Seminar Nasional Inovasi dan Pengembangan Teknologi Terapan
(SENOVTEK)
Cilacap, 20 Oktober 2022; pp:35-44

Optimalisasi *Vigenere* dan *Beaufort Cipher* Menggunakan Teknik *Fibonacci* Untuk Citra Digital

Optimization of Vigenere and Beaufort Ciphers Using Fibonacci Techniques for Digital Images

Danang Wahyu Utom[1*], Christy Atika Sari[2]
[1,2] Program Studi Teknik Informatika, Universitas Dian Nuswantoro
Email: [1]danang.wu@dsn.dinus.ac.id, [2]christy.atika.sari@dsn.dinus.ac.id

*Penulis korespondensi: **danang.wu@dsn.dinus.ac.id**

ABSTRAK

Salah satu Algoritma Kriptografi yang cukup popular adalah Algoritma Vigenere Cipher. Hingga sekarang, tindak kejahatan digital atau *cybercrime* yang ada di Indonesia terus meningkat, salah satu tindakan *cybercrime* yang sering terjadi dan cukup berbahaya adalah terjadinya kebocoran, manipulasi, hingga penyalahgunaan data digital. Tujuan dilakukannya penelitian ini adalah sebagai salah satu cara penanggulangan kasus kebocoran data dengan memanfaatkan Algoritma Vigenere dan Beaufort Cipher dan optimasi Teknik Fibonacci yang diterapkan pada data citra digital. Hasil dari penelitian ini didapatkan nilai entropy tertinggi yaitu sebesar 7,991. Pengujian yang dilakukan menggunakan UACI terhadap cipher RGB menghasilkan nilai persentasi sebesar 44% dan terhadap cipher CMY sebesar 44,3%. Sedangkan hasil pada nilai NPCR tertinggi didapatkan dari cipher citra RGB sebesar 99,8% dan cipher citra CMY sebesar 99,8%. Dengan perolehan nilai tersebut, dapat disimpulkan bahwa proses enkripsi yang dilakukan dapat berjalan dengan baik. Selain itu, citra yang dihasilkan tetap memiliki kualitas baik dengan perolehan nilai entropy yang mendekati 8. Kesimpulan lain, dengan nilai yang ditunjukkan oleh hasil NPCR, mengartikan bahwa cipher image memiliki kemiripan yang sangat rendah jika dibandingkan dengan citra aslinya. Untuk proses dekripsi, didapatkan kesimpulan bahwa prosesnya berjalan dengan baik, dibuktikan dengan nilai dechiper image yang sama persis dengan citra aslinya, ditunjukkan dari Nilai MSE, UACI, NPCR adalah 0, dan PSNR adalah inf.

Kata kunci: *Kriptografi, Vigenere Cipher, Beaufort Cipher, Fibonacci, Citra Digital.*

ABSTRACT

One of the most popular Cryptographic Algorithms is the Vigenere Cipher Algorithm. Until now, digital crime or cybercrime in Indonesia continues to increase, one of the cybercrime actions that often occurs and is quite dangerous is the occurrence of leakage, manipulation, and misuse of digital data. The purpose of this research is as a way to overcome data leakage cases by utilizing the Vigenere and Beaufort Cipher Algorithms and optimization of the Fibonacci Technique which is applied to digital image data. The results of this study obtained the highest entropy value of 7.991. Tests carried out using UACI on RGB ciphers yielded a percentage value of 44% and 44.3% for CMY ciphers. While the results for the highest NPCR value were obtained from RGB image ciphers of 99.8% and CMY image ciphers of 99.8%. With the acquisition of these values, it can be concluded that the encryption process carried out can run well. In addition, the resulting image still has good quality with the acquisition of an entropy value close to 8. Another conclusion, with the value shown by the NPCR results, means that the cipher image has a very low similarity when compared to the original image. For the decryption process, it was concluded that the process was going well, as evidenced by the value of the deciper image which was exactly the same as the original image, indicated by the MSE, UACI, NPCR is 0, and PSNR is inf values.

Keywords: *cryptography, vigenere cipher, beaufort cipher, fibonacci, digital image.*

1. PENDAHULUAN

Indonesia-security Incident Response Team on Internet Infrastructure (ID-SIRTII) pada tahun 2016 menginformasikan bahwa jumlah aktivitas yang ada di Indonesia mencapai hingga 135.672.988 aktivitas. Dari sejumlah tersebut, diinformasikan bahwa 47% merupakan aktivitas serangan *malware*, 44% berupa

aktivitas penipuan dunia digital [1], dan sisanya merupakan aktivitas pernyerangan situs web, pencurian dan manipulasi data [2]. Negara Indonesia pernah menduduki urutan ke-lima dalam hal aktivitas serangan *cyber*. Rentang tahun 2012 hingga 2015, tercatat terdapat sebanyak 36,6 juta aktivitas *cybercrime* yang terjadi di Indonesia [3], [4].

Algoritma Kriptografi merupakan ilmu yang mempelajari terkait penyandian data, dimana proses pengamanan data yang dilakukan oleh algoritma tersebut adalah dengan membuat pesan yang dikirim tidak dapat dibaca oleh penyerang karena pesan tersebut diacak sehingga menjadi pola kata atau kalimat yang tidak dapat terbaca [3], [5]–[7]. Perkembangan Kriptografi diketahui sudah dimulai sejak 4000 tahun yang lalu, dimana masih merupakan jaman mesir kuno pada saat itu. Ilmu Kriptografi cukup berperan penting pada saat perang dunia kedua, tokoh yang menggunakan ilmu kriptografi adalah Hitler. Hitler memanfaatkan system pengamanan kriptografi yang digunakan pada mesin enigma untuk mengirimkan pesan ke para tentaranya. Pada penelitian ini digunakan kombinasi antara dua algoritma kriptografi, yaitu Algoritma Vigenere [8], [9] dan Beaufort Cipher [10]–[13], dimana kedua algoritma tersebut merupakan salah satu dari beberapa cipher substitusi. Cara kerja cipher subtitusi adalah denngan mengganti setiap hurus yang ada pada pesan asli (*plaintext*) menjadi huruf acak yang ditentukan sesuai rumus sehingga menghasilkan pesan baru (*ciphertext*) yang tidak dapat dibaca karena hurufnya telah mengacak. Selain menggunakan Algoritma Kriptografi, digunakan pula Deret Fibonacci [4]. Deret Fibonacci merupakan perhitungan deret angka yang dimulai dengan dua angka awal, kemudian untuk mendapatkan angka selanjutnya dilakukan penjumlahan antara dua angka sebelumnya.

Muhammad Haidlar Al K., Bambang Hidayat, dan Nur Andini pada tahun 2018 [4] melakukan penelitian penggunaan Deret Fibonacci yang dikombinasikan dengan Metode LSB dan DCT yang diterapkan pada pengamanan data citra sebagai Tindakan pengamanan Steganografi ganda. Digunakan Teknik steganografi karena Muhammad Haidlar dkk ingin melakukan penyisipan pesan ke dalam gambar. Deret Fibonacci diterapkan pada saat proses penyisipan, yaitu dengan merubah pesan ke dalam bentuk kode biner. Selanjutnya dilakukan pemilihan koefisien DC untuk penyisipan. Kesimpulan yang didapat menunjukkan bahwa system yang diteliti dapat menghasilkan citra stego dengan nilai PSNR yang didapat lebih dari 40dB dan mendapatkan nilai BER = 0 ketika pesannya diekstraksi. Robbi Rahim dkk, pada tahun 2018 [8] melakukan penelitian terkait pengkombinasian dalam penggunaan Algoritma Vigenere Cipher dan One Time Pad untuk system pengamanan data. Dari mengkombinasi kedua algoritma tersebut, dihasilkan ciphertext yang berbeda dengan panjang yang ebrbeda pula. Semakin panjang pesan yang ingin dilakukan proses pengamanan, semakin terlindungi juga keamanannya dan ciphertext juga akan semakin sulit untuk diketahui isinya. Penggunaan kombinasi kedua algoritma tersebut dapat menghasilkan hasil yang lebih baik jika diterapkan pada Three-pass Protocol sehingga proses pendistribusian kunci tidak diperlukan dan dapat meminimalisir kejadian kunci yang digunakan dapat diketahui oleh pihak penyerang.

Mohamed Boussif, Noureddine Aloui, dan Adnene Cherif, pada tahun 2020 [14] melakukan penelitian terkait perlindungan kepada data citra DICOM dengan menggunakan algoritma enkripsi baru menggunakan Arnold Transform dan *vigenere cipher*. DICOM memiliki kepanjangan *digital imaging and communications in medicine*. Data citra yang digunakan dilakukan pre-proses dengan cara memisahkan data citra menjadi blok berukuran 16x16 piksel, dan dilakukan proses enkripsi sebanyak tiga kali. Tahap pertama adalah dengan mentransformasikan nilai k1, k2, k3, dan k4 yang sebelumnya berupa 16 piksel vector, menjadi matriks 16x16 piksel. Selanjutnya, dilakukan proses enkripsi *block-by-block* dengan menggunakan Algoritma Vigenere Cipher. Untuk setiap blok yang ada, digunakan Arnold Transform untuk memodifikasi kunci yang ada. Penelitian yang dilakukan menghasilkan kesimpulan bahwa proses pengamanan data yang dilakukan dapat lulus dari serangan sebagai bentuk pengujian. Waktu yang dibutuhkan untuk proses enkripsi juga lebih cepat dibandingkan dengan menggunakan algoritma enkripsi gambar yang lain.

Joni Saputra, M. Afriansyah, dan Herliana Rosika pada tahun 2021 [15] melakukan penelitian terkait proses penyandian pesan dengan mengimplementasikan Algoritma Current yang dikombinasikan dengan Deret Fibonacci dan Rumus Hexagonal. Pada penelitian ini digunakan sebanyak 26 key untuk melakukan proses enkripsi dan dekripsi. Proses pertama adalah dengan melakukan perhitungan Fibonacci dengan tujuan didapatkannya angka awal. Selanjutnya, dua digit terakhir dari deret Fibonacci yang telah dibuat diambil. Untuk angka-angka Fibonacci yang telah dibuat dan merepresentasikan setiap huruf plaintext, deret yang hanya memiliki satu angka disisipkan angka 1, 2, 3, dan 4. Setelah itu, dilakukan proses perhitungan Hexagonal. Kunci yang dimiliki Algoritma Current merupakan variable akhir yang dibutuhkan untuk menyempurnakan algoritma dari proses perhitungan menggunakan Deret Fibonacci dan Hexagonal. Pada penelitian ini, didapatkan kesimpulan bahwa kombinasi perhitungan menggunakan rumus matematika pada

Deret Fibonacci dan Hexagonal Geometri dalam proses pengamanan data dengan Algoritma *Current* dapat menghasilkan *ciphertext* baru. Niria Laila dan Anita Sindar RMS pada tahun 2018 [9] melakukan penelitian terkait pengimplementasian Algoritma Steganografi LSB untuk citra digital dengan menggunakan enkripsi dari algoritma vigenere cipher. Langkah pertama yang dilakukan pada penelitian ini adalah menginputkan pesan dan file kunci, yang kemudian file pesan dan kunci dikonversi menjadi bilangan decimal. Selanjutnya adalah menggunakan Algoritma vigenere cipher untuk merubah ciphertexr menjadi bilangan binary yang kemudia ciphertext tersebut disisipkan ke dalam media gambar x dengan menggunakan Algoritma LSB. Kesimpulan yang didapatkan dari penelitian ini adalah penggunaan kombinasi antara Algoritma Vigenere Cipher dan LSB dapat menjaga keamanan pesan dan dapat dilakukan dekripsi dan decoding disaat yang sama sehingga didapatkan Kembali pesan yang asli tanpa adanya kerusakan meskipun hanya sedikit.

Berdasarkan literatur dan permasalahan diatas, maka dalam penelitian ini telah dikembangkan optimasi vigenere cipher dan beaufort cipher melalui teknik fibonanci. Hasil eksperimen telah dipaparkan pada bab pembahasan dan telah menghasilkan nilai UACI NPCR cukup tinggi.

2. METODE PENELITIAN

2.1 Kriptografi

Kriptografi merupakan ilmu untuk mengamankan pesan supaya isi dari pesan tetap terjaga kerahasiaannya. Pengertian lain terkait kriptografi adalah bahwa kriptografi merupakan ilmu yang menerapkan teknik matematika untuk melakukan pengamanan data/pesan [16], [17]. Terdapat beberapa komponen yang dimiliki Kriptografi, yang pertama adalah Plaintext yang merupakan pesan asli yang belum dilakukan apa-apa. Kedua adalah *Ciphertext* yang merupakan hasil dari *plaintext* yang telah diolah menggunakan algoritma kriptografi. Ketiga adalah *Cryptography Key* atau biasa disebut dengan "kunci", dimana kegunaan kunci ini adalah sebagai salah satu komponen untuk dilakukannya proses enkripsi dan dekripsi. Terakhir adalah proses Enkripsi dan Dekripsi, dimana Enkripsi merupakan proses pengubahan plaintext menjadi ciphertext, dan Dekripsi merupakan proses pengembalikan ciphertext menjadi plaintext.

2.2 Vigenere Cipher

Vigenere Cipher termasuk ke dalam kriptografi klasik. Algoritma ini diperkenalkan pertama kali pada abah ke-16 oleh Blaise de Vigenere. Vigenere Cipher merupakan algoritma pengembangan dari Caesar Cipher. Caesar dan Vigenere Cipher sangat mirip satu sama lain, yang membedakan adalah pada Caesar cipher, proses enkripsi dilakukan dengan cara menggeser setiap huruf pada pesan satu kali ke kanan dengan menggunakan patokan hurufnya yang menjadi focus pergeseran. Jika huruf pada plaintext adalah "a", maka hurup akan berubah menjadi "b" pada ciphertextnya [3], [7], [18], [19]. Sedangkan Vigenere Cipher menggunakan huruf dari kunci untuk menggeser satu langkan pesan aslinya [9], [12]. Rumus Algoritma Vigenere Cipher ditunjukkan pada persamaan (1). Rumus matematika untuk proses Enkripsi dan Dekripsi ditunjukkan pada persamaan (2) dan persamaan (3).

$$C_i = E_k(P_i) = (P_i + K_i)\ mod\ 26 \quad (1)$$

Dimana C_i = ciphertext ke *I*, P_i = Plaiktext ke *I*, dan K_i= Kunci ke *i*.

$$C = (P + K)\ mod\ 26 \quad (2)$$

$$P = (C - K)\ mod\ 26 \quad (3)$$

Dimana *C* = Ciphertext, *P* = Plaintext dan *K* = Kunci.

2.3 Beaufort Cipher

Beaufort Cipher memiliki kunci dimana kunci tersebut merupakan urutan karakter K yang digunakan, sementara k1 didapatkan dari banyaknya pergeseran yang dimulai dari huruf ke-I yang mirip dengan Vigenere Cipher. Hal tersebut dapat diartikan dengan pembangkitan kunci harus berjumlah sama dengan karakter pada *plaintext* yang akan diproses [11], [12], [20]. Algoritma ini mengharuskan setiap karakter pada plaintextnya memiliki pasangan kunci, atau bisa disebut dengan proses secara stream. Hal tersebut membuat algoritma ini memiliki kemiripan yang sangat mirip dengan Vigenere Cipher [20]. Rumus Beaufort Cipher ditunjukkan pada persamaan (4) untuk enkripsi, dan persamaan (5) untuk dekripsi.

$$C_i = E_k(M_i) = (K_i - M_i)\ mod\ 26 \quad (4)$$

$$M_i = D_k(C_i) = (K_i - C_i)\ mod\ 26 \quad (5)$$

Dimana M_i = plaintext, C_i = ciphertext, E_k = fungsi enkripsi, Ki = key, D_k = fungsi dekripsi.

2.4 Deret Fibonacci

Deret Fibonacci dimulai dengan dua angka pertama, mulai angka ketia dan selanjutnya ditemukan dengan cara melakukan perhitungan penjumlahan dua angka sebelumnya [4], [15]. Jika dua angka pertama adalah 1 dan 5, maka deretnya akan menjadi seperti ini: 2, 5, 7, 12, 19, 31, …, dan seterusnya. Rumus matematika untuk deret Fibonacci ditunjukkan pada persamaan (6).

$$f(n) = f(n-1) + f(n-2) \quad (6)$$

2.5 Kebutuhan Data

Digunakan data citra berformat .bmp (bitmap) dimana gambar dengan format tersebut merupakan susunan dari banyak titik. Format .bmp dapat digunakan untuk gambar yang berukuran 1, 4, 8, 16, 24, dan 32 bitu pada setiap pikselnya. Data citra yang digunakan didapatkan dari *sipi.usc.edu/database* dan *http://www.imageprocessingplace.com/root_files_V3/image_databases.html*. Data yang digunakan ada sebanyak 17 data citra dengan masing-masing ukurannya adalah 256 x 256 piksel dan 512 x 512 piksel. Data citra dibagi menjadi dua bagian, yaitu sebanyak 2 data citra digunakan sebagai data kunci, dan 15 data citra sisanya digunakan sebagai citra asli. Citra asli memiliki format .tiff dan .jpg, maka dilakukan preproses dulu dengan merubah formatnya menjadi .bmp.

Gambar-1. Sampel beberapa data citra yang akan digunakan

3. HASIL DAN PEMBAHASAN

3.1 Pengolahan Data

Gambar 2 menampilkan data citra yang akan digunakan sebagai data kunci, sementara data citra sisanya yang berjumlah sebanyak 15 data digunakan sebagai data citra asli. Proses enkripsi citra dengan menggunakan Vigenere Cipher, Beaufort Cipher dan Teknik Fibonacci. Citra kunci 1 berupa citra_tujuh.bmp dan citra kunci 2 berupa citra_tiga.bmp. Citra kunci 1 akan digunakan sebagai kunci pada proses menggunakan Vigenere Cipher, sedangkan citra kedua akan digunakan pada Beaufort Cipher.


citra_tujuh.bmp citra_tiga.bmp

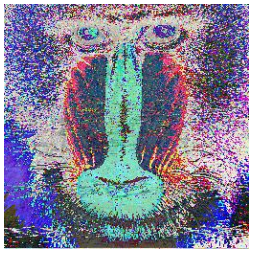
Gambar-2. Data citra yang digunakan sebagai kunci



citra_tujuh.bmp (citra kunci 1) citra_tiga.bmp (citra kunci 2) citra_satu.bmp (citra asli)

Gambar-3. Citra CMY

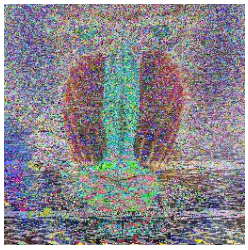
Tahap pertama, semua data citra termasuk citra kunci diubah yang pada awalnya berupa citra RGB menjadi citra CMY. Pada Gambar 3 ditunjukkan sampel dari penampilan perubahan citra RGB menjadi citra CMY. Setelahnya, data citra kunci 1 dan 2 baik RGB maupun CMY, dilakukan perubahan pada nilai pixelnya menjadi array 1 dimensi. Proses ini dilakukan untuk mempermudah proses perhitungan enkripsi dan dekripsi dan mempermudah proses pengacakan nilai piksel dengan memanfaatkan metode deret Fibonacci. Pada proses perhitungan Fibonacci, apabila panjang citra kunci melebihi bilangan Fibonacci yang digunakan, maka bilangan Fibonacci akan Kembali mulai dari 1. dan jika bilangan bilangan Fibonacci lebih panjang dari bilangan pada citra kunci, bilangan Fibonacci akan dimodulo dengan panjang kunci. Pada tahap kedua, dilakukan proses enkripsi menggunakan Algoritma Vigenere Cipher dan citra kunci 1. Citra asli RGB dan CMY dienkripsikan dengan citra kunci 1 yang sudah melalui proses pengacakan nilai piksel menggunakan Teknik Fibonacci. Citra asli dengan warna RGB akan dienkripsi dengan citra kunci RGB, begitu pula untuk citra CMY. Citra asli CMY akan dienkripsikan dengan citra kunci CMY. Gambar 4 menampilkan hasil perbedaan dari citra RGB dan CMY yang telah melalui proses enkripsi.

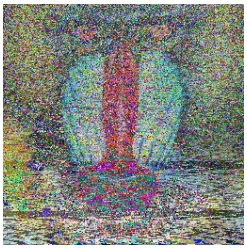


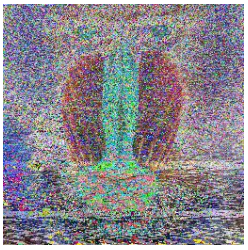

Citra RGB Citra CMY

Gambar-4. Tampilan perbedaan hasil enkripsi dari citra RGB dan CMY

Pada tahap ketiga, citra yang telah melalui proses enkripsi menggunakan Algoritma Vigenere Cipher dilanjutkan dengan proses enkripsi menggunakan Algoritma Beaufort Cipher. Citra kunci yang digunakan sama dengan citra kunci yang digunakan pada proses enkripsi menggunakan Algoritma Vigenere Cipher. Pada tahap ini, hasil citra yang telah melalui proses enkripsi tampak tidak cukup baik, bisa dibilang beberapa bagian tampak rusak. Hasil enkripsi citra CMY dikonversikan kembali ke RGB setelah melalui proses enkripsi dengan Beaufort Cipher. Gambar 5 menampilkan bagaimana hasil enkripsi dengan algoritma kedua.

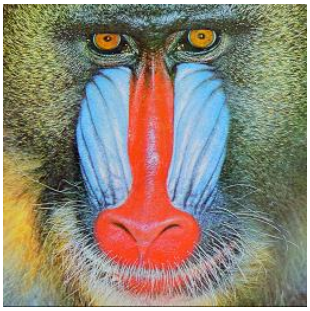

Citra RGB


Citra CMY

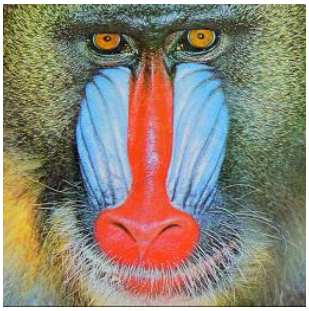

Citra CMY yang sudah dikonversi ke Citra RGB

Gambar-5. Tampilan perbedaan hasil enkripsi dari citra RGB dan CMY

Pada proses dekripsi, hasil citra yang dihasilkan cukup baik. Gambar 6 menampilkan tampilan citra yang telah melalui proses enkripsi, kembali menjadi citra asli setelah melalui proses dekripsi.


Citra RGB


Citra CMY


Citra CMY dalam RGB

Gambar-6. Hasil dekripsi citra RGB, CMY, dan CMY dalam RGB

3.2 Pengujian

Pengujian dilakukan supaya dapat diketahui kualitas dari citra hasil proses kriptografi. Dalam tahap pengujian, semua citra yang digunakan selama proses harus dalam keadaan berwarna RGB supaya hasil yang dihasilkan dapat dibandingkan. Termasuk citra CMY yang diubah terlebih dahulu menjadi citra RGB sebelum dilakukannya pengujian. Digunakan beberapa metode perhitungan untuk pengujian, yaitu Entropy, UACI, dan NPCR.

Tabel-1. Hasil pengujian Entropy

No.	Nama	Entropy Citra Asli	Entropy Cipher Vigenere + Beaufort + Fibonacci (RGB)	Entropy Cipher Vigenere + Beaufort + Fibonacci (CMY)
1	citra_satu.bmp	7.775	7.979	7.979
2	citra_dua.bmp	6.726	7.859	7.859
3	citra_empat.bmp	7.427	7.957	7.957
4	citra_lima.bmp	7.537	7.985	7.985
5	citra_enam.bmp	7.704	7.991	7.991
6	citra_delapan.bmp	6.446	7.856	7.856

Berdasarkan Tabel 1, ditunjukkan hasil perhitungan pengujian entropy pada ke-6 sampel data. Semakin dekat nilai entropy yang diperoleh dengan 8, dapat diartikan bahwa citra tersebut memiliki citra yang beragam dan derajat grayscale dari citra tersebut tersebar secara merata. Dari hasil yang ditampilkan Tabel 1, dapat disimpulkan bahwa kombinasi Vigenere dengan Beaufort Cipher dan Fibonacci menghasilkan cipher image yang bagus dengan nilai entropy tertinggi mencapai 7.991 pada citra_enam.bmp.

Tabel-2. Hasil pengujian UACI pada cipher image RGB dan CMY

No.	Nama	UACI Cipher Vigenere + Beaufort + Fibonacci (RGB)	UACI Cipher Vigenere + Beaufort + Fibonacci (CMY)
1	citra_satu.bmp	32,9%	32,9%
2	citra_dua.bmp	40,1%	39,8%
3	citra_empat.bmp	30,4%	30,4%
4	citra_lima.bmp	37,9%	37,9%
5	citra_enam.bmp	36,1%	36,2%
6	citra_delapan.bmp	44%	44,3%

Tabel-3. Hasil pengujian UACI pada plain image RGB dan CMY

No.	Nama	UACI Decipher Vigenere + Beaufort + Fibonacci (RGB)	UACI Decipher Vigenere + Beaufort + Fibonacci (CMY)
1	citra_satu.bmp	0%	0%
2	citra_dua.bmp	0%	0%
3	citra_empat.bmp	0%	0%
4	citra_lima.bmp	0%	0%
5	citra_enam.bmp	0%	0%
6	citra_delapan.bmp	0%	0%

Pada Tabel 3 menunjukkan perhitungan UACI dari cipher image. UACI digunakan untuk mengetahui perbedaan nilai pixel antara citra asli dengan citra terenkripsi. Nilai ideal untuk UACI adalah 33.46% [4]. Dari Tabel 3, terdapat sebanyak 4 cipher image dari 6 citra asli yang memenuhi kriteria nilai UACI yang ideal. Nilai UACI tertinggi dihasilkan oleh cipher image citra_delapan.bmp untuk enkripsi RGB sebesar 44% dan untuk enkripsi CMY sebesar 44.3%. Tabel 4 menampilkan hasil perhitungan UACI untuk decipher image. Untuk hasil dekripsi, semua *decipher image* menghasilkan nilai 0% berarti bahwa semua *decipher image* tidak mengalami perubahan nilai pixel sama sekali dari citra aslinya.

Tabel-4. Hasil pengujian NPCR pada cipher image RGB dan CMY

No.	Nama	NPCR Cipher Vigenere + Beaufort + Fibonacci (RGB)	NPCR Cipher Vigenere + Beaufort + Fibonacci (CMY)
1	citra_satu.bmp	99,7%	99,6%
2	citra_dua.bmp	99,8%	99,8%
3	citra_empat.bmp	99,6%	99,6%
4	citra_lima.bmp	99,7%	99,7%
5	citra_enam.bmp	99,7%	99,7%
6	citra_delapan.bmp	99,6%	99,6%

Tabel-5. Hasil pengujian NPCR pada plain image RGB dan CMY

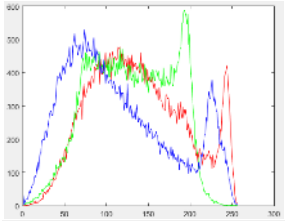
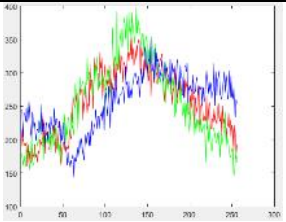
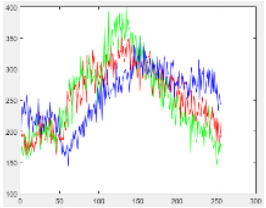
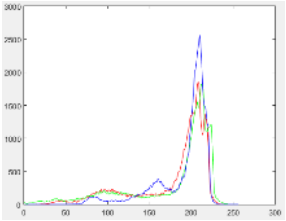
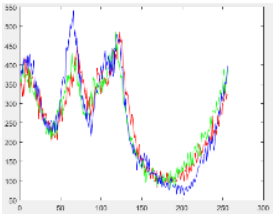
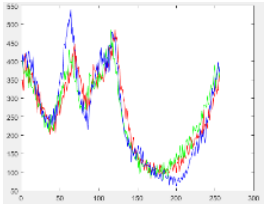
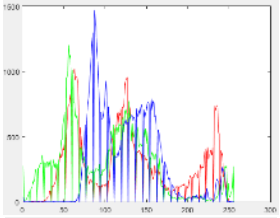
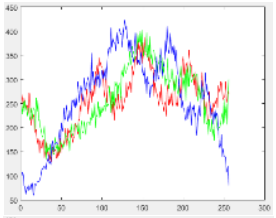
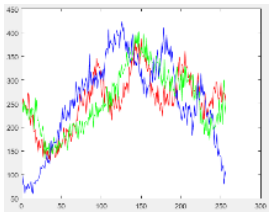
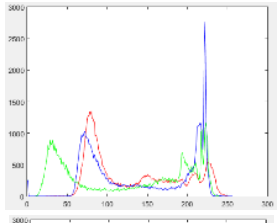
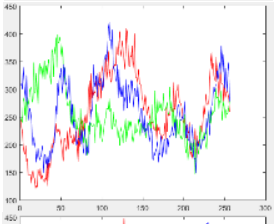
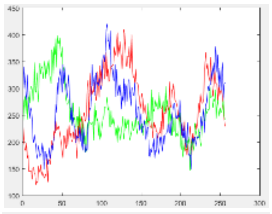
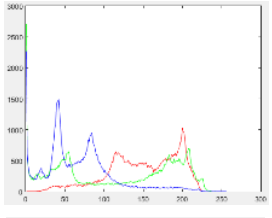
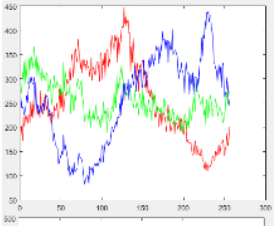
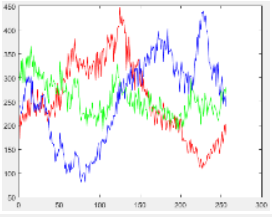
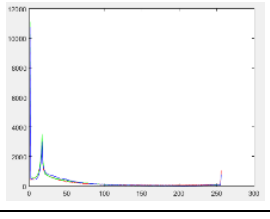
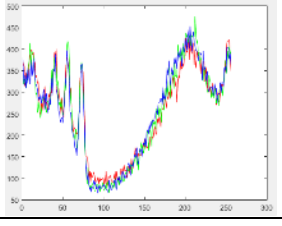
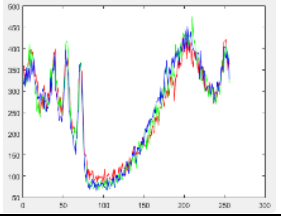
No.	Nama	NPCR Decipher Vigenere + Beaufort + Fibonacci (RGB)	NPCR Decipher Vigenere + Beaufort + Fibonacci (CMY)
1	citra_satu.bmp	0%	0%
2	citra_dua.bmp	0%	0%
3	citra_empat.bmp	0%	0%
4	citra_lima.bmp	0%	0%
5	citra_enam.bmp	0%	0%
6	citra_delapan.bmp	0%	0%

Tabel 4 dan 5 merupakan hasil perhitungan NPCR dari *cipher image* dan *decipher image*. Nilai NPCR yang ideal untuk cipher image adalah 99.61% [Muhammad haidlar 2018]. Dari tabel 5 cipher image RGB yang paling tinggi adalah 99.8% yaitu *cipher image* dari gambar citra_dua.bmp. Sedangkan untuk hasil enkripsi CMY, nilai NPCR tertinggi juga berada pada citra_dua.bmp dengan nilai 99.8 %. Untuk decipher image pada tabel 6 semua *decipher image* memiliki nilai 0% yang berarti bahwa proses dekripsi berhasil, karena *decipher image* sama persis dengan citra aslinya.

3.3. Histogram

Pada Tabel 6 menunjukkan histogram dari citra asli, *cipher image* kombinasi Vigenere Beaufort dan Fibonacci, cipher image Vigenere dan cipher image Beaufort. Semua *cipher image* mengalami perubahan histogram yang cukup terlihat jelas.

Tabel-6. Hasil pengujian histogram

No.	Nama	Histogram Citra Asli	Histogram Vigenere + Beaufort + Fibonacci (RGB)	Histogram Vigenere + Beaufort + Fibonacci (CMY)
1	citra_satu.bmp			
2	citra_dua.bmp			
3	citra_empat.bmp			
4	citra_lima.bmp			
5	citra_enam.bmp			
6	citra_delapan.bmp			

Untuk cipher image Vigenere menghasilkan histogram yang cukup berbeda dari citra aslinya, namun tidak terlalu signifikan perbedaannya. Untuk cipher image Beaufort menghasilkan histogram yang lebih berbeda lagi dari histogram citra asli. Dan untuk cipher image kombinasi Vigenere Beaufort dan Fibonacci menghasilkan histogram yang jauh lebih berbeda dari citra aslinya dibandingkan dengan histogram yang menggunakan 1 algoritma enkripsi saja. Untuk histogram cipher image RGB dan CMY yang sudah diubah ke RGB terlebih dahulu memiliki kemiripan namun tidak 100% mirip, ada beberapa perbedaan di histogramnya yang mungkin tidak terlalu terlihat jelas untuk mata manusia. Hal ini menunjukkan bahwa penyebaran nilai pixel pada cipher image kombinasi Vigenere, Beaufort dan Fibonacci jauh lebih merata dibandingkan dengan citra aslinya, sehingga dilihat dari histogramnya dapat disimpulkan bahwa proses enkripsi kombinasi Vigenere, Beaufort, dan Fibonacci dapat berjalan dengan baik.

4. KESIMPULAN

Kesimpulan yang didapatkan dari penelitian yang telah dilakukan yaitu kombinasi algoritma tersebut dapat digunakan untuk mengamankan suatu gambar dengan cukup baik. Hal ini dapat ditunjukkan dari hasil pengujian yang sudah dilakukan dalam penelitian ini. Untuk hasil histogramnya, cipher image yang dihasilkan memiliki histogram yang cukup lumayan berbeda dari histogram citra aslinya, yang menunjukkan bahwa nilai pixel pada *cipher image* terdistribusi dengan lebih merata. Untuk kualitas citra hasil enkripsi terlihat cukup acak dan lumayan tertutupi makna asli dari citra tersebut. Pengujian entropy yang telah dilakukan menghasilkan bahwa semua cipher image mengalami kenaikan entropy dari citra aslinya. Nilai entropy paling tinggi adalah 7.991 pada citra citra_enam.bmp. Evaluasi UACI menghasilkan nilai tertinggi sebesar 44% pada *cipher image accordion*.bmp, sedangkan nilai NPCR tertinggi pada *cipher image airplane*.bmp dengan nilai 99.792 %. Hasil evaluasi untuk proses dekripsinya dapat disimpulkan bahwa proses dekripsi dapat berjalan dengan baik dan benar. Dimana ditunjukkan dengan hasil perhitungan decipher image dibandingkan dengan citra asli dengan menggunakan evaluasi UACI dan NPCR = 0%. Artinya bahwa semua *decipher image* yang dihasilkan dari proses dekripsi sama persis dengan citra aslinya, atau decipher image tidak mengalami perubahan nilai pixel sama sekali dibandingkan dengan citra aslinya.

Saran untuk penelitian yang selanjutnya adalah dapat mengembangkan dan memodifikasi algoritma Vigenere Cipher, Beaufort Cipher dengan algoritma yang lain maupun dengan teknik optimasi yang lain. Kemudian dapat dikembangkan juga untuk mengenkripsi data yang lain, seperti file, dokumen teks, audio maupun video. Untuk pengembangan di citra digital dapat ditambahkan untuk format file yang lain (.jpg, .tiff, .png) dan ruang warna yang lain seperti CMYK, HSV, YCbCr maupun yang lainnya. Pada penelitian selanjutnya juga dapat ditambahkan tampilan GUI agar lebih memudahkan penggunakan aplikasi.

UCAPAN TERIMA KASIH

Terima kasih kepada LPPM Universitas Dian Nuswantoro atas Dana Hibah pada Penelitian Dasar Perguruan Tinggi Tahun Anggaran 2022.

DAFTAR PUSTAKA

[1] C. C. Ciptohartono and M. K. Dermawan, "Pencegahan Viktimisasi Pencurian Data Pribadi," *DEVIANCE: JURNAL KRIMINOLOGI*, vol. 3, no. 2, pp. 157–169, 2019.

[2] D. Z. Abidin, "KEJAHATAN DALAM TEKNOLOGI INFORMASI DAN KOMUNIKASI," *Jurnal Ilmiah Media Processor*, vol. 10, no. 2, 2015, [Online]. Available: www.usdoj.gov/criminal/cybercrimes

[3] E. Irfan Riaz Shohab Sandhu *et al.*, "An Enhanced Vigenere Cipher For Data Security," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 5, no. 03, 2016, [Online]. Available: www.ijstr.org

[4] M. H. al Kamali, B. Hidayat, and N. Andini, "STEGANOGRAFI GANDA PADA CITRA BERBASISKAN METODE LSB DAN DCT DENGAN MENGGUNAKAN DERET FIBONACCI," 2018.

[5] A. K. Sadasivuni, A. Chandrasekhar, D. Chaya, K. 2#, and S. A. Kumar, "SYMMETRIC KEY CRYPTOSYSTEM FOR MULTIPLE ENCRYPTIONS," *International Journal of Mathematics Trends and Technology*, [Online]. Available: http://www.ijmttjournal.org

[6] L. B. Handoko and A. D. Krismawan, "SUPER ENCRYPTION APPLICATION OF CRYPTOGRAPHY USING COMBINATION OF COLUMNAR TRANSPOSITION AND VIGENERE CIPHER," in *Seminar Nasional LPPM UMP*, 2020, pp. 534–539.

[7] F. Mushtaq Sher Ali and F. Hassan Sarhan, "Enhancing Security of Vigenere Cipher by Stream Cipher," *Int J Comput Appl*, vol. 100, no. 1, pp. 975–8887, 2014.

[8] D. Suprihant *et al.*, "Combination Vigenere Cipher and One Time Pad for Data Security," *International Journal of Engineering & Technology*, vol. 7, no. 2, pp. 92–94, 2018.

[9] N. Laila and A. S. Rms, "IMPLEMENTASI STEGANOGRAFI LSB DENGAN ENKRIPSI VIGENERE CIPHER PADA CITRA," *Computer Science Informatics Journal*, vol. 1, no. 2, 2018.

[10] C. Irawan, E. H. Rachmawanto, C. A. Sari, and C. A. Sugianto, "SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM," in *Semnas LPPM UMP*, 2020, pp. 556–563.

[11] M. Fadlan, Suprianto, Muhammad, and Y. Amaliah, "Double layered text encryption using beaufort and hill cipher techniques," Nov. 2020. doi: 10.1109/ICIC50835.2020.9288538.

[12] A. Rachmadsyah, A. Perdana, and A. Budiman, "Kombinasi Algoritma Beaufort Cipher Dan Vigenere Cipher Untuk Pengamanan Pesan Teks BerbasisMobile ApplicationAdryan," *Jurnal Minfo Polgan*, vol. 9, no. 2, pp. 12–17, 2020.

[13] E. Ndruru and T. Zebua, "Pembangkitan Kunci Beaufort Cipher Dengan Teknik Blum-blum Shub pada Pengamanan Citra Digital," *Bulletin of Information Technology (BIT)*, vol. 3, no. 2, pp. 149–154, 2022, doi: 10.47065/bit.v3i1.302.

[14] M. Boussif, N. Aloui, and A. Cherif, "Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher," *IET Image Process*, vol. 14, no. 6, pp. 1209–1216, May 2020, doi: 10.1049/iet-ipr.2019.0042.

[15] J. Saputra *et al.*, "Implementasi Algoritma Current Dengan Deret Fibonnaci Dan Ru-mus Hexagonal Untuk Menyandikan Pesan," *SIJ*, vol. 4, no. 2, pp. 134–138, 2021.

[16] E. H. Rachmawanto and C. A. Sari, "KEAMANAN FILE MENGGUNAKAN TEKNIK KRIPTOGRAFI SHIFT CIPHER," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.

[17] E. Rahmawan Pramudya and L. Budi Handoko, "KRIPTOGRAFI VIGENERE UNTUK MENGAMANKAN PESAN TEKS BERBASIS OCR (OPTICAL CHARACTER RECOGNITION)," in *Proceeding SENDIU*, 2021, pp. 460–467.

[18] L. Budi Handoko, "SEKURITI TEKS MENGGUNAKAN VIGENERE CIPHER DAN HILL CIPHER," *Bit (Fakultas Teknologi Informasi Universitas Budi Luhur)*, vol. 19, no. 1, pp. 37–47, 2022.

[19] B. B. Ahamed and M. Krishnamoorthy, "SMS Encryption and Decryption Using Modified Vigenere Cipher Algorithm," *Journal of the Operations Research Society of China*, Aug. 2020, doi: 10.1007/s40305-020-00320-x.

[20] E. Ndruru and T. Zebua, "Generate Beaufort Cipher Key Based on Blum-Blum Shub For Secure Digital Image," *Instal : Jurnal Komputer*, vol. 13, no. 1, 2021.