Jurnal Teknik Informatika (JUTIF)
Vol. 4, No. 5, October 2023, pp. 995-999

DOI: https://doi.org/10.52436/1.jutif.2023.4.5.659
p-ISSN: 2723-3863
e-ISSN: 2723-3871

DIGITAL DATA SECURITY WITH APPLICATION OF CRYPTOGRAPHY AND DATA COMPRESSION TECHNIQUES

Adam Prayogo Kuncoro[*1], Dinar Mustofa[2], Dwi Krisbiantoro[3], Tarwoto[4]

[1,2]Informatics, Faculty of Computer Science, Universitas Amikom Purwokerto, Indonesia
[3,4]Information Systems, Faculty of Computer Science, Universitas Amikom Purwokerto, Indonesia
Email: [1]adam@amikompurwokerto.ac.id, [2]dinar.mustofa@amikompurwokerto.ac.id,
[3]dwikris@amikompurwokerto.ac.id, [4]tarwoto@amikompurwokerto.ac.id

(Article received: October 25, 2022; Revision: November 19, 2022; published: October 15, 2023)

Abstract

The need for digital data security is to ensure that the data and information we have are confidential and can only be accessed by authorized users. And no one can change the information in it, thus ensuring complete accuracy. The functions of data security are confidentiality, authentication, integrity, and anti-repudiation. Compression techniques are used to protect digital data because they aim to make less storage space and allow us to transfer more data over the internet. This study aims to plan to prove the application of a combination of 2 (two) techniques, namely compression and cryptography to digital data with the aim of increasing the security of the data. This research has the result that the compression technique of the Huffman method is the most effective in compressing digital data into the smallest file size compared to other compression methods. It can compressed the data size by around 30% (thirty percent) to 40% (forty percent) compared to the original data size. And coupled with data security with cryptographic encryption techniques so that files remain safe when transferred over the network.

Keywords: *data compression, digital data security, encryption, cryptography*.

PENGAMANAN DATA DIGITAL DENGAN PENERAPAN TEKNIK KRIPTOGRAFI DAN KOMPRESI DATA

Abstrak

Kebutuhan akan keamanan data digital adalah untuk memastikan bahwa data serta informasi yang kita miliki bersifat rahasia dan hanya dapat diakses oleh pengguna yang memiliki wenang. Serta tidak ada yang dapat mengubah informasi di dalamnya, sehingga memastikan keakuratan yang lengkap. Fungai dari keamanan data adalah kerahasiaan, otentikasi, integritas, dan anti-penyangkalan. Teknik kompresi digunakan untuk melindungi data digital karena bertujuan agar menjadikan lebih sedikit ruang penyimpanan dan memungkinkan kita dapat mentransfer lebih banyak data melalui internet. Penelitian ini bertujuan untuk merencanakan pembuktian penerapan gabungan 2 (dua) teknik yaitu kompresi dan kriptografi terhadap data digital dengan tujuan untuk meningkatkan keamanan pada data tersebut. Penelitian ini memiliki hasil bahwa teknik kompresi metode Huffman menjadi paling efektif dalam mengkompresi data digital menjadi ukuran file terkecil dibandingkan dengan metode kompresi yang lain. Yaitu dapat mengkompresi ukuran data dengan besaran sekitar 30% (tiga puluh persen) hingga 40% (empat puluh persen) dibandingkan ukuran data aslinya. Serta ditambah dengan pengamanan data dengan teknik enkripsi kriptografi agar file tetap aman saat ditransferkan melalui jaringan.

Kata kunci: *enkripsi, keamanan data digital, kompresi data, kriptografi*.

1. PENDAHULUAN

Kebutuhan akan keamanan data digital adalah untuk memastikan bahwa data serta informasi yang kita miliki bersifat rahasia dan hanya dapat diakses oleh pengguna yang memiliki wenang. Serta tidak ada yang dapat mengubah informasi di dalamnya, sehingga memastikan keakuratan yang lengkap. Tujuan dari keamanan data adalah kerahasiaan, otentikasi, integritas, dan anti-penyangkalan [1]. Teknik kompresi digunakan untuk melindungi data digital karena bertujuan agar menjadikan lebih sedikit ruang penyimpanan dan memungkinkan kita dapat mentransfer lebih banyak data melalui internet [2]. Penerapan teknik kompresi ini akan meningkatkan kecepatan transfer data dari *hard drive* ke memori *external*. Enkripsi data dikenal sebagai salah satu teknik yang berfungsi untuk melindungi informasi (data digital) dari ancaman penyadapan [3]. Teknik

enkripsi mengubah data dari format tertentu, yang disebut *plaintext*, ke format lain, yang disebut teks *ciphertext*, menggunakan kunci enkripsi [4]. Salah satu bagian dari teknik enkripsi pada data digital adalah kriptografi.

Penelitian ini bertujuan untuk merencanakan pembuktian penerapan gabungan 2 (dua) teknik yaitu kompresi dan kriptografi terhadap data digital dengan tujuan untuk meningkatkan keamanan pada data tersebut. Dengan menerapkan 2 (dua) teknik tersebut diharapkan dapat memperkecil ukuran kapasitas data digital serta membuat aman agar tidak dapat diakses oleh pihak yang tidak berkepentingan.

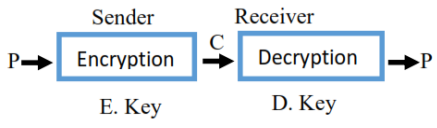
Urgensi penelitian ini berupa pembuktian efektifitas penerapan teknik kompresi dan teknik kriptografi terhadap data digital agar menjadi salah satu teknik pengamanan data dan informasi, sehingga tidak mudah diakses atau disadap oleh pihak yang tidak memiliki wewenang.

2. METODE PENELITIAN

Penelitian ini menggunakan metode eksperimental yaitu penelitian yang bertujuan menggali informasi [5] berdasarkan hasil pembuktian penerapan teknik kompresi dan kriptografi pada data digital dengan maksud meningkatkan keamanan dan efisiensi kapasitas penyimpanan data. Eksperimen penerapan teknik kompresi dan kriptografi yang diterapkan pada data digital sehingga dapat dikategorikan ke dalam ranah keilmuan *IT security*, enkripsi data digital, maupun data *security*. Terlebih dahulu disampaikan tentang pemahaman dasar pada kedua teknis tersebut.

2.1. Kriptografi

Kriptografi merupakan disiplin ilmu yang mempelajari teknik enkripsi naskah asli (*plaintext*) yang tersusun acak, dengan memanfaatkan kunci enkripsi sehingga naskah tersebut berubah menjadi teks yang sulit terbaca (*ciphertext*) oleh user yang tidak memiliki kunci dekripsi [6]. Teknik yang digunakan dalam kriptografi adalah metode *scrambling*, yaitu teknik pengubahan teks biasa menjadi teks sandi [7]. Teknik *scrambling* tersebut dikenal dengan istilah enkripsi dan dekripsi. Yang mana, terdapat tiga fungsi dasar di dalam algoritma kriptografi sendiri, yaitu *key*, *encryption*, dan *decryption* [8]. Penerapan teknik kriptografi untuk keamanan data menjadi penting salah satunya saat melakukan transmisi informasi pada jaringan internet. Sehingga, data digital lebih aman dan tetap terjaga dari adanya *spamming* atau peretasan informasi secara ilegal [9]. Ilustrasi proses teknik dasar kriptografi terlampir pada Gambar 1.



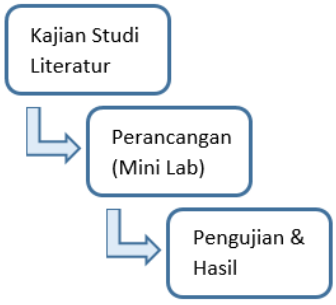
Gambar 1. Ilustrasi proses teknik dasar kriptografi

Literatur berdasarkan penelitian terdahulu yang menerapkan teknik kriptografi pada data digital menggunakan metode *AES-Cryptography* menuliskan hasil penelitian bahwa berhasil mengamankan data digital [10] dan terdapat hasil pengujian dengan prosentase validitas sebesar 85% (delapan puluh lima persen) aman dari ancaman teknik *brute-force* [11]. Penelitian lainnya yang menerapkan teknik kriptografi yaitu menggunakan metode DES (*Data Encryption Standard*) merupakan penerapan algoritma kunci-simetri 56-bit kunci data digital yang teknisnya mengubah susunan data digital sehingga menjadi sulit dibaca atau dianalisa [12].

2.2. Kompresi data digital

Teknik kompresi digunakan karena mampu memadatkan atau memampatkan data dan mengembalikannya sama persis seperti semula [13]. Tidak ada informasi yang hilang atau harus dikurangi dalam proses untuk mengurangi ukuran besar data [14]. Sehingga akan efektif diterapkan pada data digital agar ruang penyimpanan atau memori digital mampu menampung lebih banyak data dibandingkan tanpa penerapan teknik kompresi. Penelitian terdahulu melakukan pembuktian penerapan teknik kompresi terhadap data digital menggunakan metode *Run Length Encoding* berhasil mengkompresi data digital hingga rata-rata penurunan kapasitas berkas sebesar 40% (empat puluh persen) [15]. Penelitian lainnya yang masih berkaitan dengan teknik kompresi data digital, menerapkan algoritma *LZW-Compression* menghasilkan besaran kapasitas *file* yang lebih kecil tetapi kualitas data masih sama seperti semula, sehingga peneliti berkesimpulan algoritma tersebut berhasil mengkompresi data digital menjadi lebih efektif [16].

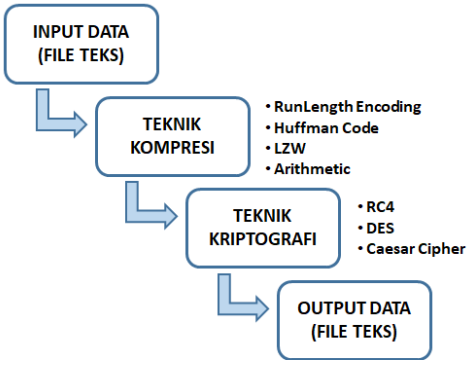
Tahap alur penelitian yang dilakukan bermula dengan tahap studi literatur dimaksudkan untuk mengkaji beberapa penelitian serupa yang telah dilakukan sebelumnya berkaitan dengan kompresi data digital dan implementasi enkripsi sebagai teknik keamanannya. Selanjutnya dilakukan perancangan dengan ruang lingkup internal atau mini lab dengan basis kronologi kondisi data digital yang diujikan menyerupai dari penelitian sebelumnya yang pernah dilakukan. Terakhir yaitu proses pengujian dan pengambilan hasil kesimpulan pada penelitian ini. Alur proses penelitian diilustrasikan pada Gambar 2.



Gambar 2. Ilustrasi alur tahap penelitian

3. HASIL DAN PEMBAHASAN

Hasil penelitian ini terlebih dahulu kami berikan penjelasan terkait alur proses penerapan pengamanan data digital yang menggunakan gabungan teknik kriptografi dan teknik kompresi, ilustrasi alur prosesnya terpaparkan pada Gambar 3.

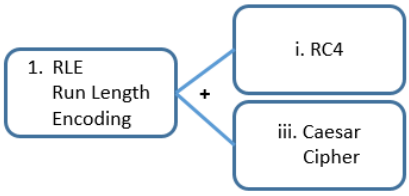


Gambar 3. Ilustrasi alur kerja penerapan pengamanan data digital dengan cara penggabungan teknik kriptografi dan kompresi data

Bagan alur kerja tertampil pada Gambar 2 merupakan ilustrasi proses penerapan teknis kompresi dan enkripsi kriptografi pada penelitian ini. Penerapan teknik kompresi menggunakan 4 (empat) metode, dan teknik enkripsi kriptografi menggunakan 3 (tiga) metode. Kedua teknik pengamanan data digital tersebut diterapkan pada sebuah data teks yang kemudian akan diukur analisis kinerja yang berhubungan dengan besaran ukuran file, rasio kompresi, dan durasi waktu pemrosesan eksekusi terhadap file data teks. Alur kerjanya adalah mengambil file teks yang akan diproses kompresi data digital, setelah itu output apa pun yang dihasilkan akan dianjutkan ke bagian enkripsi untuk mengenkripsi file teks tersebut.

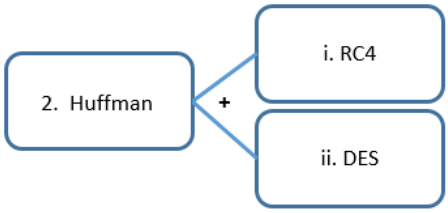
Empat teknik kompresi yang digunakan yaitu RLE (Run Length Encoding), Huffman Coding, LZW, dan Arithmetic. Sedangkan pada enskripsi kriptografi terdapat 3 teknik yaitu RC4, Caesar Cipher dan DES. Tujuan diterapkan kombinasi kedua teknik pengamanan ini guna membuktikan bagaimana hasil pengamanan terhadap sebuah file teks digital.

Kombinasi yang disimulasikan dalam penelitian ini untuk mengamankan data teks digital antara lain: RLE + (RC4 & Caesar Cipher); Huffman + (RC4 & DES); LZW + (RC4 & DES); dan Arithmetic + (RC4 & DES). Dengan simulasi terhadap 5 (lima) file teks digital berspesifikasi ukuran file yang berbeda-beda, rasio kompresi dan waktu eksekusi yang disamakan.



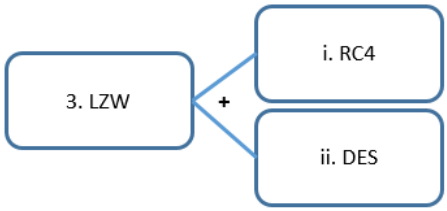
Gambar 4. Ilustrasi penggabungan teknik kompresi RLE dengan 2 (dua) teknik enkripsi RC4 dan Caesar Cipher.

Gambar 4 mengilustrasikan kondisi penggabungan teknik kompresi RLE (*Run Length Encoding*) dengan teknik enkripsi RC4 dan Caesar Cipher akan diterapkan pada lima file teks digital yang telah disiapkan.



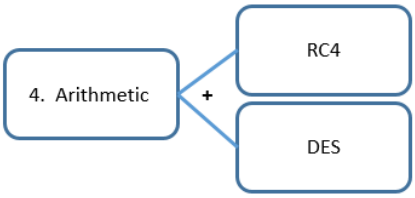
Gambar 5. Ilustrasi penggabungan teknik kompresi Huffman dengan 2 (dua) teknik enkripsi RC4 dan DES

Gambar 5 mengilustrasikan kondisi penggabungan teknik kompresi Huffman dengan teknik enkripsi RC4 dan DES akan diterapkan pada lima file teks digital yang telah disiapkan.



Gambar 6. Ilustrasi penggabungan teknik kompresi LZW dengan 2 (dua) teknik enkripsi RC4 dan DES

Gambar 6 mengilustrasikan kondisi penggabungan teknik kompresi LZW dengan teknik enkripsi RC4 dan DES akan diterapkan pada lima file teks digital yang telah disiapkan.



Gambar 7. Ilustrasi penggabungan teknik kompresi Arithmetic dengan 2 (dua) teknik enkripsi RC4 dan DES

Gambar 7 mengilustrasikan kondisi penggabungan teknik kompresi Arithmetic dengan teknik enkripsi RC4 dan DES akan diterapkan pada lima file teks digital yang telah disiapkan.

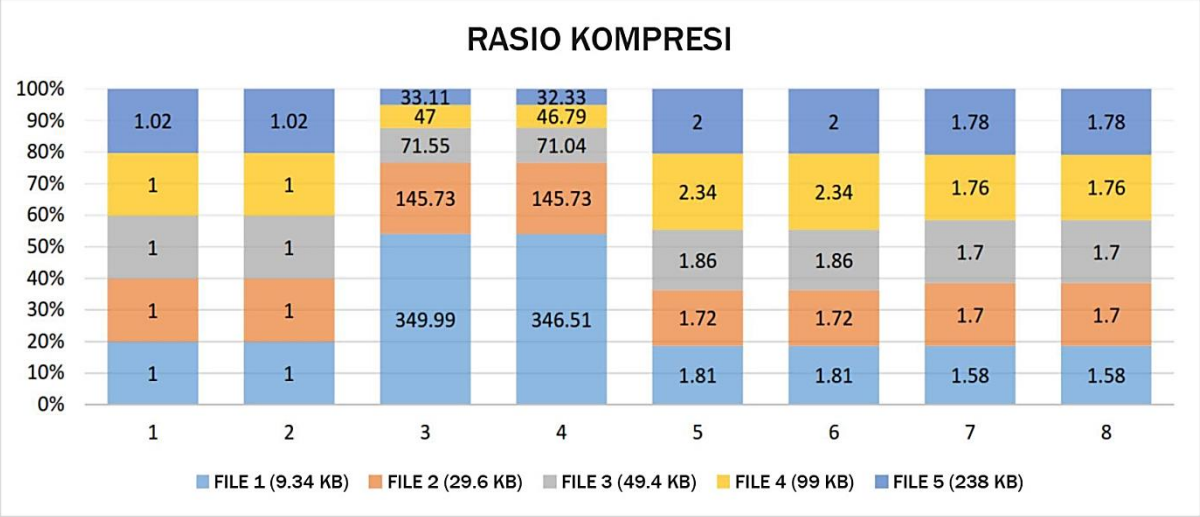
Berdasarkan 4 (empat) skema yang telah direncanakan tentang penerapan pengamanan file digital dengan menggabungkan teknik kompresi dan teknik enkripsi, kemudian dilakukan proses pengujian terhadap 5 (lima) file teks digital dengan simulasi kondisi besaran kapasitas file yang berbeda-beda. Pengujian terhadap penggabungan dengan kombinasi metode kedua teknik, dimaksudkan untuk pembuktian skema gabungan manakah yang menjadi kondisi pengamanan data digital paling efektif. Guna membuktikan kombinasi manakah yang tingkat keamanannya baik dan rasio kompresi data yang baik.

DOI: https://doi.org/10.52436/1.jutif.2023.4.5.659
p-ISSN: 2723-3863
e-ISSN: 2723-3871

Tabel 1. Data hasil pengujian dengan skema simulasi yang telah direncanakan.

File	Original (O) File size (in Bytes)	O + 1	1 + i	1 + iii	**O + 2**	**2 + i**	**2 + ii**	O + 3	3 + i	3 + ii	O + 4	4 + i	4 + ii
1	9571	9324	9324	9324	**289**	**289**	**296**	5272	5272	5280	6057	6057	6064
2	30320	30314	30314	30314	**645**	**645**	**648**	17574	17574	17576	17767	17767	17768
3	50587	50585	50585	50585	**707**	**707**	**712**	27102	27102	27104	29732	29732	29736
4	101433	101418	101418	101418	**696**	**696**	**704**	43268	43268	43268	57444	57444	57448
5	243945	243906	243906	243906	**697**	**697**	**704**	121643	121643	121649	136546	136546	136552

Tabel 1 menunjukkan hasil pengujian terhadap lima file dengan kondisi besaran kapasitas yang berbeda-beda. Semua teknik yang digunakan menunjukkan kombinasi mana yang lebih baik. Sebagaimana tersampaikan pada Tabel 1 bahwa kombinasi teknik kompresi metode Huffman telah menghasilkan besaran kapasitas file paling kecil dibandingkan dengan metode kompresi yang lain.



Gambar 7. Hasil pengujian terhadap rasio kompresi file digital.

Gambar 7 merupakan hasil pengujian rasio kompresi dari lima file teks yang berbeda. Pada pengujian ini dapat diperoleh hasil uji bahwa penerapan metode Huffman memberikan rasio rompresi yang lebih baik di antara semua teknik lainnya hampir 50-80% (lima puluh persen hingga delapan puluh persen). Jadi secara keseluruhan metode kompresi terbaik adalah Huffman kemudian LZW, kemudian Arithmetic, kemudian RLE (Run Length Encoding) dengan runutan hasil yang efektif untuk kompresi file digital.

4. KESIMPULAN

Berdasarkan pengujian yang dilakukan terhadap 5 (lima) file teks digital kondisi berbeda-beda dengan menerapkan penggabungan teknik kompresi data dan teknik enkripsi kriptografi, diperoleh hasil bahwa teknik kompresi metode Huffman yang menghasilkan kapasitas file paling kecil dan efisien dalam besaran data digital, serta memiliki tingkat keamanan karena dikombinasikan dengan pengamanan multi-enkripsi kriptografi. Hal ini menjadi dampak positif dalam memproses data secara efisien hemat kapasitas data digital, dan memudahkan mentransfer data melalui jaringan dikarenakan ukuran file yang dikompresi menjadi lebih kecil. Dengan besaran ukuran file terkompresi menjadi sekitar 30% (tiga puluh persen) hingga 40% (empat puluh persen) dibandingkan ukuran data aslinya.

UCAPAN TERIMA KASIH

Penulis menyampaikan terima kasih kepada Universitas Amikom Purwokerto yang mendukung terselenggaranya seluruh rangkaian penelitian ini.

DAFTAR PUSTAKA

[1] A. Supriyanto, "Analisis Kelemahan Keamanan pada Jaringan Wireless," *Anal. Keamanan Jar. Wirel.*, vol. XI, no. 1, pp. 38–46, 2006.

[2] E. Prayoga and K. M. Suryaningrum, "Implementasi Algoritma Huffman Dan Run Length Encoding Pada Aplikasi Kompresi Berbasis Web," *J. Ilm. Teknol. Infomasi Terap.*, vol. 4, no. 2, pp. 92–101, 2018.

[3] S. Wardoyo and R. Fahrizal, "Aplikasi Teknik Enkripsi Dan Dekripsi File Dengan Algoritma Blowfish Pada Perangkat Mobile Berbasis Android," *Setrum Sist. Kendali-*

Tenaga-elektronika-telekomunikasi-komputer, vol. 3, no. 1, p. 43, 2016.

[4] H. Situmorang, "Keamanan Basis Data dengan Teknik Enkripsi," *Mahajana Inf.*, vol. 1, no. 1, pp. 22–27, 2016.

[5] W. C. Easttom, *Computer Security Fundamentals*. 2011.

[6] A. Savoldi and P. Gubian, "Data hiding in SIM/USIM cards: A steganographic approach," in *Proceedings - SADFE 2007: Second International Workshop on Systematic Approaches to Digital Forensic Engineering*, 2007, pp. 86–97.

[7] B. Mondal, N. Biswas, and T. Mandal, "A Comparative study on Cryptographic Image Scrambling," *Proc. Second Int. Conf. Res. Intell. Comput. Eng.*, vol. 10, pp. 261–268, 2017.

[8] N. Aminudin *et al.*, "Nur algorithm on data encryption and decryption," *Int. J. Eng. Technol.*, vol. 7, no. 2.26 Special Issue 26, pp. 109–118, 2018.

[9] A. K. Harsa, "Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 (Rc4) Dan Steganografi Pada Citra Digital," *Inform. Mulawarman Februari*, vol. 9, no. 1, 2014.

[10] B. E. Widodo and A. S. Purnomo, "Implementasi Advanced Encryption Standard Pada Enkripsi Dan Dekripsi Dokumen Rahasia Ditintelkam Polda Diy," *J. Tek. Inform.*, vol. 1, no. 2, pp. 69–77, 2020.

[11] M. A. A. Pujari and M. S. S. Shinde, "Data Security using Cryptography and Steganography," *IOSR J. Comput. Eng.*, vol. 18, no. 04, pp. 130–139, 2016.

[12] S. K. Rao, D. Mahto, and D. A. Khan, "A Survey on Advanced Encryption Standard," *Int. J. Sci. Res.*, vol. 6, no. 1, pp. 711–724, 2017.

[13] C. Raghavendra, S. Sivasubramanian, and A. Kumaravel, "Improved image compression using effective lossless compression technique," *Cluster Comput.*, vol. 22, pp. 3911–3916, 2019.

[14] A. R. Trilaksono, "Efektivitas Penggunaan Google Drive Sebagai Media Penyimpanan Di Kalangan Mahasiswa," *J. Digit. Teknol. Inf.*, vol. 1, no. 2, p. 91, 2020.

[15] M. Jayedul and M. Nurul, "Study on Data Compression Technique," *Int. J. Comput. Appl.*, vol. 159, no. 5, pp. 6–13, 2017.

[16] H. N. Saad, F. mushtaq Jafar, and H. A. Salman, "A new compression technique in MANET: Compressed-LZW algorithm," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 16, no. 2, pp. 890–896, 2019.