada gambar citra Lena 5x5 Pixel setelah dirubah ke dalam citra *grayscale* maka nilai citra *grayscale* dapat dilihat pada tabel 4:

Tabel 4. Citra Grayscale

116	115	117,6	123	129
97,3	100	107,3	119	128
125,3	124,3	127,6	135,6	142,6
167	172	178,3	187,6	193,3
179,6	183	185	188	190,3

3.2 Hasil Uji Coba Objek Gambar

Pada aplikasi penyisipan pesan teks kedalam citra digital maka dengan ini penulis sudah melakukan beberapa kali uji coba terhadap objek gambar. Adapun hasil pengujian objek gambar dapat dilihat pada tabel 5:

Tabel 5. Hasil Pengujian Objek Gambar

NO	Objek Gambar yang Diuji	Hasil Yang Diharapkan	Hasil Pengujian	Kesimpulan
1		Setelah proses Enkripsi dan Dekripsi dilakukan di sistem maka gambar yang dimasukkan dengan yang dihasilkan tidak ada perubahan tetap sama seperti aslinya dan untuk <i>size</i> gambar (186KB) pun tidak berubah sama sekali	Hasil uji coba pada gambar ini proses Enkripsi dan Dekripsi dalam penyisipan pesan teks di sistem berjalan dengan baik sesuai yang di harapkan	Valid
2		Setelah proses Enkripsi dan Dekripsi dilakukan di sistem maka gambar yang dimasukkan dengan yang dihasilkan tidak ada perubahan tetap sama seperti aslinya dan untuk <i>size</i> gambar (79,3KB) pun tidak berubah sama sekali	Hasil uji coba pada gambar ini proses Enkripsi dan Dekripsi dalam penyisipan pesan teks di sistem berjalan dengan baik sesuai yang di harapkan	Valid
3		Setelah proses Enkripsi dan Dekripsi dilakukan di sistem maka gambar yang dimasukkan dengan yang dihasilkan tidak ada perubahan tetap sama seperti aslinya dan untuk <i>size</i> gambar (65,8 KB) pun tidak berubah sama sekali	Hasil uji coba pada gambar ini proses Enkripsi dan Dekripsi dalam penyisipan pesan teks di sistem berjalan dengan baik sesuai yang di harapkan	Valid
4		Setelah proses Enkripsi dan Dekripsi dilakukan di sistem maka gambar yang dimasukkan dengan yang dihasilkan tidak ada perubahan tetap sama seperti aslinya dan untuk <i>size</i> gambar (79,03 KB) pun tidak berubah sama sekali	Begitu juga hasil uji coba pada gambar ini proses Enkripsi dan Dekripsi dalam penyisipan pesan teks di sistem berjalan dengan baik sesuai yang di harapkan	Valid

5		Setelah proses Enkripsi dan Dekripsi dilakukan di sistem maka gambar yang dimasukkan Dengan yang dihasilkan tidak ada perubahan tetap sama seperti aslinya dan untuk <i>size</i> gambar (210 KB) pun tidak berubah sama sekali	Hasil uji coba pada gambar ini proses Enkripsi dan Dekripsi dalam penyisipan pesan teks di sistem berjalan dengan baik sesuai yang di harapkan	Valid
---	---	--	--	-------

(Sumber: Peneliti)

3.3 Pengujian Sistem Black Box Testing

Pengujian sistem *Black Box Testing* adalah pengujian yang dilakukan untuk mengamati hasil *input* dan *output* dari perangkat lunak tanpa mengetahui struktur kode dari perangkat lunak [20]. Pengujian ini dilakukan diakhir pembuatan perangkat lunak untuk mengetahui apakah perangkat lunak dapat berfungsi dengan baik. Adapun pengujian terhadap sistem yang telah dibangun dapat dilihat pada tabel 6.

Tabel 6. Hasil Pengujian Sistem

NO	Kasus Uji	Langkah Pengujian	Hasil Yang Diharapkan	Hasil Pengujian	Kesimpulan
1	Form Login	Masukkan <i>username</i> dan <i>password</i> benar klik Login	Menampilkan form menu utama	Tampil Menu Utama	Valid
		Masukkan <i>username</i> dan <i>password</i> salah klik Login	Menampilkan pemberitahuan "Password Anda Salah Bos!!! Tolong Perbaiki	Tampil Pemberitahuan Password salah	Valid
2	Form Menu Utama	Klik File	Menampilkan pilihan Form Enkripsi dan Form Dekripsi	Tampil pilihan Form Enkripsi dan Form Dekripsi	Valid
		Klik Keluar	Kembali ke Form Login	Tampil Form Login	Valid
3	Form Enkripsi ElGamal dan LSB	Klik Input Gambar	Menampilkan pencarian gambar yang ingin disisipkan pesan teks dan diinput ke dalam <i>Picturebox</i>	Tampil pencarian gambar dan <i>Picturebox</i> terisi gambar yang diinput	Valid
		Klik Proses	Menampilkan gambar yang sudah diproses maka <i>Picturebox</i> sebelah kanan akan terisi gambar yang sudah di sisipkan teks	Tampil gambar di <i>picturebox</i> sebelah kanan	Valid

		Klik Simpan	Menampilkan menu penyimpanan hasil gambar yang telah disisipkan teks	Tampil Menu penyimpanan gambar	Valid
		Klik Keluar	Maka keluar dari Form Enkripsi lalu kembali ke Menu Utama	Tampil Menu Utama	Valid
4	Form Dekripsi	Klik <i>Input</i> Gambar	Menampilkan pencarian gambar hasil dari proses Enkripsi kemudian <i>picturebox</i> terisi gambar hasil tersebut	Tampil <i>picturebox</i> terisi gambar	Valid
		Klik Proses	Menampilkan hasil pesan teks maka akan muncul hasil di Dekripsi dan Enkripsi	Tampil hasil teks di Dekripsi dan Enkripsi	Valid
		Klik Keluar	Keluar dari Form Dekripsi lalu kembali ke Menu Utama	Tampil Menu Utama	Valid
5	<i>Plaintext</i>				
		<i>Plaintext</i> yang dimasukkan Huruf Kapital semua	Menampilakan hasil <i>plaintext</i> sesuai dengan dimasukkan Karena sistem yang dirancang Huruf Kapital ataupun Huruf Kecil yang dimasukkan hasilnya tetap Huruf Kapital.	Tampil hasil <i>plaintext</i> sesuai yang dimasukkan	Valid
		<i>Plaintext</i> yang dimasukkan Huruf Kecil semua	Menampilakan hasil <i>plaintext</i> sesuai dengan yang dimasukkan	Tampil <i>plaintext</i> tidak sesuai karena sistem yang dirancang Huruf Kapital ataupun Huruf Kecil <i>plaintext</i> yang di masukkan hasilnya tetap Huruf Kapital. Tampil <i>plaintext</i> tidak sesuai karena	Tidak Valid
		<i>Plaintext</i> yang dimasukkan kombinasi angka ataupun tanda baca	Menampilkan hasil <i>plaintext</i> sesuai dengan <i>plaintext</i> yang dimasukkan	sistem yang dirancang tidak membaca angka ataupun tanda baca, dan Huruf Kapital ataupun Huruf Kecil <i>plaintext</i> yang di	Tidak Valid

(Sumber : Peneliti)

4. KESIMPULAN

Keamanan pesan teks kombinasi citra digital dengan menggunakan metode ElGamal dan LSB maka pesan teks dapat diamankan dengan baik. Dimana sistem yang dirancang dapat mengamankan pesan teks dengan cara menyisipkan ke dalam citra digital. Dalam aplikasi ini ukuran gambar yang digunakan tidak ada perubahan. Dan tingkat keamanan algoritma ini didasarkan pada kesulitan pemecahan masalah logaritma diskret pada penggandaan bilangan bulat modula prima yang besar. Menerapkan metode ElGamal dengan cara sebuah pesan dan kunci dikonversikan ke dalam bentuk kode ASCII, kemudian hasil yang didapatkan diubah kembali ke dalam bentuk karakter. Metode *Least Significant Bit* (LSB) menyisipkan pesan dengan cara merubah ASCII pesan ke dalam bilangan biner kemudian tiap-tiap angka disisipkan pada gambar.

DAFTAR PUSTAKA

- [1] K. Ardiansyah, "BAB I PENDAHULUAN Kombinasi Metode Elgamal Dengan Caesar Untuk Keamanan Pesan Yang Disisipkan Pada Gambar Menggunakan LSB," pp. 1–8, 2018.
- [2] R. S. Wenny, "Bab I Pendahuluan Pengamanan Pesan Teks Menggunakan metode ElGamal Untuk Disisipkan Pada Gambar Menggunakan LSB," pp. 1–17, 2018.
- [3] N. Laila and A. S. Rms, "IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA Implementation of LSB Steganography with Vigenere Cipher Encryption in Image," vol. 1, no. 2, pp. 47–58, 2018.
- [4] F. G. Becker, M. Cleary, and Team, "Analisa Metode End Of File Dalam Penyisipan Pesan Teks Dengan hill Cephher Pada Gambar," *Syria Stud.*, vol. 7, no. 1, pp. 37–72, 2019, [Online]. Available: https://www.researchgate.net/publication/269107473_What_is_governance/link/548173090cf22525dcb61443/download%0Ahttp://www.econ.upf.edu/~reynal/Civil_wars_12December2010.pdf%0Ahttps://think-asia.org/handle/11540/8282%0Ahttps://www.jstor.org/stable/41857625
- [5] S. dan heryanto Murti, "Penyembunyian Pesan Rahasia Pada Citra Digital dengan Teknik Steganografi Menggunakan Metode Least Significant Bit (LSB)," *J. Ilm. Wahana Pendidik.* <https://jurnal.unibrah.ac.id/index.php/JIWP>, vol. 6, no. 3, pp. 295–307, 2020, doi: 10.5281/zenodo.5563416.
- [6] P. N. Lhokseumawe, "RANCANG BANGUN APLIKASI KRIPTOGRAFI UNTUK PENGAMANAN CITRA RGB 24 BIT MENGGUNAKAN," vol. 02, no. November, pp. 109–114, 2021.
- [7] A. M. Hidayat, M. Sihombing, and A. Sihombing, "Teknik Algoritma Elgamal Dan Steganografi First of File (Fof) Untuk Penyisipan Pesan Dalam Citra," vol. 6, no. 1, pp. 191–200, 2022.
- [8] A. Y. N. Harahap, H. Gunawan, A. B. Nst, and R. E. Sari, "PENERAPAN ELGAMAL GUNA MENINGKATKAN KEAMANAN DATA TEXT DAN DOCX," *IT (INFORMATIC Tech. J.*, vol. 10, no. 1, p. 76, 2022, doi: 10.22303/it.10.1.2022.76-86.
- [9] E. W. Purwanto and S. S. S. T, "ALGORITMA KRIPTOGRAFI EL-GAMAL UNTUK PENGAMANAN PESAN PADA STEGANOGRAFI CITRA DOMAIN DISCRETE COSINE TRANSFORM DENGAN TEKNIK PENYISIPAN LEAST SIGNIFICANT BIT," vol. 5, no. 1, pp. 116–123, 2018.
- [10] I. D. FADHILAH, "Rancang Bangun Sistem Keamanan Data Dengan Metode Steganografi Lsb Berbasis Website," ... *Karya Ilmiah Mahasiswa Fakultas sains dan* p. 85, 2019. [Online]. Available: <https://journal.pancabudi.ac.id/index.php/fastek/article/view/1307>
- [11] T. Rachman, "Pembuatan aplikasi Kriptografi file menggunakan algoritma vigenere chiper," *Angew. Chemie Int. Ed.* 6(11), 951–952., pp. 10–27, 2018.
- [12] H. Desita and R. Tb, "Analisis Hasil Enkripsi Dan Dekripsi Citra Rgb 24 Bit Menggunakan Algoritma Elgamal Berdasarkan Ukuran , Dan Warna Citra Asli Analysis of the Result of Encryption and Decryption of 24-Bit Rgb Image Using Elgamal Algorithm Based on Original Image Size and ," vol. 8, no. 1, pp. 12–16, 2022.
- [13] E. Rahmansyah, "Implementasi Algoritma Elgamal Dengan Pembangkit Bilangan Prima Lehmann Dan Algoritma Least Significant Bit (LSB) Dengan Cover Image Bitmap Untuk ...," *JURIKOM (Jurnal Ris. Komputer)*, vol. 6, no. 1, pp. 79–84, 2019.
- [14] K. M. Sudrajat, "Perancangan Aplikasi Pengamanan File Teks Menggunakan Algoritma El Gamal Dan Kompresi File Teks Menggunakan Algoritma Huffman," *Pelita Inform. Inf. dan*, vol. 8, pp. 173–177, 2019, [Online]. Available: <https://ejournal.stmik-budidarma.ac.id/index.php/pelita/article/view/1814>
- [15] K. Programmer, "Penerapan Algoritma Elgamal Untuk Enkripsi Dan Dekripsi File Teks," *Payah Tidur.com*, 2020. <https://payahtidur.com/project/elgamal> (accessed Sep. 06, 2022).
- [16] M. Azlansyah and B. Setiyono, "Penyisipan Pesan pada Citra Digital Menggunakan Metode Least Significant Bit," *J. Sains dan Seni ITS*, vol. 8, no. 1, 2019, doi: 10.12962/j23373520.v8i1.37658.
- [17] I. Gunawan, "Penggunaan Algoritma Kriptografi Steganografi Least Significant Bit Untuk Pengamanan Pesan Teks dan Data Video,"

J-SAKTI (Jurnal Sains Komput. dan Inform., vol. 2, no. 1, p. 57, 2018, doi: 10.30645/j-sakti.v2i1.48.

- [18] N. Indahwati and A. Prihanto, "Penerapan Algoritma Kriptografi Asimetris Elgamal dengan Modifikasi Pembangkit Kunci terhadap Enkripsi dan Dekripsi Gambar Warna," *J. Informatics Comput. Sci.*, vol. 1, no. 02, pp. 97–103, 2020, doi: 10.26740/jinacs.v1n02.p97-103.
- [19] A. Shell, "Pengertian Implementasi Sistem," pp. 1–23, 2019.
- [20] M. M. Amin, "Komunikasi Berbasis Teks, Pengertian Pengujian Sistem Blackbox Testing," *J. Pseudocode*, vol. III, no. September, pp. 129–136, 2019.