

14/S/TEKKOM-KCBR/PK.03.08/22/JULI/2024

**PENGEMBANGAN APLIKASI WEB UNTUK KEAMANAN DATA
MEDIS MENGGUNAKAN VIGENERE CIPHER DAN LEAST
SIGNIFICANT BIT**

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana
Teknik Komputer



Oleh

Deandy Zahran Vierdansyah

NIM 2003977

PROGRAM STUDI S1 TEKNIK KOMPUTER

KAMPUS UPI DI CIBIRU

UNIVERSITAS PENDIDIKAN INDONESIA

2024

HALAMAN HAK CIPTA

**PENGEMBANGAN APLIKASI WEB UNTUK KEAMANAN DATA
MEDIS MENGGUNAKAN VIGENERE CIPHER DAN LEAST
SIGNIFICANT BIT**

oleh

Deandy Zahran Vierdansyah

NIM 2003977

Sebuah Skripsi yang Diajukan untuk Memenuhi Salah Satu Syarat Memperoleh
Gelar Sarjana Teknik pada Program Studi S1 Teknik Komputer

© **Deandy Zahran Vierdansyah** 2024

Universitas Pendidikan Indonesia

Juli 2024

Hak Cipta dilindungi oleh Undang-undang.

Skripsi ini tidak diperbolehkan seluruhnya atau sebagian, dengan dicetak ulang,
difotokopi, atau cara lainnya tanpa izin dari penulis.

Deandy Zahran Vierdansyah, 2024

**PENGEMBANGAN APLIKASI WEB UNTUK KEAMANAN DATA MEDIS MENGGUNAKAN VIGENERE
CIPHER DAN LEAST SIGNIFICANT BIT**

Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

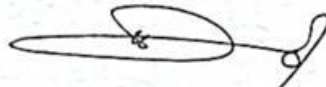
HALAMAN PENGESAHAN SKRIPSI

DEANDY ZAHNAN VIERDANSYAH

**PENGEMBANGAN APLIKASI WEB UNTUK KEAMANAN DATA
MEDIS MENGGUNAKAN VIGENERE CIPHER DAN LEAST
SIGNIFICANT BIT**

disetujui dan disahkan oleh:

Pembimbing I



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

Pembimbing II



Devi Aprianti Rimadhani Agustini, S.Si., M.Si.
NIP. 920200819890421201

**Mengetahui,
Ketua Program Studi Teknik Komputer**



Deden Pradeka, S.T., M.Kom.
NIP. 920200419890816101

HALAMAN PERNYATAAN
KEASLIAN SKRIPSI DAN BEBAS PLAGIARISME

Dengan ini saya menyatakan bahwa skripsi dengan judul “Pengembangan Aplikasi Web Untuk Keamanan Data Medis Menggunakan Vigenere Cipher Dan Least Significant Bit” ini beserta seluruh isinya adalah benar benar karya saya sendiri. Saya tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, saya siap menanggung resiko/sanksi apabila dikemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya saya ini.

Bandung, Juli 2024

Yang membuat pernyataan,



Deandy Zahran Vierdansyah

NIM. 2003977

HALAMAN UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan kehadiran Allah SWT, karena berkat rahmat dan karunia-Nyalah penulis dapat menyelesaikan skripsi yang berjudul “Pengembangan Aplikasi Web Untuk Keamanan Data Medis Menggunakan Vigenere Cipher Dan Least Significant Bit”. Adapun maksud dan tujuan dari penulisan ini adalah untuk memenuhi salah satu syarat untuk mengikuti sidang skripsi, Jurusan Teknik Komputer, Universitas Pendidikan Indonesia Kampus UPI di Cibiru.

Selama penelitian dan penulisan skripsi ini banyak sekali hambatan yang penulis alami, namun berkat bantuan, dorongan serta bimbingan dari berbagai pihak, akhirnya skripsi ini dapat terselesaikan dengan baik. Oleh sebab itu, dengan segala kerendahan hati dan penuh rasa hormat, penulis bermaksud menyampaikan terima kasih kepada :

1. Kedua orang tua di rumah yang selalu memberi dukungan secara moral dan material, serta mengirimkan doa setiap hari agar saya dapat menyelesaikan skripsi ini, kasih sayang mereka yang tak terhitung semoga Allah SWT selalu menjaga kesehatan mereka.
2. Bapak Deden Pradeka, S.T., M.Kom., selaku ketua program studi teknik komputer sekaligus dosen pembimbing pertama, atas bimbingan, dukungan, dan ilmu yang telah Bapak berikan selama proses penyusunan tugas akhir ini. Tanpa bimbingan dan saran dari bapak, saya mungkin tidak akan berhasil menuntaskan penelitian ini dengan sukses.
3. Ibu Devi Aprianti Rimadhani Agustini, S.Si., M.Si., selaku dosen pembimbing kedua atas segala bimbingan dan dukungan yang telah diberikan selama proses penelitian ini. Ibu telah menyediakan banyak pandangan yang sangat berarti, yang mendukung saya dalam menuntaskan tugas akhir ini dengan sukses.
4. Untuk semua rekan-rekan, mahasiswa Teknik Komputer angkatan 2020, yang telah menjadi teman sejati dan keluarga selama kita menjalani studi bersama. Terima kasih untuk semua dukungan, persahabatan, dan kenangan yang telah kita ukir bersama. Perjalanan ini tidak akan berarti tanpa kalian semua. Kalian adalah keluarga terpilih yang selalu mendampingi dalam setiap keadaan.

Semoga kita terus menjaga keakraban ini dan berjalan menuju masa depan yang sukses. Terima kasih untuk semua hal yang telah kita lalui bersama

Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat berbagai kekurangan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari semua pihak untuk penyempurnaan karya ini di masa mendatang. Akhir kata, semoga skripsi ini dapat memberikan manfaat serta kontribusi yang positif dalam bidang ilmu yang dipelajari.

ABSTRAK

Pengembangan teknologi informasi di bidang kesehatan, terutama dalam sistem penyimpanan data rekam medis pasien mengalami kemajuan yang pesat. Namun, perkembangan ini membawa risiko kebocoran informasi pribadi pasien di fasilitas kesehatan, seperti puskesmas dan rumah sakit. Penelitian ini bertujuan untuk mengembangkan sebuah aplikasi berbasis web yang menggunakan algoritma *Vigenere Cipher* dan *Least Significant Bit (LSB)* untuk mengamankan data medis dari akses tidak sah. Aplikasi ini mengimplementasikan kombinasi teknik kriptografi dan steganografi, termasuk penerapan *Fisher Yates Shuffle* yang digunakan untuk mengacak hasil enkripsi sebelum menyisipkannya dalam gambar *cover* seperti hasil *CT Scan* atau *Rontgen*. Algoritma *Vigenere Cipher* terbukti efektif dalam menyamarkan teks, dimana *ciphertext* yang dihasilkan menunjukkan nilai korelasi Pearson yang sangat rendah dengan *plaintext*, yaitu rata-rata hanya 0.013. Hasil tersebut menandakan keberhasilan algoritma dalam mengamankan data. Selanjutnya, teknik steganografi *LSB* yang digunakan untuk menyisipkan data yang dienkripsi ke dalam gambar *cover* seperti hasil *CT Scan* atau *Rontgen*, dari hasil pengujian nilai *MSE* yang paling kecil 0.0110 dan paling besar itu 1317.1 serta nilai *PSNR* yang paling kecil 16.9344 dB dan nilai terbesar 67.7007 dB. Kinerja sistem ini juga mengesankan dengan waktu eksekusi rata-rata hanya 0.53 detik untuk proses enkripsi dan *embedding*, serta 0.25 detik untuk dekripsi dan *extracting*, menunjukkan bahwa sistem dapat melakukan enkripsi, *embedding*, dekripsi, dan *extracting* secara efisien dan akurat, sehingga memastikan kecepatan dan keamanan data.

Kata Kunci: Keamanan Data Medis, *Vigenere Cipher*, *Least Significant Bit (LSB)*, *Fisher Yates Shuffle*, *Korelasi Pearson*, *MSE*, *PSNR*

ABSTRACT

The development of information technology in the healthcare sector, especially in patient medical record storage systems, has rapidly advanced. However, this growth also poses the risk of personal patient information leaks in health facilities, such as clinics and hospitals. This research aims to develop a web-based application utilizing the Vigenere Cipher algorithm and Least Significant Bit (LSB) to secure medical data from unauthorized access. This application implements a combination of cryptographic and steganographic techniques, including the use of the Fisher Yates Shuffle to randomize encrypted results before embedding them into cover images like CT scans or X-rays. The Vigenere Cipher has proven effective in disguising text, with the generated ciphertext showing an extremely low Pearson correlation value with the plaintext, averaging just 0.013, indicating the algorithm's success in securing data. Furthermore, the LSB steganographic technique used for embedding encrypted data into cover images such as CT scans or X-rays showed minimal mean squared error (MSE) values ranging from 0.0110 to 1317.1 and peak signal-to-noise ratio (PSNR) values from 16.9344 dB to 67.7007 dB. The system's performance is also notable with an average execution time of only 0.53 seconds for the encryption and embedding processes, and 0.25 seconds for decryption and extracting, demonstrating that the system can efficiently and accurately perform encryption, embedding, decryption, and extracting, thereby ensuring the speed and security of data.

Keywords: *Medical Data Security, Vigenere Cipher, Least Significant Bit (LSB), Fisher Yates Shuffle, Korelasi Pearson, MSE, PSNR;*

Translate pake quilboard

DAFTAR ISI

LEMBAR PENGESAHAN	i
LEMBAR PERNYATAAN	ii
HALAMAN UCAPAN TERIMAKASIH	iii
ABSTRAK	v
ABSTRACT	vi
DAFTAR ISI	vii
DAFTAR TABEL	ix
DAFTAR GAMBAR	x
DAFTAR LAMPIRAN	xi
BAB I PENDAHULUAN	1
1.1 Latar Belakang Penelitian.....	1
1.2 Rumusan Masalah Penelitian	4
1.3 Tujuan Penelitian.....	4
1.4 Batasan Penelitian	5
1.5 Manfaat Penelitian.....	5
1.5.1 Manfaat Teoritis	5
1.5.2 Manfaat Praktis	6
1.6 Struktur Organisasi Skripsi.....	6
BAB II KAJIAN PUSTAKA	8
2.1 Kriptografi	8
2.2 Steganografi.....	9
2.3 <i>Vigenere Cipher</i>	10
2.4 <i>Fisher Yates Shuffle</i>	11
2.5 <i>Least Significant Bit (LSB)</i>	12
2.6 PHP	13
2.7 Korelasi Pearson.....	13
2.8 MSE dan PSNR	14
2.9 Penelitian Terkait.....	15
BAB III METODE PENELITIAN	17
3.1 Desain Penelitian	18
3.2 Identifikasi Masalah (<i>Identify the problem</i>)	18
3.3 Mendeskripsikan Tujuan (<i>Describe the objectives</i>)	19

3.4	Desain dan Pengembangan Sistem (<i>Design & develop the artifact</i>).....	19
3.5	Desain Uji Coba Sistem (<i>Test the artifact</i>).....	25
3.6	Desain Evaluasi Hasil Uji (<i>Evaluate testing result</i>).....	27
3.7	Mengkomunikasikan Hasil Uji (<i>Communicating the testing result</i>).....	27
BAB IV HASIL DAN PEMBAHASAN.....		28
4.1	Hasil Pengembangan Aplikasi.....	28
4.2	Hasil Implementasi <i>Vigenere Cipher</i> dan LSB	30
4.2.1	Hasil Implementasi <i>Vigenere Cipher</i>	30
4.2.2	Hasil Implementasi LSB	33
4.2.3	Hasil Pengujian Enkripsi dan Dekripsi	34
4.2.4	Hasil Pengujian <i>Embedding</i> dan <i>Extracting</i>	36
4.3	Hasil Kinerja Sistem.....	37
4.3.1	Hasil Pengujian Estimasi Waktu Proses Enkripsi dan <i>Embedding</i> ..	37
4.3.2	Hasil Pengujian Estimasi Waktu Proses Enkripsi dan <i>Extracting</i> ...	39
4.3.3	Hasil Pengujian Koefisien Korelasi Pearson.....	40
4.3.4	Hasil Pengujian MSE dan PSNR	47
BAB V SIMPULAN, IMPLIKASI, DAN REKOMENDASI		51
5.1	Simpulan.....	51
5.2	Implikasi.....	52
5.3	Rekomendasi	52
DAFTAR PUSTAKA		54
LAMPIRAN.....		57

DAFTAR TABEL

Tabel 2.1 Kriteria Korelasi Pearson	14
Tabel 2.2 Penelitian Terkait	15
Tabel 3.1 Uji Coba Sistem	25
Tabel 4.1 Hasil Enkripsi dan Dekripsi	34
Tabel 4.2 Hasil Embedding dan Extracting	36
Tabel 4.3 Estimasi Waktu proses Enkripsi dan Embedding	38
Tabel 4.4 Estimasi Waktu proses Dekripsi dan Extracting	39
Tabel 4.5 Kriteria Korelasi Pearson	40
Tabel 4.6 Hasil Perhitungan Korelasi Pearson	41
Tabel 4.7 Hasil Perhitungan MSE dan PSNR	47

DAFTAR GAMBAR

Gambar 1.1 Data serangan siber di Indonesia (BSSN, 2023)	2
Gambar 2.1 Enkripsi Simetris	8
Gambar 2.2 Cara Kerja Steganografi	9
Gambar 2.3 Cara kerja Fisher Yates Shuffle	11
Gambar 2.4 Perbedaan MSB dan LSB.....	12
Gambar 3.1 Prosedur penelitian model D&D (Ellis & Levy, 2010, hlm. 111)	18
Gambar 3.2 Desain Use Case Diagram.....	20
Gambar 3.3 Flowchart Sistem.....	21
Gambar 3.4 Flowchart Enkripsi dan Embedding	22
Gambar 3.5 Flowchart Dekripsi dan Extracting	23
Gambar 3.6 Diagram Blok proses enkripsi dan embedding	24
Gambar 3.7 Diagram Blok proses dekripsi dan extracting	24
Gambar 4.1 Tampilan Halaman Login.....	28
Gambar 4.2 Tampilan Halaman Enkripsi.....	29
Gambar 4.3 Tampilan Halaman Dekripsi	29
Gambar 4.4 File PDF yang diamankan	31
Gambar 4.5 File PDF hasil enkripsi	31
Gambar 4.6 File PDF hasil shuffle.....	32
Gambar 4.7 File PDF hasil dekripsi	32
Gambar 4.8 Perbandingan Gambar LSB.....	33
Gambar 4.9 Perbandingan matriks warna kedua gambar.....	34

DAFTAR LAMPIRAN

Lampiran 1. Jadwal Penelitian	57
Lampiran 2. Kode Fungsi Enkripsi	57
Lampiran 3. Kode Fungsi Dekripsi	57
Lampiran 4. Kode Fisher Yates Shuffle	58
Lampiran 5. Kode LSB	59
Lampiran 6. Percobaan Enkripsi pakai gambar selain CT Scan dan Rontgen	59
Lampiran 7. Percobaan pada gambar pegunungan	60
Lampiran 8. Membuat tampilan Matriks warna	60
Lampiran 9. Perhitungan korelasi dengan sistem	60
Lampiran 10. Perhitungan MSE dan PSNR oleh sistem	61
Lampiran 11. Perhitungan Korelasi dengan Excel	61
Lampiran 12. File ke 5 dan gambar simulasi 5	61
Lampiran 13. Hasil dekripsi File 5 dan gambar simulasi 5	62
Lampiran 14. File ke 6 dan gambar simulasi 6	62
Lampiran 15. Hasil Dekripsi File ke 6 dan gambar simulasi 6	62
Lampiran 16. File ke 9 dan gambar simulasi 9	63
Lampiran 17. File ke 17 dan gambar simulasi 17	63
Lampiran 18. Hasil dekripsi File ke 17 dan gambar simulasi 17	63
Lampiran 19. Percobaan enkripsi dan dekripsi file ke 9 ke dalam gambar lain	64
Lampiran 20. File JSON Percobaan ke 9	65
Lampiran 21. Banyak pesan dan batas gambar percobaan ke 9	65
Lampiran 22. Perbandingan Gambar CT Scan, Rontgen, dan MRI	66