JURNAL ILMIAH TEKNOLOGI INFORMASI DAN KOMUNIKASI (JTIK) VOL 15, No.1, Maret 2024, pp. 146 - 154
p-ISSN : 2087-0868 (media cetak)
e-ISSN : 2598-9707 (media online)
http://ejurnal.provisi.ac.id/index.php/JTIKP

SUPER ENKRIPSI ALGORITMA *ROUTE CIPHER* DAN ALGORITMA *VARIABLY MODIFIED PERMUTATION COMPOSITION* (VMPC) UNTUK PENGAMAN FILE CITRA

Fadliansyah Siagian[1], Yusuf Ramadhan Nasution[2], Suhardi[3]
Universitas Islam Negeri Sumatera Utara
email : [1]fadlisgn890@gmail.com, [2]ramadhannst@uinsu.ac.id, [3]suhardi@uinsu.ac.id

ARTICLE INFO

Article history:

Received : 5 – Februari - 2024
Received in revised form : 15 – Februari - 2024
Accepted : 21 – Februari - 2024
Available online : 1 – Maret - 2024

ABSTRACT

Securing image files is a crucial aspect in addressing information security challenges. Super encryption is an approach that combines various cryptographic algorithms to enhance data security. In this research, we implement Super Encryption by combining two algorithms, namely Route Cipher and VMPC (Variably Modified Permutation Composition). Firstly, we employ the Route Cipher to encrypt image files by rearranging the pixels in the image using a specific mapping scheme. Subsequently, we apply VMPC, a key-symmetric encryption algorithm, to encrypt the previously modified image. The use of VMPC as the second layer aims to provide additional security by incorporating efficient and secure key-symmetric encryption. The results of this research demonstrate that the combination of Route Cipher and VMPC provides strong security for image files. This method introduces a high level of complexity for attackers attempting to decrypt the image without the correct key. Moreover, this Super Encryption offers higher confidentiality and resilience against attacks on image files compared to using a single encryption algorithm.
Keywords: Super Encryption, Image, Route Cipher, VMPC, Cryptography.

1. PENDAHULUAN

Mencuri dan menyalahgunakan gambar yang bersifat rahasia karena citra tersebut masih dapat dikenali dan dibaca oleh manusia adalah masalah yang dapat merugikan pihak yang memiliki akses ke data visual pengguna. Untuk mengatasi tindakan penyadapan dan pencurian citra digital ini, teknik enkripsi kriptografi dapat digunakan. Kriptografi adalah ilmu yang menggunakan teknik-teknik matematika yang berkaitan dengan keamanan data, seperti menjaga kerahasiaan, integritas informasi, dan otentikasi. Kriptografi melibatkan penggunaan algoritma untuk melakukan proses enkripsi, dan salah satu algoritma kriptografi yang berguna dalam hal ini adalah algoritma *Route Cipher* dan *Variably Modified Permutation Composition* (VMPC) [1].

Algoritma *Route Cipher* adalah sebuah teknik kriptografi klasik yang menggunakan transposisi untuk melakukan enkripsi. Pada metode ini, teks *plaintext* awalnya ditulis dalam *grid* dengan dimensi tertentu, dan kemudian dibaca berdasarkan pola yang ditentukan oleh kunci. Untuk pesan yang panjang, jumlah kemungkinan kunci bisa menjadi sangat besar sehingga sulit untuk dihitung. Namun, penting untuk diingat bahwa tidak semua kunci memiliki tingkat keamanan yang sama. Jika jalur yang salah dipilih, hal ini bisa

Received 5 – Februari - 2024; Revised 15 – Februari - 2024; Accepted 21 – Februari - 2024

p-ISSN : 2087-0868 e-ISSN : 2598-9707

menyebabkan bagian dari plaintext tetap terlihat atau malah hanya terbalik, yang dapat memberikan petunjuk kepada kriptanalisis mengenai rute yang digunakan.

Untuk meningkatkan tingkat keamanan, salah satu jenis algoritma kriptografi yang digunakan adalah *Stream Cipher*, yang merupakan algoritma berbasis bit. Dalam konteks makalah ini, digunakan algoritma Stream Cipher yang disebut *Variably Modified Permutation Composition* (VMPC). VMPC *Stream Cipher* memiliki tingkat efisiensi yang cukup baik untuk diimplementasikan pada perangkat lunak dan diklaim memberikan tingkat keamanan yang lebih tinggi dibandingkan dengan RC4, yang masih populer hingga saat ini. Keunggulan tersebut mencakup proses enkripsi dan algoritma penjadwalan kunci yang lebih baik [1].

2. TINJAUAN PUSTAKA

2.1. Keamanan Data Komputer

Perlindungan data komputer merupakan serangkaian tindakan pencegahan terhadap potensi kejahatan yang memanfaatkan komputer sebagai sarana. Upaya keamanan mencakup aspek perlindungan fisik terhadap ruang server dan infrastruktur pendukung, pengaturan keamanan akses yang melibatkan pengguna manusia, pencegahan terhadap virus dan upaya pencurian data, serta menjaga keamanan sistem operasi komputer. Dalam membangun keamanan komputer harus mempertimbangkan aspek *confidentialy*, *integrity*, *authentication*, *non-repudiation* dan *availability* [2].

2.2. Kriptografi

Kriptografi berasal dari bahasa Yunani, dengan "*crypto*" yang berarti rahasia dan "*graphia*" yang berarti penulisan atau tulisan. Kriptografi adalah suatu teknik penyandian pesan yang digunakan untuk memastikan bahwa pesan dapat dikirim dan diterima secara aman. Tujuan utama dari kriptografi adalah menjaga kerahasiaan data dan mencegah penyalahgunaan data oleh pihak yang tidak berwenang [3].

2.3. Route Cipher

Route Cipher merupakan sebuah varian cipher yang merupakan perluasan dari *rail fence cipher*. Algoritma ini memiliki kemiripan dengan *rail fence cipher* karena melibatkan penggunaan rute, namun dalam *Route Cipher*, rute yang digunakan dapat memiliki berbagai bentuk, termasuk rute yang melingkar ke dalam atau rute khusus. Biasanya, kunci yang digunakan dalam *Route Cipher* adalah cara untuk membaca pesan [4].

2.4. Variably Modified Permutation Composition

Algoritma Variably Modified Permutation Composition (VMPC) merupakan variasi dari algoritma RC4 yang diciptakan oleh Bartosz Zoltak pada tahun 2004. Algoritma ini adalah algoritma enkripsi yang beroperasi pada tingkat *byte*, di mana *keystream* dihasilkan oleh sebuah *generator keystream* dan digunakan untuk mengenkripsi teks dengan menggunakan kunci dan *plaintext* [5].

2.5. Citra Digital

Citra digital adalah gambar yang terdiri dari sejumlah titik yang disebut piksel. Piksel adalah elemen terkecil dari citra yang memiliki dua atribut, yaitu koordinat dan intensitas warna. Kuantisasi citra, atau berapa banyak nilai yang dapat digunakan untuk merepresentasikan warna dalam citra, tergantung pada kedalaman piksel. Kedalaman piksel ini ditentukan oleh jumlah bit yang digunakan untuk menggambarkan intensitas warna piksel tersebut. Semakin banyak bit yang digunakan, semakin besar kedalaman warna, dan semakin banyak variasi warna yang dapat direpresentasikan dalam citra digital [6].

3. METODOLOGI PENELITIAN

3.1. Pembelajaran Literatur

Pada tahap ini, dilakukan pengumpulan informasi yang diperlukan untuk proses perancangan aplikasi. Studi literatur ini mencakup pemahaman konsep-konsep yang relevan, termasuk kriptografi, serta pemahaman terhadap metode algoritma Route Cipher dan VMPC.

3.2. Pengumpulan Data

Pada tahap ini, data yang diperlukan untuk pengembangan aplikasi dikumpulkan. Data ini dapat diperoleh dari berbagai sumber, seperti artikel, jurnal, buku, dan sumber-sumber internet yang relevan dengan perancangan aplikasi.

3.3. Analisis dan Perancangan

Tahap perancangan sistem dalam sebuah penelitian merupakan langkah yang diambil setelah semua kebutuhan yang diperlukan untuk sistem yang akan dikembangkan terkumpul. Dalam konteks perancangan sistem aplikasi keamanan *file* BMP, sistem ini terdiri dari dua bagian utama, yaitu menu enkripsi dan menu dekripsi. Menu enkripsi digunakan untuk mengamankan *file* BMP dengan menggunakan algoritma *Route Cipher* dan VMPC. Pada menu ini, pengguna dapat memilih *file* BMP yang ingin diamankan dan

p-ISSN : 2087-0868 e-ISSN : 2598-9707

memasukkan kunci enskripsi. Sementara itu, menu dekripsi digunakan untuk mengembalikan *file* BMP yang telah diamankan ke bentuk aslinya. Pada menu ini, pengguna memasukkan *file* BMP hasil enkripsi dan kunci dekripsi yang sama yang digunakan pada proses enkripsi.

3.4. Implementasi dan Pengujian

Tahap terakhir adalah implementasi aplikasi berdasarkan analisis yang telah dilakukan sebelumnya. Tahap implementasi ini melibatkan penulisan kode program berdasarkan analisis dan perancangan yang telah dilakukan sebelumnya. Bahasa pemrograman yang digunakan untuk membangun aplikasi ini adalah C# (C *Sharp*), dan penggunaan aplikasi SharpDevelop dalam proses penulisan kode programnya. Setelah implementasi, langkah selanjutnya adalah melakukan pengujian aplikasi.

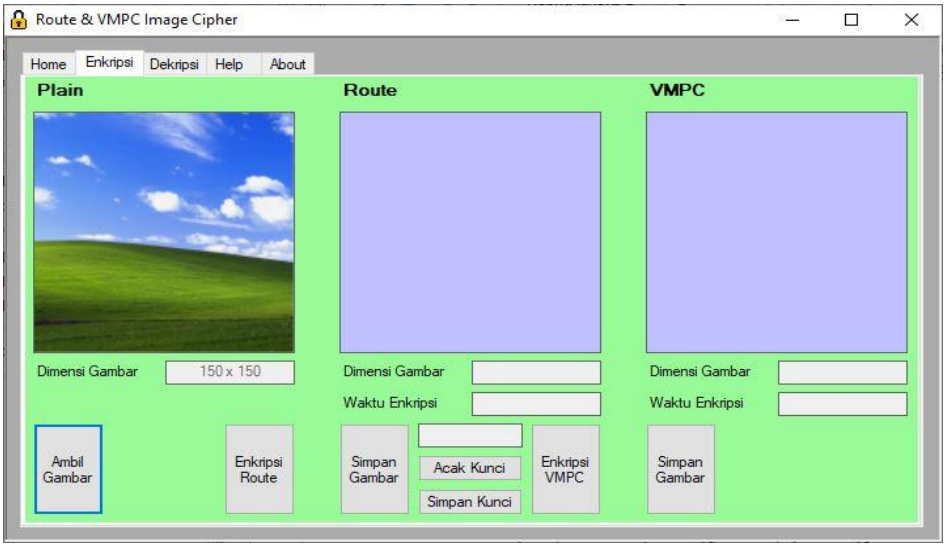
4. HASIL DAN PEMBAHASAN

Pengujian sistem adalah proses pengujian yang bertujuan untuk menentukan apakah sistem berhasil dalam menjalankan proses enkripsi dan dekripsi dengan menggunakan algoritma *Route Cipher* dan algoritma *Variably Modified Permutation Composition* (VMPC), dengan menerapkan teknik super enkripsi pada *file* citra berformat BMP. Citra yang akan diuji memiliki ukuran 150 x 150 piksel.

Gambar 1. Citra yang akan diuji

4.1. Pengujian Enkripsi Citra

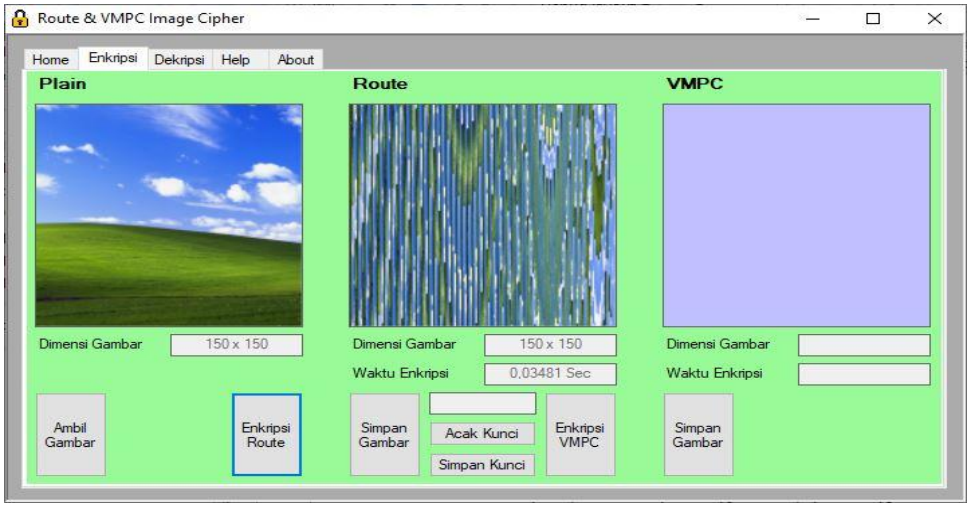
Pada sistem, pilih menu enkripsi lalu klik *button* ambil gambar untuk menginputgambar. Kotak dialog pencarian *file* akan tampil, lalu pilih *file* citra yang akan dienkripsi dimana pada kasus ini adalah *fle* citra *bitmap*. *File* citra yang sudah diambil akan ditampilkan beserta dimensi gambarnya.



Gambar 2. Proses input Plainimage

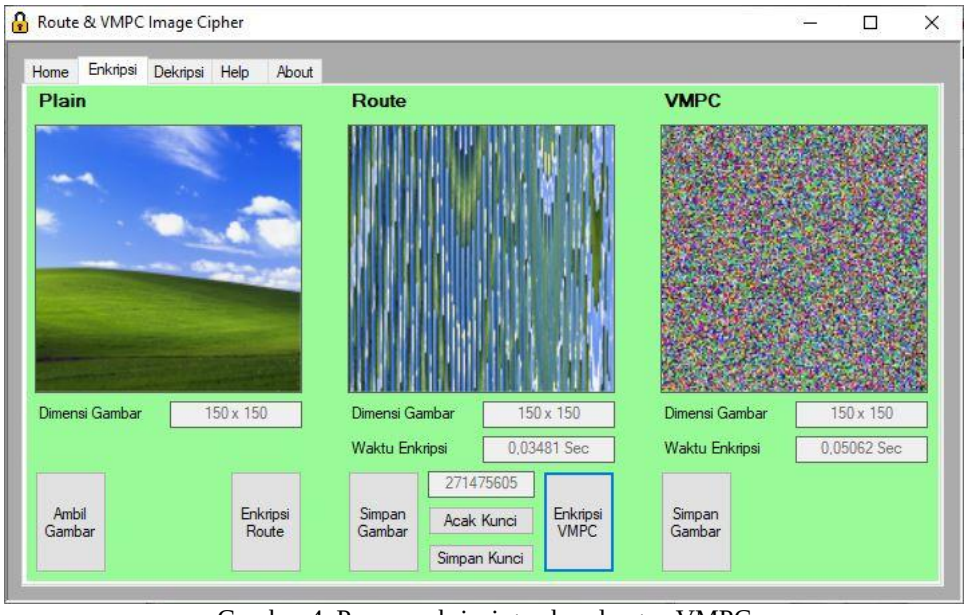
p-ISSN : 2087-0868 e-ISSN : 2598-9707

Setelah berhasil menginput *plainimage*, selanjutnya adalah melakukan proses enkripsi pertama. Klik *button* enkripsi *route* untuk mengenkripsi gambar dasar dengan *route cipher*. Maka gambar yang dienkripsi akan muncul beserta ukuran dimensi gambar dan waktu enkripsi gambar.



Gambar 3. Proses enkripsi gambar route cipher

Selanjutnya klik *button* acak kunci untuk memunculkan kunci VMPC dengan angka acak. Klik *button* simpan kunci maka akan muncul kotak dialog untuk menyimpan kunci yang diacak dengan ektensi VMPC. Ketika kunci VMPC sudah ada klik *button* enkripsi VMPC untuk mengenkripsi gambar route dengan algoritma VMPC. Gambar yang telah dienkripsi akan muncul beserta ukuran dimensi gambar dan waktu proses enkripsi gambar.



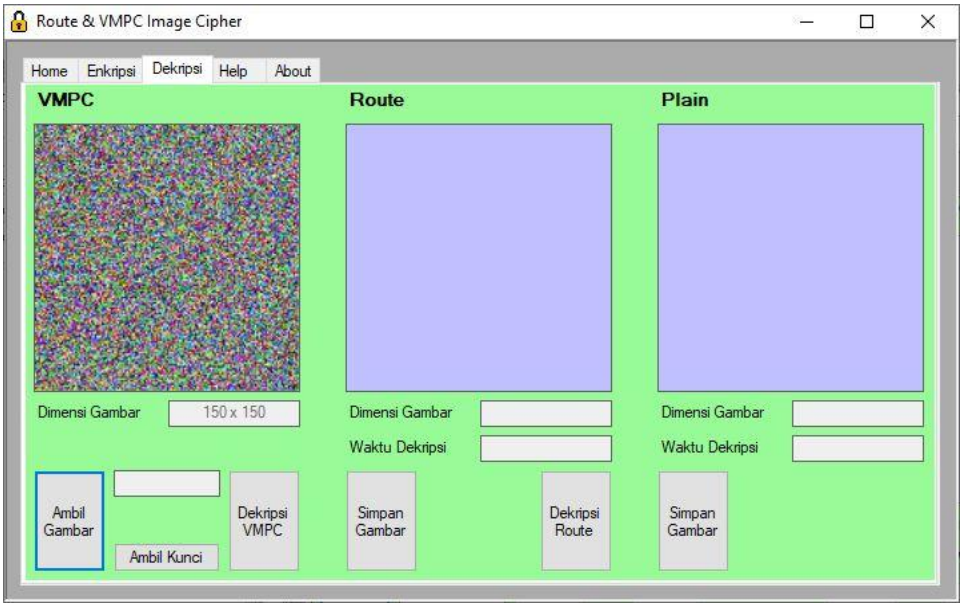
Gambar 4. Proses enkripsi gambar dengan VMPC

p-ISSN : 2087-0868 e-ISSN : 2598-9707

Setelah gambar berhasil dienkripsi. Klik *button* simpan gambar untuk menyimpan gambar yang telah dienkipsi dengan VMPC. Gambar akhir enkripsi beserta kunci VMPC yang telah disimpan, dapat dikirimkan ke orang yang dituju untuk melakukan dekripsi gambar.

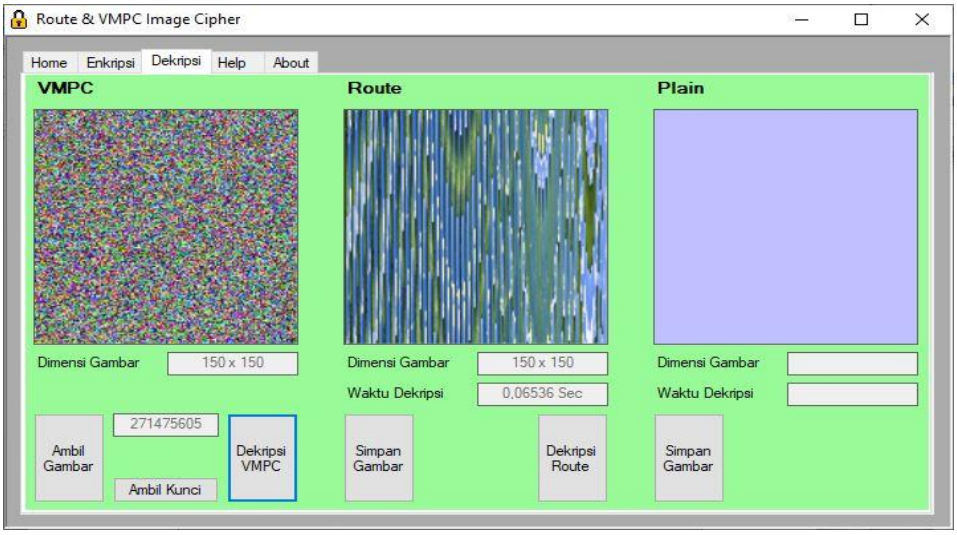
4.2. Pengujian Dekripsi Citra

Setelah pengirim memberikan gambar yang telah di enkripsi dan juga kunci VMPC, maka penerima dapat melakukan dekripsi untuk gambar yang dienkripsi. Pada sistem, pilih menu dekripsi lalu klik *button* ambil gambar untuk menginputgambar yang dienkripsi. Kotak dialog pencarian *file* akan tampil, lalu pilih *file* citra yang akan didekripsi dimana pada kasus ini adalah *fle* citra *bitmap*. *File* citra yang sudah diambil akan ditampilkan beserta dimensi gambarnya.



Gambar 5. Proses input gambar enkripsi VMPC

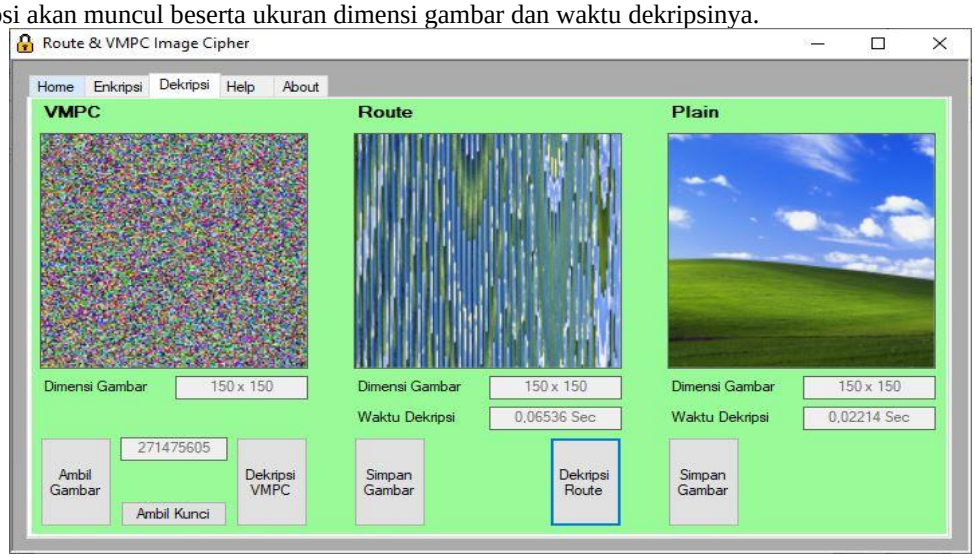
Selanjutnnya klik *button* ambil kunci, untuk memasukkan kunci VMPC yang telah diberikan oleh pengirim. Setelah kunci *VMPC* sudah ada, klik *button* dekripsi VMPC untuk mengdekripsi gambar dengan algoritma VMPC. Gambar yang telah di dekripsi akan muncul beserta ukuran dimensi gambar dan waktu dekripsinya.



Gambar 6. Proses dekripsi gambar dengan VMPC

p-ISSN : 2087-0868 e-ISSN : 2598-9707

Gambar yang telah didekripsi akan didekripsi lagi untuk mendapatkan gambar awal pengirim. Klik *button* dekripsi route untuk mengdekripsi gambar menggunakan algoritma *route cipher*. Gambar yang telah didekripsi akan muncul beserta ukuran dimensi gambar dan waktu dekripsinya.



Gambar 7. Proses dekripsi gambar dengan route cipher

Setelah proses dekripsi selesai, maka gambar awal dari pengirim dapat dilihat. Klik *button* simpan gambar untuk menyimpan *plainimage*.

4.3. Waktu Proses Enkripsi

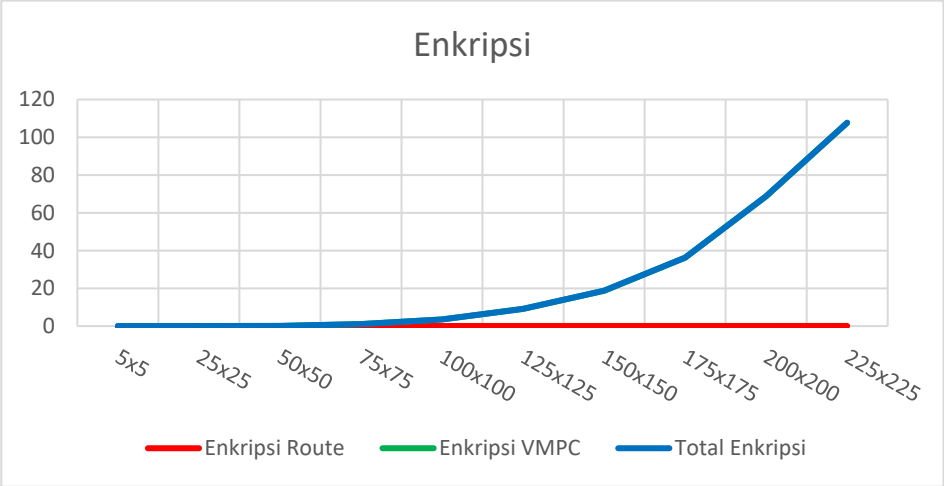
Pengujian waktu dan proses enkripsi ini menggunakan sampel sebanyak 10 gambar. Masing-masing gambar memiliki ukuran piksel yang berbeda-beda, yaitu 5x5, 25x25, 50x50, 75x75, 100x100, 125x125, 150x150, 175x175, 200x200 dan 225x225. Berikut hasil pengujian enkripsi berdasarkan ukuran citra.

Tabel 1. Perbandingan lama waktu proses enkripsi gambar

Resolusi Citra	Waktu Enkripsi Route Cipher	Waktu Enkripsi VMPC	Total Waktu Proses Enkripsi
5x5	0,00193 Sec	0,00234 Sec	0,00427 Sec
25x25	0,01130 Sec	0,01443 Sec	0,01556 Sec
50x50	0,00286 Sec	0,08014 Sec	0,08300 Sec
75x75	0,00733 Sec	1,01545 Sec	1,02278 Sec
100x100	0,01158 Sec	3,51677 Sec	3,52835 Sec
125x125	0,01562 Sec	9,09278 Sec	9,10840 Sec
150x150	0,02373 Sec	18,72778 Sec	18,75151 Sec
175x175	0,03334 Sec	36,24075 Sec	36,27409 Sec
200x200	0,03864 Sec	68,73594 Sec	68,77458 Sec
225x225	0,06762 Sec	107,66523 Sec	107,73285 Sec

Pada tabel diatas setiap resolusi gambar yang berbeda memiliki waktu proses enkripsi yang berbeda pula. Maka grafik perbandingan waktu dapat dilihat di grafik dibawah.

p-ISSN : 2087-0868 e-ISSN : 2598-9707



Gambar 8. Grafik waktu proses enkripsi gambar terhadap waktu

Pada gambar grafik diatas waktu proses enkripsi berdasarkan ukuran piksel diatas, dapat disimpulkan bahwa semakin besar ukuran piksel dari suatu citra maka semakin lama pula waktu yang digunakan untuk proses enkripsi.

4.4. Waktu Proses Dekripsi

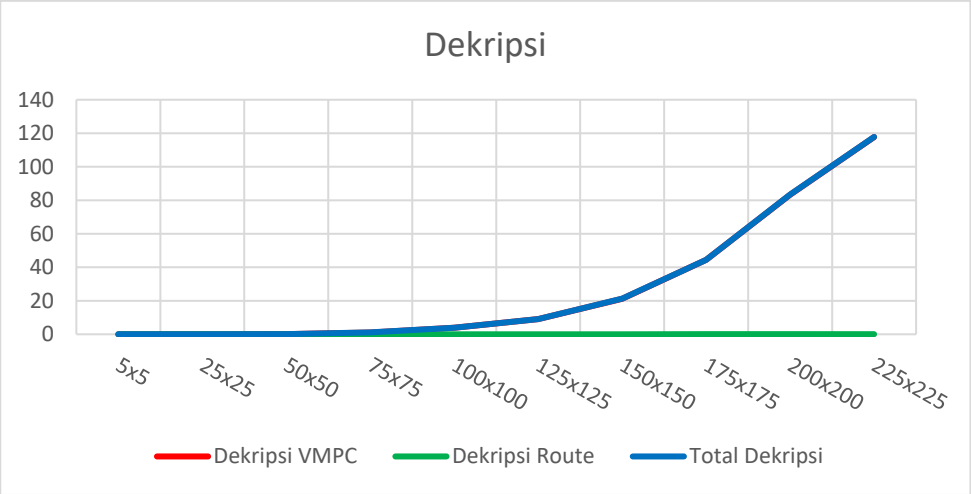
Pengujian waktu dan proses dekripsi ini menggunakan sampel sebanyak 10 gambar. Masing-masing gambar memiliki ukuran piksel yang berbeda-beda, yaitu 5x5, 25x25, 50x50, 75x75, 100x100, 125x125, 150x150, 175x175, 200x200 dan 225x225. Berikut hasil pengujian dekripsi berdasarkan ukuran citra.

Tabel 2. Perbandingan lama waktu proses dekripsi gambar

Resolusi Citra	Waktu Dekripsi VMPC	Waktu Dekripsi Route Cipher	Total Waktu Proses Dekripsi
5x5	0,00163 Sec	0,00036 Sec	0,00199 Sec
25x25	0,01516 Sec	0,00118 Sec	0,01634 Sec
50x50	0,07071 Sec	0,00407 Sec	0,07478 Sec
75x75	1,08970 Sec	0,00826 Sec	1,09796 Sec
100x100	3,90094 Sec	0,01631 Sec	3,91725 Sec
125x125	9,02185 Sec	0,02178 Sec	9,04363 Sec
150x150	21,23718 Sec	0,03383 Sec	21,27101 Sec
175x175	44,37304 Sec	0,04178 Sec	44,41482 Sec
200x200	83,33432 Sec	0,04947 Sec	83,38379 Sec
225x225	117,72471 Sec	0,05316 Sec	117,77787 Sec

Pada tabel diatas setiap resolusi gambar yang berbeda memiliki waktu proses dekripsi yang berbeda pula. Maka grafik perbandingan waktu dapat dilihat di grafik dibawah.

p-ISSN : 2087-0868 e-ISSN : 2598-9707



Gambar 9. Grafik waktu proses enkripsi gambar terhadap waktu

Pada gambar grafik diatas waktu proses dekripsi berdasarkan ukuran piksel diatas, dapat disimpulkan bahwa semakin besar ukuran piksel dari suatu citra maka semakin lama pula waktu yang digunakan untuk proses dekripsi.

4.5. Perbandingan Ukuran Gambar Setelah Diuji

Pengujian perbandingan ukuran gambar dilakukan untuk melihat apakah ada perubahan ukuran gambar awal setelah dienkripsi dan dekripsi. Berikut hasil perbandingan ukuran gambar setelah diuji.

Tabel 3. Perbandingan ukuran gambar setelah enkripsi dan dekripsi

Resolusi	Plainimage	Enkripsi Route	Enkripsi VMPC	Dekripsi VMPC	Dekripsi Route
5x5	134 B	155 B	223 B	155 B	152 B
25x25	3 KB	1 KB	3 KB	1 KB	1 KB
50x50	10 KB	2 KB	9 KB	2 KB	2 KB
75x75	23 KB	6 KB	20 KB	6 KB	5 KB
100x100	40 KB	27 KB	34 KB	27 KB	24 KB
125x125	62 KB	47 KB	53 KB	47 KB	43 KB
150x150	88 KB	63 KB	76 KB	63 KB	51 KB
175x175	120 KB	100 KB	103 KB	100 KB	93 KB
200x200	157 KB	117 KB	135 KB	117 KB	109 KB
225x225	198 KB	147 KB	170 KB	143 KB	124 KB

Dapat dilihat pada tabel di atas. Bahwa *plainimage* hasil proses enkripsi-dekripsi jika dibandingkan dengan plainimage awal sebelum dilakukannya proses enkripsi-dekripsi dari seluruh sampel, menunjukan ukuran yang berbeda-beda. Gambar awal akan memiliki ukuran yang lebih kecil setelah dienkripsi dan gambar nya akan mengecil lagi setelah di dekripsi

5. KESIMPULAN DAN SARAN

5.1. Kesimpulan

Metode super enkripsi yang melibatkan algoritma Route Cipher dan algoritma VMPC mampu memberikan keamanan pada file citra dengan ekstensi BMP. Teknik *super* enkripsi yang melibatkan algoritma *Route Cipher* dan algoritma VMPC untuk mengamankan file citra bitmap berhasil diimplementasikan. Hasilnya terlihat dari percobaan sistem, di mana citra yang telah dienkripsi dan didekripsi berhasil dikembalikan ke citra aslinya tanpa mengubah ukuran atau dimensi gambar. Citra *file bitmap* akan dienkripsi dengan algoritma *route cipher* dan algoritma VMPC menggunakan software Sharp Develop 5.1 dengan Bahasa C #.

p-ISSN : 2087-0868 e-ISSN : 2598-9707

5.2. Saran

Sistem yang telah dikembangkan dalam penelitian ini hanya dirancang untuk mengamankan file citra dengan ekstensi bitmap. Diharapkan pada penelitian selanjutnya, sistem dapat diperluas untuk mengamaVMPCnkan berbagai jenis file citra dengan ekstensi lainnya. Pada penelitian selanjutnya, diharapkan sistem yang dirancang agar dapat dijalan di platform berbasis web dan mobile. Diharapkan perbakaikan untuk sistem aplikasi yang dirancang mampu melakukan enkripsi dan dekripsi tanpa mengubah ukuran citra yang asli.

6. DAFTAR PUSTAKA

Referensi Cetak:

[1] Budi, Sarwo, et al. "Pengaman File Dokumen Menggunakan Kombinasi Metode Subtitusi dan Vigenere Cipher" *ILKOM Jurnal Ilmiah*, 11(3), 222-230, 2019.

[2] Bangun, M. S. "Implementasi Algoritma Route Cipher Dalam Pengamanan File Pdf. Building Informatics" *Technology and Science (BITS)*, 1(1), 1-6, 2019.

[3] Munawar, Zen, M Kom, & Novianti, Indah Putri. "Keamanan Jaringan Komputer Pada Era Big Data" *Jurnal Sistem Informasi-J-SIKA*, 2, 1–7, 2020.

[4] Yusfrizal, Y. "Rancang Bangun Aplikasi Kriptografi Pada Teks Menggunakan Metode Reverse Chiper Dan Rsa Berbasis Android" *JTIK (Jurnal Teknik Informatika Kaputama)*, *3*(2), 29–37, 2019.

[5] Irdayani, Irdayani. "Keamanan Citra Menggunakan Algoritma Route Cipher" *Majalah Ilmiah INTI*, 6(2), 246-249, 2019.

[6] Budiman, M. A., et al. "The Implementation Of RC4 + and Variably Modified Permutation Composition Algorithms In The Three-Pass Protocol Scheme For Data Security" *Journal Of Physics Conference Series*, 1235, 2019.

[7] Hardi, S. M., et al. "Comparative analysis run-length encoding algorithm and fibonacci code algorithm on image compression" *Journal of Physics Conference* Series, 1235, 2019.