

DIGITAL IMAGE ENCRYPTION BERBASIS ENKRIPSI ALGORITMA IMETRIS BEAUFORT CIPHER DAN AFFINE CIPHER

Agus Salim Pane^{1✉}, Arnes Sembiring², Arief Budiman³

^{1,3} Teknik Informatika, Universitas Harapan Medan

²Magister Informatika, Universitas Medan Area

Email ¹: agussalim19@gmail.com

²arnessembiring@staff.uma.ac.id

³arif@gmail.com

Abstrak

Penelitian ini bertujuan untuk mengamankan file citra digital dengan menerapkan kombinasi dua algoritma enkripsi simetris, yaitu Beaufort Cipher dan Affine Cipher. Proses enkripsi dilakukan dalam dua tahap, dimana citra digital dienkripsi menggunakan algoritma Beaufort Cipher, kemudian hasil enkripsi tersebut kembali dienkripsi menggunakan Affine Cipher. Hasil penelitian menunjukkan bahwa pengamanan citra digital berbasis enkripsi dengan menerapkan algoritma simetris Beaufort Cipher dan Affine Cipher dapat meningkatkan tingkat keamanan citra secara signifikan. Proses enkripsi ganda yang melibatkan kedua algoritma ini bisa menciptakan lapisan keamanan tambahan yang menyulitkan pihak yang tidak berwenang untuk melakukan dekripsi. Dengan menggabungkan kekuatan kedua algoritma tersebut, citra digital dapat terlindungi dari berbagai ancaman, termasuk akses ilegal dan pencurian data.

Kata Kunci : *Enkripsi, Dekripsi, Citra Digital, Beaufort Cipher, Afiine Cipher*

1. PENDAHULUAN

Keamanan data menjadi salah satu isu krusial dalam era digital saat ini. Dengan meningkatnya jumlah informasi yang disimpan dan dikirimkan secara digital, perlindungan terhadap data digital, termasuk citra, menjadi sangat penting. Citra digital sering digunakan dalam berbagai aplikasi seperti media sosial dan rentan terhadap ancaman seperti pencurian data, pemalsuan, dan akses tidak sah. Salah satu bidang kajian keamanan citra digital yang dapat digunakan sampai saat ini adalah kriptografi. Kriptografi merupakan salah satu teknik pengamanan data dengan melakukan proses penyandian atau enkripsi terhadap data yang ingin diamankan sehingga makna aslinya tidak lagi dapat dimengerti.

Beaufort Cipher dan *Affine Cipher* adalah dua jenis algoritma enkripsi simetris yang memiliki karakteristik unik. *Beaufort Cipher* adalah salah satu algoritma kriptografi klasik yang termasuk dalam kategori *cipher* substitusi. *Beaufort Cipher* dapat memberikan tingkat keamanan yang lebih baik dibandingkan dengan *cipher* substitusi sederhana, terutama jika kunci yang digunakan cukup panjang dan acak [1]. Algoritma *Beaufort Cipher* adalah teknik kriptografi yang efektif untuk mengamankan pesan, dengan cara yang mirip dengan *Vigenere Cipher* tetapi dengan cara pengulangan

yang berbeda [2]. Di sisi lain, *Affine Cipher* merupakan pengembangan dari algoritma *Caesar Cipher* [3] yang memanfaatkan operasi aritmatika sederhana untuk mengenkripsi data. Tingkat keamanan algoritma *Affine Cipher* relatif rendah apabila hanya diimplementasikan secara mandiri tanpa adanya kombinasi dengan metode lain [4]. Penggunaan algoritma kriptografi tunggal dalam metode enkripsi memiliki kelemahan tergantung dari jenis algoritma yang digunakan. Oleh karena itu, dengan menggabungkan kedua algoritma ini, maka diharapkan keamanan citra digital dapat ditingkatkan.

Penelitian sebelumnya telah menunjukkan potensi algoritma *Beaufort Cipher* dalam enkripsi data, termasuk citra digital. Diantara penelitian terdahulu yang signifikan dilakukan oleh Devia Pertiwi et al., (2023) mengkaji penggunaan algoritma *Beaufort Cipher* dan *ROT13* untuk pengamanan citra digital.

Hasil penelitian ini menunjukkan bahwa kombinasi kedua algoritma tersebut mampu meningkatkan tingkat keamanan citra digital, terutama dalam konteks transmisi data melalui jaringan yang rentan terhadap serangan. Penelitian ini memperkuat argumen bahwa algoritma klasik seperti *Beaufort Cipher* masih relevan dan efektif bila digunakan dalam kombinasi dengan metode kriptografi lain.

Dalam penelitian Ihsan & Doğan, (2023)

mengusulkan algoritma baru yang disebut *Improved Affine Algorithm* (IAA) untuk enkripsi citra warna. *Affine Cipher* biasanya digunakan untuk enkripsi teks biasa. Dalam penelitian ini, di kombinasikan dengan *Linear Feedback Shift Register* (LFSR), dan enkripsi XOR. Hasil penelitian menunjukkan bahwa algoritma enkripsi citra yang diusulkan adalah aman dan kuat, serta dapat mengungguli algoritma lainnya.

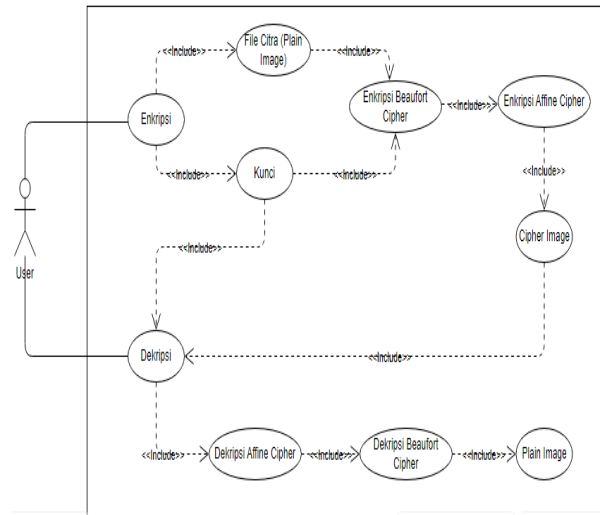
Berdasarkan hasil kajian dari penelitian-penelitian terdahulu tersebut, terlihat bahwa penggabungan antara algoritma klasik dalam kriptografi dapat meningkatkan keamanan data digital secara signifikan. Penelitian ini juga memberikan dasar yang kuat bagi penelitian yang akan dilakukan, dimana algoritma *Beaufort Cipher* dan *Affine Cipher* akan digabungkan untuk meningkatkan keamanan citra digital melalui proses enkripsi ganda. Pembaruan dalam penelitian ini terletak pada algoritma yang digunakan dalam teknik kriptografi, yaitu dengan menggabungkan algoritma simetris *Beaufort Cipher* dan *Affine Cipher* dalam mengamankan citra digital dari akses yang tidak sah.

2. METODE PENELITIAN

Analisis sistem bertujuan untuk menyelesaikan masalah yang ada terhadap suatu ruang lingkup (sistem) untuk mendapatkan kinerja utama yang terstruktur dari sistem yang dibangun. Analisis sistem dapat dilakukan dengan menguraikan fungsi dari sub sistem, bagaimana proses dari sub-sub sistem dan hasil dari proses sistem yang dibangun. Pada tahap analisis sebuah sistem ada beberapa proses yang dilakukan, yaitu analisis kebutuhan fungsional sistem dan analisis kebutuhan non-fungsional sistem.

Kebutuhan fungsional sistem membahas tentang fungsi-fungsi yang harus ada pada sistem yang dirancang. Sedangkan kebutuhan non-fungsional membahas tentang fungsi-fungsi yang berperan sebagai pelengkap sistem. Pemodelan sistem pada penelitian ini merupakan serangkaian proses merancang aplikasi enkripsi dengan perpaduan algoritma simetris *Beaufort Cipher* dan algoritma *Affine Cipher* sebelum masuk tahap pembangunan sistem atau *coding*. Pemodelan sistem yang digunakan adalah *Unified Modeling Language* (UML).

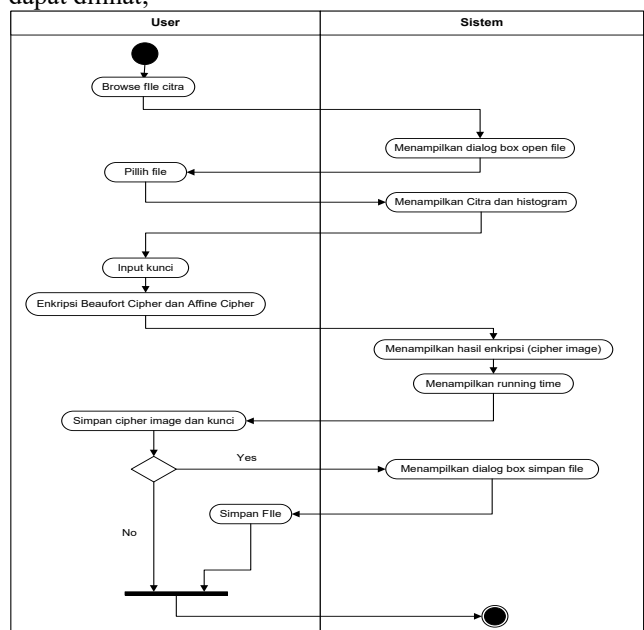
Use case diagram merupakan deskripsi fungsi dari sebuah sistem dari perspektif pengguna (*user*). *Use case diagram* bekerja dengan cara mendeskripsikan hubungan antara *user* dengan sistem melalui sebuah alur bagaimana sebuah sistem digunakan. Gambar 3.1 merupakan *use case diagram* sistem pada aplikasi enkripsi dengan perpaduan algoritma simetris *Beaufort Cipher* dan algoritma *Affine Cipher*.



Gambar 1 Use Case Diagram Sistem

Gambar 1 merupakan *use case diagram* dari aplikasi sistem dengan satu aktor (*user*), dimana *user* tersebut dapat melakukan proses enkripsi pada *file* citra dengan menggunakan perpaduan algoritma *Beaufort Cipher* dan algoritma *Affine Cipher*. *User* juga dapat melakukan dekripsi dengan menggunakan algoritma yang sama untuk mengembalikan pada citra asli.

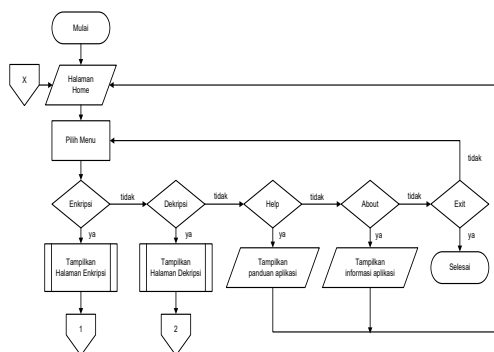
Penelitian ini *activity diagram* sistem terbagi menjadi dua, yaitu *activity diagram* enkripsi dan *activity diagram* dekripsi. Adapun *activity diagram* enkripsi dapat dilihat;



Gambar 2 Activity Diagram Enkripsi

Activity diagram enkripsi pada gambar 3.2 terdapat dua kotak dimana kotak paling kiri pada gambar menunjukkan aktivitas yang dilakukan oleh *user*, sedangkan kotak sebelah kanan adalah respon yang diberikan sistem terhadap aktivitas yang dilakukan *user*. Sedangkan *activity diagram* dekripsi akan menggambarkan bagaimana hubungan aliran kerja yang telah dijelaskan pada *use case* enkripsi.

Flowchart sistem pada penelitian ini digunakan untuk menunjukkan arus pekerjaan secara keseluruhan dari sistem enkripsi dengan perpaduan algoritma simetris *Beaufort Cipher* dan algoritma *Affine Cipher* yang akan dibangun. Bagan ini menjelaskan urutan dari prosedur-prosedur dengan simbol-simbol tertentu yang ada didalam sistem. *Flowchart* sistem dimulai dengan menampilkan halaman utama (*home*) seperti berikut ini:



Gambar 3 Flowchart Sistem

Flowchart sistem pada gambar 3 dimulai dengan menampilkan halaman utama (halaman *home*) pada saat aplikasi dijalankan. Pada halaman utama terdapat sejumlah menu yang dapat diakses oleh *user*, jika memilih menu enkripsi maka sistem akan menampilkan halaman enkripsi, menu dekripsi akan menampilkan halaman dekripsi, menu *help* akan menampilkan halaman *help*, menu *about* akan menampilkan halaman *about*, dan menu *exit* akan menutup aplikasi.

Sistem dibangun berbasis desktop dengan menggunakan bahasa pemrograman C# pada perangkat lunak *Microsoft Visual Studio*. *Interface* yang akan dirancang pada sistem ini memiliki lima bagian utama sesuai dengan fungsi masing-masing, yaitu halaman utama (*home*), halaman enkripsi, halaman dekripsi, halaman *help*, dan halaman *about*.

3. HASIL DAN PEMBAHASAN

Dalam penelitian ini bahasa pemrograman yang digunakan adalah *Visual C#* pada perangkat *Microsoft Visual Studio.NET*. Pembahasan yang terdapat pada bagian implementasi program mencakup ruang lingkup spesifikasi perangkat keras (*hardware*), perangkat lunak (*software*) dan hasil dari tampilan program ketika

sedang dijalankan.

Implementasi Sistem

Halaman Home

Halaman halaman *home* merupakan tampilan utama pada saat program aplikasi dijalankan. Pada halaman ini terdapat lima buah menu yang terletak pada *sidebar* sebelah atas yang dapat diakses oleh *user*, yaitu menu '*Home*', menu '*Enkripsi*', menu '*Dekripsi*', menu '*Help*', menu '*About*', dan menu '*Exit*' untuk menutup aplikasi. Gambar 4 merupakan tampilan dari hasil implementasi sistem.

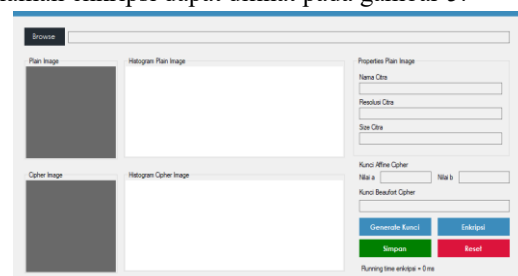


Gambar 4 Implementasi Halaman Home

Gambar 4 merupakan tampilan dari hasil implementasi pada halaman utama atau halaman *home*. Pada halaman ini terdapat lima buah menu yang dapat diakses oleh *user*, yaitu menu '*Home*', menu '*Enkripsi*' untuk menampilkan halaman proses enkripsi pada *file* citra, menu '*Dekripsi*' untuk menampilkan halaman proses dekripsi citra dari hasil enkripsi sebelumnya, menu '*Help*' untuk menampilkan halaman *help*, menu '*About*' untuk menampilkan halaman *about*, dan menu '*Exit*' untuk menutup aplikasi.

Halaman Enkripsi

Citra digital akan di enkripsi terlebih dahulu dengan menggunakan algoritma *Beaufort Cipher*, kemudian akan dienkripsi kembali dengan menggunakan algoritma *Affine Cipher*. Proses enkripsi dilakukan secara ganda yang bertujuan untuk meningkatkan tingkat keamanan pada citra digital. Adapun hasil implementasi dari halaman enkripsi dapat dilihat pada gambar 5.

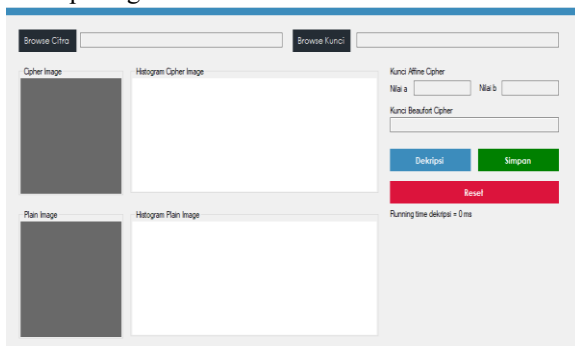


Gambar 5 Implementasi Halaman Enkripsi

Gambar 5 merupakan tampilan dari hasil implementasi sistem pada halaman enkripsi. Pada halaman ini akan dilakukan proses enkripsi secara ganda yang bertujuan untuk meningkatkan tingkat keamanan pada citra digital.

Halaman Dekripsi

Halaman dekripsi dapat diakses dengan memilih menu 'Dekripsi' yang terdapat pada *sidebar* halaman utama. Adapun hasil implementasi dari halaman enkripsi dapat dilihat pada gambar 6.

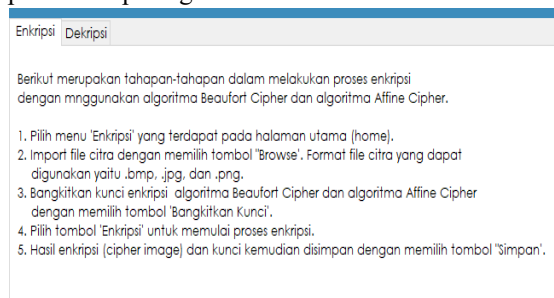


Gambar 6 Implementasi Halaman Dekripsi

Gambar 6 merupakan tampilan dari hasil implementasi sistem pada halaman dekripsi. Halaman dekripsi difungsikan untuk melakukan proses dekripsi untuk mendapatkan kembali citra asli (*plain image*) dari hasil enkripsi sebelumnya. Citra hasil enkripsi (*cipher image*) akan didekripsi terlebih dahulu dengan menggunakan algoritma *Affine Cipher*, lalu akan didekripsi lagi dengan algoritma *Beaufort Cipher* sehingga diperoleh kembali citra asli (*plain image*).

Halaman Help

Halaman *help* dapat diakses dengan memilih menu 'Help' yang terdapat pada *sidebar* halaman utama. Adapun hasil implementasi sistem dari halaman *help* dapat dilihat pada gambar 7



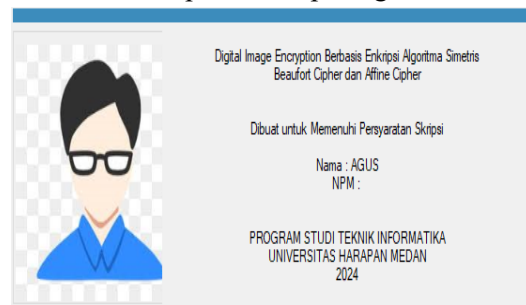
Gambar 7 Implementasi Halaman Help

Gambar 7 merupakan tampilan dari hasil implementasi sistem pada halaman *help*. Halaman *help* merupakan halaman yang berisikan bantuan atau

petunjuk untuk cara penggunaan aplikasi.

Halaman About

Halaman *about* dapat diakses dengan memilih menu 'About' yang terdapat pada *sidebar* halaman utama. Adapun hasil implementasi sistem dari halaman *about* dapat dilihat pada gambar 8



Gambar 8 Implementasi Halaman About

Gambar 8 merupakan tampilan dari hasil implementasi sistem pada halaman *help*. Halaman *about* merupakan halaman yang berisikan informasi mengenai aplikasi.

Hasil Pengujian Sistem

Pada hasil pengujian ini memberikan gambaran tentang variasi citra uji yang akan digunakan dalam penelitian, baik dari segi dimensi (*dimensions*) maupun ukuran (*size*) citra yang semakin besar, yang akan membantu dalam proses analisis kinerja algoritma enkripsi yang diuji. Citra yang akan diuji terdiri dari lima buah citra yang memiliki *dimensions* dan *size* yang bervariasi. Tujuannya adalah agar setiap citra yang diuji memiliki nilai *size* yang semakin besar.

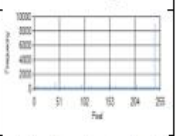
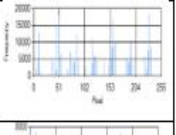
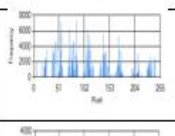
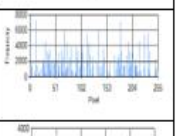
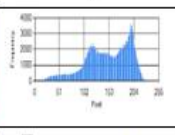
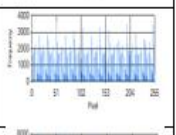
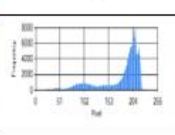
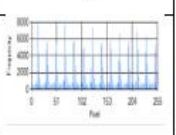
Adapun sampel data uji citra digital yang akan digunakan dalam penelitian ini dapat disajikan pada tabel 1.

Tabel 1 Sampel Citra Uji

No.	Sampel	Dimensions	Size
1.		158 x 158 piksel	73,4 KB
2.		461 x 461 piksel	623 KB
3.		500 x 480 piksel	703 KB
4.		497 x 497 piksel	724 KB
5.		512 x 512 piksel	768 KB

Tabel 1 menunjukkan lima sampel citra uji yang digunakan dalam penelitian untuk proses enkripsi dengan menggunakan kombinasi algoritma *Beaufort Cipher* dan *Affine Cipher*. Setiap sampel memiliki dimensi dan ukuran *file* yang bervariasi. Adapun hasil pengujian dapat disajikan pada tabel 2.

Tabel 2 Hasil Pengujian

No	Plain Image	Histogram Plain Image	Cipher Image	Histogram Plain Image
1.				
2.				
3.				
4.				
5.				

Tabel 4.2 menampilkan hasil pengujian yang dilakukan terhadap lima buah sampel citra uji. Visualisasi ini berguna untuk menjelaskan atau menganalisis efektivitas teknik enkripsi pada citra digital. Kunci yang digunakan untuk algoritma *Beaufort Cipher* yaitu 118 dan untuk kunci algoritma *Affine Cipher* terdiri dari dua nilai parameter, yaitu parameter *a* dengan nilai 95 dan parameter *b* dengan nilai 155. Setiap citra asli (*plain image*) disertai dengan histogram yang mewakili distribusi intensitas piksel. Citra yang dienkripsi (*cipher image*) muncul sebagai versi yang lebih acak dari citra asli (*plain image*). Histogram dari citra yang dienkripsi (*cipher image*) umumnya menunjukkan distribusi intensitas piksel yang lebih seragam dibandingkan dengan histogram dari citra asli (*plain image*). Ini menunjukkan efek dari menerapkan algoritma enkripsi pada berbagai jenis citra uji yang digunakan yang membuat gambar yang dienkripsi (*cipher image*) lebih sulit untuk dianalisis.

4. REFERENSI

- [1] E. Ndruru and T. Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital," *Bull. Inf. Technol.*, vol. 3, no. 2, pp. 149–154, 2022, doi: 10.47065/bit.v3i2.302.
- [2] I. Ilham and A. H. Hasugian, "Kombinasi Algoritma Vigenere dan Beaufort Cipher dalam Mengamankan Script Coding," *J. Teknol. Sist. Inf. dan Apl.*, vol. 6, no. 3, pp. 262–268, 2023, doi: 10.32493/jtsi.v6i3.30118.
- [3] A. Fitri, C. Sintya, F. A. Salsabilah, and ..., "Algoritma Affine Chiper pada Enkripsi dan Deskripsi untuk Keamanan Informasi Berbasis Android," *J. Pendidik. ...*, vol. 7, pp. 471–476, 2023, [Online]. Available: <https://garuda.kemdikbud.go.id/documents/detail/3300088>
- [4] R. Gusmana, H. Haryansyah, and F. Fitria, "Implementasi Algoritma Affine Cipher Dan Caesar Cipher Dalam Mengamankan Data Teks," *Sebatik*, vol. 26, no. 2, pp. 517–524, 2022, doi: 10.46984/sebatik.v26i2.2084.
- [5] A. Devia Pertiwi, A. Fauzi, and S. Syahputra, "Application Of Super Encryption Using Rot 13 Algorithm Method and Algorithm Beaufort Cipher For Image Security Digital," *J. Artif. Intell. Eng. Appl.*, vol. 2, no. 3, pp. 2808–4519, 2023, [Online]. Available: <https://ioinformatic.org/>
- [6] A. Ihsan and N. Doğan, "Improved affine encryption algorithm for color images using LFSR and XOR encryption," *Multimed. Tools Appl.*, vol. 82, no. 5, pp. 7621–7637, 2023, doi: 10.1007/s11042-022-13727-w.