ISSN: 2962-3545
Prosiding SAINTEK: Sains dan Teknologi Vol.3 No.1 Tahun 2024
Call for papers dan Seminar Nasional Sains dan Teknologi Ke-3 2024
Fakultas Teknik, Universitas Pelita Bangsa, Januari 2024

Pengamanan Email melalui Steganografi Penerapan One Time Pad dan Metode LSB pada Gambar Lampiran

Securing Email through Steganography Implementation of One Time Pad and LSB Method on Attached Images

Ravansa Rahman Santosa[1], Ajie Rafli Pamungkas[2], Muhammad Khrisna Faisal Zuhri[3]
[1,2,3]Teknik Informatika, Fakultas Teknik, Universitas Pelita Bangsa
[1]ravansa04@mhs.pelitabangsa.ac.id, [2]ajirafli@mhs.pelitabangsa.ac.id,
[3]muhammadkhrisna12@mhs.pelitabangsa.ac.id

Abstract

Innovative solutions are being researched in response to the growing dangers to digital communication security, especially through email. The integration of steganography with One Time Pad and the Least Significant Bit (LSB) technique in picture attachments is the main emphasis of this study's email security approach. Confidential information is hidden in photos using steganography, and a one-time key from One Time Pad adds an extra layer of security. Information can be embedded into photographs using the LSB approach without drastically changing how they look. The system is built throughout implementation by creating algorithms for the LSB method on image attachments and the One Time Pad application on emails. Effective confidentiality concealment is ensured by the integration process, which does not jeopardize system performance or document authenticity. System performance and security are measured through testing. According to test results, this method can offer strong security against eavesdropping attempts and stop unwanted modifications to picture attachments. Analysis of the results shows that using the LSB approach in conjunction with One Time Pad can be a useful way to improve email security. The system's high degree of security is one of its strongest points; its implementation complexity is one of its weaknesses. However, the study's findings provide the groundwork for future advancements in digital communication security, particularly with regard to email systems.

Keywords: *Email Security, Steganography, One Time Pad, Least Significant Bit, Cryptography*

Abstrak

Tingkat ancaman yang meningkat terhadap keamanan komunikasi digital, terutama melalui email, mendorong penelitian untuk mencari solusi baru. Studi ini menggabungkan Steganografi dengan One Time Pad dan Metode Least Significant Bit (LSB) pada gambar lampiran untuk melindungi email. Steganografi menyembunyikan data sensitif dalam gambar, sementara One Time Pad memberikan lapisan keamanan tambahan melalui kunci yang digunakan sekali. Metode LSB memungkinkan penambahan informasi ke gambar tanpa mengubah tampilan visualnya. Sistem dikembangkan pada tahap implementasi dengan merancang algoritma untuk menggunakan One Time Pad pada email dan menggunakan Metode LSB, seperti yang ditunjukkan pada gambar lampiran. Proses integrasi memastikan bahwa informasi rahasia dapat disembunyikan dengan sukses tanpa mengurangi kinerja dokumen atau keaslian. Pengujian sistem dilakukan untuk mengevaluasi kinerja dan keamanan sistem. Hasil pengujian menunjukkan bahwa metode ini dapat melindungi terhadap serangan pengintaian dan mencegah perubahan yang tidak sah pada lampiran gambar. Hasil analisis menunjukkan bahwa kombinasi Metode LSB dan One Time Pad dapat menjadi metode yang efektif untuk meningkatkan keamanan email. Kelebihan sistem ini adalah tingkat keamanan yang tinggi, tetapi keterbatasannya adalah implementasi yang sulit. Namun, hasil penelitian ini memberikan dasar untuk pengembangan lebih lanjut dalam keamanan komunikasi digital, terutama email.

Kata kunci: *Keamanan Email, Steganografi, One Time Pad, Least Significant Bit, Kriprografi*

Pendahuluan

Berbagi data dan informasi dengan begitu cepat adalah salah satu keuntungan dari kemajuan pesat teknologi dan komunikasi saat ini [1]. Data atau informasi ada yang bersifat umum, yang berarti banyak orang dapat melihatnya, ada juga yang bersifat pribadi atau rahasia, yang berarti hanya beberapa orang yang dapat melihatnya [2]. Oleh karena itu, kerahasiaan dan keamanan ini sangat penting untuk menjaga data aman selama pertukaran data [3]. Email, salah satu alat komunikasi paling umum di dunia bisnis dan personal, adalah salah satu jenis serangan yang dapat mengancam keamanan data. Stenografi adalah salah satu dari banyak metode dan teknik yang dapat digunakan untuk mengatasi masalah ini [4]. Akibatnya, sangat penting untuk melindungi konten email. Secara umum, kriptografi adalah seni dan ilmu untuk menjaga kerahasian pesan [5]. Steganografi adalah seni dan ilmu menyembunyikan pesan rahasia di antara pesan lain sehingga orang tidak dapat mengetahui keberadaannya [6, 7]. Dua algoritma penting untuk pengembangan steganography adalah yang untuk mengembedding dan mengekstrak [8]. Gambar digital terdiri dari sinyal frekuensi elektromagnetik yang telah disampling untuk menentukan ukuran titik gambar yang disebut piksel [9]. Salah satu metode steganografi citra digital adalah *Least Significant Bit* (LSB), teknik yang menyembunyikan pesan pada lokasi bit terendah pada gambar digital [10, 11]. Cipher aliran satu kali (OTP) enkripsi dan dekripsi satu karakter setiap kali [12]. Steganografi digunakan dalam situasi ini untuk memasukkan pesan rahasia ke dalam gambar lampiran email, yang melindungi data yang dikirimkan. Penelitian ini berfokus pada penggunaan dua metode kriptografi yang kuat *One Time Pad* (OTP) dan metode *Least Significant Bit* (LSB) pada gambar lampiran email. Dengan menggabungkan OTP dan LSB pada gambar lampiran email, penelitian ini bertujuan untuk menciptakan sistem keamanan yang kuat dan dapat diandalkan. Tanpa sistem keamanan, metode LSB dapat dibongkar dengan mudah melalui analisis frekuensi dengan menyelesaikan bit terendah [13, 14]. Selain itu, diharapkan bahwa metode ini akan memberikan tingkat keamanan yang lebih tinggi daripada metode konvensional yang digunakan saat ini untuk mengamankan email. Penelitian ini akan mengevaluasi kemanjuran kombinasi metode OTP dan LSB dalam melindungi data email. Penelitian ini diharapkan akan memberikan gambaran yang lebih baik tentang bagaimana steganografi dapat meningkatkan keamanan email di dunia digital yang semakin kompleks dan rentan.

Metode Penelitian

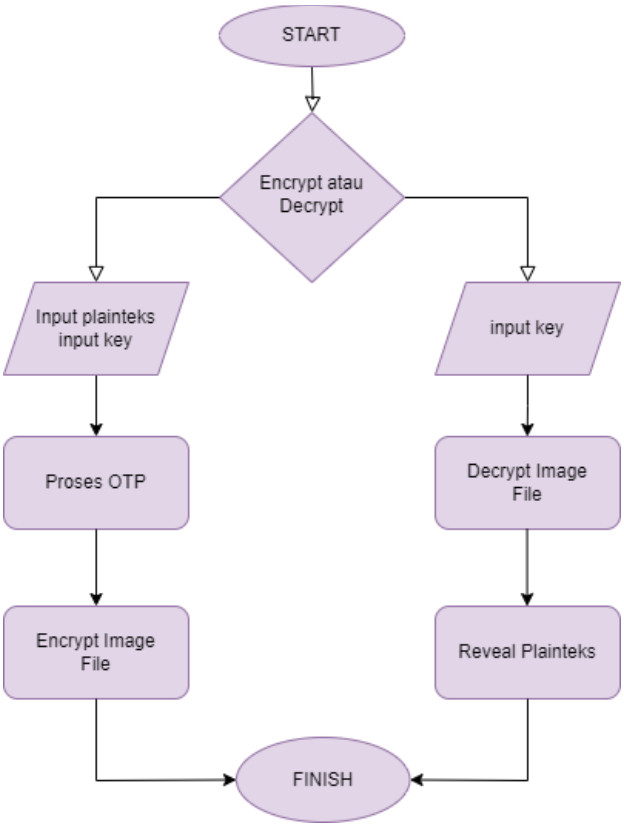
Metode penelitian yang dapat diterapkan pada penelitian ini mencakup serangkaian langkah-langkah sistematis. Berikut adalah rincian metode penelitian yang mungkin relevan:

1. Analisis

   Dalam penelitian ini, dilakukan analisis terhadap metode steganografi yang akan diterapkan untuk pengamanan email. Dua proses utama dalam implementasi steganografi adalah proses enkripsi dan dekripsi menggunakan *One Time Pad*. Proses enkripsi melibatkan penyisipan pesan rahasia ke dalam gambar, sedangkan proses dekripsi adalah ekstraksi pesan asli dari gambar tersebut. Enkripsi adalah proses memasukkan dokumen ke dalam gambar dan dekripsi adalah proses ekstraksi untuk mengeluarkan dokumen atau pesan asli [15].

2. Desain Program

   Aplikasi steganografi yang diusulkan akan dibuat untuk menyembunyikan pesan rahasia pada gambar lampiran email. Metode yang akan digunakan adalah Steganografi dengan *Penerapan One Time Pad* dan Metode LSB (*Least Significant Bit*) pada Gambar. Gambar alur desain program terlihat pada gambar 1 berikut:



Gambar 1. Alur desain program

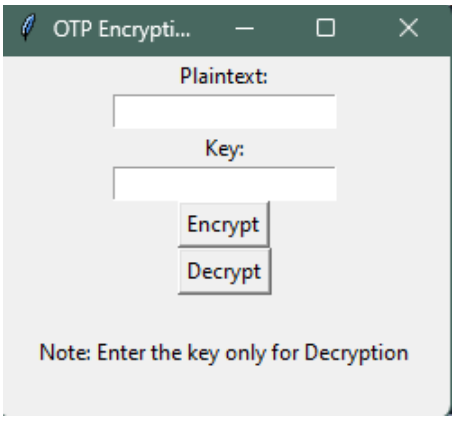
3. Implementasi Program

   Selanjutnya menerapkan program melalui steganografi menggunakan bahasa pemrograman Python, dengan penyatuan metode *One Time Pad* dan pendekatan *Least Significant Bit* (LSB) pada gambar lampiran, adalah fokus utama dalam penelitian ini. Proses implementasi ini melibatkan pengembangan solusi keamanan email, di mana teks pesan dapat dienkripsi menggunakan *One Time Pad*, dan hasilnya disematkan secara rahasia dalam piksel gambar lampiran dengan menggunakan metode LSB.

Hasil dan Pembahasan

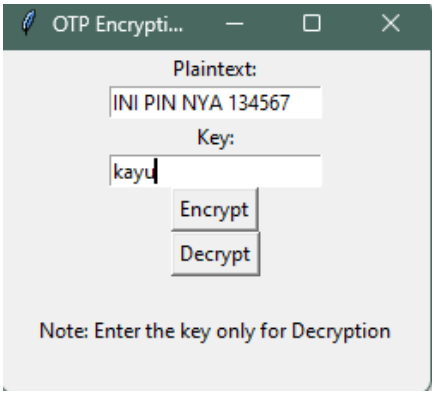
1. Hasil Penelitian

Berikut merupakan tampilan awal yang ditampilkan saat program dijalankan. Pada tampilan ini terdapat beberapa pilihan yang tersedia yaitu *Encrypt* dan *Decrypt*. Gambar 2. menunjukkan tampilan utama program.

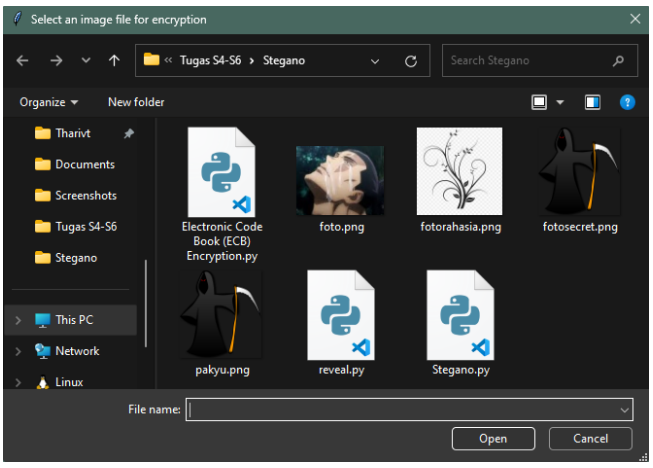


Gambar 2. Tampilan utama program

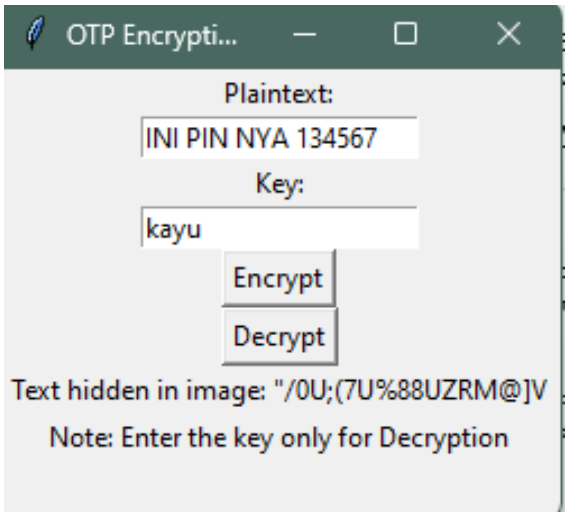
Setelahnya, pengguna dapat memasukkan teks biasa (*plaintext*) dan kunci (*key*) untuk mengamankan hasil enkripsi menggunakan metode OTP, *(One Time Pad)* yang kemudian akan disematkan dalam gambar melalui teknik steganografi. Pada Gambar 3. terlihat teks yang akan di enkripsi ke dalam gambar. Gambar 4. Menunjukan tampilan untuk memilih gambar yang akan di pilih. Pada Gambar 5. adalah tampilan yang muncul setelah enkripsi telah berhasil.



Gambar 3. Tampilan masukan teks dan key untuk enkripsi

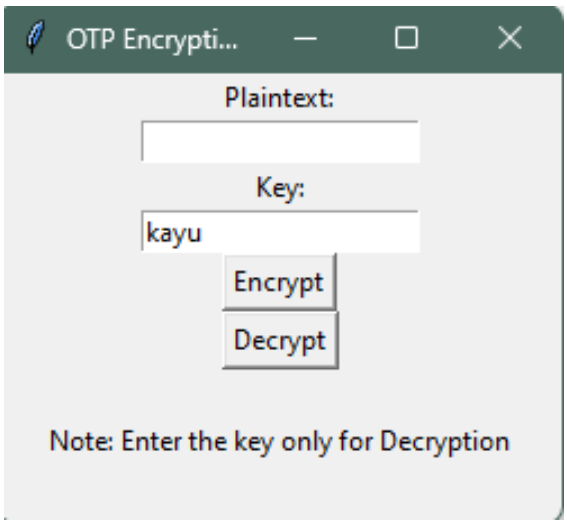


Gambar 4. Pilih foto

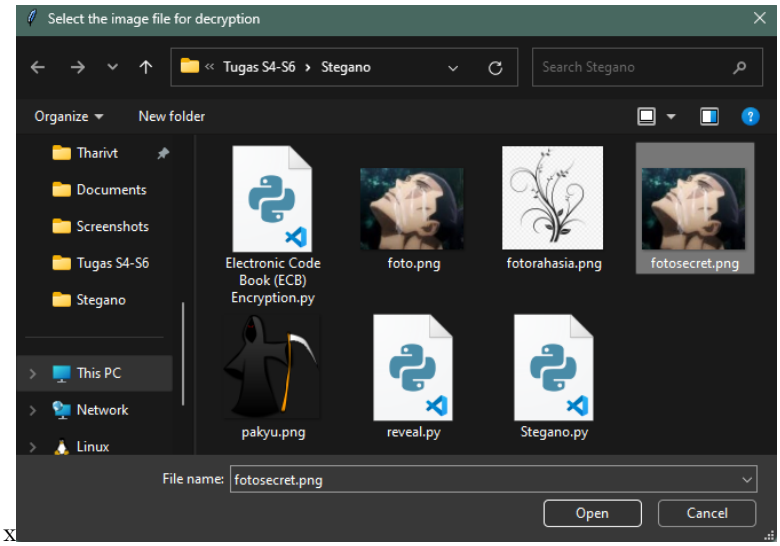


Gambar 5. Tampilan hasil enkripsi

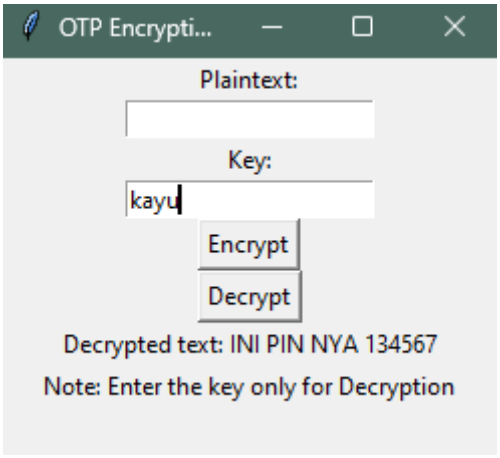
Setelahnya, pengguna dapat memasukkan kunci (*key*) enkripsi Gambar 6. dan gambar yang sudah terenkripsi yang sesuai untuk mendekripsi hasilnya Gambar 7. dengan menggunakan metode OTP (*One Time Pad*). Proses ini kemudian akan menghasilkan teks asli yang disembunyikan dalam gambar, melalui penerapan teknik steganografi. Gambar 8. Menunjukan tampilan teks yang sudah di dekripsi.



Gambar 6. Decrypt



Gambar 7. Pilih gambar untuk di decrypt



Gambar 8. Tampilan hasil program setelah decrypt

2. Pembahasan

Pada proses enkripsi menyembunyikan pesan bertujuan untuk mengubah pesan asli (*plaintext*) ke bentuk yang rahasia (*ciphertext*). Contoh perhitungan dengan menggunakan algoritma OTP (*One Time Pad*) adalah sebagai berikut:

Input Plainteks : INI PIN NYA 134567
Kunci : kayu
Plainteks
char = I = 73 = 01001001
char = N = 78 = 01001110
char = I = 73 = 01001001
char = [Spasi] = 32 = 00100000
char = P = 80 = 01010000
char = I = 73 = 01001001
char = N = 78 = 01001110

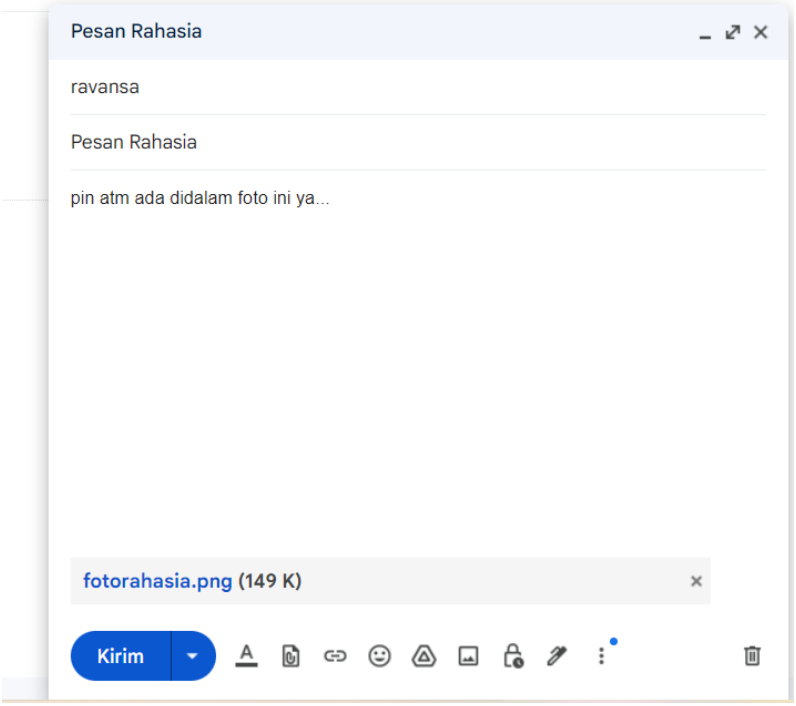
char = [Spasi] = 32 = 00100000
char = N = 78 = 01001110
char = Y = 89 = 01011001
char = A = 65 = 01000001
char = [Spasi] = 32 = 00100000
char = 1 = 49 = 00110001
char = 3 = 51 = 00110011
char = 4 = 52 = 00110100
char = 5 = 53 = 00110101
char = 6 = 54 = 00110110
char = 7 = 55 = 00110111

Kunci (*Key*)
char = K = 107 = 01101011
char = A = 97 = 01100001
char = Y = 121 = 01111001
char = U = 117 = 01110101
char = K = 107 = 01101011
char = A = 97 = 01100001
char = Y = 121 = 01111001
char = U = 117 = 01110101
char = K = 107 = 01101011
char = A = 97 = 01100001
char = Y = 121 = 01111001
char = U = 117 = 01110101
char = K = 107 = 01101011
char = A = 97 = 01100001
char = Y = 121 = 01111001
char = U = 117 = 01110101
char = K = 107 = 01101011
char = A = 97 = 01100001

Pengoperasian XOR Pada Biner Plainteks ke Biner Kunci per Bit
01001001 XOR 01101011 = 34 = "
01001110 XOR 01100001 = 47 = /
01001001 XOR 01111001 = 45 = 0
00100000 XOR 01110101 = 7 = U
01010000 XOR 01101011 = 57 = ;
01001001 XOR 01100001 = 47 = (
01001110 XOR 01111001 = 49 = 7
00100000 XOR 01110101 = 5 = U
01001110 XOR 01101011 = 23 = %
01011001 XOR 01100001 = 40 = 8
01000001 XOR 01111001 = 49 = 8
00100000 XOR 01110101 = 44 = U
00110001 XOR 01101011 = 12 = Z
00110011 XOR 01100001 = 43 = R
00110100 XOR 01111001 = 11 = M
00110101 XOR 01110101 = 48 = @
00110110 XOR 01101011 = 58 =]

00110111 XOR 01100001 = 26 = V
Hasil enkripsi = "/0U;(7U%88UZRM@]V

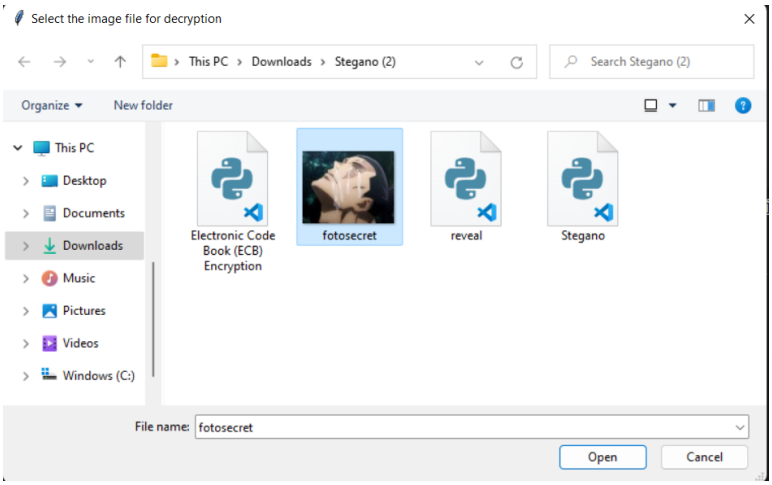
Berikut adalah implementasi mengirim pesan tersembunyi dengan lempiran gambar melalui Email. Gambar 9. Menunjukan pengiriman gambar via email



Gambar 9. Mengirim gambar via email

Setelah pesan berisi foto rahasia terkirim, selanjutnya pada perangkat penerima unduh foto rahasia tersebut, lalu jalankan program steganografi dan masukkan kunci "kayu" Gambar 10. dan file foto yang telah dienkripsi untuk melakukan dekripsi Gambar 11. Maka teks yang tersembunyi, yaitu "INI PIN NYA 134567" akan terungkap seperti di Gambar 12.

Gambar 10. Memasukan key



Gambar 11. Memilih file foto

Gambar 12. Proses dekripsi

Kesimpulan

Penelitian ini bertujuan meningkatkan keamanan komunikasi digital, khususnya melalui email, dengan mengintegrasikan Steganografi, *One Time Pad*, dan Metode *Least Significant Bit* (LSB) pada lampiran gambar. Hasil penelitian menunjukkan bahwa pendekatan ini efektif dalam menyediakan tingkat keamanan yang tinggi terhadap serangan pengintaian dan mencegah perubahan tidak sah pada lampiran gambar. Penerapan *One Time Pad* (OTP) pada email menyediakan lapisan keamanan tambahan melalui penggunaan kunci yang hanya digunakan sekali. Steganografi dengan metode LSB digunakan untuk menyembunyikan pesan rahasia dalam gambar tanpa mengubah tampilan visualnya secara signifikan. Pengujian sistem menunjukkan tingkat keamanan yang tinggi dan performa yang memadai. Kelebihan sistem ini terletak pada tingkat keamanan yang tinggi, terutama karena kombinasi Steganografi, OTP, dan metode LSB. Namun, kompleksitas implementasi menjadi keterbatasan yang harus diperhatikan. Meskipun demikian, hasil penelitian ini memberikan landasan untuk pengembangan lebih lanjut dalam pengamanan komunikasi digital, terutama di platform email.

Daftar Rujukan

[1] I. A. Susanto dan A. Solichin, "Enkripsi Data Penggajian Dengan Algoritma Caesar Cipher Dan Vigenere Cipher Pada Pt . Kemasindo Cepat Nusantara," SKANIKA, vol. 1, no. 1, pp. 399-404, 2018.

[2] Yusup, Irvan Maulana, Carudin Carudin, and Intan Purnamasari. "Implementasi Algoritma Caesar Cipher Dan Steganografi Least Significant Bit Untuk File Dokumen." Jurnal Teknik Informatika dan Sistem Informasi 6.3 (2020).

[3] N. Azis, "Perancangan aplikasi enkripsi dekripsi menggunakan metode caesar chiper dan operasi xor," Ikraith-Informatika, vol. 2, no. 1, pp. 72-80, 2018.

[4] Wijaya, Bayu Angga, et al. "St eganography Text Message Using LSB and DCT Methods." Jurnal Mantik 5.3 (2021): 1825-1832.

[5] Syahril, Muhammad, and Hendra Jaya. "Aplikasi steganografi pengamanan data nasabah di Standard Chartered Bank menggunakan metode Least Significant Bit dan RC4." Seminar Nasional Sains dan Teknologi Informasi (SENSASI). Vol. 2. No. 1. 2019.

[6] Taburet, T., Bas, P., Sawaya, W. and Fridrich, J., 2020. Natural steganography in JPEG domain with a linear development pipeline. IEEE Transactions on Information Forensics and Security, 16, pp.173-186.

[7] Edisuryana, M., Isnanto, R.R. and Somantri, M., 2013. Aplikasi Steganografi Pada Citra Berformat Bitmap Dengan Menggunakan Metode End Of File. Transient: Jurnal Ilmiah Teknik Elektro, 2(3), pp.734-742.

[8] H. Azis and F. Fattah, "Analisis Layanan Keamanan Sistem Kartu Transaksi Elektronik Menggunakan Metode Penetration Testing," Ilk. J. Ilm., vol. 11, no. 2, p. 167, 2019, doi: 10.33096/ilkom.v11i2.447.167-174.

[9] Setiadi, D.R.I.M., 2019. Payload Enhancement on Least Significant Bit Image Steganography Using Edge Area Dilation. International Journal of Electronics and Telecommunications, 65.

[10] Bansal, K., Agrawal, A. and Bansal, N., 2020, June. A survey on steganography using least significant bit (lsb) embedding approach. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184) (pp. 64-69). IEEE.

[11] Hasugian, Penda Sudarto Hasugian, and Agustina Simangunsong. "Implementation Of Least Significant Bit (LSB) Algorithm For Data Security In Digital Imagery." Jurnal Info Sains: Informatika dan Sains 10.2 (2020): 6-12.

[12] Prahmana, I. Gusti. "IMPLEMENTASI ALGORITMA OTP DAN STEGANOGRAFI EOF DALAM PENYISIPAN PESAN TEKS PADA CITRA." JTIK (Jurnal Teknik Informatika Kaputama) 6.2 (2022): 457-465.

[13] Sari, I.Y., Muttaqin, M., Jamaludin, J., Simarmata, J., Rahman, M.A., Iskandar, A., Pakpahan, A.F., Abdul Karim, S., Giap, Y.C., Hazriani, H. and Yendrianof, D., 2020. Keamanan Data dan Informasi. Yayasan Kita Menulis.

[14] Fathurrahmad, F., and Ester, E., 2020. Development And Implementation Of The Rijndael Algorithm And Base-64 Advanced Encryption Standard (AES) For Website Data Security. International Journal of Scientific & Technology Research, 9(11), pp.6-11.

[15] Wiranata, Ade Davy, and Rima Tamara Aldisa. "Aplikasi Steganografi Menggunakan Least Significant Bit (LSB) dengan Enkripsi Caesar Chipper dan Rivest Code 4 (RC4) Menggunakan Bahasa Pemrograman JAVA." Jurnal JTIK (Jurnal Teknologi Informasi dan Komunikasi) 5, no. 3 (2021): 277-281.