Penerapan Algoritma Kriptografi Route Cipher Dengan Metode Arah Jarum Jam Pada Aplikasi Pengaman Citra Digital

Application of Route Cipher Cryptography Algorithm with Clockwise Method in Digital Image Security Applications

Mhd Fauzi Fasha[1], Khairuddin Nasution[2], Oris Krianto Sulaiman[3]
[1,2,3] Universitas Islam Sumatera Utara

e-mail: [1]mhdfasha12@gmail.com, [2]Khairuddin_nst@uisu.ac.id, [3]Oris.ks@ft.uisu.ac.id

ABSTRAK

Masalah keamanan data atau informasi menjadi masalah penting di era teknologi informasi saat ini. Kerahasiaan data merupakan hal yang sangat penting untuk diperhatikan terutama jika data tersebut berisi informasi yang sensitif dan sangat rahasia dan hanya bisa diketahui oleh pihak yang bersangkutan. Citra merupakan salah satu bentuk informasi yang banyak disalahgunakan oleh pihak-pihak yang tidak bertanggung jawab sehingga dapat merugikan individu, organisasi, maupun perusahaan besar. Teknik Kriptografi merupakan metode yang dapat digunakan untuk menjaga keamanan data atau informasi tersebut. Algoritma route cipher merupakan salah satu teknik kriptografi klasik yang menggunakan transposisi dalam melakukan enkripsi. Kekuatan algoritma ini yaitu kunci yang lebih banyak dan rumit. Hasil pengujian berupa citra hasil enkripsi dan dekripsi, perbandingan ukuran data citra asli dengan citra hasil enkripsi dan dekripsi, dan waktu proses enkripsi dan dekripsi.
Kata kunci: kriptografi, kriptografi klasik, route cipher, citra.

ABSTRACT (11pt Bold Italic)

The problem of data or information security is an important problem in the current era of information technology. Confidentiality of data is very important to note, especially if the data contains sensitive and highly confidential information and can only be known by the parties concerned. Image is one form of information that is widely misused by irresponsible parties so that it can harm individuals, organizations, and large companies. Cryptographic technique is a method that can be used to maintain the security of the data or information. The route cipher algorithm is one of the classical cryptographic techniques that uses transposition in encryption. The strength of this algorithm is more and more complicated keys. The test results are in the form of encrypted and decrypted images, comparison of the size of the original image data with the encrypted and decrypted images, and the encryption and decryption process time.
***Keywords**: cryptography; classic cryptography; image*

1. PENDAHULUAN

Kemajuan teknologi ini juga diikuti dengan semakin mudahnya memperoleh data atau informasi. Pengiriman dan penyimpanan data bisa dilakukan dengan cepat, mudah, dan praktis. Proses penyimpanan data atau informasi ini perlu untuk diperhatikan dari aspek keutuhan, kerahasiaan, dan keamanannya. Informasi yang diperoleh dapat berupa file teks, citra, audio maupun video yang dikemas secara digital.

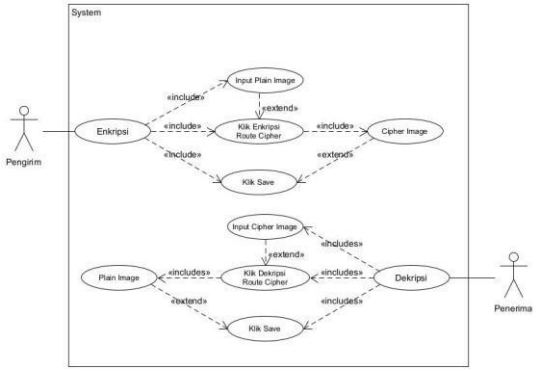
Pada zaman teknologi saat ini, citra menjadi salah satu dari sekian banyaknya bentuk informasi yang digunakan dalam pertukaran data atau informasi. Namun tidak jarang informasi tersebut disalah-gunakan oleh pihak-pihak yang tidak memiliki otoritas dan tidak bertanggung jawab, seperti manipulasi ataupun rekayasa citra. Sehingga data citra ini yang bersifat pribadi atau rahasia perlu untuk diamankan agar menghindari hal-hal yang dapat merugikan pribadi, organisasi, kelompok, maupun perusahaan. Hal seperti inilah yang menyebabkan pentingnya untuk mengamankan citra digital. Salah satu metode yang dapat memecahkan masalah yang disebutkan di atas adalah dengan menggunakan teknik pengamanan data atau teknik kriptografi (cryptography).

Kriptografi adalah ilmu mengenai teknik enkripsi yang mengacak suatu data menggunakan kunci publik (public key) sehingga sulit dibaca oleh orang yang tidak memiliki kunci privat (private key) (Kromodimoeljo, 2010). Penggunaan kriptografi digunakan untuk mencegah adanya penyadapan data pada pengiriman dengan cara penyandian data (Kusumaningtyas, 2018). Penyandian data dengan cara mengubah teks asli (plaintext) menjadi teks yang tersandi (ciphertext) yang tidak mempunyai makna dan tidak dapat dibaca. Metode yang digunakan dengan menggunakan enkripsi untuk penyandian dan dekripsi untuk membuka penyandian tersebut. Proses enkripsi merubah data asli (plaintext) menjadi teks sandi (ciphertext). Sedangkan proses dekripsi merubah data tersandikan (ciphertext) menjadi data asli (plaintext) ketika data diterima.

2. METODE PENELITIAN

Usecase Diagram

Usecase diagram pada perancangan ini bertujuan untuk menjelaskan bagaimana interaksi antara aktor dan sistem dengan apa saja yang berjalan pada sistem tersebut. Usecase diagram ini terbagi dua bagian, yaitu pengirim dan penerima. Berikut adalah desain model usecase diagram pada sistem yang akan dirancang.



Proses pengamanan file citra dimana dapat memproseskan enkripsi dan dekripsi dengan algoritma *route cipher*.dan pengirim dan penerima dapat menyimpan hasil proses enkripsi dan dekripsi file citra tersebut.

3. HASIL DAN PEMBAHASAN

Tahap implementasi merupakan tahap yang dilakukan dengan cara menerapkan algoritma route cipher dengan metode searah jarum jam ke sistem keamanan data citra digital pada aplikasi pengamanan file citra berekstensi *.jpeg dibuat dengan menggunakan bahasa pemrograman C#. Penerapan algoritma route cipher dengan metode searah jarum jam melakukan pemanggilan fungsi dengan menuliskan kodingan pada file CS (C Sharp) untuk mengenkripsikan dan mendekripsikan file citra tersebut.

Maka, data citra digital yang telah dienkripsikan atau didekripsikan dapat disimpan ke dalam memori perangkat pengguna. Berikut ini tampilan data citra digital tersebut di dalam memori perangkat pengguna.

Prosedur Pengujian Black Box

Setelah tahap-tahap dalam metode prototyping dilakukan di antaranya analisa kebutuhan sistem, desain sistem dan kodingan, maka langkah selanjutnya adalah melakukan pengujian sistem. Pada tahap pengujian sistem ini, penulis melakukan pengujian terhadap setiap fungsi yang ada pada aplikasi yang telah dirancang. Metode pengujian yang digunakan yaitu metode black box dimana pengujian ini dilakukan untuk memfokuskan pada persyaratan fungsional sistem pada aplikasi yang telah dirancang.

Pada tahap pengujian ini, penulis melakukan pengujian secara bertahap pada setiap fungsi yang ada yaitu:

1. Fungsi Cari
2. Fungsi Enkripsi
3. Fungsi Dekripsi
4. Fungsi Simpan

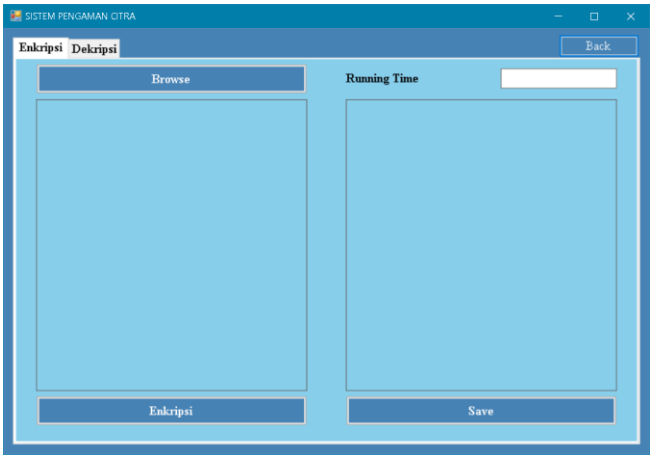
No.	Pengujian	Skenario Pengujian	Hasil yang Diharapkan	Hasil Pengujian
1.	Fungsi Cari	Mencari dan memasukkan ke *picturebox*	Berhasil memasukkan ke *picture box*	Berhasil
2.	Fungsi Enkripsi	Mengenkripsikan data citra digital	Berhasil menghasilkan *cipher image*	Berhasil
3.	Fungsi Dekripsi	Mendekripsikan data citra digital	Berhasil menghasilkan *plain image*	Berhasil
4.	Fungsi Simpan	Menyimpan hasil data citra digital ke memori perangkat pengguna	Hasil data citra digital berhasil tersimpan di memori perangkat pengguna	Berhasil

Hasil Tampilan *Form* Utama

Pada tampilan *form* utama menampilkan judul dan biodata yang di bawahnya terdapat tombol untuk memulai aplikasi pengaman citra yang langsung ditujukan ke *form* enkripsi dan deskripsi.

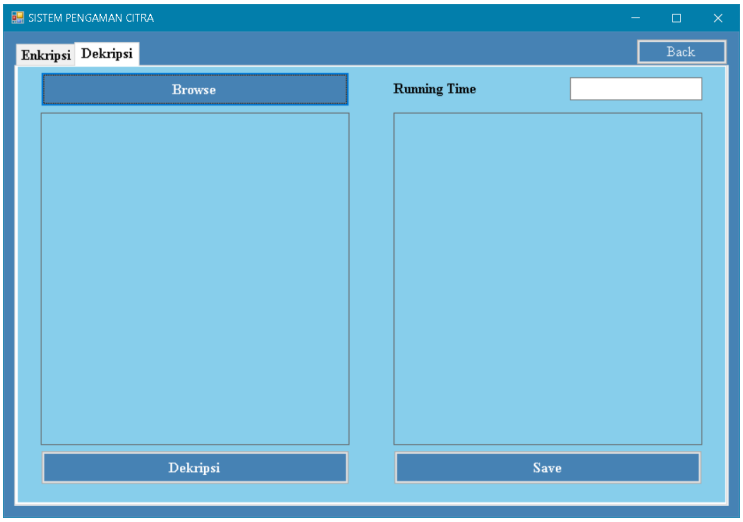
Hasil Tampilan Form Enkripsi

Form enkripsi digunakan untuk melakukan proses enkripsi, dimana terdapat tombol *browse*/pencarian yang berfungsi untuk mencari dan memasukkan gambar yang terdapat di direktori, kemudian diproses dengan tombol enkripsi, dan akan menampilkan hasil *file* yang diproses dan waktu proses di kolom *Running Time*, kemudian bisa disimpan di direktori yang diinginkan dengan nama *file* yang baru dan tetap dengan ekstensi *.jpeg.



Hasil Tampilan *Form* Deskripsi

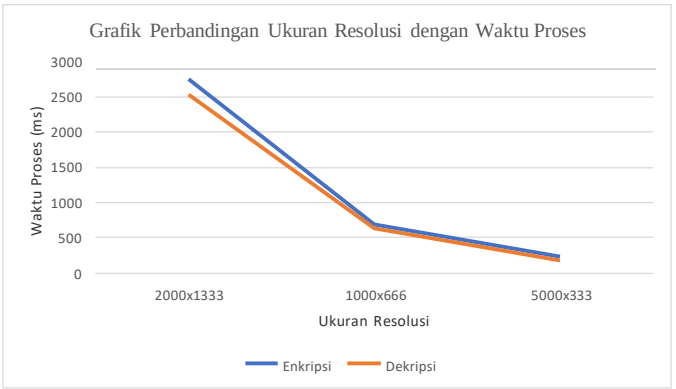
Form deskripsi digunakan untuk melakukan proses deskripsi, dimana terdapat tombol *browse*/pencarian yang berfungsi untuk mencari dan memasukkan gambar yang terdapat di direktori, kemudian diproses dengan tombol deskripsi, dan akan menampilkan hasil *file* yang diproses dan waktu proses di kolom *Running Time*, kemudian bisa disimpan di direktori yang diinginkan dengan nama *file* yang baru dan tetap dengan ekstensi *.jpeg.



Hasil Waktu Proses Enkripsi dan Dekripsi

Resolusi Citra	Ukuran File Citra	Waktu Proses Enkripsi (ms)	Ukuran Setelah Proses Enkripsi	Waktu Proses Deskripsi (ms)	Ukuran Setelah Proses Deskripsi
500 X 333	79,7 Kb	236 ms	650 Kb	179 ms	650 Kb
1000 X 666	207 Kb	684 ms	2,54 Mb	679 ms	2,54 Mb
2000X 1333	592 Kb	2752 ms	10,1 Mb	2734 ms	10,1 Mb

Data yang telah diperoleh dari tabel, akan dikonversikan ke dalam bentuk grafik perbandingan ukuran resolusi dengan waktu proses enkripsi dan dekripsi yang dapat dilihat pada sebagai berikut.



Berdasarkan pada gambar grafik, dapat menyimpulkan bahwa besarnya ukuran resolusi citra berbanding lurus secara linear dengan besarnya waktu proses yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi pada algoritma tersebut.

4. KESIMPULAN

Berdasarkan pengamatan dari setiap tahap-tahap yang dilakukan oleh penulis pada perancangan sistem pada aplikasi pengamanan file citra untuk mengenkripsikan dan mendekripsikan file citra berekstensi *.jpeg dengan menggunakan algoritma route cipher dengan metode searah jarum jam. Maka, penulis dapat menyimpulkan bahwa:

1. Aplikasi pengamanan file citra dapat membantu mengirimkan file citra bersifat rahasia dengan cara menggunakan algoritma route cipher dengan metode searah jarum jam agar dapat meningkatkan keamanan dan kepriviasian pada file citra tersebut.
2. Berdasarkan grafik hubungan ukuran resolusi dengan waktu proses enkripsi dan dekripsi, besarnya ukuran resolusi citra berbanding lurus secara linear dengan besarnya waktu proses yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi pada algoritma tersebut.
3. Berdasarkan tabel hasil pengujian waktu proses enkripsi dan dekripsi dapat menyatakan bahwa citra beresolusi 1000×666 membutuhkan waktu proses enkripsi 75% lebih cepat dan waktu proses dekripsi 69.5% dari citra bereolusi 2000×1333 dan citra beresolusi 500×333 membutuhkan waktu proses enkripsi 71% lebih cepat dan waktu dekripsi 75.5% lebih cepat dari citra bereolusi 1000×666. Dalam hal ini dapat membuktikan bahwa besarnya ukuran resolusi berbanding lurus secara linear terhadap lama waktu proses yang dibutuhkan.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Dosen Pembimbing dan Universitas Islam Sumatera Utara serta seluruh pihak yang membantu dalam proses pembuatan penelitian ini.

DAFTAR PUSTAKA

Bangun, Meylisa Siska. 2019. "ImplementasiAlgoritma Route Cipher DalamPengamanan File Pdf. Building of Informatics". *Technology and Science (BITS*). 1(1). 1-6.

Kusumaningtyas, Juwita Artanti. 2018. "Analisa Algoritma Ciphers Transposition: Study Literature". *Jurnal Institut Agama Islan Negeri (IAIN) Salatiga*. 1(1). 1-12.

Nafi'iyah, Nur. 2015. "Algoritma Kohonen Dalam Mengubah Citra Grayleve Menjadi Citra Biner". *Jurnal Ilmiah Teknologi dan Informasia ASIA (JITIKA*). 9(2). 49-55.

Prayitno, Arif. 2017. "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition". *Jurnal Elektronik Sistem Informasi Dan Komputer (STMIK) Rina Mulia.* 3(1). 1-10.

Rouse, Margaret. 2012.C# Definition.[Online]. Tersedia: https://searchwindevelopment.techtarget.com/definition/C

Rouse, Margaret. 2014. Object-oriented programming defition. [Online]. Tersedia: programming.

Rouse, Margaret. 2012. C# Definition.[Online]. Tersedia: https://searchwindevelopment.techtarget.com/definition/C

Rouse, Margaret. 2014. Object-oriented programming defition. [Online]. Tersedia: programming.

Tobing, Nova Fitri Wahyuni Lbn. 2019. "Perancangan Aplikasi Penyandian File Teks Menggunakan Algoritma Route Cipher Berbasis Dekstop*". Jurnal Pelita Informatika Teknik Informatika STMIK Budi Darma Medan*. 8(1), 57-62.