KOMBINASI ALGORITMA ONE TIME PAD DAN CHAOTIC SEQUENCE DALAM OPTIMASI ENKRIPSI GAMBAR

De Rosal Ignatius Moses Setiadi
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Dian Nuswantoro Semarang
Email: moses@dsn.dinus.ac.id

Eko Hari Rachmawanto
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Dian Nuswantoro Semarang
Email: eko.hari@dsn.dinus.ac.id

Christy Atika Sari
Fakultas Ilmu Komputer, Program Studi Teknik Informatika
Universitas Dian Nuswantoro Semarang
Email: atika.sari@dsn.dinus.ac.id

ABSTRAK

Pada makalah ini, kriptografi dipilih sebagai teknik untuk mengamankan data, khusunya data gambar. Teknik kriptografi mempunyai kelebihan yaitu menyamarkan pesan yang termuat pada media tertentu, sehingga orang lain akan mengetahui pada media tersebut terdapat suatu pesan rahasia. algoritma yang terpilih untuk melakukan proses enkripsi dan dekripsi yaitu One Time Pad (OTP). Algoritma tersebut kuat dan aman apabila memenuhi kriteria pengoerasian, salah satunya yaitu mengacak kunci yang akan digunakan secara random dan tidak menggunakan kunci tersebut untuk operasi lain. Hal ini tentu menyulitkan ketika panjang kunci yang dimaksud harus sama panjang dengan data induk yang akan dienkripsi, sehingga perlu adanya suatu algoritma lain yang dapat membantu mengacak kunci. Dalam makalah ini dipilih Chaotic Sequeces Generator. Hasil eksperimen telah menunjukkan bahwa penggunakan OTP saja dinilai kurang efisien, sedangkan hasil eksperimen pada enkripsi dan dekripsi gambar menggunakan OTP-Chaotic Sequences mempunyai nilai PSNR lebih tinggi dibanding dengan OTP yang telah dilakukan oleh paper pembanding. Sedangkan lama waktu proses hampir sama antara OTP dengan OTP-Chaotic Squences. Nilai PSNR tertinggi yang dihasilkan melalui algoritma OTP pada paper pembanding yaitu 8,9 dB pada gambar peppers.bmp, sedangkan algoritma kombinasi yang telah dilakukan dengan OTP-Chaotic Sequences yaitu 8,4 dB. Sedangkan pada gambar lena.bmp, pada paper pembanding diketahui nilai PSNR yang didapat yaitu 9,26 dB, sedangkan pada eksperimen dengan kombinasi OTP-Chaotic Sequences yaitu 9,2 dB. Pada eksperimen tersebut, gambar yang telah di uji coba sebanyak 5 gambar grayscale berukuran 256x256 piksel.

Kata kunci: OTP, Chaotic Squences, kriptografi, gambar grayscale, PSNR.

ABSTRACT

In this paper, cryptography is chosen as a technique for securing data, especially image data. Cryptography techniques have advantages that disguise the message contained on certain media so that others will know the media there is a secret message. The algorithm chosen to perform the encryption and decryption process is One Time Pad (OTP). The algorithm is robust and secure when it meets the criteria of coordination, one of which is to scramble the key to be used randomly and not to use the key for another operation. This is certainly difficult when the key length should be the same length as the parent data to be encrypted, so there needs to be another algorithm that can help randomize the key. In this paper selected Chaotic Sequence Generator. Experimental results have shown that OTP use alone is considered inefficient, while experimental results on image encryption and decryption using OTP-Chaotic Sequences have higher PSNR valuescompared to OTP that have been done by comparative papers. While the processing time is almost the same between OTP with OTP-Chaotic Sequences. The highest PSNR value generated through the OTP algorithm in the comparative paper is 8.9 dB in the peppers.bmp image, while our combined algorithm with OTP-Chaotic Sequences is 8.4 dB. While in the picture lena.bmp, in the comparative paper known PSNR value obtained is 9.26 dB, while the experiment with our OTP-Chaotic Sequences combination of 9.2 dB. In the experiment, the images we have tested are 5 grayscale images measuring 256x256 pixels.

Keywords: *OTP, Chaotic Sequences, cryptography, grayscale images, PSNR.*

1. PENDAHULUAN

Peran teknik *data hiding* dalam mengamankan data dirasa sangat berimbas positif untuk menekan keinginan pihak yang tidak berkepentingan untuk melakukan tindakan *hacking* maupun *cracking*. Beberapa teknik data hiding menurut Setiadi terdapat tiga buah teknik yang telah digunakan oleh berbagai peneliti antara lain watermarking, steganografi dan kriptografi [1]. Masing-masing teknik tersebut memiliki keunggulan dan kelemahan, misalnya watermarking yang biasanya sering digunakan untuk melakukan *copyright protection* dan data authentication, steganografi digunakan untuk berkomunikasi secara rahasia sedangkan kriptografi digunakan untuk proteksi file. Menurut Cheddad dan Sari, dalam penelitiannya menyebutkan beragam kriteria untuk membedakan tiga metode tersebut[2][3], seperti tampak pada Tabel 1 berikut.

Tabel 1. Perbedaan steganografi,watermarking dan kriptografi [2]

Kriteria	*Steganografi*	*Watermarking*	*Kriptografi*
Media induk yang digunakan	*Berbagai data digital*	*Berbagai file*	*Berbagai file*
Data rahasia	*payload*	*File watermark*	*Plainteks*
Kunci	*Optional*	*Tidak perlu*	*Optional*
Model deteksi	*Blind detection*	*Memerlukan file induk*	*Blind detection*
Jenis serangan	*Steganalisis*	*Image processing*	*Kriptanalis*
Dapat dideteksi jika	*Terdeteksi secara kasat mata*	*Di replace*	*Di de-cipher*
Tujuan operasi	*Komunikasi rahasia*	*Copyright protection*	*Proteksi data*
Aspek yang dicapai	*Aspek kapasitas maupun imperceptibility*	*Aspek robustness maupun imperceptibility*	*Aspek robustness*

Berdasarkan Tabel 1, masing-masing metode digunakan untuk tujuan tertentu dengan media yang sedikit berbeda. Di sisi lain, baik watermarking, steganografi maupun kriptografi mempunyai kesamaan yaitu penggunaan suatu algoritma untuk melakukan proses *data hiding*. Algoritma tersebut semakin berkembang sesuai dengan ragam media dan kombinasi terhadap algoritma yang telah diteliti. Dalam karya ilmiah ini dipilih kriptografi sebagai metode *data hiding* karena mempunyai tujuan untuk proteksi terhadap data. Berdasarkan *state of the art* mengenai kriptografi pada media gambar pada Tabel 2, kriptografi telah dilakukan dalam berbagai media dan algoritma. Beberapa kombinasi algoritma misalnya kombinasi antara steganografi dan watermarking, watermarking dan kriptografi atau steganografi dan kriptografi. Pada teknik steganografi biasanya digunakan algoritma spasial domain yaitu *Least Significant Bit* (LSB) dan *End Of File* (EOF), sedangkan pada teknik watermarking dapat menggunakan spasial maupun frekuensi domain antara lain LSB, *Discrete Cosine Transform* (DCT), *Discrete Wavelet Transform* (DWT), *Slantlet Transform* (SLT), atau *Tcebichef Transform* (TT). Dalam kasus tertentu, terdapat pula peneliti yang menggunaan fungsi invers, dekomposisi seperti pada algoritma *Inversebit*, *bitshifting*, *Singular Value Decompsition* (SVD). Pada teknik kriptografi, dapat digunakan bentuk operasi stream atau blok cipher yang terbagi dalam model kriptografi klasik maupun modern seperti *Blowfish, Vernam Cipher*, *One Time Pad* (OTP), *ShiftCipher*, *Data Encryption Standard* (DES) dan masih banyak algoritma lain yang akan dipaparkan lebih lanjut pada Gambar 1.

Tabel 2. *State of the art data hiding*

Nama Peneliti	*Tahun*	*Media*	*Algoritma*									
			Watermarking		*Steganografi*			*Kriptografi*				
			DCT	*SLT*	*DCT*	*SLT*	*DCT*	*EOF*	*VC*	*BL*	*SC*	*BS*	*OTP*
MA Faizal	*2012*	*Gambar*	*	*									
Rachmawanto	*2013*	*Gambar*			*		*						
Rachmawanto EH	*2014*	*Gambar*			*		*						
Sari CA	*2015*	*Teks*									*		
Rachmawanto EH	*2015*	*Multimedia*						*					
Astuti YP	*2016*	*Password*								*			
Sari CA	*2016*	*Teks*									*		
Rachmawanto EH	*2016*	*All*							*				
Astuti YP	*2016*	*Password*								*			
Sari CA	*2016*	*Gambar*							*			*	

Nama Peneliti	*Tahun*	*Media*	*Algoritma*							
			Watermarking		*Steganografi*			*Kriptografi*		
			DCT	*SLT*	*DCT*	*SLT*	*DCT EOF*	*VC*	*BL*	*SC*	*BS*	*OTP*
Rachmawanto EH	*2016*	*Gambar*	*	*								
Setiadi	*2017*	*Gambar*					*					*

Catatan:
DCT : *Discrete Cossine Transform*
SLT : *Slantlet Transform*
EOF : *End of File*
VC : *Vernam Cipher*
BL : *Blowfish*
SC : *Shift Cipher*
BS : *Bit Shiffting*
OTP : *One Time Pad*

Bedasarkan Tabel 2, diketahui bahwa penulis telah melakukan beberapa penelitian pendahulu yang berhubungan dengan topik data hiding. Pada penelitian sebelumnya, kriptografi *One Time Pad* telah kombinasikan dengan steganografi DCT. Pada penelitian tersebut digunakan sejumlah media gambar *grayscale* dengan format *.bmp dan telah diuji menggunakan *Peak Signal to Noise Ratio* (PSNR) dengan perolehan nilai PSNR tertinggi yaitu 51,33 dB dan *Normalized Cross Correlation* (NCC) dengan dua macam serangan yaitu *JPEG Compression* dan *median filter*. Rata-rata perolehan NCC setelah mengalami serangan *JPEG ompression* yaitu 0,9 dan *median filtering* yaitu 0,8.

Dalam penelitian ini telah dipilih algoritma *One Time Pad* (OTP) dan *Chaotic Squence* (CS). Hal ini dilakukan untuk mengetahui performa dari OTP-CS dalam melakukan enkripsi dekripsi pada gambar. Untuk lebih jelas mengenai algoritmaa yang dipilih, dapat dibaca pada point 2.

2. METODOLOGI PENELITIAN

2.1 Kriptografi One Time Pad (OTP)

Pada Tabel 2 telah dijelaskan mengenai *state of the* art dengan bebrapa algoritma salah satunya yaitu *One Time Pad*. OTP merupakan pengembangan dari *Vernam Cipher*. Algoritma OTP merupakan bagian dari block cipher dalam kriptografi klasik menggunakan operasi XOR. OTP akan mejadi algoritm yang tidakterpecahkan apabila memenuhi syarat sebagai berikut:

a) Panjang kunci harus sama dengan panjang plainteks
b) Kunci yang digunakan harus acak dan hanya boleh digunakan satu kali saja

Untuk lebih jelas, OTP diperasikan menggunakan Persamaan (1) untuk proses enkripsi dan Persamaan (2) untuk proses dekripsi berikut ini:

$$E(x) = (P(x) + K(x)) \bmod 26 \quad (1)$$

$$D(x) = (C(x) + K(x)) \bmod 26 \quad (2)$$

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

OTP telah digunakan oleh Setiadi pada tahun 2017[1], dimana penelitian tersebut telah dilaksanakan dengan mengkombinasikan algoritma DCT pada teknik steganografi. Hasil enkripsi pada 10 gambar yang digunakan menunjukkan bahwa nilai PSNR tertinggi yang didapat yaitu 51, 33 dB dan nilai NCC dari semua gambar yaitu 1. Penelitian lain yang telah dilaksanakan oleh Upadhyay dan Nene pada tahun 2016[4], menggunakan *One Time Pad* dengan Quantum Superposisi dan proses penyisipan yang dilakukan dengan lebih cepat. Pada ranah sistem terdistribusi[5], OTP telah diimplementasikan dalam mengamankan data pesan dengan MPICH2 dan VAN MPICH2 oleh Rekhate dkk.Sedangkan pada karya

ilmiah ini, terdaat kontribusi terhadap hasil implementasi OTP yang dikombinasikan dengan *Chaotic Sequence* yang bertujuan untuk menghasilkan model enkripsi yang lebih baik.

2.2 Chaotic Sequence

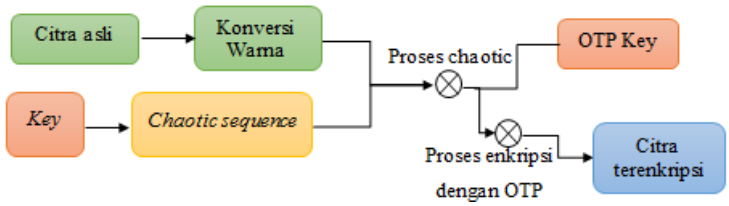
Chaotic Sequence atau merupakan bentuk dari PN *Sequence Generator* merupakan salah satu fungsi dalam matlab yang menghasilkan urutan angka biner acak. *Chaotic Sequence* menggunakan *linear-feedback shift register (LFSR)*. LFSR diimplementasikan dengan konfigurasi generator *shift register* sederhana (SSRG atau Fibonacci). Urutan PN dapat digunakan dalam pengacakan dan descrambler pseudorandom. Hal ini juga dapat digunakan dalam sistem *direct sequence-spread-spectrum*.

Pada kriptografi citra penggunaan teori pengacakan seperti *chaotic sequence* sudah dilakukan pada beberapa penelitian seperti[6]. Pada penelitian tersebut dijabarkan mengenai teori pengacakan berfungsi untuk melakukan korelasi dengan *copyright* yang akan disisipkan sehingga menghasilkan nilai yang akan disisipkan pada citra digital. Korelasi tersebut biasanya menggunakan operator xor dalam mengapplikasikannya pada proses penyisipan *copyright*. Listing program menggunakan *chaotic sequence* yang dilakukan pada peneliitan ini dapat dilihat sebagai berikut:

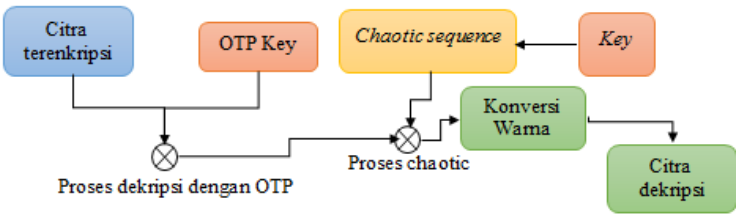
```
sd1 =[0 0 0 0 1];
PN1=[];
for j=1:G
    PN1=[PN1 sd1(5)];
    if sd1(1)==sd1(4)
        temp1=0;
    else temp1=1;
    end
    sd1(1)=sd1(2);
    sd1(2)=sd1(3);
    sd1(3)=sd1(4);
    sd1(4)=sd1(5);
    sd1(5)=temp1;
end
```

3. HASIL DAN PEMBAHASAN

Pada penelitian ini proses dekripsi dan enkripsi dapat dilihat pada Gambar 1 dan Gambar 2.



Gambar 1. Usulan Skema Proses Enkripsi Citra



Gambar 2. Usulan Skema Proses Dekripsi Citra

Sedangkan gambar yang digunakan untuk penelitian yaitu 5 gambar *grayscale* dengan ukuran 512x512 piksel.

(a) (b) (c) (d) (e)

Gambar 3. Data Gambar Untuk Eksperimen: (a) Baboon, (b) Cameraman, (c) Girl, (d) Lena, (e) Peppers

Pada penelitian ini digunakan 3 buah alat evaluasi yaitu *Mean Square Error* (MSE), *Peak Signal to Noise Ratio* (PSNR), *Bit Error Ratio* (BER) dan *Core Corrleation* (CC). Untuk MSE dan PSNR, perhitungan dilakukan berdasarkan Persamaan 1 dan Persamaan 2. Masing-masing persamaan dapat dijabarkan sebagai berikut.

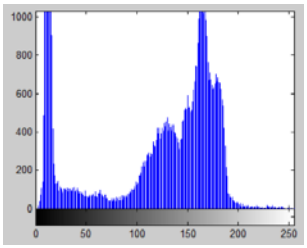
$$MSE = \sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\sum_{k=0}^{8}\left[g(i,j,k) - f(i,j,k)\right]^2 \quad (1)$$

Dimana:
M, N = jumlah bari dan kolom dalam piksel
g(i,j,k) = input image
f(i,j,k) = output image

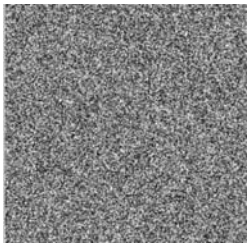
$$PSNR_{dB} = 10\log 10\left(\frac{255^2}{\sqrt{MSE}}\right) \quad (2)$$

Di bawah ini merupakan hasil enkripsi menggunakan OTP-CS pada gambar grayscale.

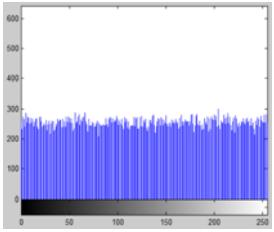
Cameraman.bmp (gambar asli)



Histogram gambar cameraman.bmp sebelum enkripsi



Hasil enkripsi gambar cameraman.bmp



Histogram gambar cameraman.bmp setelah proses enkripsi

Hasil dekripsi pada gambar cameraman.bmp

Gambar 4. Hasil Proses Enkripsi Dan Dekripsi Pada Gambar Cameraman.bmp

Selanjutnya proses enkripsi dan dekripsi telah diuji coba menggunakan ke empat gambar yang lain menggunakan MSE dan PSNR seperti tampak pada Tabel 1 berikut.

Tabel 3. Hasil proses enkripsi dengan OTP-CS

Nama Gambar	*Ukuran Gambar*	*OTP*		*OTP-PN*	
		MSE	*PSNR*	*MSE*	*PSNR*
Cameraman		*9344.3275*	*8.4253*	*9338.8778*	*8.4279*
Lena		*7664.3119*	*9.2861*	*7728.9811*	*9.2496*
Babbon	*256x256 piksel*	*6889.3729*	*9.7490*	*6939.8648*	*9.7173*
Fishingboat		*7577.5455*	*9.3355*	*7570.7215*	*9.3394*
Peppers		*8348.0128*	*8.9150*	*8294.9062*	*8.9427*

Berdasarkan Tabel 3, eksperimen dilakukan menggunakan dua buah alat evaluasi yaitu MSE dan PSNR. Pada percobaan proses enkripsi menggunakan OTP dan OTP yang telah dikombinasi dengan PN, dapat dilihat bahwa nilai PSNR terbaik yang telah diperoleh mendekati nilai 0 yang berarti proses enkripsi berhasil. Nilai PSNR yang rendah membutkikan bahwa proses enkripsi telah dilakukan dengan baik. Nilai PSNR terbaik yang diperoleh yaitu 8.4253 dB menggunakan OTP, sedangkan menggunakan OTP-PN menghasilkan PSNR terbaik yaitu 8.4279 dB. Nilai PSNR fishingboat dan peppers menggunakan OTP lebih baik dibanding OTP-PN, sedangkan tiga gambar yang lain membuktikan bahwa OTP-PN menghasilkan nilai PSNR lebih baik.

4. KESIMPULAN

Berdasarkan eksperimen yang telah dilakukan pada 5 buah gambar *grayscale* berukuran 256x256 piksel berformat .bmp, dapat diambil kesimpulan bahwa proses enkripsi data menggunakan algoritma OTP-PN menghasilkan nilai PSNR yang lebih tinggi dibandingnkan OTP pada beberapa gambar. PSNR tertinggi dari optimasi OTP menggunakan PN yaitu 8.4279 dB sedangkan MSE terbaik yaitu 9338.8778. hasil enkripsi ditandai dengan keberhasilan proses dekripsi gambar melalui histogram. Histogram proses enkripsi dan gambar hasil dekripsi menggambarkan nilai PSNR dan MSE yang telah diperoleh. Untuk penelitian lanjutan, dapat digunakan algoritma optimasi lain sehingga payload gambar dapat lebih maksimal.

UCAPAN TERIMA KASIH

Karya ilmiah ini merupakian salah satu luaran dari penelitian internal yang dibiayai oleh Udinus pada tahun 2017 sesuai nomor SK Penelitian Nomor 035/A.38.04/UDN-09/III/2017.

DAFTAR PUSTAKA

[1] D.R.I.M, Setiadi, E. H. Rachmawanto, and C. A. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *J. Appl. Intell. Syst.*, vol. 2, no. 1, pp. 1–11, 2017.

[2] A. Cheddad, J. Condell, K. Curran, and P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, Mar. 2010.

[3] 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.

[4] G. Upadhyay and M. J. Nene, "One Time Pad Generation Using Quantum Superposition States," in *International Conference On Recent Trends In Electronics Information Communication Technology, May 20-21, 2016, India*, 2016, no. 1, pp. 1882–1886.

[5] V. Rekhate, "Secure and Efficient Message Passing in Distributed Systems using One-Time Pad," in *2016 International Conference on Computing, Analytics and Security Trends (CAST) College of Engineering Pune, India. Dec 19-21, 2016 Secure*, 2016, pp. 393–397.

[6] C. Jeyamala, S. GopiGanesh, and G. S. Raman, "An image encryption scheme based on one time pads — A chaotic approach," in *2010 Second International conference on Computing, Communication and Networking Technologies*, 2010, pp. 1–6.