

OPTIMISASI INTERAKSI MANUSIA DAN KOMPUTER UNTUK MEMPERCEPAT PROSES ENKRIPSI VIGENÈRE CIPHER DENGAN MD5 DAN PENYISIPAN PESAN PADA GAMBAR STEGANOGRAFI

Asep Suryanta ¹, Yohanes Dwi Cahyono ², Ire Puspa Wardhani ³

^{1,2} Poltekad Kodiklatad

³ STMIK Jakarta STI&K

zenirakal@gmail.com

ABSTRAK

Keamanan informasi merupakan aspek krusial dalam pengelolaan data di era digital, dan teknologi kriptografi serta steganografi memainkan peran penting dalam menjaga kerahasiaan dan integritas data. Salah satu teknik enkripsi yang banyak digunakan adalah Vigenère Cipher, yang dapat dipadukan dengan algoritma hash MD5 untuk meningkatkan tingkat keamanannya. Namun, proses enkripsi menggunakan Vigenère Cipher dengan MD5 dan penyisipan pesan ke dalam gambar menggunakan steganografi sering kali memerlukan waktu yang signifikan, terutama saat operator harus menangani sejumlah besar pesan. Penelitian ini bertujuan untuk mengoptimalkan interaksi manusia-komputer (HCI) guna mempercepat proses enkripsi Vigenère Cipher dengan MD5 dan penyisipan pesan ke dalam gambar melalui teknik steganografi. Dengan merancang antarmuka yang lebih intuitif dan efisien, penelitian ini memungkinkan operator untuk mempercepat tugas mereka dalam proses enkripsi dan penyisipan pesan ke dalam gambar sehingga mengurangi potensi kesalahan, serta meningkatkan produktivitas secara keseluruhan.

Kata Kunci : *Interaksi Manusia dan Komputer, Kriptografi, Vigenere Cipher, MD5, Steganografi.*

1. PENDAHULUAN

Teknologi informasi dibuat dengan tujuan untuk membantu kehidupan manusia supaya menjadi lebih mudah, efektif dan efisien. Demikian juga sistem informasi, ditujukan untuk membantu kehidupan manusia supaya pekerjaan yang tadinya sulit, memakan banyak waktu dan tenaga bisa menjadi lebih cepat dikerjakan dan lebih mudah dengan adanya sistem informasi.

Sistem informasi dibangun dengan syarat-syarat tertentu yang harus dipenuhi sehingga sistem informasi tersebut bisa dikatakan sukses, syarat tersebut diantaranya adalah mudah digunakan, aman, efektif dan efisien. Sistem informasi yang tidak memenuhi syarat-syarat tersebut bisa dikatakan bahwa sistem informasi tersebut tidak berhasil [1].

Dalam konteks pengamanan informasi, antarmuka yang ramah pengguna dan intuitif sangat diperlukan untuk memastikan bahwa proses yang kompleks, seperti enkripsi data dan penyisipan steganografi, dapat dilakukan dengan mudah dan cepat, mengurangi kemungkinan kesalahan dan meningkatkan produktivitas pengguna.

Salah satu metode enkripsi yang banyak digunakan untuk melindungi pesan adalah Vigenère Cipher, sebuah algoritma yang mengenkripsi teks menggunakan kunci yang berbeda untuk setiap karakter, menjadikannya lebih aman daripada metode enkripsi sederhana [2]. Meskipun Vigenère Cipher memiliki kelemahan dalam tingkat keamanan [3], penggabungannya dengan algoritma hash MD5 dapat meningkatkan keamanannya lebih lanjut. MD5

berfungsi untuk menghasilkan hash unik dari pesan yang dienkripsi, memberikan lapisan tambahan untuk menjaga kerahasiaan informasi yang sensitif [4].

Namun, meskipun teknologi ini sudah efektif dalam meningkatkan keamanan pesan, tantangan utama yang dihadapi adalah proses yang memakan waktu. Operator seringkali harus menangani sejumlah besar pesan untuk dienkripsi dan disisipkan dalam gambar menggunakan steganografi. Steganografi sendiri adalah teknik untuk menyembunyikan pesan dalam media lain, seperti gambar, sehingga pesan tersebut tidak terdeteksi oleh pihak yang tidak berwenang. Proses penyisipan pesan ini, yang melibatkan pengolahan gambar dan data, dapat memperlambat kinerja operator dan meningkatkan potensi kesalahan [5].

Oleh karena itu, penelitian ini bertujuan untuk mengoptimalkan HCI dalam rangka mempercepat proses enkripsi Vigenère Cipher dengan MD5 dan penyisipan pesan ke dalam gambar menggunakan teknik steganografi [6]. Dengan merancang antarmuka pengguna yang lebih intuitif dan efisien, penelitian ini memungkinkan operator untuk mempercepat proses enkripsi dan penyisipan pesan, mengurangi kesalahan operasional, serta meningkatkan produktivitas secara keseluruhan [7].

Dengan demikian, penelitian ini tidak hanya berfokus pada keamanan data, tetapi juga pada efisiensi dan kecepatan dalam pelaksanaannya, dengan harapan memberikan kontribusi terhadap pengembangan sistem pengamanan informasi yang lebih aman, cepat, dan mudah dioperasikan [8].

2. TINJAUAN PUSTAKA

Interaksi manusia dan komputer atau human computer interaction (HCI) merupakan suatu disiplin ilmu yang mengkaji komunikasi atau interaksi di antara pengguna dengan sistem. Peran utama HCI adalah untuk menghasilkan sebuah sistem yang berguna, aman, produktif, efektif, efisien dan fungsional [1]. Dalam konteks pengamanan informasi, HCI berkontribusi dalam penyederhanaan proses yang kompleks, seperti enkripsi data, sehingga pengguna dapat menjalankan tugasnya dengan lebih mudah dan minim kesalahan.

Salah satu metode enkripsi yang sering digunakan untuk melindungi pesan adalah Vigenère Cipher, sebuah algoritma kriptografi klasik yang mengenkripsi teks menggunakan kunci yang berbeda untuk setiap karakter. Algoritma ini memberikan tingkat keamanan yang lebih tinggi dibandingkan metode substitusi sederhana karena sifatnya yang polialfabetik [2]

Meskipun demikian, kelemahan Vigenère Cipher, seperti rentannya terhadap analisis kunci, menjadi perhatian utama dalam pengembangan sistem yang lebih aman. Kombinasi dengan algoritma hash seperti MD5 dapat meningkatkan keamanan pesan dengan memastikan integritas data melalui hash unik, memberikan lapisan perlindungan tambahan [4].

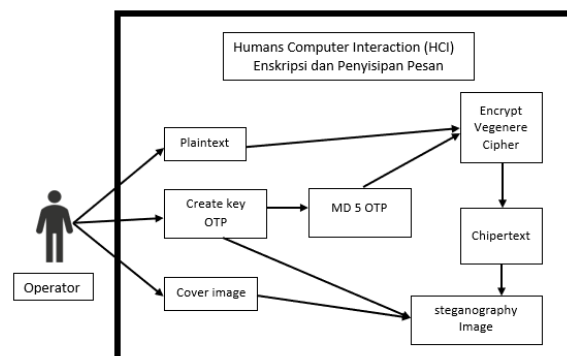
Selain enkripsi, teknik steganografi juga memainkan peran penting dalam pengamanan informasi. Steganografi adalah seni dan ilmu menyembunyikan pesan rahasia di dalam media lain, seperti gambar, audio, atau video, sehingga keberadaan pesan tersebut tidak terdeteksi oleh pihak yang tidak berwenang. Teknik ini melibatkan proses penyisipan data yang cermat agar tidak merusak media asli dan memastikan pesan tetap tersembunyi. Kombinasi antara kriptografi dan steganografi memberikan tingkat keamanan berlapis, di mana pesan tidak hanya dienkripsi tetapi juga disembunyikan, menjadikannya lebih sulit diakses oleh pihak yang tidak berwenang [5].

Dengan peran HCI yang mendukung antarmuka pengguna yang intuitif dan efektif, baik proses enkripsi menggunakan Vigenère Cipher maupun penyisipan pesan melalui steganografi dapat dilakukan dengan lebih efisien, mengurangi potensi kesalahan, dan meningkatkan produktivitas operator.

3. METODE PENELITIAN

Dalam penelitian ini, fokus utama adalah pada pembuatan antarmuka pengguna yang intuitif dan efisien untuk [9] memudahkan operator dalam proses enkripsi pesan menggunakan Vigenère Cipher dan penyisipan pesan ke dalam gambar melalui teknik

steganografi. Antarmuka ini dirancang untuk menyederhanakan tugas operator, mengurangi potensi kesalahan, serta meningkatkan produktivitas dalam melakukan enkripsi dan penyisipan pesan rahasia. Langkah awal melibatkan pemahaman mendalam tentang konsep dasar HCI, steganografi, Vigenère Cipher, dan algoritma MD5, yang kemudian digunakan untuk mengembangkan prototipe antarmuka yang optimal. Pengujian dilakukan untuk mengevaluasi efektivitas dan efisiensi antarmuka dalam mendukung operator menyelesaikan proses enkripsi dan penyisipan pesan dengan cepat dan akurat. Dapat dilihat pada Gambar di bawah ini.

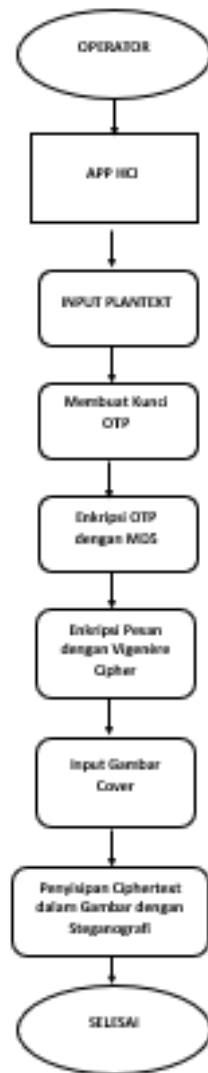


Gambar 1. Alur Interaksi HCI [10]

Gambar diatas menunjukkan alur interaksi yang dimulai dari operator dalam proses enkripsi dan penyisipan pesan dengan menggunakan Human-Computer Interaction (HCI).

Pertama, operator menyediakan tiga komponen utama: pesan asli atau plaintext, kunci sekali pakai (One-Time Pad atau OTP) untuk keamanan tambahan, dan gambar yang akan menjadi media penyisipan pesan. Kunci OTP yang telah dibuat akan dienkripsi terlebih dahulu menggunakan algoritma MD5 untuk menghasilkan nilai hash yang unik [11]. Selanjutnya, plaintext dan hasil MD5 dari OTP tersebut diproses menggunakan algoritma Vigenère Cipher, menghasilkan ciphertext. Ciphertext ini adalah bentuk terenkripsi dari pesan asli dan siap untuk disisipkan ke dalam gambar. Sebagai langkah terakhir, ciphertext disisipkan ke dalam gambar menggunakan teknik steganografi, sehingga gambar akhir berfungsi sebagai media yang menyimpan pesan rahasia tanpa mudah terdeteksi oleh pihak yang tidak berwenang. Proses ini mengoptimalkan keamanan dan kerahasiaan pesan yang dikirimkan.

Berikut adalah diagram alur untuk pembuatan Human-Computer Interaction (HCI) dalam proses enkripsi dan penyisipan pesan steganografi.



Gambar 1. Diagram Alur [12]

4. HASIL DAN PEMBAHASAN

Tahap perancangan aplikasi ini bertujuan untuk memudahkan operator dalam melakukan enkripsi pesan hingga penyisipan pesan tersebut ke dalam gambar menggunakan teknik steganografi. Berikut adalah tahapan perancangan aplikasi:

- a. Input Data dan Kunci Rahasia: Aplikasi dirancang untuk memungkinkan operator memasukkan pesan atau plaintext yang ingin dienkripsi serta kunci rahasia (One-Time Pad atau OTP) yang akan digunakan sebagai bagian dari proses enkripsi. Kunci rahasia ini berfungsi sebagai perlindungan tambahan untuk memastikan bahwa pesan hanya bisa diakses oleh pihak yang memiliki kunci tersebut.

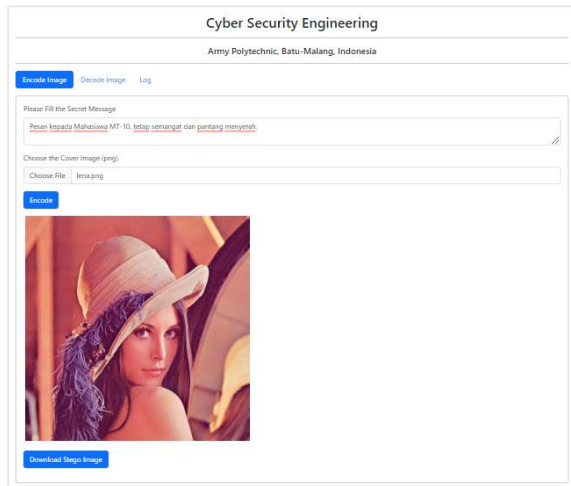
- b. Enkripsi dengan Vigenère Cipher: Setelah menerima pesan dan kunci OTP, aplikasi akan mengenkripsi pesan menggunakan algoritma Vigenère Cipher. Algoritma ini mengubah plaintext menjadi ciphertext yang lebih aman dan sulit ditebak. Proses ini membantu menjaga kerahasiaan pesan dari pihak yang tidak berwenang.
- c. Hashing dengan MD5: Untuk meningkatkan keamanan, kunci OTP yang digunakan akan dienkripsi terlebih dahulu dengan algoritma MD5 untuk menghasilkan hash unik. Hash MD5 ini berfungsi sebagai lapisan keamanan tambahan yang menguatkan tingkat perlindungan pesan, sehingga semakin sulit untuk dipecahkan oleh pihak luar tanpa kunci yang benar.
- d. Penyisipan Pesan dengan Steganografi: Setelah pesan terenkripsi dihasilkan, aplikasi akan menyisipkan ciphertext ke dalam gambar dengan teknik steganografi. Proses ini membuat pesan rahasia tersembunyi di dalam gambar, sehingga tidak mudah dideteksi oleh pihak yang tidak berwenang. Operator dapat memilih gambar yang akan dijadikan media penyimpanan pesan rahasia.
- e. Antarmuka Pengguna yang Intuitif: Aplikasi ini dirancang dengan antarmuka yang sederhana dan intuitif, sehingga memudahkan operator dalam mengoperasikan seluruh proses, mulai dari enkripsi hingga penyisipan pesan. Dengan demikian, operator dapat melakukan tugasnya dengan cepat, mengurangi kemungkinan kesalahan, dan meningkatkan efisiensi kerja [13].

Hasil akhir dari aplikasi ini adalah gambar yang telah berisi pesan rahasia dalam bentuk ciphertext yang disisipkan, sehingga pesan dapat dikirim dengan aman dan hanya bisa diakses oleh penerima yang memiliki kunci dekripsi yang sesuai. Adapun tampilan aplikasi yang sudah dibuat dapat dilihat pada gambar dibawah ini:



Gambar 2. Tampilan Awal Aplikasi

Berikut adalah proses memasukan pesan yang akan di enkripsi dan media gambar yang akan disisipkan pesan setelah di enkripsi.



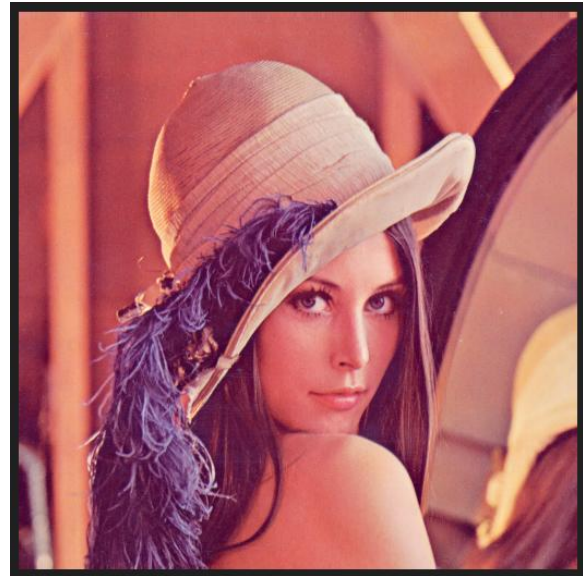
Gambar 3. Tampilan Proses Input Data

Berikut adalah tampilan dimana pesan yang di enkripsi dengan algoritma MD5 dan vegenere cipher sudah berhasil diproses yang dapat dilihat melalui Tab “LOG”.



Gambar 4. Tampilan Layout “Log”

Berikut adalah hasil Enkripsi Plaintext yang sudah di sisipkan ke *Image Steganography*.



Gambar 5. Hasil Gambar Steganografi

Pengujian selanjutnya dilakukan untuk memastikan bahwa suatu event atau input menjelaskan proses yang tepat dan menghasilkan output yang sesuai dengan rancangan yang telah dibuat, berikut hasil pengujian untuk aplikasi ini.

Tabel 1. Pengujian Aplikasi [8]

Skenario Uji	Text case	Hasil yang diharapkan	Keterangan
Memilih Button Encode Image	Memilih Button Encode Image	Menampilkan tampilan Input pesan yang akan di enkripsi	Sesuai
Memasukan Plaintext Berita	Memasukan Plaintext Berita	Menampilkan tampilan Layout text untuk mengetik pesan yang akan di enkripsi	Sesuai
Memilih Button Choose File	Memilih Button Choose File	Menampilkan tampilan Button untuk memilih file image yang akan disisipkan pesan yang sudah di enkripsi	Sesuai
Memilih Button Encode	Memilih Button Encode	Menampilkan tampilan Butoon untuk memproses pesan yang sudah di enkripsi dan di sisipkan kedalam image steganografi	Sesuai
Memilih Button Log	Memilih Button Log	Menampilkan tampilan Butoon untuk mengecek apakah proses enkripsi dan penyisipan berita berhasil dilakukan	Sesuai

Dari hasil pengujian enkripsi pesan, di dapatkan hasil bahwasanya proses pesan yang di enkripsi kemudian di sisipkan kedalam steganografi berhasil dilakukan dengan cara mengecek kedalam menu Tab “LOG” tanpa mengalami error ataupun kerusakan.

5. KESIMPULAN DAN SARAN

Kesimpulan dari Aplikasi Human-Computer Interaction (HCI) yang dirancang untuk menyederhanakan proses enkripsi dan steganografi dengan antarmuka yang intuitif yakni memudahkan operator tanpa memerlukan pemahaman teknis yang

mendalam. Dengan mengintegrasikan enkripsi Vigenere Cipher, hashing MD5, dan teknik steganografi, aplikasi ini memberikan keamanan berlapis, memastikan pesan terenkripsi tetap tersembunyi dan sulit diakses oleh pihak yang tidak berwenang. Sistem ini juga meningkatkan efisiensi operasional melalui proses yang cepat dan terintegrasi, memungkinkan penyisipan pesan ke dalam gambar dapat dilakukan dengan mudah. Secara keseluruhan, aplikasi ini menawarkan solusi keamanan data yang praktis, efektif, dan komprehensif bagi pengguna.

Adapun saran kedepan untuk meningkatkan kualitas aplikasi HCI dalam enkripsi dan steganografi, disarankan untuk memperbarui antarmuka pengguna agar lebih fleksibel, interaktif, dan dilengkapi visualisasi proses serta panduan bagi pengguna baru. Selain itu, dukungan untuk berbagai format media, seperti video dan audio, dapat ditambahkan guna memperluas penerapannya dalam pengamanan data. Optimasi performa dan skalabilitas juga menjadi prioritas, terutama untuk penggunaan skala besar, sehingga dapat mempercepat proses enkripsi, hashing, dan penyisipan pesan tanpa mengurangi keamanan. Dengan pengembangan ini, aplikasi diharapkan semakin aman, efisien, dan relevan untuk kebutuhan masa depan.

DAFTAR PUSTAKA

- [1] S. Sekolah Terang Bangsa, "Penerapan Model Human Computer Interaction (HCI) dalam Analisis Sistem Informasi," 2011.
- [2] L. Budi Handoko, "SEKURITI TEKS MENGGUNAKAN VIGENERE CIPHER DAN HILL CIPHER," 2022.
- [3] A. Ibezato Zalukhu, Z. Sitorus, and N. Septiani, "Enhancing Text Messages with a Combination of Vigenère Cipher and One Time Pad Using Random Key LFSR," *Jurnal Sains dan Teknologi*, vol. 6, no. 1, pp. 52–57, doi: 10.55338/saintek.v6i1.3190.
- [4] S. Hajar, "Analisa Metode Message Digest 5 (Md5) Untuk Mendeteksi Orisinalitas Citra Digital," 2021.
- [5] W. S. Sari, E. H. Rachmawanto, D. R. I. M. Setiadi, and C. A. Sari, "A Good Performance OTP encryption image based on DCT-DWT steganography," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 15, no. 4, pp. 1987–1995, Dec. 2017, doi: 10.12928/TELKOMNIKA.v15i4.5883.
- [6] M. Dedi Irawan, "IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER DENGAN PHP," 2017.
- [7] R. Pushpakumar *et al.*, "Human-Computer Interaction: Enhancing User Experience in Interactive Systems," in *E3S Web of Conferences*, EDP Sciences, Jul. 2023. doi: 10.1051/e3sconf/202339904037.
- [8] I. Mahardika Seno, A. Puspita Sari, and W. Gunawan, "Aplikasi Enkripsi dan Dekripsi untuk Keamanan Komunikasi Data pada SMS (Short Message Service) Berbasis Android Menggunakan Algoritma Blowfish," 2019.
- [9] A. C. Ferariani, A. Senubekti, and T. Sumarni, "OPTIMALISASI PENGALAMAN PENGGUNA MELALUI DESAIN ANTARMUKA PENGGUNA INTUITIF MELALUI SISTEM MONEV SOP," 2024.
- [10] S. Sekolah Terang Bangsa, "Penerapan Model Human Computer Interaction (HCI) dalam Analisis Sistem Informasi," 2011.
- [11] "13. JURNAL PENINGKATAN KEAMANAN LOGIN WEBSITE DENGAN".
- [12] D. Sinaga, "APLIKASI ENKRIPSI DAN DEKRIPSI DENGAN METODE VIGENERE CIPHER BERBASIS ANDROID."
- [13] T. F. M. Syafei and A. Hidayatullah, "Analisis Penerapan UI/UX Dalam Meningkatkan Pengalaman Pengguna Pada Sistem Reservasi Amadeus," *JUSTINFO | Jurnal Sistem Informasi dan Teknologi Informasi*, vol. 1, no. 1, pp. 1–8, Dec. 2023, doi: 10.33197/justinfo.vol1.iss1.2023.1252