TEKNOMATIKA, Vol.12, No.01, Maret 2022
P-ISSN : 2087-9571, E-ISSN : 2541-335X



# Implementasi Multi Algoritma pada Aplikasi Enkripsi dalam Mengamankan File

## IMPLEMENTATION OF MULTIPLE ALGORITHMS ON ENCRYPTION APPLICATIONS IN SECURING FILES

**Yudi Septianto [1]; Guntoro Barovih [2]*; Pujiono[3]**
*[1,2,3] STMIK PalComTech: Jl. Basuki Rahmat No. 05, Palembang 30129, Indonesia*
*[1,2,3] Jurusan S1 Informatika STMIK PalComTech Palembang*
*e-mail: [1]yudiseptianto69@gmail.com;[*2]guntoro@palcomtech.ac.id; [3]pujiono201099@gmail.com;*

**Abstrak**

Beberapa orang berpikir file dan pesan dalam sistem digital cukup aman dan tidak memerlukan keamanan ekstra. Kenyataannya adalah bahwa banyak file yang dinyatakan aman dapat dicuri. Berbagai cara mengelola file, baik dalam bentuk file gambar, file dokumen yang berisi informasi rahasia dari institusi atau file pribadi. Mulai dari penambahan password hingga hingga enkripsi pada file. Penelitian ini fokus pada penerapan algoritma huffman sebagai kompresi algoritma file dan penerapan algoritma RC4 dalam penerapan enkripsi file dokumen. Serta metode enkripsi End of File dalam enkripsi steganografi. Tujuan penelitian ini yaitu untuk mengamankan berkas penting berupa file digital yang terdapat di FISIP Universitas Sriwijaya. Metode prototipe digunakan untuk pengembangan sistem. Pengujian menggunakan metode pengujian blackbox dan pengujian heuristik. Hasil tes pada file terenkripsi menggunakan algoritma RC4 sulit dilakukan dekripsi dan file steganografi yang diperoleh tidak dapat dibaca jika mengalami perubahan pada gambar fisik

**Kata kunci** — encryption ; huffman; RC4; Akhir berkas; Kegunaan Heuristik.

**Abstrak**

Some people think files and messages in digital systems are quite secure and don't require extra security. The reality is that many files that are otherwise secure can be stolen by irresponsible people. Various ways to managefiles, whether in the form of image files, document files containing confidential information from institutions or personal files. Starting from the addition of passwords to encryption on files. The research focused on the application of huffman algorithm as a file algorithm compression and the application of RC4 algorithm in the application of document file encryption. As well as the End of File encryption method in steganography encryption. The purpose of this research is to secure important files in the form of digital files contained in FISIP Universitas Sriwijaya. The system development method used is the prototype method. Testing uses blackbox testing methods and heuristic testing. Test results on encrypted files using the RC4 algorithm are difficult to decryptand the steganography files obtained cannot be read if undergoes changes to the physical image.

**Kata kunci** — encryption ; huffman; RC4; End of File; Usability Heuristic.

## 1. PENDAHULUAN

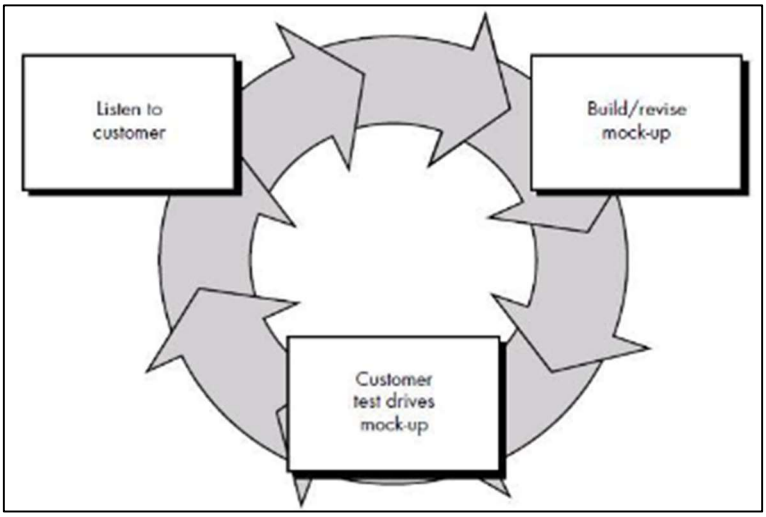
Pesatnya perkembangan teknologi memberikan manfaat yang sangat besar bagi aktivitas manusia, salah satunya adalah kemudahan bertukar informasi. Koneksi internet yang terus berkembang menjadi tulang punggung yang sangat penting dalam aktivitas pertukaran data. Namun perkembangan teknologi juga berdampak buruk bagi masyarakat, salah satunya kerentanan data yang dimiliki oleh orang lain (pencurian data). Pencurian data ini melibatkan berbagai kegiatan mulai dari kegiatan pencurian data yang aktif di jaringan dengan memasang berbagai malware hingga random target hingga social engineering yang dilakukan pelaku kepada target atau korban. Tingkat serangan terhadap sistem dari Januari hingga April 2021 ada sebanyak 159 kasus dan dari 5 tindakan penyerangan tertinggi 40% menjadi lebih dari 50% didominasi oleh tindakan informasi gathering dengan menyebarkan malware dari berbagai media komunikasi data, terutama dari email yang memasukkan malware dalam file *lampiran*[1]. Untuk mencegah kebocoran data banyak hal yang dilakukan mulai dari mengamankan jalur komunikasi dengan menerapkan berbagai sistem firewall, beralih port komunikasi dari port default mereka,

menonaktifkan jalur komunikasi di sisi lokal jaringan dengan menerapkan NAT, untuk mengenkripsi file ketika data informasi ditransmisikan melalui jaringan.

Keamanan file adalah banyak cara yang harus dilakukan mulai dari melindungi file dengan kata sandi hingga mengacak data file dengan menerapkan algoritma kriptografi untuk mengacak file sehingga tidak dapat dibaca. Kriptografi memiliki banyak jenis algoritma yang dapat digunakan dalam enkripsi dan dekripsi file. Salah satunya adalah blowfish, algoritma ini diterapkan pada sistem android untuk mengenkripsi dan mendekripsi file hanya file yang digunakan adalah file dalam bentuk gambar, video dan dokumen, algoritma ini menggunakan kunci simetris untuk mengenkripsi dan mendekripsi[2]. Algoritma Data Encryption Standard (DES) juga digunakan dalam mengenkripsi pesan dengan menerapkan kunci simetris berukuran 64-bit dan 56-bit[3]. Rivest Code 5 (RC5) juga digunakan dalam mengenkripsi file, algoritma ini menggunakan metode chipper blok dengan menggunakan kunci simetri dalam mengacak file untuk dienkripsi[4]. Berbagai cara untuk mengamankan file salah satunya dengan menggabungkan algoritma kriptografi yang digunakan. Salah satunya dengan menggabungkan RC dengan RSA, penambahan algoritma RSA digunakan untuk melindungi data yang telah dienkripsi dari hasil algoritma RC, dengan harapan proses pencurian data semakin dilakukan[5]. Penelitian ini menggunakan penggabungan dua yaitu Huffman dan RC4. Algoritma Huffman digunakan untuk mengompres karakter pada pesan atau file dengan mengelompokkan karakter untuk membuat pohon Huffman yang kemudian mengkodekan dan membentuk bit-code[6]–[9]. Algoritma RC4 adalah salah satu algoritma kriptografi modern ke dalam kategori algoritma symmetric dalam proses enkripsi dan dekripsi. Algoritma ini biasanya digunakan untuk mengacak pesan, file baik dalam file teks atau gambar[10]. Algoritma RC4 dalam studi kasus lain digunakan dalam mengamankan pesan singkat yang dikirim dari smartphone dikombinasikan denganprotokol Diffie-Hellman dalam menghasilkan kunci simetris[11]. Tujuan penerapan beberapa algoritma adalah untuk meningkatkan keamanan data dari tindakan pencurian data. Baik dilakukan dari jalur komunikasi jaringan atau dengan mencuri informasi langsung ke sistem komputer secara offline. Studi ini menggunakan kombinasi algoritma Huffman sebagai kompresi file dan algoritma RC4 sebagai algoritma enkripsi dan deskripsi, serta menerapkan metode End of File untuk memasukkan pesan pada media gambar. Metode Eof adalah menambahkan byte atau ukuran ke file yang menjadi media penyisipan pesan, tetapi tidak mengubah kualitas file gambar[12]. Ketiga algoritma ini difokuskan dan diimplementasikan pada perangkat lunak berbasis web. Tujuannya adalah untuk menyediakan perangkat lunak yang dapat digunakan dan dapat disesuaikan dengan sistem internal lainnya atau dapat digunakan secara mandiri untuk mengamankan file penting lainnya. Pengujian aplikasi menggunakan metode kotak hitam untuk menguji interaksi antara modul aplikasi

## 2. METODE PENELITIAN

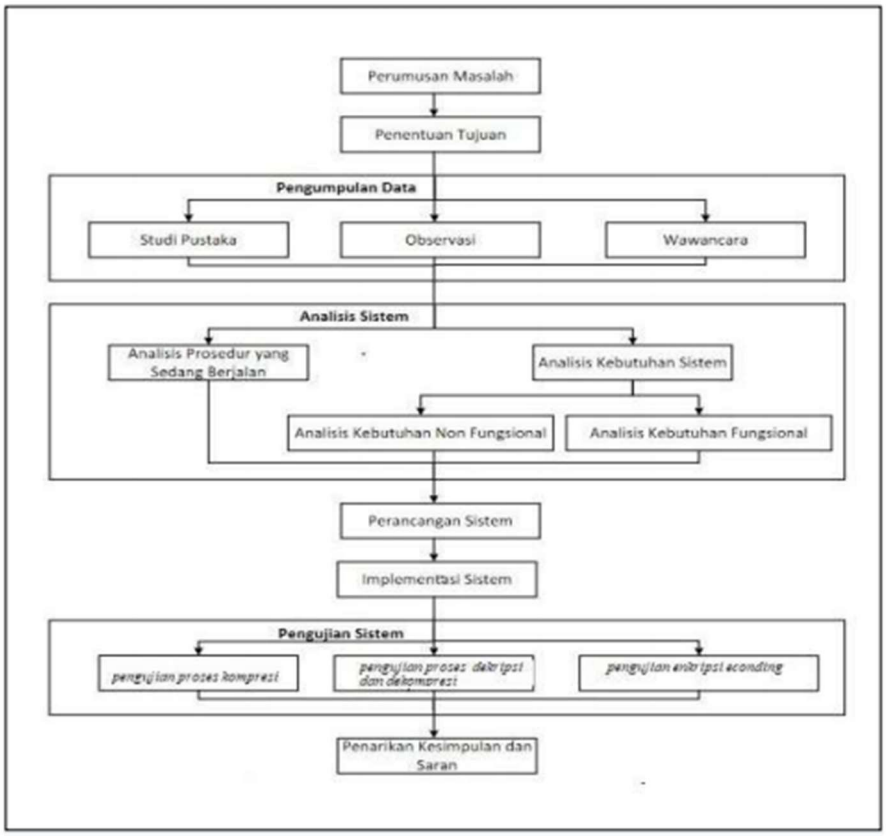
Dalam menentukan suatu prosedur, gambar, tahapan, waktu dan tempat pengambilan data, maka diperlukan suatu metode penelitian yaitu metode deskriptif, yang digunakan untuk menggambarkan dan mewakili objek sesuai dengan kondisi yang ada[13]. Metode prototipe adalah metode yang digunakan untuk menggambarkan bentuk awal suatu sistem yang menggambarkan ide-ide, bereksperimen dengan desain dan mencari sebanyak mungkin masalah dan tahap penyelesaian dalam pembuatan sistem[14],[15]. Metode ini memungkinkan pengguna untuk mengetahui tahap seperti apa yang dilakukan dalam mengembangkan sistem sampai sistem dapat berfungsi dengan baik.




Gambar 1. Prototipe Model[13]

## A. Teknik Pengumpulan Data

Proses pengumpulan data melibatkan teknik wawancara yang dilakukan pada pengguna file data atau arsip penting baik pengguna independen atau pengguna di suatu institusi. Pengamatan tingkat pencurian data serta pola penggunaan dan pertukaran data file digital. Studi pustaka dalam pengembangan sistem yang kemudian diterjemahkan dalam diagram, tampak pada gambar 2.




Gambar 2. Diagram Alur Penelitian

TEKNOMATIKA, Vol.12, No.01, Maret 2022
P-ISSN : 2087-9571, E-ISSN : 2541-335X

## B. Analisis Sistem

Analisis yang digunakan dalam penelitian ini yaitu analisis masalah dan analisis kebutuhan.

1. Analisis Masalah

Dokumen harus dirahasiakan dan rahasia agar tidak disalahgunakan oleh pihak yang tidak berwenang. Security system data yang lemah yang berdiri sendiri mengakibatkan munculnya potensi pencurian dokumen. Salah satu cara untuk mengamankan dokumen yang sangat mungkin adalah dengan mengubah nilai dokumen asli menjadi dokumen terenkripsi yang sulit dibaca.

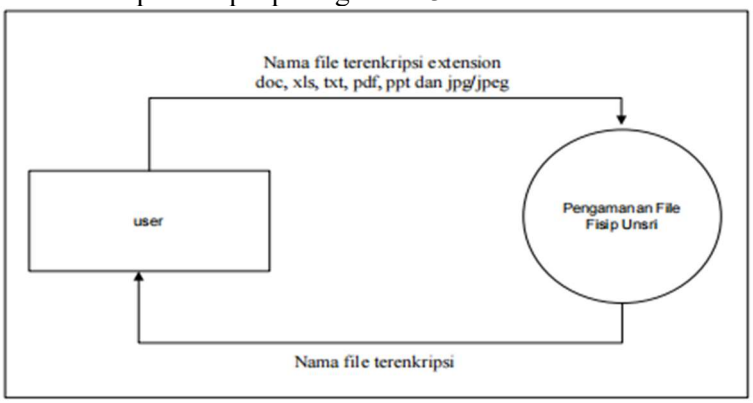
2. Analisis Kebutuhan

Analisis kebutuhan dalam penelitian, yaitu : fungsional dan non-fungsional.

a. fungsionalitas meliputi: sistem mampu mengenkripsi file menggunakan algoritma RC4, sistem kompresi file menggunakan algoritma Huffman, sistem dapat memverifikasi integritas file dengan kecocokan nilai hash, sistem mampu mendekripsi dari file enkripsi ke file asli, sistem mampu memasukkan pesan pada gambar gambar dan sistem mampu melakukan ekstraksi pesan dan mendekripsi pesan dari gambar gambar.
b. Kebutuhan non-fungsional: dalam kebutuhan fungsional penelitian ini hanya mengacu bahasa pemrograman PHP dan database MySql.

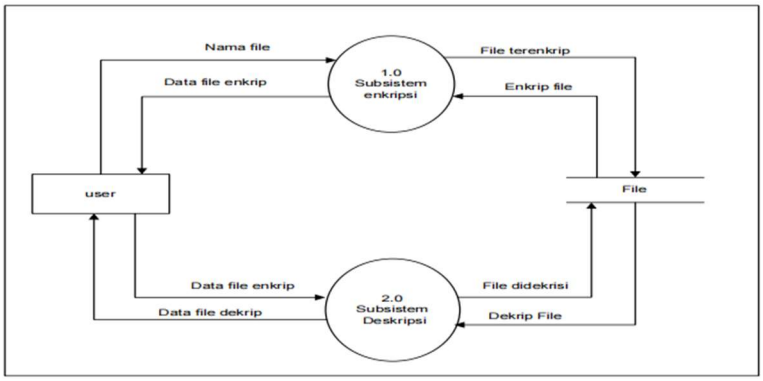
## C. Perancangan Sistem

Desain sistem mencakup desain desain database, desain Diagram Aliran Data, Diagram Hubungan Entitas. Aplikasi yang dibangun terdapat terminator, yang merupakan users system. Data flow yang masuk ke sistem berupa file. Ekstensinya diperbolehkan dienkripsi dalam bentuk file berupa doc, xls, txt, pdf, ppt dan jpg atau jpeg. Aliran data yang dihasilkan oleh sistem dalam bentuk ekstensi file terenkripsi. tampakpada gambar 3.



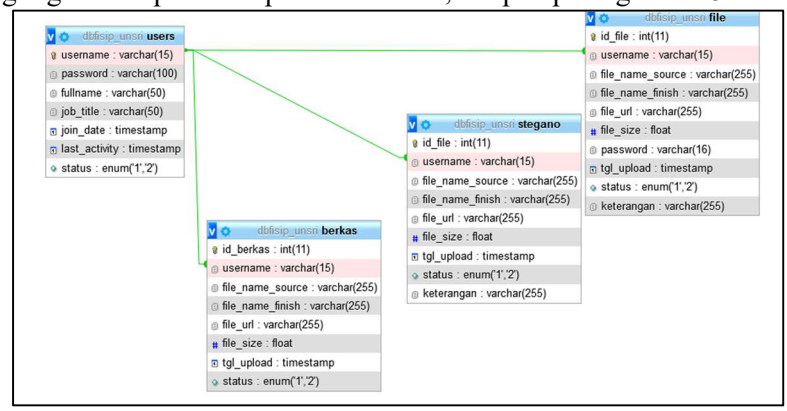

Gambar 3. Diagram data flow

Sistem kriptografi dibangun menjadi dua sub sistem, yaitu enkripsi dan dekripsi, tampak pada gambar 4.




Gambar 4. Sub system encrypt-decrypt

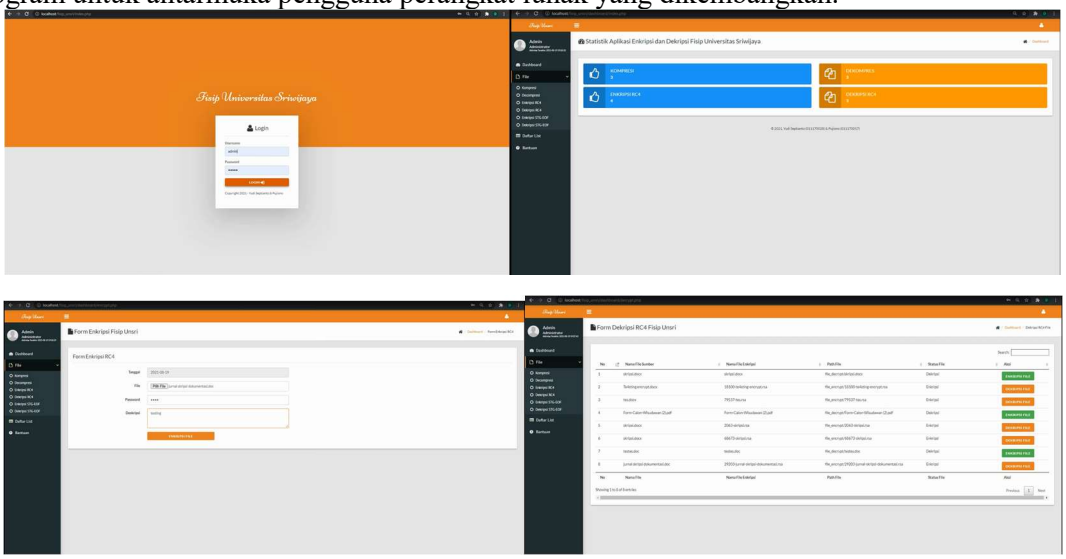
Diagram database dari perangkat lunak yang dikembangkan dan desain database ini mengacu pada ERD yang digunakan pada tahap desain sistem, tampak pada gambar 5.




Gambar 5. Hubungan tabel database

## D. Implementasi System

Berdasarkan referensi desain database, desain antarmuka pengguna perangkat lunak yang akan dibangun dan penerapan kode program. Gambar 6 adalah hasil dari implementasi kode program untuk antarmuka pengguna perangkat lunak yang dikembangkan.



Gambar 6. Antarmuka pengguna aplikasi

TEKNOMATIKA, Vol.12, No.01, Maret 2022
P-ISSN : 2087-9571, E-ISSN : 2541-335X

**E. Pengujian system**

Tes ini adalah untuk menguji interkoneksi antara modul atau fungsi dalam aplikasi menggunakan black-box testing[16], [17]. Melakukan heuristik untuk melihat kelayakan sistem dari pengembang sistem[18], [19]. Penilaian kegunaan heuristik melibatkan pengembang aplikasi sebagai responden. Selain perangkat lunak, tes juga diuji pada hasil enkripsi untuk melihat hasil tes resistensi file enkripsi. Tes dilakukan pada kedua file terenkripsi menggunakan file RC4 dan steganografi. Tes ini melibatkan alat generator dekripsi menggunakan kata sandi.

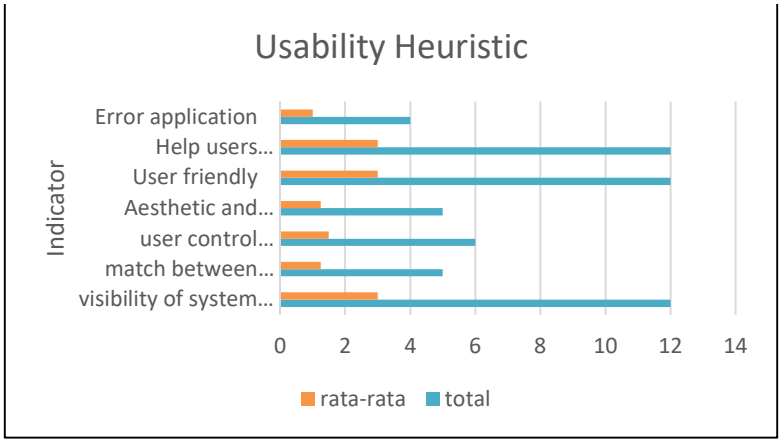
## 3. HASIL DAN PEMBAHASAN

Pengujian perangkat lunak menggunakan pengujian blackbox di mana tes ini dilakukan untuk melihat fungsi dari semua bagian dari sistem perangkat lunak yang dikembangkan. Dari hasil tes yang dilakukan ditemukan bahwa semua modul berjalan dengan baik seperti yang diharapkan.

Tabel 1. Rekapitulasi modul integrase hasil tes (pengujian blackbox)

| Tidak | Formulir yang diuji | Informasi | Berharap | Hasil tes |
|---|---|---|---|---|
| 1 | Pengujian pada formulir login | Dalam formulir login pengguna memasukkan username dan password kemudian klik tombol login. | Pengujian *login* "sukses" kemudian di direct ke menu utama. Jika salah maka kembali ke menu login dan masukkan *nama pengguna* dan *passwaord.* | Keberhasilan |
| 2 | Pengujian pada *Kirim* formulir. mengunggah *berkas* | Pada saat pengguna Mengirim/mengunggah file, lalu file Ini dalam dekripsi dan kemudian pergi ke folder enkrip. | Ketika file telah enkripsi *dan* file dienkripsi pergi ke folder enscript dengan data acak. file Berarti successful | Keberhasilan |
| 3 | Pengujian pada kontak pada daftar daftar | Pada *formulir* kontak Masuk ke pengguna dapat melihat *file* yang telah dikirim. baik dalam database Dan dalam aplikasi itu sendiri | Pengujian ketika pengguna melihat kontak masuk maka akan menampilkan *file* yang telah dikirim oleh pengguna lain | Keberhasilan |
| 4 | Simuasi | Pada *formulir* ini Simulasi dilakukan untuk melihat kunci pribadi, kunci digital hasil dari hasil dekripsi dan dekripsi | Pada *formulir* ini Simulasi dilakukan untuk melihat kunci pribadi dan digital hasil dekripsi dan Hasil dekripsi | Keberhasilan |
| 5 | Pengujian Kompresi | Berkas dalam kompresi adalah Mengurangi/meningkatkan dari file sebelumnya | Berkas terkompresi dikurangi/ditingkatkan ketika dikompresi | Keberhasilan |
| 6 | Pengujian penyisipan pesan ke dalam gambaran | Pada saat pengguna mengirim/menjelajahi file iklan, lalu file Ada di dekripsi gambar dan kemudian masuk ke folder enkripsi | Ketika file telah enkripsi gambar dan kemudian file terenkripsi masuk ke folder enkripsi dalam bentuk format gambar, File ini berarti berhasil | Keberhasilan |

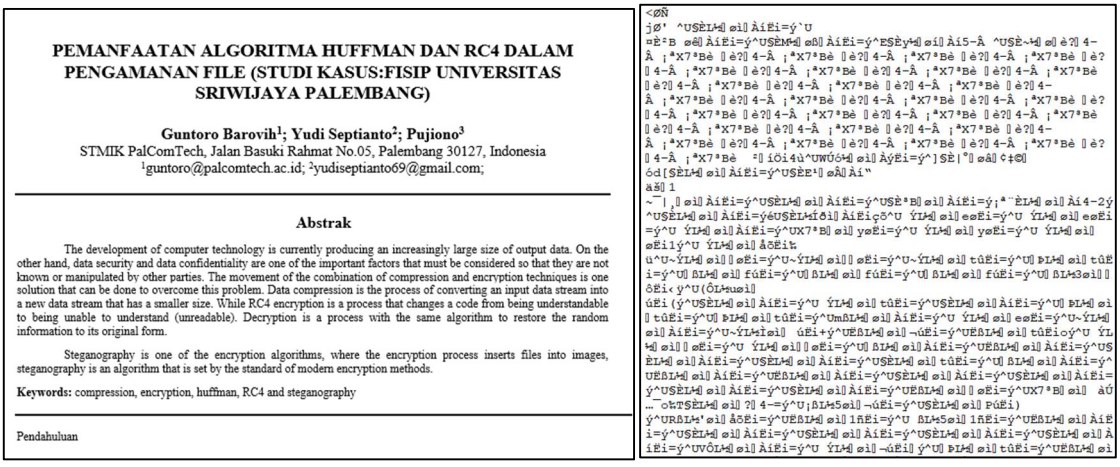
Selain pengujian integrasi antar modul, pengujian kegunaan heuristik juga dilakukan pada perangkat lunak yang dikembangkan untuk mendapatkan hasil seperti yang diharapkan dan mudah digunakan oleh pengguna. Kegunaan heuristik atau evaluasi heuristik digunakan untuk melihat cacat dalam sistem yang sedang[20] dikembangkan[20], [21].




Gambar 7. Penilaian Kegunaan Heuristik

Gambar 7 menjelaskan penilaian responden terhadap penggunaan aplikasi, antara lain :

1. Secara fungsional seluruh sistem berjalan dengan baik, namun ada beberapa indikator yang memiliki penilaian yang dianggap penting untuk ditingkatkan, antara lain visibilitas status sistem, User friendly, Help users system status dengan rating rata-rata 3.
2. Dalam beberapa indikator penilaian rata-rata responden memberikan skor 1,5. Untuk kecocokan indikator antara sistem dan dunia nyata, kontrol pengguna, desain Estetika dan minimalis, aplikasi Error, yang menyatakan sebagai masalah kecil yang tidak terlalu dianggap sebagai prioritas rendah untuk diperbaiki.
3. Secara teknis modul aplikasi mulai dari kompresi file, enkripsi RC4 dan dekripsi dan enkripsi steganografi dan dekripsi dalam hal ini EoF sangat bagus, hanya saja dari segi antarmuka pengguna masih memiliki banyak hal untuk ditingkatkan.



**PEMANFAATAN ALGORITMA HUFFMAN DAN RC4 DALAM PENGAMANAN FILE (STUDI KASUS:FISIP UNIVERSITAS SRIWIJAYA PALEMBANG)**

**Guntoro Barovih[1]; Yudi Septianto[2]; Pujiono[3]**
STMIK PalComTech, Jalan Basuki Rahmat No.05, Palembang 30127, Indonesia
[1]guntoro@palcomtech.ac.id; [2]yudiseptianto69@gmail.com;

**Abstrak**

The development of computer technology is currently producing an increasingly large size of output data. On the other hand, data security and data confidentiality are one of the important factors that must be considered so that they are not known or manipulated by other parties. The movement of the combination of compression and encryption techniques is one solution that can be done to overcome this problem. Data compression is the process of converting an input data stream into a new data stream that has a smaller size. While RC4 encryption is a process that changes a code from being understandable to being unable to understand (unreadable). Decryption is a process with the same algorithm to restore the random information to its original form.

Steganography is one of the encryption algorithms, where the encryption process inserts files into images, steganography is an algorithm that is set by the standard of modern encryption methods.

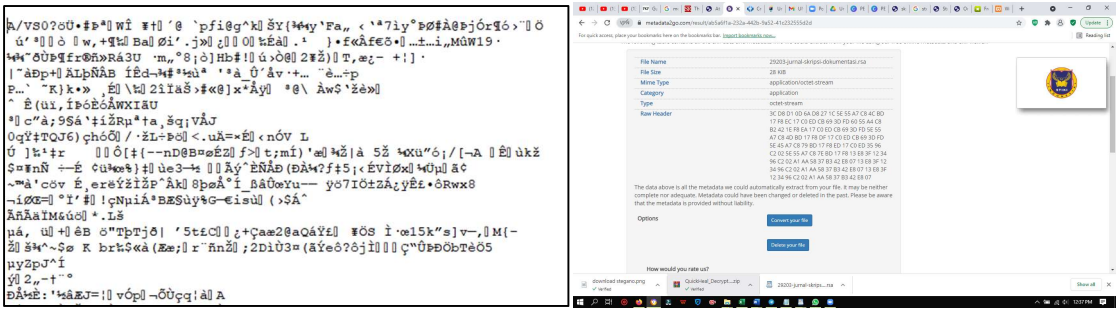
**Keywords:** compression, encryption, huffman, RC4 and steganography

Pendahuluan

Gambar 8. Huffman dan RC4 enkripsi file plaintext dan file

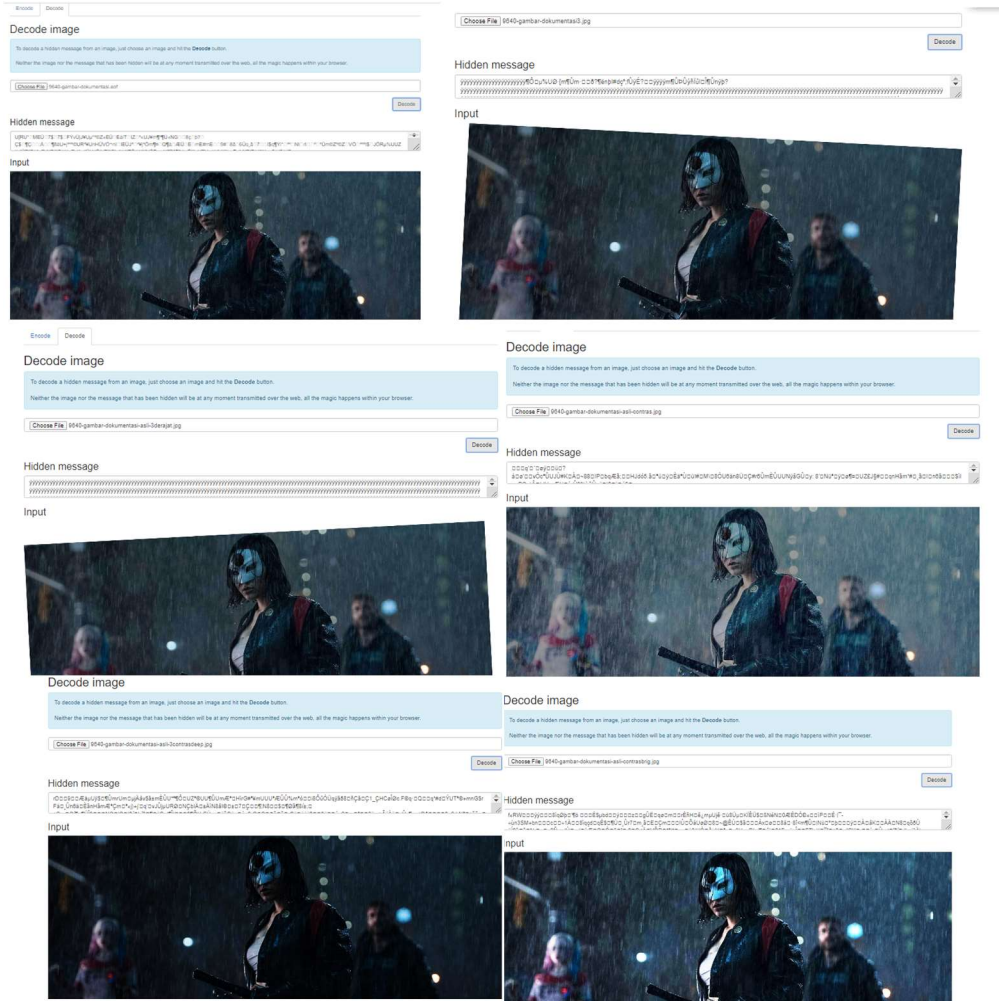
Gambar 8 menjelaskan bentuk file dokumen sebelum dan sesudah proses enkripsi menggunakan penggabungan algoritma Huffman untuk melakukan kompresi file dan RC4 untuk mengenkripsi file yang dihasilkan dari kompresi file. Tes pembobolan file dilakukan untuk melihat apakah file masih dapat dibaca menggunakan kata sandi acak menggunakan alat ensipt RC4 dan generator dekripsi. Diperoleh bahwa dari hasil tes file yang didekripsi dalam generator dengan kata sandi acak masih belum bisa dibaca. Meskipun ekstensi pada file yang didekripsi telah diubah ke file asli. Tampak pada gambar 9.

TEKNOMATIKA, Vol.12, No.01, Maret 2022
P-ISSN : 2087-9571, E-ISSN : 2541-335X



Gambar 9. Hasil forced file breakup (dekripsi)

Tes juga dilakukan pada file steganografi. Tes dilakukan dengan menggunakan generator alat yang tersedia di internet untuk menguji apakah pesan pada gambar yang digunakan sebagai media yang dimasukkan pesan dapat dibaca dengan mudah. Berdasarkan hasil tes yang diperoleh untuk ekstraksi antar gambar dapat dilakukan, gambar yang menjadi media penyisipan pesan dapat dibaca namun pesan yang dimasukkan pada gambar tidak dapat dibaca.

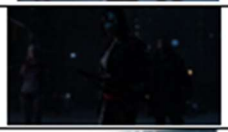


Gambar 10 Hasil tes steganografi mengubah sudut dan kecerahan gambar

Berdasarkan pengujian pesan shortsripsian melalui aplikasi yang dikembangkan diperoleh pengujian seperti pada tabel 2. Diuji dengan melakukan serangan oleh ketahanan yaitu resistensi gambar digital terhadap serangan dari kedua persimpangan, rotasi, perubahan tingkat kecerahan

gambar. Hasil tes menunjukkan bahwa dalam proses turnaround, perubahan tingkat kecerahan gambar dan tingkat perubahan warna RGB mengakibatkan ukuran file gambar yang telah dimasukkan pesan rahasia meningkat dalam ukuran. Namun, dari semua tes pemutaran dan pemotongan gambar ingital, perubahan kontras dalam file gambar digital mengakibatkan tidak ada pengungkapan ulang pesan rahasia yang telah ditempelkan sebelumnya, tetapi pada pengujian perubahan pada rgb tingkat warna pesan masih dapat dibaca menggunakan aplikasi yang dikembangkan.

Tabel 2 menguji deskripsi file steganografi

| Gambaran | Ukuran (kb, byte) | Deskripsi uji |
|---|---|---|
|  | 463 KB | Gagal |
|  | 296 KB | gagal |
|  | 576 KB | Berhasil |
|  | 190 KB | berhasil |
|  | 459 KB | gagal |
|  | 432 KB | gagal |
|  | 416KB | gagal |

Selain mengukur kinerja aplikasi dan pengujian dekripsi pesan steganografi, juga menguji waktu pemrosesan file, juga melihat perbedaan ukuran antara file sebelum mengompresi dengan file setelah mengompresi. Hasil pengujian kinerja kompresi tampak pada tabel 3.

Tabel 3 Pengujian Kinerja Kompresi dalam Hitungan Detik

| Tipe Berkas | Ukuran Sebelum | Ukuran Setelah | Rasio Kompresi | Waktu Kompresi | Total Waktu |
|---|---|---|---|---|---|
| *Docx* | 102 KB | 101 KB | 6,6% | 0.095 | 0.118 |
| *Pdf* | 233 KB | 232 KB | 6,0% | 0.020 | 0.049 |
| *Jpg* | 759 KB | 759 KB | 0% | 0 | 0.056 |

Dalam hasil kompresi file terlihat bahwa *file* teks. Rasio kompresi lebih besar dan waktu kompresi file lebih lama jika dibandingkan *file* teks tipe dokumen (.pdf, .docx,). dimana rasio kompresi kecil dan waktu kompresi yang lebih cepat. Algoritma Huffman tidak berlaku untuk file yang memiliki format file .jpg. Karena algoritma ini bekerja dengan mengumpulkan jumlah

karakter yang sama ke dalam nomor byte. Sedangkan dalam file format JPD atau sejenisnya adalah file yang dihitung menggunakan pixel.

## 4. KESIMPULAN

Adapun simpulan yang bisa dijabarkan dari hasil penelitian ini, antara lain:

1. Algoritma dalam penelitian ini menggunakan algoritma Huffman untuk proses kompresi file dokumen dan algoritma pada enkripsi file, sedangkan algoritma yang digunakan dalam enkripsi steganografi adalah End of File.
2. Dari hasil pengujian blackbox dijelaskan bahwa secara keseluruhan aplikasi ini bekerja dengan baik. Berdasarkan uji kegunaan heuristik, aplikasi dapat digunakan secara massal oleh pengguna biasa.
3. Ada perubahan fisik pada gambar seperti perubahan sudut (rotasi) gambar, perubahan kontras gambar, kedalaman warna gambar akan mempengaruhi isi pesan yang terdapat dalam gambar. Sehingga pesan dalam gambar tidak dapat dibaca dan file mengalami perubahan ukuran file sehingga pesan tidak dapat dibaca.
3. Algoritma kompresi Huffman hanya dapat dilakukan pada file tipe dokumen tetapi tidak dapat digunakan pada file tipe gambar.

## UCAPAN TERIMA KASIH

Penelitian yang telah dilakukan berdasarkan kebutuhan pengguna untuk mengamankan file penting. Ucapan Terima kasih kepada FISIP Universitas Sriwijaya yang bersedia memberikan kesempatan untuk melakukan penelitian ini.

## DAFTAR PUSTAKA

[1] BSSN, “Rekap Serangan Siber (Januari – April 2020),” *Badan Syber dan Sandi Negara*, 2020. https://bssn.go.id/rekap-serangan-siber-januari-april-2020/ (accessed Jul. 30, 2021).

[2] 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, doi: 10.36055/setrum.v3i1.497.

[3] R. Primartha, “Penerapan Enkripsi Dan Dekripsi File Menggunakan Algoritma Data Encryption Standard (DES),” *J. Res. Comput. Sci. Appl. Informatics Eng. Dep. Sriwij. Univ.*, vol. 01, no. 01, pp. 1–19, 2011.

[4] S. H. Suryawan and Hamdani, “Pengamanan Data File Dengan Menggunakan Algoritma Enkripsi Rivest Code 5,” *J. Inform. Mulawarman Ed. Juli*, vol. 8, no. 2, pp. 44–49, 2013, doi: http://dx.doi.org/10.30872/jim.v8i2.106.

[5] Yusfrizal, “Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan RSA Berbasis Android,” *J. Tek. Inform. Kaputama*, vol. 3, no. 2, pp. 29–37, 2019.

[6] A. P. U. Siahaan, “Implementasi Teknik Kompresi Teks Huffman,” *J. Inform. Ahmad Dahlan*, vol. 10, no. 2, 2016, doi: 10.26555/jifo.v10i2.a5070.

[7] E. Satir and H. Isik, “A Huffman compression based text steganography method,” *Multimed. Tools Appl.*, vol. 70, no. 3, pp. 2085–2110, 2014, doi: 10.1007/s11042-012-1223-9.

[8] N. Sangwan, "Text Encryption with Huffman Compression," *Int. J. Comput. Appl.*, vol. 54, no. 6, pp. 29–32, 2012, doi: 10.5120/8572-2307.

[9] R. Kumar, A. Malik, S. Singh, and S. Chand, "A high capacity email based text steganography scheme using Huffman compression," in *2016 3rd International Conference on Signal Processing and Integrated Networks (SPIN)*, 2016, pp. 53–56, doi: 10.1109/SPIN.2016.7566661.

[10] D. R. Saragi, J. M. Gultom, J. A. Tampubolon, and I. Gunawan, "Pengamanan Data File Teks (Word) Menggunakan Algoritma RC4," *J. Sist. Komput. dan Inform.*, vol. 1, no. 2, p. 114, 2020, doi: 10.30865/json.v1i2.1745.

[11] D. Hendarsyah and R. Wardoyo, "Implementasi Protokol Diffie-Hellman Dan Algoritma RC4 Untuk Keamanan Pesan SMS," *IJCCS (Indonesian J. Comput. Cybern. Syst.*, vol. 5, no. 2, pp. 14–25, 2015, doi: 10.22146/ijccs.1997.

[12] A. Fauzi and R. P. Rahayu, "Penerapan Metode End Of File Pada Steganografi Citra Gambar dengan Memanfaatkan Algoritma Affine Cipher sebagai Keamanan Pesan," *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 2, pp. 117–123, 2017.

[13] P. Yoko, R. Adwiya, and W. Nugraha, "Penerapan Metode Prototype dalam Perancangan Aplikasi SIPINJAM Berbasis Website pada Credit Union Canaga Antutn," *J. Merpati*, vol. 7, no. 3, pp. 212–223, 2019, [Online]. Available: http://jurnal.univbinainsan.ac.id/index.php/jusim/article/download/331/228.

[14] I. Rijayana and R. Istambul, "Design of Web-Based Reservation of Residential House Design ApplicationUsing the Prototype Method," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 11, pp. 1229–1233, 2021, doi: https://doi.org/10.17762/turcomat.v12i11.6023.

[15] Rifa'atunnisa, E. Satria, and R. Cahyana, "PENGEMBANGAN APLIKASI ZAKAT BERBASIS ANDROID MENGGUNAKAN METODE PROTOTYPE," *J. Algoritm.*, vol. 11, no. 2, pp. 213–219, 2015, doi: https://doi.org/10.33364/algoritma/v.11-2.213.

[16] S. Supriyono, "Software Testing with the approach of Blackbox Testing on the Academic Information System," *Int. J. Inf. Syst. Technol.*, vol. 3, no. 2, pp. 227–233, 2020.

[17] D. Febiharsa, I. M. Sudana, and N. Hudallah, "Uji Fungsionalitas (BlackBox Testing) Sistem Informasi Lembaga Sertifikasi Profesi (SILSP) Batik Dengan AppPerfect Web Test Dan Uji Pengguna," *JOINED J.*, vol. 1, no. 2, pp. 117–126, 2018, [Online]. Available: http://e-journal.ivet.ac.id/index.php/jiptika/article/view/752.

[18] R. Yáñez Gómez, D. Cascado Caballero, and J.-L. Sevillano, "Heuristic Evaluation on Mobile Interfaces: A New Checklist," *Sci. World J.*, vol. 2014, p. 434326, 2014, doi: 10.1155/2014/434326.

[19] G. F. Tondello, D. L. Kappen, E. D. Mekler, M. Ganaba, and L. E. Nacke, "Heuristic evaluation for gameful design," *CHI Play 2016 - Proc. Annu. Symp. Comput. Interact. Play Companion*, pp. 315–323, 2016, doi: 10.1145/2968120.2987729.

[20] A. Sivaji, A. Abdullah, and A. G. Downe, "Usability testing methodology: Effectiveness of heuristic evaluation in E-government website development," *Proc. - AMS 2011 Asia*

TEKNOMATIKA, Vol.12, No.01, Maret 2022
P-ISSN : 2087-9571, E-ISSN : 2541-335X

*Model. Symp. 2011 - 5th Asia Int. Conf. Math. Model. Comput. Simul.*, no. June, pp. 68–72, 2011, doi: 10.1109/AMS.2011.24.

[21] T. Purnama, I. M. A. Pradnyana, and K. Agustini, "Usability Testing Menggunakan Metode Heuristic Evaluation Pada Aplikasi E-Musrenbang Bappeda Kabupaten Badung," *J. Pendidik. Teknol. dan Kejuru.*, vol. 16, no. 1, p. 87, 2019, doi: 10.23887/jptk-undiksha.v16i1.17949.