KOMBINASI CIPHER SUBTITUSI (BEAUFORT DAN VIGENERE) PADA CITRA DIGITAL

De Rosal Ignatius Moses Setiadi[1], Cahaya Jatmoko[2], Eko Hari Rachmawanto[3], Christy Atika Sari[4]
[1,2,3,4]Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro Semarang
Jl. Imam Bonjol 207 Semarang, 50131
Telp. (024) 3517261
E-mail: [1]moses@dsn.dinus.ac.id, [2]jatmoko14@gmail.com, [3]eko.hari@dsn.dinus.ac.id,
[4]atika.sari@dsn.dinus.ac.id

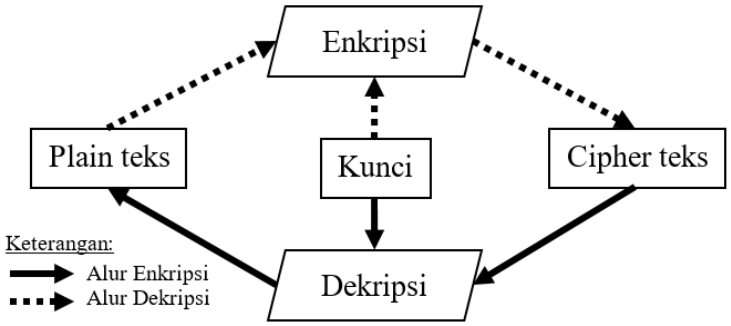
ABSTRAK

Riset tentang kriptografi pada citra terus berkembang. Banyak metode yang telah diterapkan pada kriptografi citra. Algoritma Vigenere merupakan algoritma yang cukup populer dan masih dikembangkan sampai saat ini. Vigenere memiliki kelebihan dalam komputasi yang cepat, dan kuat terhadap serangan. Beaufort cipher murupakan salah satu turunan dari algoritma Vigenere yang menggunakan operator pengurangan pada kunci. Penelitian ini mengusulkan kombinasi algoritma Beaufort dan Vigenere cipher dengan menggunakan dua kunci untuk meningkatkan keamanan. Metode diusulkan dalam penelitian ini diimplementasikan untuk enkripsi pada citra digital dan diukur dengan nilai MSE, PSNR dan analisis histogram. Hasil pengukuran dari kombinasi kedua metode ini didapatkan kualitas enkripsi yang lebih baik dibandingkan dengan metode Beaufort atau Vigenere saja.

Kata Kunci: Beaufort cipher, Vigenere cipher, Kriptografi, Enkripsi, Citra digital

1. PENDAHULUAN

Kriptografi merupakan ilmu yang digunakan untuk mengamankan data dengan cara menyandian data dengan algoritma tertentu [1]. Hal ini sudah banyak diterapkan dari zaman romari kuno hingga era digital saat ini. Kriptografi dapat digunakan untuk menyandikan banyak hal seperti pesan teks, citra, audio, video, kode file, alamat IP, dan sebagainya. Algoritma tentang kriptografi terus dikembangkan untuk meningkatkan keamananya. Citra digital merupakan salah satu media yang cukup populer diteliti pada bidang kriptografi [2]. Secara umum terdapat dua proses utama dalam kriptografi, yaitu enkripsi dan dekripsi. Enkripsi merupakan proses untuk mengubah bentuk pesan asli menjadi bentuk sandi, sedangkan proses dekripsi berarti sebaliknya [3]. Kedua proses tersebut tentunya membutuhkan minimal sebuah kunci. Gambaran umum kedua proses tersebut dapat dilihat pada gambar 1.



Gambar 1. Gambaran umum proses enkripsi dan dekripsi

Dalam ilmu kriptografi kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi sekaligus adalah kriptografi simetris [4]. Salah satu kriptografi simetris klasik yang populer adalah Vigenere *cipher*. Algoritma Vigenere juga merupakan algoritma kriptografi subtitusi. Kriptografi subtitusi merupakan teknik yang merubah *plain* teks dengan *cipher* teks berdasarkan kunci. Terdapat beberapa turunan dari Vigenere cipher, salah satunya Beaufort *cipher* [5]. Teknik kriptografi semacam ini memiliki kekuatan yang bergantung pada kunci. Enkripsi akan semakin kuat apabila kunci yang digunakan benar-benar acak, dengan ukuran yang sama dengan *plain* teks, dan hanya digunakan sekali saja [6]. Ide yang diusulkan pada penelitian ini adalah mengkombinasikan kedua algoritma dengan kunci ganda agar hasil enkripsi semakin sulit untuk didekripsi oleh pihak yang tidak berwenang.

2. METODE PENELITIAN

2.1 Kriptografi dengan Metode Subtitusi

Kriptografi merupakan teknik yang telah dilakukan untuk mengamanan pesan rahasia sejak jaman dahulu hingga saat ini [7]. Metode yang digunakan dari jaman dulu merupakan kriptografi klasik [6]. Kriptografi klasik umumnya menggunakan metode subtitusi dan metode transposisi. Metode subtitusi merupakan metode yang melakukan penyandian dengan merubah makna dan isi pesan berdasarkan kunci. Sedangkan metode transposisi

merupakan metode yang melakukan pengacakan isi pesan dengan menggunakan kunci. Umumnya kunci yang digunakan adalah kunci simetris. Yang dimaksud dengan kunci simetris adalah kunci yang digunakan untuk melakukan proses enkripsi dan dekripsi [4]. Hill, Caesar, Beaufort, dan Vigenere *cipher* merupakan jenis kriptografi subtitusi yang paling populer dan banyak digunakan. Pada metode subtitusi kunci akan memiliki peranan penting dalam kekuatan penyandian, semakin baik kunci maka semakin kuat hasil enkripsi. Penelitian ini sendiri akan melakukan penggabungan dua metode subtitusi, yaitu Beaufort dan Vigenere *cipher*.

2.2 Vigenere *Cipher*

Vigenere *cipher* adalah algoritma kriptografi yang sangat populer pada masanya. Vigenere *cipher* menerapkan metode subtitusi didalamnya. Kunci yang digunakan pada algoritma ini adalah kunci simetris [7]. Kunci ini sangat mempengaruhi kualitas enkripsi citra semakin acak kunci yang digunakan maka hasil enkripsi juga semakin kuat [1]. Kunci yang digunakan sebaiknya memiliki ukuran yang besarnya sama dengan *plain* teks serta hanya sekali digunakan. Akan tetapi hal ini berdampak negatif pada *plain* teks yang memiliki ukuran yang besar dan panjang karena ukuran kunci yang digunakan juga harus besar [8]. Apabila kunci tersebut benar-benar acak, sekali digunakan, memiliki ukuran yang sama dengan plain teks, serta hanya ada dua salinan kunci untuk pengirim dan penerima maka algoritma ini akan sangat sulit dipecahkan [9]. Vigenere *cipher* menggunakan operasi XOR atau modulo dalam melakukan operasi enkripsi dan dekripsi [10]. Rumus Vigenere *cipher* untuk proses enkripsi dan dekripsi dapat dihitung dengan formula (1) dan formula (2).

$$Cc = (Pc + k)\ mod\ 256 \quad (1)$$

$$Pc = (Cc - k)\ mod\ 256 \quad (2)$$

dimana:

Cc = Citra cipher,
Pc = Citra plain,
k = kunci, nilai kunci dalam range 0-255 atau modulo 256

256 dipilih sebagai konstanta pembagi karena citra yang digunakan adalah citra keabuat yang memiliki nilai piksel antara 0-255

2.3 Beaufort *Cipher*

Beaufort *cipher* merupakan metode kriptografi subtitusi turunan dari Vigenere *cipher* [5] yang menggunakan teknik substraksi [11]. Rumus yang digunakan pada Beaufort *cipher* sangat identik dengan Vigenere *cipher*. Kesamaan dari kedua teknik ini adalah penggunaan fungsi modulo atau sisa hasil bagi maupun jenis kunci yang yang digunakan. Perbedaan dari kedua metode ini adalah peranan kunci, dalam Vigenere *cipher* kunci digunakan sebagai penambah plain teks dan pengurang cipher teks. Sedangkan dalam formula yang digunakan Beaufort cipher, kunci digunakan untuk dikurangkan dengan plain teks maupun cipher teks. Untuk lebih jelas dapat diperhatikan rumus enkripsi dan dekripsi Beaufort cipher pada formula (3) dan formula (4).

$$Cc = (k - Pc)\ mod\ 256 \quad (3)$$

$$Pc = (k - Cc)\ mod\ 256 \quad (4)$$

2.4 Metode yang Diusulkan

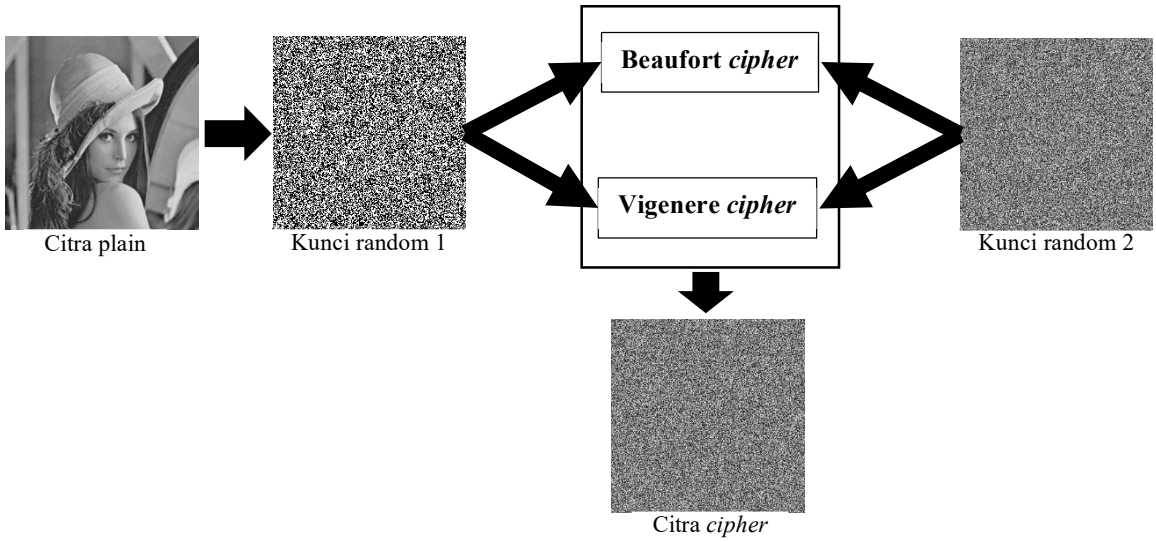
Metode yang diusulkan pada penelitian ini adalah mengkombinasikan Beaufort *cipher* dan Vigenere *cipher* dengan kunci acak. Agar kedua metode dapat dikombinasikan ditambahkan kunci acak tambahan sebagai penentu algoritma yang digunakan. Ukuran kedua kunci sama dengan ukuran citra, perbedaannya yaitu kunci pertama menggunakan kedalaman 8 bit sedangkan kunci tambahan menggunakan kedalaman 1 bit. Kedua kunci digunakan pada proses enkripsi maupun dekripsi. Untuk lebih jelasnya dapat dilihan pada sub bagian 2.4.1 dan 2.4.2.

2.4.1 Enkripsi yang diusulkan

Berikut adalah langkah-langkah proses enkripsi yang diusulkan:

1. Baca citra plain dengan ukuran $m * n$, lalu simpan pada pada variable Pc
2. Buat kunci acak $k1$ yang terdiri bilangan biner dengan ukuran $m * n$.
3. Buat kunci acak lain $k2$ yang terdiri dari bilangan bulat yang merupakan sisa hasil bagi 256.
4. Lakukan enkrispsi berdasarkan kunci acak $k1$, bila $k1_{mn}$ bernilai 1 lakukan Beaufort cipher pada piksel citra plain Pc_{mn}, bila $k1_{mn}$ bernilai 0 lakukan Vigenere *cipher* pada piksel citra *plain* Pc_{mn}.
5. Dapatkan citra *cipher* Cc.

Untuk memberi gambaran lebih jelas dapat melihat gambar 2.



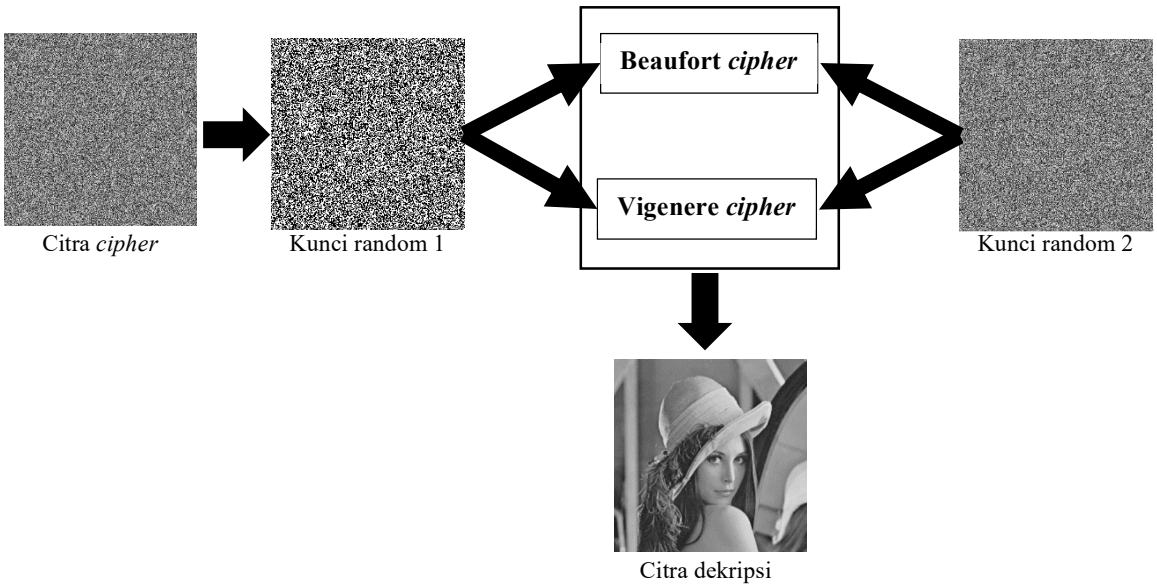
Gambar 2. Proses enkripsi yang diusulkan

2.4.2 Dekripsi yang diusulkan

Berikut adalah langkah-langkah proses enkripsi yang diusulkan:

1. Baca citra *cipher* dengan ukuran $m * n$, lalu simpan pada pada variable Cc
2. Baca kunci acak $k1$ dan kunci acak lain $k2$
3. Lakukan dekripsi berdasarkan kunci acak $k1$, bila $k1_{mn}$ bernilai 1 lakukan Beaufort *cipher* pada piksel citra *cipher* Cc_{mn}, bila $k1_{mn}$ bernilai 0 lakukan Vigenere *cipher* pada piksel citra *cipher* Cc_{mn}.
4. Dapatkan citra dekripsi Dc.

Untuk memberi gambaran lebih jelas dapat melihat gambar 3.



Gambar 3. Proses enkripsi yang diusulkan

2.5 Pengukuran Kualitas Kriptografi pada Citra

Pada penelitian ini akan digunakan tiga macam alat ukur untuk mengetahui kualitas enkripsi yang digunakan, yaitu, *Peak Signal to Noise Ratio* (PSNR), *Mean Square Error* (MSE) dan analisis histogram [12]. PSNR merupakan perhitungan nilai terbesar sinyal derau yang mempengaruhi perubahan citra, semakin tinggi nilai PSNR maka hasil enkripsi semakin mirip dengan citra asli atau *plain*. Semakin rendah nilai PSNR maka kualitas enkripsi semakin baik. Sedangkan MSE merupakan nilai kuadrat kesalahan pada sebuah citra, nilai MSE didapatkan dengan mambandingkan citra asli atau *plain* dengan citra hasil enkripsi. Semakin besar nilai MSE maka kualitas enkripsi semakin baik. Untuk melakukan kalkulasi nilai MSE dan PSNR dapat menggunakan formula (5) dan formula (6).

$$\text{MSE} = \frac{1}{\text{MN}} \sum_{\text{X}=1}^{\text{M}} \sum_{\text{y}=1}^{\text{N}} (\text{P}_{\text{xy}} - \text{C}_{\text{xy}})^2 \quad (5)$$

$$\text{PSNR} = 10\,\text{Log}_{10}\left(\frac{255^2}{\text{MSE}}\right) \quad (6)$$

Dimana:
x, y = koordinat citra
M,N = dimensi citra
P = Citra *plain* atau asli
C = Citra *chiper* atau hasil enkripsi

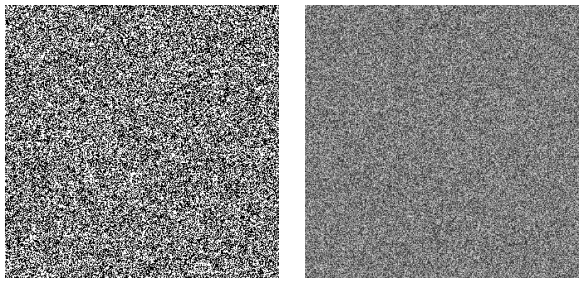
Sedangkan analisis histogram dilakukan untuk mengetahui distribusi nilai piksel citra hasil enkripsi, apabila histrogram sangat berbeda dengan histogram citra asli maka mengindikasikan bahwa hasil enkripsi baik. Faktor lain yang perlu diamati adalah distribusi nilai piksel dalam histogram, apabila distribusi nilai piksel semakin seragam maka hasil enkripsi semakin baik.

3. HASIL EKSPERIMEN

Dataset citra yang digunakan pada penelitian ini diambil dari [13]. Jenis citra yang digunakan adalah citra tes standar dengan tipe keabuan atau dengan kedalaman 8 bit. Seluruh citra berukuran 512*512. Seluruh citra yang digunakan berekstansi tif, dan tidak dilakukan modifikasi atau prapengolahan terlebih dahulu sebelum diproses. Citra tersebut dipilih agar penelitian ini lebih mudah untuk dilakukan komparasi dengan penelitian sebelum maupun penelitian berikutnya. Gambar 4 menampilkan citra yang digunakan pada penelitian ini.

cameraman.tif lena_gray_512.tif mandril_gray.tif woman_darkhair.tif

Gambar 4. Dataset Citra yang digunakan



Kunci acak biner Kunci acak keabuan

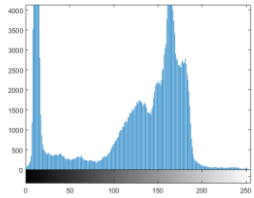
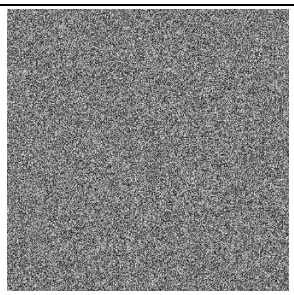
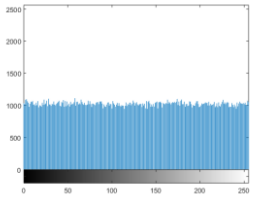
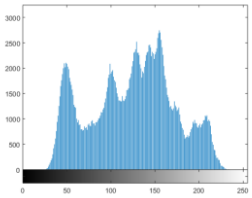
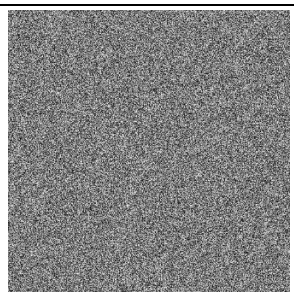
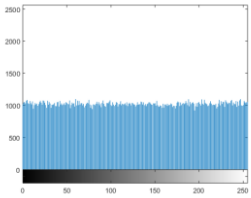
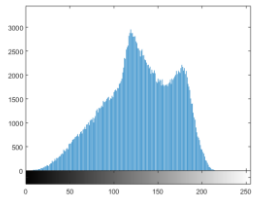
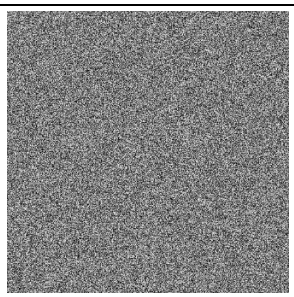
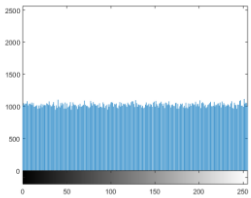
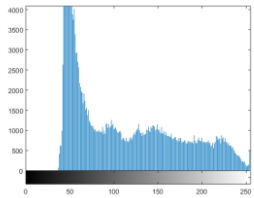
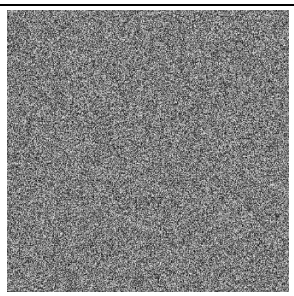
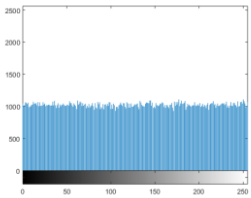
Gambar 5. Contoh kunci acak yang digunakan

Selanjutnya dilakukan proses enkripsi dengan metode yang diusulkan. Sebelum dilakukan enkripsi dibuat dua kunci acak dengan pembangkit fungsi acak. Gambar 5 diatas menunjukan contoh kunci acak yang digunakan. Kunci pertama merupakan kunci acak dengan nilai biner dan kunci kedua adalah kunci acak dengan nilai *range* nilai 0-255, dimana kedua kunci memiliki ukuran yang sama dengan ukuran citra plain. Tabel 1 menunjukan nilai PSNR dan MSE hasil enkripsi berikut dengan komparasi dengan metode Vigenere dan Beaufort saja. Sedangkan Tabel 2 menunjukan hasil evaluasi analisis histogram.

Tabel 1. Evaluasi Hasil Enkripsi Citra dengan MSE dan PSNR

Nama Citra	*PSNR (dB)*			*MSE*		
	Metode usulan	*Beaufort*	*Vigenere*	*Metode usulan*	*Beaufort*	*Vigenere*
cameraman.tif	8.4028	8.4146	8.3987	9392.9383	9367.4133	9401.8592
lena_gray_512.tif	9.2110	9.2230	9.2163	7798.0379	7776.4607	7788.4492
mandril_gray.tif	9.6277	9.6357	9.6309	7084.4516	7071.5059	7079.2392
woman_darkhair.tif	8.2715	8.2868	8.2852	9681.2869	9647.2223	9650.7275

Tabel 2. Evaluasi Hasil Enkripsi Citra dengan Analisis Histogram

Nama Citra	*Histogram Asli*	*Hasil Enkripsi*	*Histogram hasil enkripsi*
cameraman.tif			
lena_gray_512.tif			
mandril_gray.tif			
woman_darkhair.tif			

Dapat diamati pada tabel 1 tampak bahwa nilai PSNR dan MSE pada metode yang diusulkan tampak lebih unggul, walaupun selisih nilai yang didapatkan tidak cukup signifikan. Secara teori pun seharusnya metode yang diusulkan akan lebih rumit untuk didekripsi karena menerapkan kombinasi dua metode. Hasil enkripsi berikut histogram citra juga tampak distribusi nilai piksel yang seragam dan relatif rata dan dibandingkan citra asli bentuk juga sangat berbeda sekali. Selanjutnya juga dilakukan uji coba metode dekripsi, yang ditunjukan pada tabel 3 dibawah ini.

Tabel 3. Evaluasi Hasil Dekripsi Citra dengan MSE dan PSNR

Nama Citra	*PSNR (dB)*			*MSE*		
	Metode usulan	*Beaufort*	*Vigenere*	*Metode usulan*	*Beaufort*	*Vigenere*
cameraman.tif	inf	inf	inf	0	0	0
lena_gray_512.tif	inf	inf	inf	0	0	0
mandril_gray.tif	inf	inf	inf	0	0	0
woman_darkhair.tif	inf	inf	inf	0	0	0

Hasil dekripsi citra yang ditunjukan pada tabel 3 membuktikan bahwa metode yang diusulkan dapat melakukan dekripsi dengan sempurna. Hal ini ditunjukan dengan nilai PSNR yang inf (*infinity*/ tak terhingga).

Nilai PSNR inf berarti citra dekripsi sama persis dengan citra asli. Begitu juga dengan nilai 0 pada MSE juga menunjukan tidak ada nilai piksel yang salah atau berubah jika dibandingkan dengan citra asli.

4. KESIMPULAN

Penelitian ini mengusulkan kombinasi algoritma Vigenere dan Beaufort *cipher* yang diterapkan pada citra digital. Citra yang diujikan adalah citra keabuan dengan ukuran 512*512 dengan format ekstensi tif. Berdasarkan hasil percobaan yang dilakukan mennjukan bahwa kombinasi kedua algoritma berhasil diterapkan untuk enkripsi citra. Kualitas enkripsi juga lebih unggul dibandingkan dengan metode sebelumnya, dimana pengukuran kualitas menggunakan PSNR dan MSE. Hasil analisis histogram juga menunjukan bahwa histogram yang dihasilkan memiliki distribusi yang relatif seragam pada tiap pikselnya, hal ini menunjukan bahwa kualitas enkripsi sangat baik. Proses dekripsi citra juga dapat berjalan dengan sempurna dimana dibuktikan nilai inf pada PSNR dan nilai 0 pada MSE.

DAFTAR PUSTAKA

[1] D. Sinaga, C. Umam, D. R. I. M. Setiadi and E. H. Rachmawanto, "Teknik Super Enkripsi Menggunakan Transposisi Kolom Berbasis Vigenere Cipher Pada Citra Digital," *Dinamika Rekayasa,* vol. 14, no. 1, 2018.

[2] J. Li, Y. Xing, C. Qu and J. Zhang, "An Image Encryption Method Based on Tent and Lorenz Chaotic Systems," in *International Conference on Software Engineering and Service Science (ICSESS)*, Beijing, 2015.

[3] A. E. Handoyo, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari and A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," *Jurnal Teknologi dan Sistem Komputer,* vol. 6, no. 1, pp. 37-43, 2018.

[4] R. Jain and J. Sharma, "Symmetric Color Image Encryption Algorithm using Fractional DRPM and Chaotic Baker Map," in *International Conference On Recent Trends In Electronics Information Communication Technology*, 2016.

[5] N. Widyastuti, "Pengembangan Metode Beaufort Cipher menggunakan Pembangkit Kunci Chaos," *Jurnal Teknologi,* vol. 7, no. 1, pp. 73-82, 2014.

[6] D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Implementasi One Time Pad Kriptografi pada Gambar Grayscale dan Gambar Berwarna," Semarang, 2017.

[7] F. M. S. Ali and F. H. Sarhan, "Enhancing Security of Vigenere Cipher by Stream Cipher," *International Journal of Computer Applications ,* vol. 100, no. 1, pp. 1-4, 2014.

[8] O. Tornea, M. E. Borda, V. Pileczki and R. Malutan, "DNA Vernam Cipher," in *International Conference on E-Health and Bioengineering*, Iaşi, 2011.

[9] R. Shukla, H. O. Prakash, R. Bhushan, S. Venkataraman and G. Varadan, "Sampurna Suraksha: Unconditionally Secure And Authenticated One Time Pad Cryptosystem," in *International Conference on Machine Intelligence Research and Advancement*, Katra, 2013.

[10] P. Hernawandra, Supriyadi and U. T. Lenggana, "Aplikasi Steganografi Menggunakan LSB 4 Bit Sisipan dengan Kombinasi Algoritme Substitusi dan Vigenere Berbasis Android," *Jurnal Teknologi dan Sistem Komputer,* vol. 6, no. 2, pp. 44-50, 2018.

[11] K. Alallayah, M. Amin, W. A. El-Wahed and A. Alhamami, "Attack and Construction of Simulator for Some of Cipher Systems Using Neuro-Identifier," *The International Arab Journal of Information Technology,* vol. 7, no. 4, pp. 365-372, 2010.

[12] D. R. I. M. Setiadi, E. H. Rachmawanto and C. A. Sari, "Kombinasi Algoritma One Time Pad dan Chaotic Sequence dalam Optimasi Enkripsi Gambar," *Jurnal Teknik Mesin, Elektro, dan Ilmu Kompurter (SIMETRIS),* vol. 8, no. 2, pp. 483-488, 2017.

[13] R. C. Gonzalez, R. E. Woods and S. L. Eddins, "ImageProcessingPlace.com," [Online]. Available: http://www.imageprocessingplace.com/downloads_V3/root_downloads/image_databases/standard_test_images.zip. [Accessed Maret 2018].