Pengamanan Pesan Sandi Menggunakan Kombinasi Metode Enkripsi Vigenere dan Metode Steganografi Least Significant Bit (LSB) dengan Teknik Distribusi Pesan Linear Congruential Generator (LCG)

Diajukan Sebagai Syarat untuk Menyelesaikan
Pendidikan Program Strata-1 Pada
Jurusan Teknik Informatika

Oleh:
Ahmad Syauqi Syuhada
NIM: 09021281924087

JURUSAN TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS SRIWIJAYA
2023

LEMBAR PENGESAHAN SKRIPSI

Pengamanan Pesan Sandi Menggunakan Kombinasi Metode Enkripsi Vigenere dan Metode Steganografi Least Significant Bit (LSB) dengan Teknik Distribusi Pesan Linear Congruential Generator (LCG)

Oleh:

Ahmad Syauqi Syuhada

NIM: 09021281924087

Palembang, Desember 2023

Pembimbing 1

Osvari Arsalan, S.Kom., M. T
NIP 198806282018031001

Pembimbing 2

Rizki Kurniati, M. T
NIP 199107122019032016

Mengetahui,

Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom
NIP 197812222006042003

TANDA LULUS UJIAN KOMPREHENSIF SKRIPSI

Pada hari Senin tanggal 27 November 2023 telah dilaksanakan ujian komprehensif skripsi oleh Jurusan Teknik Informatika Fakultas Ilmu Komputer Universitas Sriwijaya

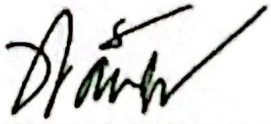
Nama : Ahmad Syauqi Syuhada
NIM : 09021281924087
Judul : Pengamanan Pesan Sandi Menggunakan Kombinasi Metode Enkripsi Vigenere dan Metode Steganografi Least Significant Bit (LSB) dengan Teknik Distribusi Pesan Linear Congruential Generator (LCG)

dan dinyatakan LULUS.

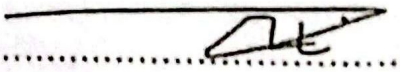
1. Ketua Penguji

Yunita, M. Cs.
NIP 198306062015042002 ..... 

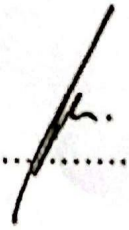
2. Penguji

Samsuryadi, M.Kom., Ph.D.
NIP 197102041997021003 ..... 

3. Pembimbing I

Osvari Arsalan, S.Kom., M. T.
NIP 198806282018031001 ..... 

4. Pembimbing II

Rizki Kurniati, M. T.
NIP 199107122019032016 ..... 

Mengetahui,
Ketua Jurusan Teknik Informatika

Alvi Syahrini Utami, M.Kom.
NIP 197812222006042003

HALAMAN PERNYATAAN BEBAS PLAGIAT

Yang bertanda tangan di bawah ini:

Nama : Ahmad Syauqi Syuhada

NIM : 09021281924087

Program Studi : Teknik Informatika Reguler

Judul Skripsi : Pengamanan Pesan Sandi Menggunakan Kombinasi Metode Enkripsi Vigenere dan Metode Steganografi Least Significant Bit (LSB) dengan Teknik Distribusi Pesan Linear Congruential Generator (LCG)

Hasil Pengecekan *iThenticate/Turnitin*: 5%

Menyatakan bahwa laporan proyek saya merupakan hasil karya sendiri dan bukan hasil penjiplakan/plagiat. Apabila ditemukan unsur penjiplakan/plagiat dalam laporan proyek ini, maka saya bersedia menerima sanksi akademik dari Universitas Sriwijaya sesuai dengan ketentuan yang berlaku.

Demikian, pernyataan ini saya buat dengan sebenarnya dan tidak ada paksaan oleh siapa pun.

Palembang, Desember 2023

Ahmad Syauqi Syuhada

NIM 09021281924087

MOTTO DAN PERSEMBAHAN

"Jadilah pintar seperti Abdullah Bin Mas'ud, bagaikan telaga yang dapat menghilangkan haus orang-orang yang menemuinya"

Umar Bin Khattab

Kupersembahkan Karya Tulis ini kepada:

- Allah SWT
- Orang Tua dan Saudaraku
- Dosen Pembimbing
- Teman-teman Seperjuangan
- Universitas Sriwijaya

ABSTRACT

The exchange of information, still vulnerable amid technological advancements, prompts software developers to enhance digital security strategies. This research conducts experiments by combining three layers of security—Vigenere encryption, Least Significant Bit (LSB) method, and Linear Congruential Generator (LCG) method—as a solution to improve digital security. To assess the accuracy of the security model, the generated images are measured using Peak Signal-to-Noise Ratio (PSNR) calculations. Information is encrypted using Vigenere encryption, which encrypts each plaintext character in the input data with a different key. The encrypted data is then concealed in the least significant bits of color pixels using the LSB method. Augmented with the LCG method to randomly distribute the data bits within the bits of a PNG image, enhancing overall security. The images resulting from all processes are then evaluated by examining the matrix of the generated image (PSNR). A higher PSNR value indicates a better-quality image, and vice versa. All data hidden within the images can be retrieved precisely as the original condition when needed. The data used in this study consists of KPM photos in PNG format, with variations of hidden data in TXT format. All experiments conducted were successfully re-extracted only if the correct keywords were entered. The average PSNR value obtained from the experiments reached 77.230.

***Keywords**: Vigenere Chiper, Least Significant Bit (LSB), Linear Congruential Generator (LCG)*

ABSTRAK

Pertukaran informasi yang masih rentan di tengah kemajuan teknologi merespon para pengembang perangkat lunak untuk meningkatkan strategi keamana digital. Penelitian ini melakukan eksperimen dengan menggabungkan 3 lapisan keamanan, yaitu enkripsi vigenere, metode *Least Significant Bit* (LSB) dan metode *Linear Congruential Generator* (LCG), sebagai solusi untuk meningkatkan keamanan digital. Untuk mengetahui tingkat akurasi model pengamanan, citra yang dihasilkan diukur menggunakan perhitungan *Peak Signal-to-Noise Ratio* (PSNR). Informasi akan dienkripsi menggunakan Enkripsi Vigenere yang mengenkripsi setiap karakter plainteks pada data yang diinput dengan kunci yang berbeda. Data yang sudah dienkripsi akan disembunyikan di dalam bit-bit terkahir *pixel* warna menggunakan metode LSB. Dilengkapi dengan metode LCG untuk menyebarkan bit-bit data secara acak di dalam bit-bit citra PNG sehingga keamanan menjadi lebih kuat. Citra yang dihasilkan dari semua proses kemudian dihitung dengan melihat matriks dari citra yang dihasilkan (PSNR). Semakin besar nilai PSNR, maka semakin bagus citra yang dihasilkan, begitu pun sebaliknya. Semua data yang sudah disembunyikan di dalam citra dapat diambil kembali ketika dibutuhkan persis dengan kondisi semula. Data yang digunakan dalam penelitian ini adalah foto KPM dengan format PNG dan variasi data yang disembunyikan dengan format TXT. Semua percobaan yang dilakukan berhasil diekstrak kembali hanya jika dimasukkan kata kunci yang benar. Dari hasil percobaan didapatkan nilai rata-rata PSNR mencapai 77.230.

Kata Kunci: Enkripsi Vigenere, *Least Significant Bit* (LSB), *Linear Congruential Generator* (LCG).

KATA PENGANTAR

Alhamdulillah, segala puji dan syukur hanya untuk Allah sebagai satu-satunya Ilahi Rabbi yang atas Rahmat dan Karunia-Nya yang melimpah kepada penulis sehingga dapat menyelesaikan dengan baik tugas akhir ini. Selesainya tugas akhir ini sebagai bukti telah memenuhi syarat menyelesaikan program Strata-1 Program Studi Teknik Informatika Fakultas Ilmu Komputer di Universitas Sriwijaya.

Sepanjang perjalan proses menyelesaika tugas akhir ini, banyak pihak yang telah membantu dan berperan dengan memberi dukungan, arahan serta serta bantuan baik secara langsung ataupun tidak. Oleh karena itu, penulis ingin mengucapkan terimakasih tiada hingga kepada:

1. Allah swt. atas nikmat, kekuatan, kelancaran, kesabaran, kemudahan, kesehatan dan segala Rahmat yang selalu tercurah sehingga penulis dapat menyelesaikan tugas akhir ini dengan rasa syukur yang begitu dalam.
2. Kedua orang tua serta saudara-saudara yang sudah mendukung dan mendoakan agar tetap semangat dan berproses dalam menempuh masa studi.
3. Ketua jurusan Teknik Informatika, Ibu Alvi Syahrini Utami, M.Kom. yang telah kooperatif dan suportif dalam membantu menyelesaikan tugas akhir.
4. Bapak Osvari Arsalan, M.T. dan Ibu Rizki Kurniati, M.T. selaku dosen pembimbing tugas akhir yang telah dengan sabar memberikan saya bimbingan, saran, motivasi serta waktunya agar saya dapat menyelesaikan tugas akhir.

5. Seluruh Civitas Akademika Fakultas Ilmu Komputer Universita Sriwijaya yang telah memberikan ilmu selama masa studi Strata-1.
6. Teman-teman seperilmuan di Keluarga Informatika Regular A Indralaya yang sudah menemani menimba ilmu koding semenjak awal perkuliahan di Universita Sriwijaya sampai sekarang.
7. Kawan-kawan, kakak dan adik seperjuangan di LDF WIFI dan LDK NADWAH yang sudah semangat dalam menjaga nafas dakwah di tanah layo.
8. Sobat-sahabat snake yang sudah menampung dan menyambut ketidakjelasan penulis ketika masa sulit maupun mudah dalam masa-masa menimba ilmu di tanah orang.
9. Pasukan Berkuda Idralaya yang telah menjadi tempat menuangkan kesah dan resah menjadi semangat selama proses penyelesaian tugas akhir serta banyaknya pengalaman baru yang tak terlupakan.
10. Seluruh pihak yang tidak dapat disebutkan satu persatu yang telah terlibat dalam pengerjaan tugas akhir secara langsung maupun tidak langsung hingga akhirnya tugas akhit ini dapat berakhir dengan baik.
11. *The one and only, my self,* yang sudah berjuang dan berdiri dengan dua kakinya sendiri untuk menimba ilmu di tanah perantauan. Kamu hebat! Kamu Kuat!

Penulis menyadari bahwa dalam penyusunan dan penyelesaian tugas akhir ini masih jauh dari kata sempurna, karena mungkin masih terdapat kesalahan dan kekurangan atas sebab terbatasnya pengetahuan dan pengalaman. Oleh sebab itu,

penulis mengharapkan kritik dan saran yang membangun untuk kemajuan kemampuan penulis ke depannya. Besar harapan penelitian ini dapat bermanfaat bagi orang banyak.

Indralaya, 19 Oktober 2023

Ahmad Syauqi Syuhada

09021281924087

DAFTAR ISI

Halaman

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Pendahuluan

Pada bab I ini akan membahas tentang latar belakang masalah, rumusan masalah, tujuan dan manfaat dari penelitian, serta batasan masalah. Setiap subbab pada bab ini berisi penjelasan keseluruhan gambaran penelitian secara umum.

1.2 Latar Belakang Masalah

Pertumbuhan ilmu pengetahuan dan teknologi yang terus meningkat mendorong pesatnya transformasi digital di dunia, termasuk Indonesia. Pesatnya perkembangan teknologi juga berdampak terhadap pertukaran informasi. Namun, ternyata data yang dipertukarkan masih rentan terhadap *cyber crime.* Pusat Informasi Kriminal Nasional (Pusiknas) melaporkan bahwa polri telah menindak 8.831 kasus terkait kejahatan siber terhitung sejak 1 Januari sampai 22 Desember 2022 dimana manipulasi data dan *hacking* masuk dalam 5 kasus yang paling banyak terjadi. Selain itu, dikutip dari BBC pada 18 Juli 2023 bahwa 337 juta data yang diduga dari Dukcapil Kemendagri telah diretas dan ditawarkan dalam forum online *hacker* BreachForums. Pencurian data ini disebabkan karena data yang tidak diamankan sesuai standar yang baik.

Berkembangnya kasus kejahatan cyber telah memberikan dorongan bagi para pengembang perangkat lunak untuk merancang strategi keamanan yang beragam dengan menggunakan berbagai metode dan tingkat perlindungan. Dari penerapan enkripsi simetris dan asimetris hingga penggunaan enkripsi jaringan,

berbagai pendekatan diambil untuk memitigasi risiko keamanan. Selain itu, teknik steganografi serta metode distribusi data juga diterapkan dalam upaya untuk meningkatkan keamanan data.

Penerapan keamanan data dengan menyisipkan informasi ke dalam media lain dapat menghindari kecurigaan ataupun tahan terhadap deteksi yang dapat dilakukan pihak yang tidak bertanggung jawab ketika pertukaran informasi dilakukan. Enkripsi juga perlu diterapkan untuk menjaga integritas data serta pencegahan akses tidak sah.

Solusi yang pernah dilakukan untuk memberikan keamanan data pernah dilakukan oleh Ami Aisiah (2017) dengan melakukan enkripsi menggunakan *Advanced Encryption Standard* (AES) didapatkan hasil bahwa enkripsi yang dilakukan dapat memberikan keamanan yang efektif dan efisien karena pola algoritma yang cukup acak dan kecepatan komputasi yang unggul.

Penelitian steganografi dan kriptografi lainnya dalam pengamanan data pernah dilakukan sebelumnya oleh (Purba et al., 2021) di Telkom Akses Kabanjahe, perusahaan yang menyediakan layanan jaringan internet, menggunakan metode LSB dan enkripsi *Vigenere*. Penelitian di Telkom Akses Kabanjahe mendapatkan hasil bahwa informasi rahasia yang sebelumnya sudah disisipkan ke dalam gambar dapat dipulihkan kembali sama persis dengan kondisi awal dan terdapat perubahan dimensi citra yang terjadi tetapi perubahan tersebut tidak nampak secara kasat mata. Oleh karena itu, penelitian ini melakukan pengujian pengamanan data menggunakan metode enkripsi *Vigenere*, metode LSB dan penerapan metode LCG.

1.3 Rumusan Masalah

Untuk lebih menjamin keamanan data dalam foto KPM yang dalam penelitian ini menggunakan metode enkripsi *Vigenere,* metode LSB dan metode LCG agar aman dari pihak yang tidak bertanggung jawab, maka rumusan masalah dari penelitian ini adalah sebagai berikut:

1. Bagaimana menerapkan sistem keamanan dengan menggunakan metode enkripsi *Vigenere*, metode LSB dan metode LCG pada gambar.
2. Bagaimana tingkat ketepatan dalam menghindari kecurigaan terhadap penyembunyian data menggunakan metode enkripsi *Vigenere,* metode LSB dan metode LCG pada citra digital yang diukur menggunakan *Peak Signal-to-Noise Ratio* (PSNR).

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah :

1. Memberikan keamanan dengan menerapkan sistem keamanan dengan menggunakan metode enkripsi *Vigenere,* metode LSB dan metode LCG pada gambar.
2. Mengetahui tingkat ketepatan dalam menghindari kecurigaan terhadap penyembunyian data menggunakan metode enkripsi *Vigenere,* metode LSB dan metode LCG pada citra digital yang diukur menggunakan *Peak Signal-to-Noise Ratio* (PSNR).

1.5 Manfaat Penelitian

Dari penelitian ini diperoleh manfaat sebagai berikut:

1. Menghasilkan sistem keamanan yang dapat menjaga kerahasiaan data yang

disimpan.

2. Menghasilkan sistem keamanan yang dapat menyembunyikan data yang disimpan tanpa menimbulkan kecurigaan.

3. Penelitian dapat menjadi rujukan untuk penelitian selanjutnya mengenai metode enkripsi *Vigenere*, metode LSB dan metode LCG.

1.6 Batasan Masalah

Agar penelitian ini jelas dan tidak keluar dari tujuan, maka perlu dilakukan pembatasan ruang lingkup masalah, yaitu sebagai berikut:

1. Citra digital yang digunakan sebagai media menyembunyikan data adalah foto Kartu Pengenal Mahasiswa (KPM) Fakultas Ilmu Komputer.

2. Variasi data *dummy* yang digunakan adalah data mahasiswa dengan format penyimpanan file .txt.

3. Citra digital yang digunakan memiliki ukuran 354 x 472 pixel dalam format .PNG.

1.7 Sistematika Penulisan

Skripsi ini disusun dengan sistematika sebagai berikut:

i. **BAB I. PENDAHULUAN**

   Pada bab ini berisi penjabaran yang menjadi landasan penelitian agar tercapainya efektifitas tujuan yang diinginkan. Penjabaran pada bab ini mencakup latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan, dan kesimpulan.

ii. **BAB II. KAJIAN LITERATUR**

Pada bab ini membahas secara rinci dasar-dasar teori yang digunakan dalam penelitian sebagai sumber ilmiah, seperti definisi steganografi, kriptografi, metode *Least Significant Bit* (LSB), metode enkripsi *Vigenere* dan metode Linear Congruential Generator (LCG) serta beberapa kajian literatur dari penelitian lain yang relevan dengan penelitian ini.

iii. **BAB III. METODOLOGI PENELITIAN**

Pada bab ini membahas secara rinci tahapan kerangka penelitian yang diperlukan, seperti instrumen penelitian, data yang digunakan, perancangan sistem yang dibangun, serta perencanaan kegiatan penelitian

iv. **BAB IV. PENGEMBANGAN PERANGKAT LUNAK**

Proses pengembangan perangkat lunak yang sudah direncanakan pada BAB III akan dibahas secara rinci pada bab ini. Termasuk di dalamnya pengujian terhadap perangkat lunak apakah sudah sesuai dengan yang direncanakan.

v. **BAB V. HASIL DAN ANALISIS PENELITIAN**

Data yang sudah didapatkan dari pengujian pada tahapan sebelumnya akan disajikan dalam bentuk tabel secara rinci. Dari data tersebut dilakukan analisa berdasarkan hasil yang didapatkan.

vi. **KESIMPULAN DAN SARAN**

Pada bab ini akan dijabarkan kesimpulan sesuai dengan rumusan masalah yang didapatkan dari hasil pengujian serta saran berdasarkan temuan dalam penelitian yang dapat dimanfaatkan untuk penelitian yang akan datang.

1.8 Kesimpulan

Pada bab pendahuluan ini telah dijabarkan landasan pikiran yang telah dipetakan menjadi latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah serta sistematika penulisan. Skripsi ini mengangkat tema kriptografi menggunakan enkripsi Vigenere, steganografi menggunakan metode LSB dan distribusi persebaran data menggunakan metode LCG.

DAFTAR PUSTAKA

Alifi, M.B., dan Suartana, M. 2020. Implementasi Teknik Steganografi pada Gambar JPEG dan PNG dengan menggunakan Metode Adaptive Minimum Error Least Significant Bit Replacement (AMELSBR). *Journal of Informatics and Computer Science* 2 (2):113-114.

Cahyadi, Tri. 2012. Implementasi Steganografi LSB Dengan Enkripsi Vigenere Chiper Pada Citra JPEG. *Transient* 1 (4): 282.

Fajrin, H. R. 2016. Perbandingan Metode Untuk Perbaikan Kualitas Citra Mammogram. *Jurnal SIMETRIS* 7(2): 661.

Hernandes, A., Hartini, Dewi, S. 2019. Steganografi Citra Menggunakan Metode Least Significant Bit (LSB) dan Linear Congruential Generator (LCG). Jurnal Teknik Informatika dan Sistem Informasi 5(2): 137-150.

Ibrahim, Ami Aisiah. 2017. Perancangan Pengamanan Data Menggunakan Algoritma AES. Jurnal Teknik Informatika STMIK Antar Bangsa III (01): 53 – 60.

Karman, J. & Nurhasan, A. 2019. Perancangan Sistem Keamanan Data Inventory Barang di Toko Nanda Berbasis Web Menggunakan Metode Kriptografi Vigenere Chiper. *Jurnal Teknologi Informasi Mura* 11 (01): 30.

Krisnawati. 2008. Metode Least Significant Bit (LSB) dan End Of File (EOF) Untuk Menyisipkan Teks Ke Dalam Citra Grayscale. *Prosiding Seminar Nasional Informatika*, UPN "Veteran" Yogyakarta: 24 Mei 2008. Hal. 44.

Laila, N & RMS, A. S. 2018. Implementasi Steganografi LSB Dengan Enkripsi Vigenere Chiper Pada Citra. *Computer Science Informatics Journal* 1 (2): 57.

Lestari, T., Nurmaesa, N., Mariana, A. R. 2017. Aplikasi Steganografi Untuk Menyisipkan Pesan Dalam Media Image. *ISSN* 7 (2): 23 – 24.

Permana, A. A. 2018. Penerapan Kriptografi Pada Teks Pesan Dengan Menggunakan Metode Vigenere Chiper berbasis android. *Jurnal Al-Azhar Indonesia Seri Sains Dan Teknologi* 4 (3): 112.

Perwitasari, R., Afwani, R., Anjarwani, S. E. 2020. Penerapan Metode Rational Unified Process (RUP) Dalam Pengembangan Sistem Informasi Medical Check Up Pada Citra Medical Centre. *JTIKA* 2(1): 77 – 78.

Purba L.C., Zarlis, M., Gunawan, I., Sumarno, Masruro, Z. 2021. Penggunaan Algoritma LSB dan Vigenere Untuk Pengamanan Data Melalui Pola Citra Digital (Studi Kasus Telkom Akses Kabanjahe). *Techsi* 13 (2): 54.

Rosa & Shalauddin. (2011). Modul Pembelajaran Rekayasa Perangkat Lunak.

Saepullah, A. & Adeyadi, M. 2019. Aplikasi Scanner Berbasis Android Untuk Menampilkan Data ID Card Menggunakan Barcode. *Jumantaka* 3(1): 104.

Sakti, D. V. S. Y., Nazori, A., Mardi, H. 2016. Pengamanan Sistem Menggunakan One Time Password Dengan Pembangkit Password Hash SHA-256 dan Pseudo Random Number Generator (PRNG) Linear Congruential Generator (LCG) di Perangkat Berbasis Android. *Journal Budiluhur* 13 (1): 4 – 5.

Sanjaya C.M.G., et al. 2019. Analisis Kekaburan Chiperteks Hasil Perulangan Enkripsi Vigenere dan Transposisi Columnar Chiper. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*, Akademi Angkatan Udara: 25 September 2019. Hal. 298.

Selpi, Marlina. 2022. Aplikasi Perpaduan Enkripsi Base64 Dengan Metode Steganografi

Distrete Consine Transform (DCT). *Jurnal Sintaks Logika* 2 (2): 38-39.
Syawal, M. F., Fikriansyah, D. C., Agani, N. 2016. Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Chiper dan Metode LSB. *Jurnal TICOM* 4 (3): 91.
Watimena, T. K. & Mufti. 2020. Keamanan Data Menggunakan Metode LSB dan Enkripsi Vigenere. *Jurnal Teknologi Informasi* 4 (1): 111.