KOMBINASI KRIPTOGRAFI KLASIK PADA MEDIA GAMBAR : SHIFT CIPHER DAN VIGENERE CIPHER

Ibnu Utomo WM[1*], Ajib Susanto[2], Eko Hari Rachmawanto[3], De Rosal Ignatius Moses Setiadi[4]
[1234] Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol 207 Semarang 50131
[*]Email: ibnu.utomo.wm@dsn.dinus.ac.id

Abstrak

Maraknya pencurian data memerlukan penangan khusus. Hal ini dikarenakan data tersebut tidak diamankan dengan teknik tertentu. Dalam penelitian ini, kriptografi dipilih sebagai teknik untuk menyandikan data. Algoritma kriptografi simteris merupakan jenis kriptografi dengan proses enkripsi dan dekripsi menggunakan kunci yang sama persis. Vigenere cipher adalah bagian dari kriptografi simteris dengan model operasi modulo 26. Termasuk pula dalam polyalphabet cipher yang dioperasikan menggunakan stream cipher. Vigenere mudah untuk digunakan dan aman. Hal ini dikarenakan panjang kunci harus sama dengan panjang plain teks. Tahapan selanjuutnya data akan diamankan dengan shift cipher, sehingga tidak mudah dideteksi dan tidak mencurigakan. Pada penelitian ini akan digunakan 2 data gambar percobaan untuk diimplementasikan pada proses enkripsi dan dekripsi. Data tersebut didapat dari SIPI database kemudian dilakukan preprocessing dan selanjutnya di olah dengan Matlab.

***Kata kunci**: kriptografi simteris; citra; vigenere cipher; shift cipher*

1. PENDAHULUAN

Pesatnya perkembangan teknologi pada akhir-akhir ini memungkinkan manunsia bisa bertukar informasi secara cepat dan luas. Jarak bukanlah sebuah kendala bagi manusia untuk bertukar informasi. Media yang digunakan untuk pertukaran informasi dapat berupa data, berkas atau file, pesan, musik, video, dan gambar. Data adalah catatan atas sekumpulan fakta. Data dalam keguaan keseharian memiliki arti pernyataan yang telah diterima apa adanya (Hemalatha, Acharya and Renuka, 2016). Jika data-data terkumpul akan menghasilkan sebuah informasi. Media pertukaran informasi tersebut dipergunakan karena dapat mempermudah dan mempercepat kegiatan komunikasi. Dengan kelancaran berkomunikasi manusia bisa menyelesaikan ururusan bisnis, pribadi, dan urusan yang lain dengan mudah. Jika pertukaran informasi dengan mengirimkan data dilakukan tanpa pengamanan data tersebut, maka kegiatan pertukaran informasi tersebut dapat dikatakan tidak aman. Karena bahaya penyadapan bisa timbul dimana saja dan kapan saja tanpa diketahui oleh pelaku pertukaran informasi. Setiap orang memiliki informasi sendiri-sendiri, informasi tersebut bisa memiliki tingkatan privasi menurut pemilik informasi itu sendiri. Bagaimanapun informasi sudah menjadi sesuatu yang sangat berharga. Bagi pebisnis, informasi bisa digunakan untuk meningkatkan keuntungan bisnis. Di dalam dunia militer, informasi bisa menjadi benda yang tak ternilai harganya. Karena dapat merubah nasib negara pemilik informasi atau pencari informasi tersebut. Bagi wartawan, informasi adalah sumber kehidupannya. Oleh karena itu informasi bisa menjadi bahan incaran bagi kalangan mana saja. Karenanya, keamanan didalam informasi adalah unsur yang harus ada. Pengaman itu sendiri pada dasarnya berfungsi untuk melindungi isi dari informasi supaya siapapun yang berusaha mengincar informasi tersebut tidak dapat membaca, merubah, ataupun memindah hak milik dan menghapusnya dari pemilik aslinya.

Masalah keamanan data merupakan sesuatu yang sangat penting bagi perusahaan maupun perkantoran. Banyak data yang bersangkutan dengan rahasia perusahaan seperti data pegawai, customer, dan lain sebagainya. Semua data tersebut biasanya disimpan dalam satu tempat, misalnya sebuah komputer yang ada di kantor tersebut. Pada umumnya komputer itu

sendiri bisa diberi password agar membatasi hak akses bagi orang yang tidak berkepentingan. Namun, apabila terdapat pengelola data yang pandai maka orang itu akan menggadakannya sebagai cadangan jika data yang utama terhapus secara tidak sengaja. Akan tetapi, itu saja tidak cukup untuk mengamankan sebuah file penting. Oleh karena itu harus ditambahkan cara lain untuk menjaga data atau file penting. Karena kerahasiaan data merupakan hal wajib dalam menjaga keamanan data.

Kejahatan yang berhubungan dengan keamanan telah banyak terjadi. Contoh dari kejahatan tersebut adalah hacker atau cracker, maling dan penyusup rumah atau perkantoran, keamanan finansial terhadap kehancuran ekonomi. Akibat telah tercatat begitu banyaknya kasus penyadapan informasi telah membuat para peneliti berfikir bagaimana menghentikannya. Salah satu caranya adalah dengan mengenkripsi file informasi tersebut. Bidang ilmu kriptografi sangat cocok untuk mempelajari enkripsi dan dekripsi. Dengan enkripsi, informasi yang dianggap penting dan rahasia dapat disembunyikan sesuai kehendak pemilik informasi. Kerahasiaan data atau informasi pada komunikasi dua arah menuntut lebih dalam hal keamanan. Maka dikembangkanlah cabang ilmu yang mendalami tentang penyandian terhadap data dan informasi dan kemudian dikenal dengan istilah Kriptografi. Kriptografi memberikan beberapa layanan yang mendukung dalam hal meningkatkan keamanan data atau informasi. Kerahasiaan merupakan sesuatu yang ditunjukkan untuk melindungi informasi supaya tidak bisa dibaca atau diakses oleh pihak yang tidak bertanggung jawab (Weir, Yan and Kankanhalli, 2012). Merubah plaintext atau pesan asli menjadi ciphertext atau pesan bersandi merupakan pengertian dari proses enkripsi. Untuk menjalankan pesan yang sudah tersandi, seseorang harus memiliki key atau kunci. Sedangkan arti dari dekripsi adalah merubah kembali ciphertext menjadi plaintext. Kunci memiliki sifat rahasia yang hanya diketahui oleh pihak yang bersangkutan.

Sebagai infotmasi lebih lanjut, untuk mengurangi bahkan menghilangkan kecurigaan terhadap teknik kriptografi maka ada sebuah teknik yang bisa digunakan dalam penyembunyian pesan kedalam suatu media yang biasa disebut dengan steganografi. Pada steganografi, media yang digunakan untuk menyembunyikan pesan dapat berupa gambar, suara, teks, dan lain-lain. Terdapat perbedaan antara teknik kriptografi dengan teknik steganografi, yaitu pesan yang tersembunyi didalam sebuah media (*cover object)* tidak bisa terlihat secara kasat mata jika tidak meneliti dengan teliti bahwa terdapat data yang telah disembunyikan dalam pesan atau media tersebut. Dengan teknik ini tingkat keamanan data bisa meningkat, pengiriman data atau pesan media bisa tersampai ke penerima tanpa ada seseorang yang bisa menyadap pesan tersebut.

Teknik kriptogafi yang akan di implementasikan pada penelitian ini adalah teknik super enkripsi dengan menggabungkan dua teknik didalam kriptografi yaitu teknik subtitusi dan teknik transposisi. Menggunakan beaufort cipher dan transposisi kolom sebagai algoritmanya. Implementasi teknologi kriptografi pada aplikasi berbasis desktop dipilih karena banyak pengguna yang bekerja dengan komputer atau laptop sehingga data atau file bisa diamankan menggunakan aplikasi tersebut tanpa harus menggunakan koneksi internet. Dengan bahasa pemrogaman matlab pada makalah ini telah di implementasikan kriptografi kombinasi shift cipher dan vigenere cipher. Ukuran gambar yang cenderung kecil mendukung digunakannya aplikasi ini. Algoritma vigenere sendiri merupakan bagian dari polyalphabetic cipher dimana anggotanya antara lain vigenere cipher, autokey cipher dan beaufort cipher. *Polyalphabetic* cipher beroperasi dengan teknik mensubtitusi huruf abjad untuk melakukan enkripsi dan dekripsi. Subtitusi adalah penggantian setiap huruf pesan asli (*plaintext*) dengan karakter yang lain (Nasution *et al.*, 2017). Yang artinya, teknik subtitusi adalah salah satu teknik kriptografi simetris dimana cara kerjanya melakukan penggantian setiap karakter pesan asli (*plaintext*) dengan objek lain. Teknik ini menerapkan konsep korespondensi satu – satu untuk tiap karakter pesan asli (*plaintext*) yang disandikan. Algoritma yang menerapkan model substitusi tersebut adalah vigenere cipher. Untuk menambah keamanan data, maka vigenere cipher dikombinasikan dengan shift cipher yang merupakan model monoalphabeth cipher. Shift cipher menggunakan model enkripsi dengan pergeseran sejumlah kunci yang mirip dengan Caesar cipher (Rachmawanto and Sari, 2015) namun shift cipher lebih aman dibanding Caesar cipher.

2. METODE

2.1. VIGENERE CIPHER

Vigenere cipher ditemukan oleh Giovan Battista Bellaso pada tahun 1553 dan dikembangkan oleh Blaisede Vigenere karena menemukan kunci yang lebih aman yaitu autokey cipher. Menurut Stalling, Vigenere cipher adalah salah satu algoritma kriptografi yang sederhana (Damara Ardy *et al.*, 2018). Vigenere cipher menggunakan bujur sangkar vigenere yang diperoleh dari perhitungan Caesar Cipher. Pada abad ke 19, Vigenere cipher dipecahkan oleh Friedrich Kasiski dengan cara mengidentifikasi panjang kunci yang digunakan. Rumus vigenere dapat dilihat pada Persamaan 1 dan Persamaan 2.

$$C_i = (P_i + k_j) mod\ 26 \quad (1)$$
$$P_i = (C_i - k_j) mod\ 26 \quad (2)$$

Dimana :

C_i = nilai decimal dari karakter cipherteks ke i

P_i = nilai decimal dari karakter plainteks ke i

K_i = nilai decimal dari kunci ke I (diasumsukan bahwa panjang kunci antara A= 0, B = 1 ...., Z = 25).

Apabila nilai dekripsi negatif, maka nilai akan ditambah dengan 26 untuk mendapat pkainteks. Gambar 1 merupakan ilustrasi operasi Vigenere cipher pada media teks.

Gambar 1. Ilustrasi operasi Vigenere cipher pada media teks alfabeth

Menggunakan *tabula rectra*, Gambar 1 merngolustrasikan model enkripsi teks alfabeth menggunakan Vigenere cipher. Kolom *tabula recta* dibaca sebagai plainteks, sedangkan baris menandakan kunci yang digunakan (Bhateja and Kumar, 2014). panjang kunci akan mereplikasi sepanjang plainteks, sehingga semakin panjang plainteks maka akan semakin aman cipherteks yang dihasilkan.

2.2. SHIFT CIPHER

Shift cipher adalah salah satu bentuk monoalphabeth cipher selain Caesar cipher. Cara kerja shift cipher sama dengan Caesar cipher yaitu menggeser plainteks sejauh kunci yang ditetapkan (Rachmawanto and Sari, 2015). Pada Shift cipher, kunci yang digunakan umumnya 13 sehingga Shift cipher dinamakan sebagai Rot 13 atau rotasi 13. Maksimal pergeseran kunci pada shift cipher yaitu 26 (Sari *et al.*, 2016). Shift cipher sama dengan Caesar cipher yang menggunakan perhitungan modulo 26 sesuai pada Persamaan 3 dan Persamaan 4.

$$C = E(P) = (P + K) \bmod (26) \quad (3)$$

Sedangkan rumus enkripsi adalah sebagai berikut:

$$P = D(C) = (C - K) \bmod (26) \quad (4)$$

Dimana:
P = plainteks
C = cipherteks
E = enkripsi
D = dekripsi
K = kunci

3. HASIL DAN PEMBAHASAN

Skema penelitian pada makalah ini telah di lakukan dengan mengoperasikan shift cipher terlebih dahulu kemudian hasil enkripsi shift cipher di enkripsi kembali dengan vigenere cipher. Media yang digunakan pada makalah ini yaitu gambar *grayscale*. Evaluasi telah di lakukan dengan menghitung nilai *Peak Signal to Noise Ratio* (PSNR), *Normalized Cross Correlation* (NCC) (Winarno *et al.*, 2017) dan histogram. Menurut Sari (Sari *et al.*, 2017), PSNR dapat dirumuskan sesuai Persamaan (5) dan Persamaan 6.

$$MSE \quad \sum_{q=0}^{Q-1}\sum_{w=0}^{W-1}\sum_{e=0}^{E-1}\|c(q,w,e) \quad w(q,w,e)\|^2 \tag{5}$$

$$PSNR_{dB} = 10\,log_{10}\left(\frac{maxval^2}{MSE}\right) \tag{6}$$

Dimana:
Q,W = baris dan kolom gambar
E = jumlah layer gambar, untuk RGB yaitu 3 sedangkan garyscale yaitu 1
c(q,w,e) = ukuran gambar asli
w(q,w,e) = ukuran pesan
maxval yaitu 2_8-1.

Sedangkan rumus *Normalized Cross Correlation* (NCC) sesuai Persamaan (7).

$$NCC = \frac{C_{rs} \times R_{rs}}{C_{rs} \times C_{rs}} \tag{7}$$

Dimana:
C_{rs} = gambar hasil enkripsi
R_{rs} = gambar hasil dekripsi

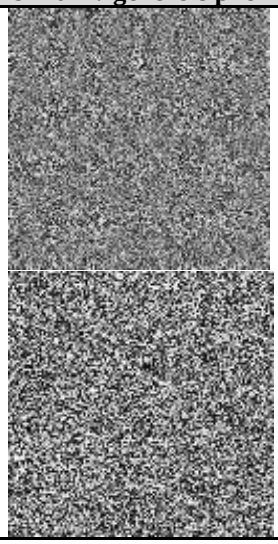
Uji coba diterapkan dengan coding dibawah ini

```
clc; clear all; close all;
prompt = 'Masukan kunci shift chiper :';
keyShif = input(prompt);
keyShif = mod(keyShif,256);
keyShif = uint8(keyShif);
%% Baca Citra
img=double(imread('lena.bmp'));
img=double(imread('pentagon.bmp'));
[m,n,o]=size(img);
figure(1)
imshow(uint8(img));
title('Original Image')
figure(2)
imhist(uint8(img))
title('Original Image Histogram')
%%Shif chiper pesan
imgR=reshape(img,[1,m*n]);
for i=1:m*n
    encShifCitra(i)=mod((imgR(i)+keyShif),256);
end
encShifCitraR=reshape(encShifCitra,[m,n]);
fprintf('\n The PSNR value after shif encryption image is %0.4f', psnr(encShifCitra,imgR));
fprintf('\n The Correlation Value after shif encryption image is %0.4f\n', corr2(img,encShifCitra));
```

Gambar 2. Potongan coding untuk implementasi

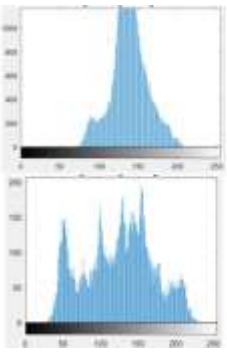
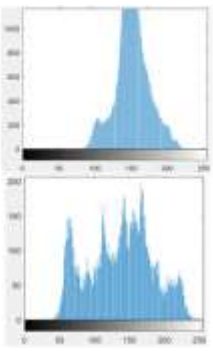
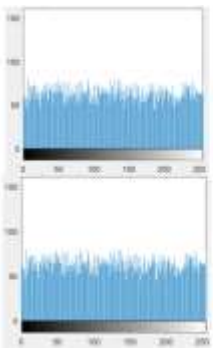
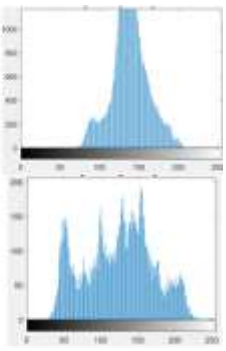
Berdasarkan uji coba yang telah dilakukans, terdapat perbedaan pada gambar asli dan gambar hasil dekripsi meskipun tidak dapat dibedakan secara visual sesuai Tabel 1. Adanya sedikit perbedaan menandakan proses kriptografi yang dilakukan telah berhasil, hal ini dihitung dengan PSNR. Adapun kunci yang digunakan pada proses enkripsi shift cipher yaitu 13. Sedangkan vigenere dioperasikan dengan file kunci yang sudah di olah sebelumnya dalam bentuk excel.

Tabel 1. Perbedaan gambar asli, gambar hasil enkripsi dan dekripsi

Gambar asli	Gambar hasil enkripsi shift cipher	Gambar hasil enkripsi shift + vigenere cipher	Gambar hasil dekripsi shift + vigenere
			

Sedangkan untuk perbedaan piksel secara visual, dapat dilihat menggunakan hasil histogram sesuai Tabel 2.

Tabel 2. Perbedaan gambar asli, gambar hasil enkripsi dan dekripsi

Histogram gambar asli	Histogram setelah enkripsi shift	Histogram setelah enkripsi shift + vigenere	Histogram gambar recovery
			

Pada Tabel 1 dapat di lihat pada gambar hasil enkripsi shift cipher yang tidak mengalami perubahan secara visual, sedangkan pada hasil enkripsi shift cipher dan vigenere cipher terlihat piksel yang teracak dan hancur sehingga tidak terlihat lagi bentuk gambar asli. Hasil ini dikategorikan sebagai bentuk enkripsi yang berhasil. Pada hasil gambar hasil dekripsi, dapat dilihat bahwa gambar enkripsi dapat di dekripsi kembali menjadi gambar asli seperti semula. Sedangkan pada Tabel 2, histogram setelah enkripsi shift cipher sedikit berbeda dengan histogram gambar asli. Model nilai piksel teracak ditunjukkan pada histogram hasil enkripsi kombinasi shift cipher dan vigenere cipher. Gambar hasil dekripsi

menunjukkan histogram yang sama dengan gambar asli. Representasi nilai PSNR dan nilai NCC dapat di lihat pada Tabel 3 berikut.

Tabel 3. Representasi PSNR dan NCC pada hasil enkripsi dan dekripsi gambar

Gambar asli	PSNR Enkripsi		PSNR dekripsi		NCC Enkripsi		NCC Dekripsi	
	Shift	Shift + Vigenere	Shift	Shift + Vigenere	Shift	Shift + Vigenere	Shift	Shift + Vigenere
Pentagon	-22,2789	-37,8892	-22,2789	inf	1	-0,0044	1	1
Lena	-22,2789	-22,2789	-38,8866	inf	1	-0,0127	1	1

4. KESIMPULAN

Berdasarkan uji coba yang telah dilakukan dengan menerapkan kombinasi shift cipher dan vigenere cipher pada media gambar *grayscale*, di didapatkan hasil sebagai berikut:

(1) Histogram gambar asli dan histogram gambar dekripsi tidak berbeda, hal ini menunjukkan proses enkripsi dan dekripsi berhasil. Pada proses enkripsi shift dan vigenere telah dihasilkan histogram dengan nilai piksel acak yang ditandai dengan rata-rata nilai piksel yang hampir sama.

(2) Uji coba perhitungan PSNR pada shift cipher kunci=13 dan vigenere cipher menggunakan file kunci excel, di dapat hasil PSNR kurang dari 0 yang menyatakan hasil enkripsi gambar sama sekali tidak dapat dibaca atau di kenali secara visual. Pada proses dekripsi, didapatkan nilai PSNR *infinitive (inf)* yang artinya piksel gambar tidak berubah sesuai gambar aslinya.

(3) Nilai NCC yang di dapat pada shift cipher daja maupun kombinasi shift cipher dan vigenere cipher menghasilkan nilai rentang NCC dalam standard yaitu antara -0 sampai 1.

DAFTAR PUSTAKA

Bhateja, A. and Kumar, S. (2014) 'Genetic Algorithm with elitism for cryptanalysis of Vigenere cipher', *2014 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*. IEEE, pp. 373–377. doi: 10.1109/ICICICT.2014.6781311.

Damara Ardy, R. *et al.* (2018) 'Digital image signature using triple protection cryptosystem (RSA, Vigenere, and MD5)', in *Proceeding of 2017 International Conference on Smart Cities, Automation and Intelligent Computing Systems, ICON-SONICS 2017*. doi: 10.1109/ICON-SONICS.2017.8267827.

Hemalatha, S., Acharya, U. D. and Renuka, A. (2016) 'Audio data hiding technique using integer wavelet transform', *International Journal of Electronic Security and Digital Forensics*. Elsevier Masson SAS, 8(2), p. 131. doi: 10.1504/IJESDF.2016.075586.

Nasution, S. D. *et al.* (2017) 'Data Security Using Vigenere Cipher and Goldbach Codes Algorithm', *International Journal of Engineering Research & Technology (IJERT)*, 6(1), pp. 360–363.

Rachmawanto, E. H. and Sari, C. A. (2015) 'Keamanan File Menggunakan Teknik Kriptografi Shift Cipher', *Techno.COM*, 14(4), pp. 329–335.

Sari, C. *et al.* (2016) 'Optimasi penyandian file menggunakan kriptografi shift cipher', in *Seminar Multi Disiplin Ilmu Unisbank (SENDI_U) ke-2 Semarang*. UNISBANK.

Sari, W. S. *et al.* (2017) 'A Good Performance OTP Encryption Image based on DCT-DWT Steganography', *TELKOMNIKA*, 15(4), pp. 1987–1995. doi: 10.12928/TELKOMNIKA.v15i4.5883.

Weir, J., Yan, W. Q. and Kankanhalli, M. S. (2012) 'Image Hatching for Visual Cryptography', *ACM Transactions on Multimedia Computing, Communications and Applications*, 8(S2). doi: 10.1109/IMVIP.2009.18.

Winarno, A. *et al.* (2017) 'Image Watermarking using Low Wavelet Subband based on 8x8 Sub-block DCT', in *International Seminar on Application for Technology of Information and Communication*, pp. 11–15.