Techno.COM, Vol. 16, No. 4, November 2017 : 337-347

Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher

Implementation of Securing Digital Image Based on Vernam Cipher Cryptography Technique

Tan Samuel Permana[1], Christy Atika Sari[2], Eko Hari Rachmawanto[3], De Rosal Ignatius Moses Setiadi[4], Egia Rosi Subhiyakto[5]

[1,2,3,4,5] Jurusan Teknik Informatika, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro; Jl. Imam Bonjol 207, Semarang
e-mail: [1]tansamuelpermana95@gmail.com, [2]christy.atika.sari@dsn.dinus.ac.id,
[3]eko.hari@dsn.dinus.ac.id, [4]moses@dsn.dinus.ac.id, [5]egia@dsn.dinus.ac.id

Abstrak

Penggunaan media online dalam melakukan aktivitas telah semakin marak terjadi pada dinamika masyarakat modern. Salah satu obyek sasaran dalam aktivitas online adalah citra digital. Citra digital ini dapat diperuntukan untuk kalangan terbatas saja sehingga mudah menjadi sasaran oleh peretas, terutama jika data citra digital tersebut bersifat penting. Disinilah kriptografi mengambil peran penting dalam mengamankan citra digital. Dengan menggunakan teknik Vernam Cipher, pesan citra digital dapat diacak dengan kunci yang berbeda untuk setiap karakter, sehingga pesan citra digital hanya dapat dibaca oleh penerima saja. Hasil enkripsi akan menghasilkan citra baru dengan adanya perubahan pada intensitas warna piksel. Dari 12 gambar dengan ukuran kurang dari 100 KB, tingkat keberhasilannya adalah 100%. Algoritma ini sangat cepat, dengan kecepatan enkripsi rata-rata 0,007785 dan dekripsi 0,006903 untuk gambar berformat JPEG dan memiliki ukuran piksel 384x384 Berdasarkan penelitian tersebut maka dapat disimpulkan bahwa Algoritma Vernam Cipher adalah algoritma yang baik untuk digunakan.

Kata kunci—Citra Digital, Keamanan, Enkripsi, Dekripsi, Vernam Cipher

Abstract

Utilization of online media in daily activities have been increasingly rampant on the modern society. One of the target object in online activities is a digital image. The digital image can be allocated to a limited circle so can be easily targeted by hackers, especially if the digital image data is important. This is where cryptography takes an important role in securing digital image. By using the technique of Vernam Cipher, each character on digital image message can be encrypted with different keys, so the digital image messages can only be read by the addressee only. The results of encryption will generate a new image with the change in intensity of color pixels. Of the 12 images with a size less than 100 KB, the success rate is 100%. This algorithm is very fast, with an average speed of encryption 0,007785 and decryption 0,006903 for JPEG images and has a pixel size of 384x384. Based on these studies it can be concluded that the Vernam Cipher Algorithm is a good algorithm to use.

Keywords—Digital Image, Security, Encryption, Decryption, *Vernam Cipher*

1. PENDAHULUAN

Teknologi merupakan sebuah kebutuhan pokok yang sudah melekat pada diri masyarakat modern. Setiap hari jutaan orang diseluruh dunia menggunakan produk dari teknologi seperti salah satunya adalah komputer. Dengan komputer kita dapat mengakses dunia maya, dan melakukan pengiriman data digital secara online, dalam hal ini obyek yang biasa

dikirimkan pada media online adalah citra digital. Namun dari adanya pengiriman secara online ini, muncul upaya-upaya tertentu oleh pihak ketiga sehingga data-data citra digital ini dapat dicuri atau diubah informasinya [1]. Data yang dapat dicuri maupun dimanipulasi ini dapat bersifat sangat penting dan rahasia, tentu pemilik data tidak ingin datanya yang penting tersebut dapat digunakan oleh pihak lain dengan tanpa seijinnya.

Untuk meningkatkan keamanan dari citra digital yang akan dikirimkan secara *online* agar dapat lebih terjaga kerahasiannya, maka dibutuhkan sebuah teknik khusus untuk melindungi pesan citra digital tersebut, yaitu dengan teknik kriptografi. Kriptografi pernah digunakan oleh Julius Caesar untuk melindungi pesan rahasia yang berhubungan dengan kepentingan militer. Teknik kriptografi itu sendiri bertujuan untuk mengamankan sebuah pesan dengan cara mengacak informasi dalam sebuah pesan sehingga tidak dapat dibaca oleh orang lain, atau bisa disebut dengan proses enkripsi. Agar penerima pesan dapat memahami isi pesan yang telah diacak tersebut, maka diperlukan proses dekripsi untuk mengembalikan pesan yang telah diacak tersebut kembali ke pesan asli. Salah satu metode yang ada dalam kriptografi adalah metode *Vernam Cipher* atau yang biasa disebut dengan *One-Time Pad* [2]. *Vernam Cipher* merupakan sebuah metode yang melakukan pengacakan pada setiap informasi yang tertanam dengan kunci yang berbeda-beda sehingga memiliki tingkat keamanan yang sangat tinggi untuk mengamankan sebuah data.

Sukhla dkk [3] dalam penelitiannya menyebutkan bahwa algoritma kunci simetris, yaitu *Vernam Cipher* dapat digunakan untuk meningkatkan keamanan data baik dalam proses enkripsi maupun dekripsi. Mamta Jain [4] dalam penelitiannya menyebutkan bahwa algoritma *Vernam Cipher* juga telah diterapkan dalam teknik steganografi untuk mengamankan data. Sari, dkk [5] dalam penelitiannya menyebutkan bahwa algoritma *Vernam Cipher* dapat digunakan untuk proses enkripsi beberapa jenis file dengan ekstensi yang berbeda-beda dan telah digabungkan dengan teknik steganografi *End of File*. Sari, dkk [6] dalam penelitiannya yang menjelaskan tentang penggunaan kriptografi *Vernam Cipher* dan *Bit Shiffting* dalam mengamankan sebuah file.

Tujuan dari makalah ini adalah untuk meningkatkan keamanan data pada pesan citra digital yang akan dikirimkan pada media *online* dengan menggunakan metode kriptografi *Vernam Cipher* sehingga pihak lain yang bukan bertindak sebagai penerima tidak dapat membaca isi dari pesan citra digital tersebut.

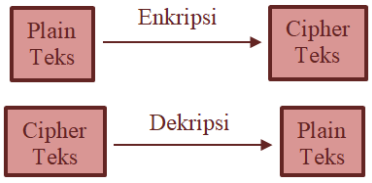
2. METODE PENELITIAN

2.1 Kriptografi

Sejak jaman dahulu, kurang lebih tahun 1900 sebelum masehi terdapat sebuah seni menyembunyikan pesan agar tidak dapat dilihat oleh orang lain, seni tersebut dinamakan kriptografi [7]. Kriptografi berasal dari bahasa asing yaitu “Crypto” atau dapat disebut rahasia dan “Graphy” atau tulisan, sehingga diartikan menjadi tulisan rahasia. Di dalam kriptografi ada sebuah plain teks. Plain teks ini bisa juga disebut sebagai pesan asli, yang nantinya dapat dienkripsikan dengan sebuah kunci (*key*) yang telah ditetapkan sehingga akan menghasilkan cipher teks atau pesan yang sudah teracak [8]. Ada proses enkripsi atau proses mengacak pesan, ada juga proses dekripsi. Proses dekripsi adalah proses mengembalikan cipher teks ke pesan semula atau pesan asli. Proses enkripsi dan dekripsi dapat dilihat pada Gambar 1. Sehingga dapat disimpulkan bahwa sebuah teknik dapat dikatakan kriptografi apabila mempunyai unsur-unsur sebagai berikut [9]:

1. Plain teks, adalah pesan awal atau asli sebelum pesan dimodifikasi.
2. Kunci, digunakan dalam proses enkripsi.
3. Enkripsi, adalah proses yang mengacak plain teks menjadi cipher teks.
4. Cipher teks, merupakan pesan acak hasil proses enkripsi.

5. Dekripsi, adalah proses mengembalikan pesan cipher teks kembali ke plain teks.



Gambar 1 Proses enkripsi dan dekripsi kriptografi

Kriptografi tidak hanya bertujuan untuk mengamankan data saja, namun juga untuk menjaga keaslian dari data tersebut dan integritasnya. Kriptografi dapat dibagi ke dalam 2 bagian yaitu kriptografi klasik dan modern [10]. Kriptografi klasik pada umumnya berbentuk kriptografi simetris yaitu kunci untuk proses enkripsi dan dekripsi sama, contohnya adalah Blowfish [11], Twofish, Shift Cipher [12], *Vernam Cipher* [13], *Caesar Cipher, dan Vigenere Cipher* [14]. Sedangkan kriptografi modern dapat berupa kriptografi simetris dan asimetris. Kriptografi simetris modern contohnya adalah *DES* (*Data Encryption Standard*). Kriptografi asimetris menggunakan kunci yang berbeda saat melakukan proses dekripsi, berbeda dengan kriptografi simetris yang kunci untuk dekripsi dan enkripsi sama. Contoh dari kriptografi asimetris modern adalah *RSA (Rivest Shamir Adleman).*

2.2 Citra Digital

Kumpulan dari piksel yang membentuk sebuah pola tertentu dinamakan citra digital. Citra biasa kita jumpai dalam kehidupan sehari-hari, misalnya lukisan, hasil fotografi, patung, dan lainnya. Citra dalam bentuk digital ini yang bisa disebut citra digital. Alat elektronik yang dapat menghasilkan citra digital beberapa diantaranya adalah komputer dan kamera digital. Citra memiliki nilai warna keabuan yang terdiri dari 0-255. 0 berarti hitam pekat, antara 0-255 keabuan, dan 255 berarti putih.

2.3 *Vernam Cipher*

*Vernam Cipher*merupakan sebuah algoritma enkripsi yang dikatakan tidak dapat dipecahkan atau *ubreakable* karena untuk memecahkan algoritma ini [9], penyerang harus menguji setiap kemungkinan kunci yang ada. Algoritma ini ditemukan oleh Gilbert Vernam pada awal abad ke-20. Penghitungan enkripsi pada *Vernam Cipher* [15] dilakukan dengan mengurangkan nilai Plain teksnya dengan menggunakan nilai kunci yang telah disediakan, setelah itu dimodulokan dengan 26 atau 256 bergabtung pada jenis media yang digunakan. Tujuan dilakukannya proses enkripsi *Vernam Cipher* adalah untuk mendapatkan ciper teks atau pesan yang telah diacak, sehingga didapatkan rumus enkripsi:

$$Ci = Pi + ki \ mod \ 26 \quad (1)$$

Jika terdapat 256 karakter, maka dimodulokan 256. ASCII sangat berperan untuk mengubah huruf alfabet menjadi biner, sehingga dapat dirumuskan:

$$Ci = Pi + ki \ mod \ 256 \quad (2)$$

Dekripsi *Vernam Cipher* mengurangkan cipher teks dengan kunci yang sama saat melakukan enkripsi, setelah itu dimodulokan 26. Tujuan dari dekripsi *Vernam Cipher* adalah mendapatkan kembali plain teks semula, maka didapatkan rumus:

$$Pi = Ci - ki \ mod \ 26 \quad (3)$$

Rumus dekripsi untuk 256 karakter juga sama, hanya saja dimodulokan 256, maka didapatkan rumus:

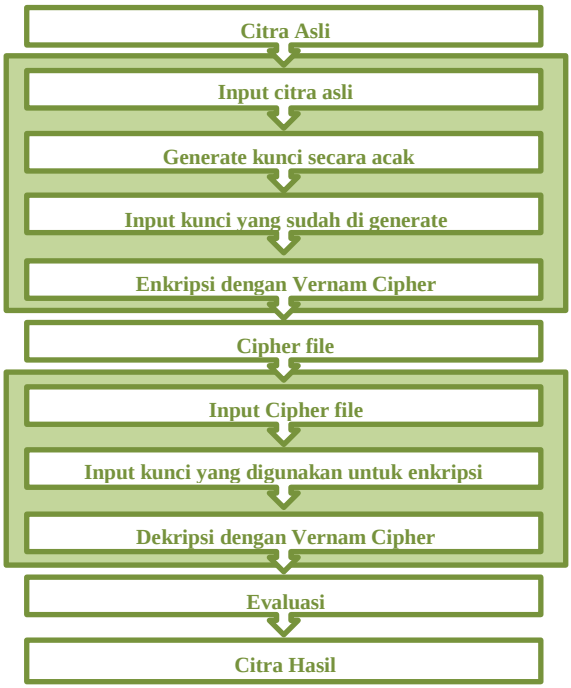
$$Pi = Ci - ki \; mod \; 256 \qquad (4)$$

Di dalam algoritma *Vernam Cipher* kunci yang digunakan dan plain teks nya harus sama panjang, dan untuk memaksimalkan keamanan, kunci harus diacak seluruhnya. Selain itu kunci hanya dapat digunakan satu kali, maksudnya adalah jika ingin melakukan proses enkripsi pada citra digital yang berbeda, maka harus menggunakan kunci yang berbeda juga.

2.4 Histogram dan Entropi

Histogram dapat menggambarkan tingkat penyebaran warna dari suatu citra digital. Pada citra digital *grayscale*, dapat dilihat kecondongan warnanya, apakah lebih condong ke hitam ataukan lebih condong ke putih dengan skala 0-255. Melalui histogram, perubahan warna pada proses enkripsi dan dekripsi dapat diketahui. Sedangkan entropi dapat digunakan untuk mengukur kualitas dari suatu citra. Semakin tinggi nilai entropinya, maka semakin baik juga citra tersebut. Entropi dapat digunakan mengetahui apakah citra hasil dekripsi sama dengan citra asli.

2.6 Proses Enkripsi dan Proses Dekripsi



Gambar 2 Proses enkripsi dan dekripsi

3. HASIL DAN PEMBAHASAN

3.1 Proses Enkripsi *Vernam Cipher*

Citra yang akan diteliti yaitu plain file berjenis file JPEG dan PNG masing-masih 6 buah yang diambil dari repositori online yaitu *petitcolas.net* dengan ukuran piksel 256x256 dan 384x384. Proses enkripsi dilakukan dengan Matlab. Citra digital memiliki model warna *grayscale*. Misal gambar yang akan dilakukan perhitungan adalah bear.jpg, dengan ukuran piksel 384x384 dan model warna *grayscale*. Gambar dapat dilihat pada Gambar 3.

(a) (b)

Gambar 3 bear.jpg; (a) gambar asli, (b) gambar hasil enkripsi

Gambar bear.jpg tersebut diambil sampel nilai warna sebagai plain teks sebanyak 5 piksel, mulai dari (baris, kolom): (1,1), (1,2), (1,3), (1,4), dan (1,5), yaitu 117, 115, 107, 100, dan 105. Setelah itu *generate* secara acak kunci untuk proses enkripsi dengan jarak antara 0-1000, lalu ambil sebanyak 5 buah nilai warna dari piksel dengan letak piksel yang sama dengan citra aslinya sehingga didapatkan nilainya yaitu 815, 824, 338, 343, dan 962. Sampel nilai warna piksel dari citra asli dan kunci dapat dilihat pada Gambar 4 dan Gambar 5.

citra_asli | kunci | citra_hasil | citra_kembali

384x384 uint8

	1	2	3	4	5
1	117	115	107	100	105

Gambar 4 Piksel nilai warna citra asli (plain teks)

citra_asli | kunci | citra_hasil | citra_kembali

384x384 double

	1	2	3	4	5
1	815	824	338	343	962

Gambar 4 Piksel nilai warna kunci

Dari plain teks dan kunci tersebut maka dapat dilakukan perhitungan cipher teks nya dengan proses enkripsi sebagai berikut:

$Ci = Pi + ki \bmod 256$

$C_{(1,1)}$ = (117+815) mod 256 = 932 mod 256 = 164

$C_{(1,2)}$ = (115+824) mod 256 = 939 mod 256 = 171

$C_{(1,3)}$ = (107+338) mod 256 = 445 mod 256 = 189

$C_{(1,4)}$ = (100+343) mod 256 = 443 mod 256 = 187

$C_{(1,5)}$ = (105+962) mod 256 = 1067 mod 256 = 43

Maka didapatkan hasil Cipher teks mulai dari baris ke-1 kolom ke-1 hingga baris ke-1 kolom ke-5, yaitu 164, 171, 189, 187, dan 43 atau lebih jelasnya dapat dilihat pada Gambar 6. Proses tersebut diteruskan hingga piksel terenkripsi seluruhnya. Citra hasil enkripsi dapat dilihat pada Gambar 7.

citra_asli | kunci | citra_hasil | citra_kembali

384x384 uint8

	1	2	3	4	5
1	164	171	189	187	43

Gambar 5 Nilai warna piksel hasil proses enkripsi

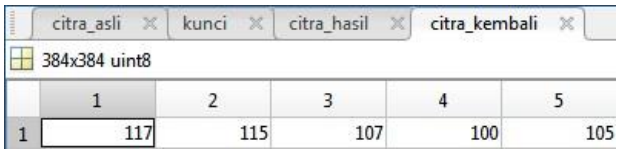
3.2 Proses Dekripsi *Vernam Cipher*

Setelah semua piksel dienkripsi, untuk proses dekripsinya dapat dilakukan perhitungan dengan cara sebagai berikut:

$Pi = Ci - ki \bmod 256$

$P_{(1,1)}$ = (164-815) mod 256 = (-651) mod 256 = 117
$P_{(1,2)}$ = (171-824) mod 256 = (-653) mod 256 = 115
$P_{(1,3)}$ = (189-338) mod 256 = (-149) mod 256 = 107
$P_{(1,4)}$ = (187-343) mod 256 = (-156) mod 256 = 100
$P_{(1,5)}$ = (43-962) mod 256 = (-919) mod 256 = 105

Maka didapatkan hasil plain teks semula yaitu 117, 115, 107, 100, dan 105 atau dapat dilihat pada Gambar 8. Proses dekripsi dilanjutkan sampai piksel telah terhitung seluruhnya. Jika nilai warna piksel hasil proses dekripsi sama dengan nilai warna piksel citra awal atau sebelum proses enkripsi, maka citra dapat dikatakan telah kembali seperti semula. Citra hasil dekripsi harus sama dengan citra asli.



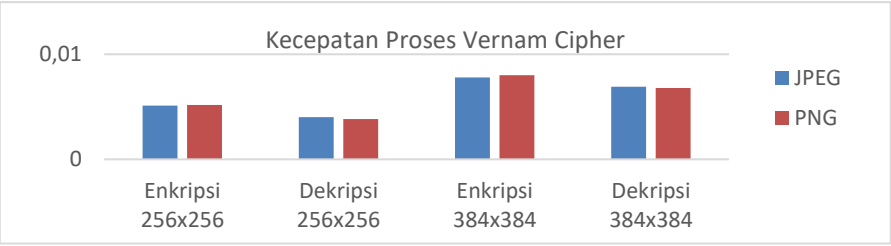
Gambar 6 Nilai warna piksel hasil proses dekripsi

3.3 Hasil Percobaan dan Hasil Analisa

Tabel 1 Lama proses enkripsi dan dekripsi

No	Nama	Waktu Pemrosesan (detik)			
		256x256		384x384	
		Enkripsi	Dekripsi	Enkripsi	Dekripsi
1	bear.jpg	0,005415	0,004126	0,007226	0,006416
2	brandyrose.jpg	0,005358	0,003914	0,007962	0,007061
3	f16.jpg	0,004585	0,004029	0,008166	0,007232
Rata-rata		**0,005119**	**0,004023**	**0,007785**	**0,006903**
4	pueblo_bonito.png	0,005356	0,003873	0,007946	0,006921
5	skyline_arch.png	0,004208	0,003806	0,008861	0,006995
6	waterfall.png	0,005924	0,003836	0,007225	0,006436
Rata-rata		**0,005163**	**0,003838**	**0,008011**	**0,006784**

Kecepatan proses enkripsi algoritma *Vernam Cipher* lebih cepat dari kecepatan proses dekripsi, hal ini dapat dilihat pada rata-rata waktu pemrosesan pada Tabel 1. Pada citra dengan ukuran piksel 256x256 terlihat bahwa proses dekripsi lebih cepat sekitar 0,001 detik. Hal yang sama juga terjadi pada citra digital dengan ukuran piksel 384x384 yang kecepatan proses dekripsinya lebih cepat sekitar 0,001 detik. Selain itu, ukuran piksel yang lebih besar mengakibatkan waktu pemrosesan enkripsi dan dekripsi menjadi lebih lama. Perbedaan jenis file antara *JPEG* dan *PNG* hanya sedikit mengakibatkan perubahan dalam waktu pemrosesan.



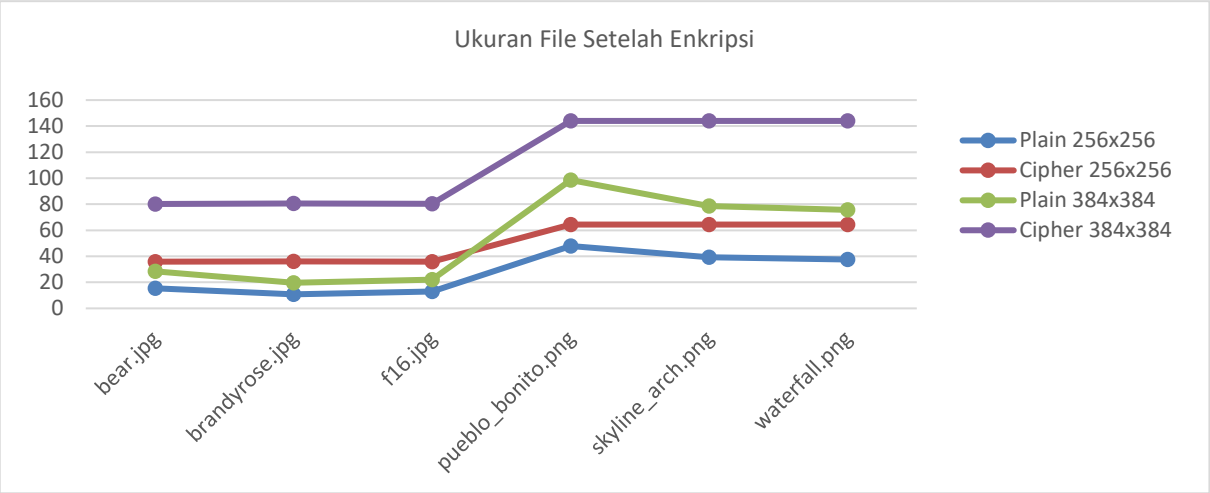
Gambar 7 Grafik perbandingan kecepatan proses enkripsi dan dekripsi

Gambar 9 menunjukan grafik perbedaan kecepatan proses enkripsi dan dekripsi. Grafik tersebut menunjukan proses enkripsi memakan waktu yang lebih lama dari proses dekripsi.

Tabel 2 Perubahan ukuran file citra digital

No	Nama	Ukuran File Citra (KB)			
		256x256		384x384	
		Plain	Cipher	Plain	Cipher
1	bear.jpg	15,5	35,9	28,5	80,2
2	brandyrose.jpg	10,8	36	19,7	80,5
3	f16.jpg	12,9	35,9	22,1	80,4
Rata-rata		**13,1**	**35,9**	**23,4**	**80,4**
4	pueblo_bonito.png	47,9	64,4	98,6	144
5	skyline_arch.png	39,3	64,4	78,5	144
6	waterfall.png	37,6	64,4	75,6	144
Rata-rata		**41,6**	**64,4**	**84,2**	**144**

Pada Tabel 2 terlihat bahwa proses enkripsi pada citra menyebabkan ukuran file menjadi lebih besar. Perubahan ukuran terjadi baik untuk file jenis *JPEG* maupun PNG.



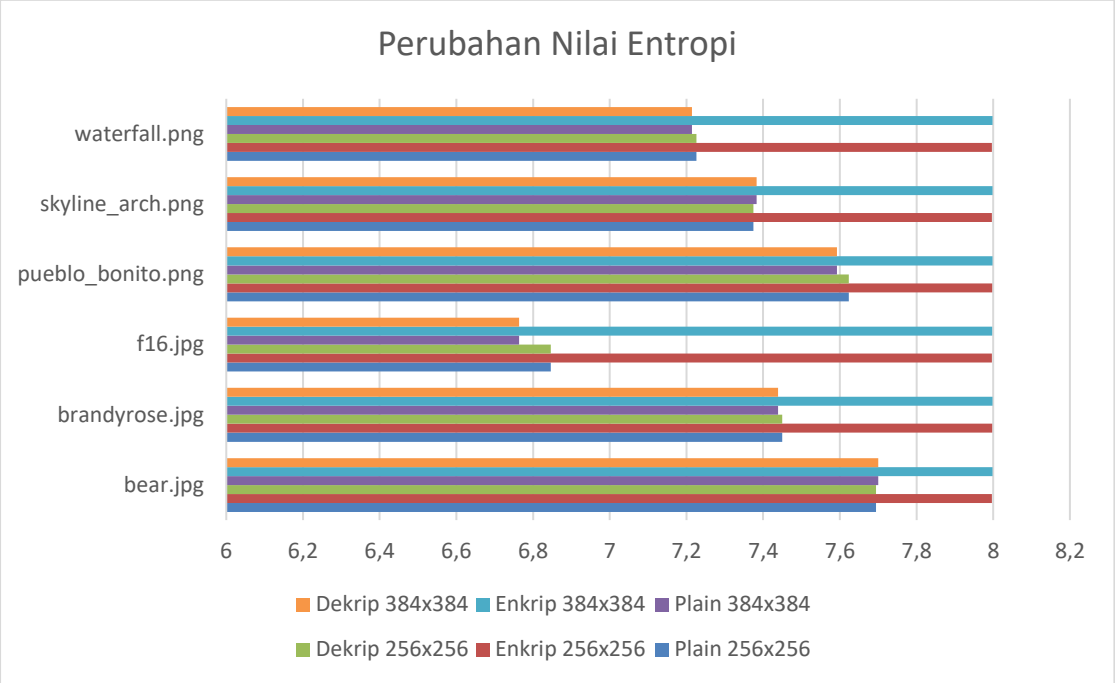
Gambar 8 Grafik perubahan ukuran file citra

Gambar 10 menunjukan grafik perbedaan ukuran yang terjadi setiap proses enkripsi. Ukuran file citra akan membesar setelah dilakukan proses enkripsi.

Tabel 3 Kualitas citra kriptografi

No	Nama	Entropi					
		256x256			384x384		
		Plain	Cipher	Dekrip	Plain	Cipher	Dekrip
1	bear.jpg	7,6941	7,9968	7,6941	7,6999	7,9986	7,6999
2	brandyrose.jpg	7,4497	7,9971	7,4497	7,4389	7,9984	7,4389
3	f16.jpg	6,8463	7,9966	6,8463	6,7639	7,9978	6,7639
4	pueblo_bonito.png	7,6235	7,9971	7,6235	7,5927	7,9986	7,5927
5	skyline_arch.png	7,3744	7,9969	7,3744	7,3826	7,9984	7,3826
6	waterfall.png	7,2262	7,9969	7,2262	7,2147	7,9983	7,2147

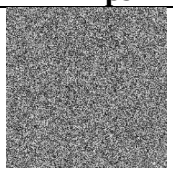
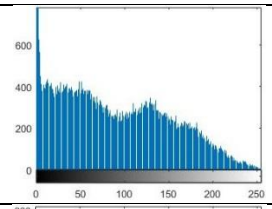
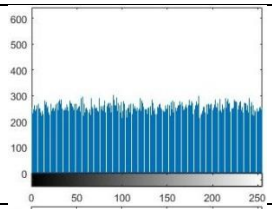
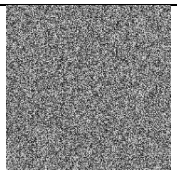
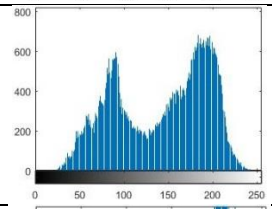
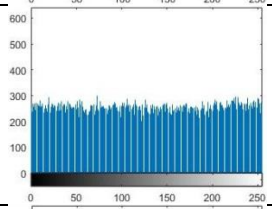
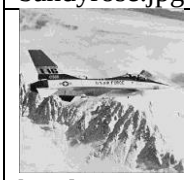
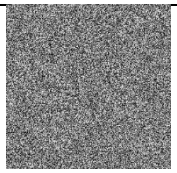
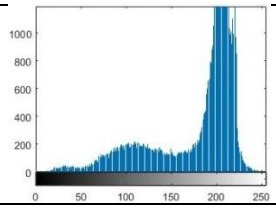
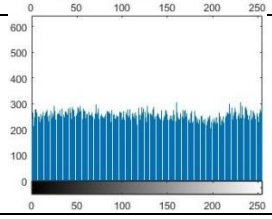
Tabel 3 memperlihatkan bahwa nilai entropi dari citra digital hasil dekripsi sama dengan citra awal, hal ini menjukan bahwa proses dekripsi telah berjalan dengan baik. Perbedaan nilai entropi pada citra digital hasil enkripsi atau cipher file menunjukan bahwa adanya perubahan nilai warna yang terjadi saat proses enkripsi.

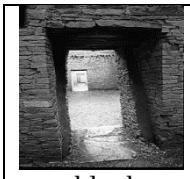
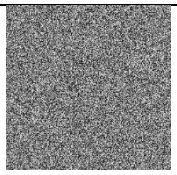
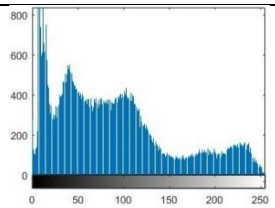
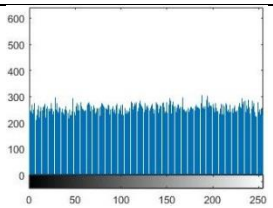
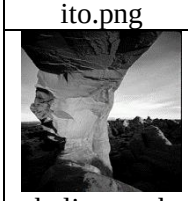
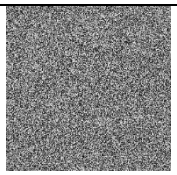
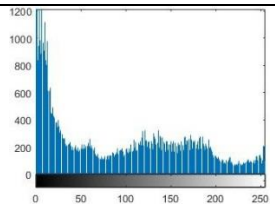
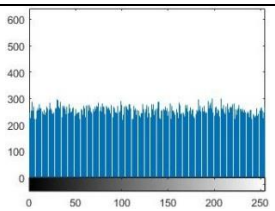
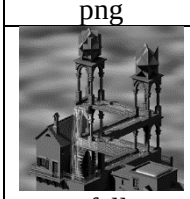
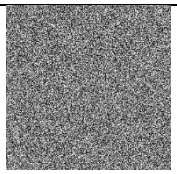
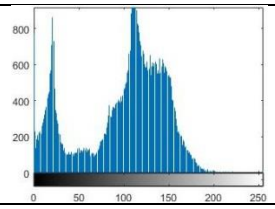
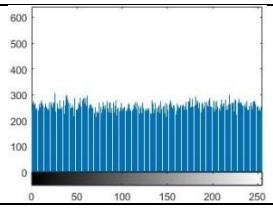


Gambar 9 Grafik perubahan nilai entropi

Gambar 11 menunjukan grafik perubahan nilai entropi setiap dilakukannya proses enkripsi dan dekripsi. Citra yang telah berhasil didekripsi akan memiliki nilai yang sama dengan citra asli.

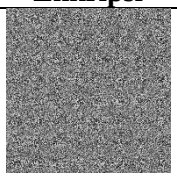
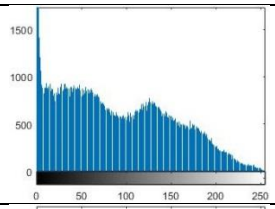
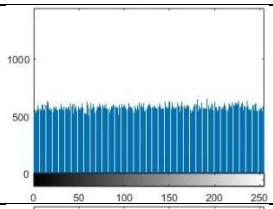
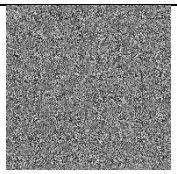
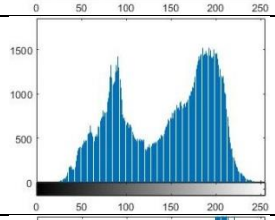
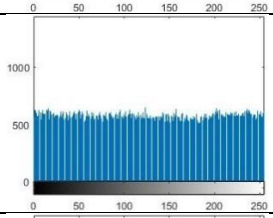
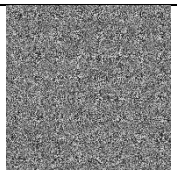
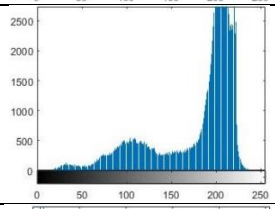
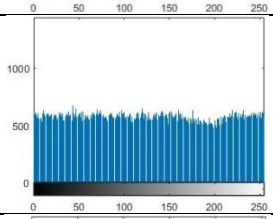
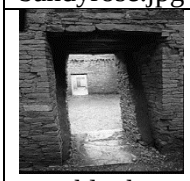
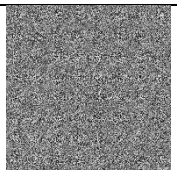
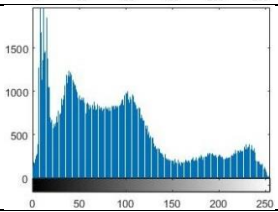
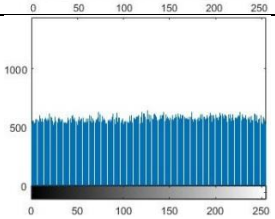
Tabel 4 Analisa histogram citra berukuran piksel 256x256

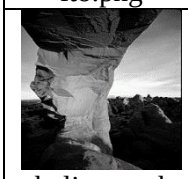
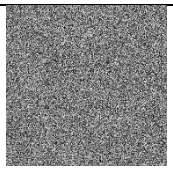
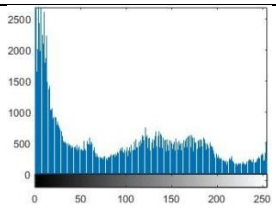
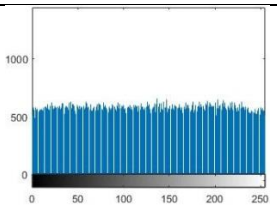
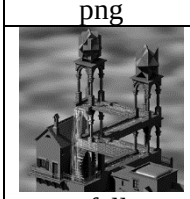
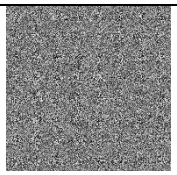
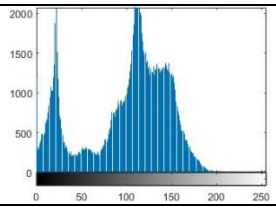
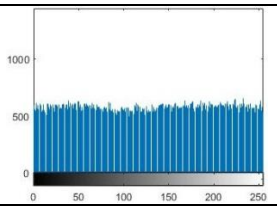
Citra Awal	Citra Hasil Enkripsi	Histogram Citra Awal	Histogram Hasil Enkripsi
 bear.jpg			
 bandyrose.jpg			
 bandyrose.jpg			

 pueblo_bonito.png			
 skyline_arch.png			
 waterfall.png			

Histogram pada Tabel 4 menunjukan bahwa citra asli dan citra yang dienkripsi memiliki tingkat persebaran warna yang berbeda, dimana untuk citra hasil enkripsi dengan algoritma *Vernam Cipher*, tingkat distribusi warnanya merata sehingga tidak dapat memberikan petunjuk sama sekali untuk dilakukannya dekripsi oleh pihak lain.

Tabel 5 Analisa histogram citra berukuran piksel 384x384

Citra Awal	**Citra Hasil Enkripsi**	**Histogram Citra Awal**	**Histogram Hasil Enkripsi**
 bear.jpg			
 bandyrose.jpg			
 bandyrose.jpg			
 pueblo_bon			

ito.png			
 skyline_arch.png			
 waterfall.png			

Tabel 5 menunjukan ada perubahan persebaran warna yang terjadi setelah proses enkripsi dilakukan. Hal ini menunjukan bahwa persebaran warna pada histogram merata sehingga penyerang tidak mendapatkan petunjuk untuk memecahkan algoritma ini.

4. KESIMPULAN

Kesimpulan yang didapatkan setelah melakukan penelitian "Peningkatan Keamanan Citra Digital Berbasis Metode Kriptografi *Vernam Cipher"* adalah algoritma *Vernam Cipher* sangat kuat dan cepat karena kunci untuk setiap karakter telah dibuat secara acak. Selain itu, kelebihan lainnya adalah setiap nilai warna dalam piksel dienkripsi dengan kunci yang berbeda-beda menyebabkan penyerang harus mencoba segala kemungkinan kunci yang ada. Dalam penelitian ini, algoritma *Vernam Cipher* memiliki kecepatan proses yang sangat cepat, dengan kecepatan proses enkripsi tercepat yaitu 0,005119 detik dan kecepatan proses dekripsi tercepat yaitu 0,003838 detik. Adapun kelemahan pada algoritma ini adalah kunci yang digunakan terlalu panjang. Meskipun kunci yang digunakan terlalu panjang, kecepatan proses tidak terpengaruh.

5. SARAN

Saran-saran yang berguna untuk kemajuan penelitian ini kedepannya adalah proses kriptografi yaitu enkripsi dan dekripsi tidak hanya dapat diterapkan sebatas pada citra digital dengan model warna *grayscale* saja, namun dapat juga diterapkan pada citra digital dengan model warna lain seperti *RGB* (*Red, Green, and Blue*). Selain itu perlunya pengembangan dengan GUI untuk mempermudah pengaplikasian proses enkripsi dan dekripsi terhadap citra digital. Untuk peningkatan algoritma, pada penelitian selanjutnya dapat mengggunakan kombinasi *random key generator*.

DAFTAR PUSTAKA

[1] M. A. Faizal, H. Rahmalan, E. H. Rachmawanto, and C. A. Sari, "Impact Analysis for Securing Image Data using Hybrid SLT and DCT," *Int. J. Futur. Comput. Commun. 2012*, vol. 1, no. 3, p. 2012, 2012.

[2] L. Erawan, C. A. Sari, and E. H. Rachmawanto, "Lalang_Erawan_Implementasi_Kriptografi_Simetris_OTP (1)," in *Seminar Nasional Multidisiplin Ilmu Universitas Budi Luhur Jakarta*, 2017.

[3] R. Shukla, H. O. Prakash, R. P. Bhushan, S. Venkataraman, and G. Varadan, "Sampurna Suraksha: Unconditionally Secure and Authenticated One Time Pad Cryptosystem," in *2013 International Conference on Machine Intelligence and Research Advancement*, 2013, pp. 174–178.

[4] M. Jain and S. K. Lenka, "Secret data transmission using vital image steganography over transposition cipher," in *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015, pp. 1026–1029.
[5] C. A. Sari and E. H. Rachmawanto, "Gabungan Algoritma Vernam Chiper Dan End of File," *Techno.COM*, vol. 13, no. 3, pp. 150–157, 2014.
[6] C. A. Sari and E. H. Rachmawanto, "Penyembunyian Data Untuk Seluruh Ekstensi File Menggunakan Kriptografi Vernam Cipher dan Bit Shiffting," *J. Appl. Intell. Syst.*, vol. 1, no. 3, pp. 179–190, 2016.
[7] D. Nilesh and M. Nagle, "The new cryptography algorithm with high throughput," in *2014 International Conference on Computer Communication and Informatics*, 2014, pp. 1–5.
[8] C. Sari, E. Rachmawanto, Y. Astuti, and L. Umaroh, "Optimasi penyandian file menggunakan kriptografi shift cipher," in *Seminar Multi Disiplin Ilmu Unisbank (SENDI_U) ke-2 Semarang*, 2016.
[9] O. Tornea, M. E. Borda, V. Pileczki, and R. Malutan, "DNA Vernam Cipher," *Proc. 3rd Int. Conf. E-Health Bioeng. - EHB 2011*, pp. 24–27, 2011.
[10] E. H. Rachmawanto and C. A. Sari, "Keamanan File Menggunakan Teknik Kriptografi Shift Cipher," *Techno.COM*, vol. 14, no. 4, pp. 329–335, 2015.
[11] Y. P. Astuti, E. H. Rachmawanto, and C. A. Sari, "Optimasi Enkripsi Password Menggunakan Algoritma Blowfish," *Techno.COM*, vol. 15, no. 1, pp. 15–21, 2016.
[12] Sukrisno and E. Utami, "IMPLEMENTASI STEGANOGRAFI TEKNIK EOF DENGAN GABUNGAN ENKRIPSI RIJNDAEL , SHIFT CIPHER DAN FUNGSI HASH MD5," *Semin. Nas. Teknol. 2007 (SNT 2007)*, no. November, pp. 1–16, 2007.
[13] E. Rachmawanto, C. Sari, Y. Astuti, and L. Umaroh, "KRIPTOGRAFI VERNAM CIPHER UNTUK MENCEGAH PENCURIAN DATA PADA SEMUA EKSTENSI FILE," in *PROSIDING SEMINAR NASIONAL MULTI DISIPLIN ILMU & CALL FOR PAPERS UNISBANK (SENDI_U) KE-2 Tahun 2016*, 2016, pp. 46–51.
[14] S. Garg, S. Khera, and A. Aggarwal, "Extended Vigenere Cipher with Stream Cipher," *Int. J. Eng. Sci. Comput.*, vol. 6, no. 5, pp. 5176–5180, 2016.
[15] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017.