TIN: Terapan Informatika Nusantara
Vol 1, No 8, Januari 2021, Hal 390-394
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Implementasi Algoritma Playfair Dan Discrete Wavelet Transform Dalam Penyisipan Teks Pada Citra Digital

Indra Setiawan

Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: indrasetiawan3iv7@gmail.com

Abstrak−Kriptografi adalah teknik untuk menyandikan pesan dan watermarking adalah teknik untuk menyembunyikan pesan pada suatu media digital. Kombinasi ini digunakan sebagai suatu sistem untuk mengamankan pesan karena pesan mengalami dua proses pengamanan, yaitu enkripsi dan penyisipan kedalam citra digital. Citra yang digunakan sebagai cover objec adalah citra berformat JPEG. Karakter yang digunakan pada proses enkripsi adalah penggunaan tabel 5x5. Pada proses penyisipan ditambahkan bit bit pesan yang telah di ubah kedalam bentuk biner, dan disisipi pada akhir biner citra. Hasil dari skripsi ini adalah pesan yang akan di sisipin teks kedalam citra akan di enkripsi terlebih dahulu dan dirubah kedalam biner, tanpa merubah bentuk dari sebuah citra.

Kata Kunci: Citra Digital; Kriptografi; Playfair; Watermarking; Discrete Wavelet Transform (DWT)

Abstract−Cryptography is a technique for encoding messages and watermarking is a technique for hiding messages on a digital media. This combination is used as a system to secure messages because messages undergo two security processes, namely encryption and insertion into a digital image. The image used as the cover object is a JPEG image format. The characters used in the encryption process are the use of the 5x5 table. In the insertion process, message bits are added which have been converted into binary form, and are inserted at the end of the binary image. The result of this thesis is that the message that will be inserted in the text into the image will be encrypted first and converted into binary, without changing the shape of an image.

Keywords: Digital Image; Cryptography; Playfair; Watermarking; Discrete Wavelet Transform (DWT)

1. PENDAHULUAN

Proses penyisipan pesan atau gambar dalam suatu gambar pada dasarnya digunakan untuk memberikan sebuah tanda atau lisensi bahwa gambar tersebut merupakan milik seseorang atau bisa juga untuk mengidentifikasi kepemilikan atas gambar tersebut. Pada kriptografi dengan media citra (*image*), pengirim pesan melakukan proses penyisipan (*embedding*) pesan yang hendak dikirim secara rahasia ke dalam citra sebagai tempat menyimpannya yang disebut *cover image*, dengan menggunakan kunci tertentu, sehingga dihasilkan citra dengan pesan yang tersembunyi di dalamnya yang disebut *stego image*.

DWT (*Discrete wavelet transform)* merupakan salah satu kakas yang banyak digunakan dalam teknik *blind watermarking* dan *escrow watermarking* dengan *domain transform*. *Watermarking* yang berbasis *wavelet* adalah pendekatan yang populer karena kekuatannya melawan *malicious attack*. *Transformasi wavelet diskrit/Discrete wavelet transform* membagi sebuah dimensi sinyal menjadi dua bagian, yaitu frekuensi tinggi (*highpass filter)* dan frekuensi rendah (*lowpass filter)*, biasa disebut dengan dekomposisi. Hasil proses dekomposisi adalah koefisien *Discrete wavelet transform* (DWT) yang terbagi dalam rentang frekuensi (*subband)* dari citra asli.

Kombinasi antara kriptografi dan *waterwarking* dapat dilakukan untuk lebih meningkatkan keamanan pada pesan yang hendak disembunyikan. Pesan teks yang hendak disembunyikan, dienkripsi terlebih dahulu dengan teknik kriptografi, setelah *ciphertext* dihasilkan, kemudian *ciphertext* disisipkan pada *file* gambar dengan teknik *Watermarking*. Hal ini dilakukan agar pesan teks yang telah dienkripsi tidak menimbulkan kecurigaan pada orang banyak saat melihat *ciphertext* dari pesan teks yang dihasilkan. Kecurigaan yang dimaksud adalah susunan huruf yang tidak memiliki arti pada *ciphertext* akan mengundang orang untuk berfikir bahwa ada pesan rahasia dibalik pada susunan huruf tersebut.

Dalam masalah perkembangan teknologi lainnya penulis ingin menguji suatu sistem untuk penyisipan pesan terenkripsi pada suatu citra. Wadah penampung untuk teks adalah gambar. Dalam enkripsi pesan menggunakan algoritma *Playfair* dengan teknik manual. Sedangkan untuk citra, teks akan dimasukkan ke dalam citra tanpa merubah bentuk asli citra. Hasil dari pengujian ini adalah gambar tersisipi teks terenkripsi tanpa merubah bentuk gambar.

2. METODOLOGI PENELITIAN

2.1 Implementasi

Implementasi berasal dari bahasa inggris yaitu *to* implementasi yang berarti mengimplementasikan. Implementasi merupakan penyediaan sarana untuk melaksanakan sesuatu yang menimbulkan dampak atau akibat terhadap sesuatu. Sesuatu yang dilakukan untuk menimbulkan dampak atau akibat itu dapat berupa undang-undang, peraturan pemerintah, keputusan peradilan dan kebijakan yang di buat oleh lembaga-lembaga pemerintah dalam kehidupan kenegaraan. “implementasi bermuara pada aktivitas, tindakan, atau adanya mekanisme suatu sistem. implementasi bukan sekedar aktivitas, tetapi suatu kegiatan yang terencana dan untuk mencapai tujuan kegiatan”(Setyaningsih, 2015).

TIN: Terapan Informatika Nusantara
Vol 1, No 8, Januari 2021, Hal 390-394
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

2.2 Algoritma Playfair Cipher

Cipher ini mengenkripsi pasangan huruf (biagram atau diagraf), bukan huruf tunggal seperti pada *cipher* klasik lainnya. Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf di dalam *ciphertext* menjadi datar (flat)(Putera, Siahaan, Mesran, & Solihin, 2018).

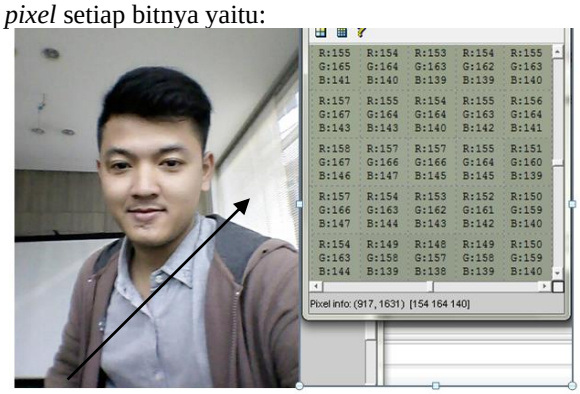
2.3 Keamanan Algoritma *Playfair*

Algoritma dekripsi kebalikan dari algoritma enkripsi. Caranya, untuk setiap pasangan huruf *ciphertext*, tentukan titik sudut empat persegi panjang yang terbentuk dari pasangan huruf tersebut. Dua huruf titik sudut menyatakan pasangan huruf *ciphertext*, sedangkan dua huruf pada titik sudut yang lain menyatakan pasangan huruf *plainteks*nya. Urutan huruf pada pasangan *plainteks* tersebut mengikuti arah empat persegi panjang yang dibentuk oleh pasangan huruf *ciphertext*.

Sayangnya ukuran poligram didalam *playfair cipher* tidak cukup besar. Hanya dua huruf sehingga *playfair chiper* tidak aman. Meskipun *playfair cipher* sulit dipecahkan dengan analisis frekuensi relatif huruf-huruf, namun ia dapat dipecahkan dengan analisis frekuensi kemunculan pasangan huruf, misalnya pasangan huruf TH dan HE paling sering muncul. Dengan menggunakan tabel frekuensi kemunculan pasangan huruf di dalam bahasa inggris dan *ciphertext* yang cukup banyak, *playfair* dapat dipecahkan(Arius, 2008; Ariyus & Dony, 2006; Munir, 2008).

3. HASIL DAN PEMBAHASAN

Strategi penyisipan citra ke dalam media citra yang digunakan adalah dengan metode *Discrete Wavelet Transform* (DWT). Di mana setiap bit data citra akan digantikan dengan bit paling rendah di dalam media citra. Langkah pertama yang dilakukan adalah mencari nilai RGB asli pada setiap bit citra. Adapun rumus yang dipakai untuk mencari RGB, berikut contoh gambar citra dan *pixel* setiap bitnya yaitu:



Gambar 1. Citra R, G, B, Asli dan nilai *Pixel* setiap bitnya.

Pada citra warna di atas akan dilakukan transformasi ke citra *grayscale* dengan cara menghitung rata-rata elemen warna *Red*, *Green*, *Blue*. Secara matematis perhitungannya adalah sebagai berikut.

$$f_o(X,Y) = \frac{f_i^R(X,Y) + f_i^G(X,Y) + f_i^B(X,Y)}{3}$$

Dari hasil gambar dan nilai *pixel* R,G,B di atas akan dirubah kebentuk *pixel grayscale.* Perhitungan fungsi negasi dilakukan seperti berikut: Setiap titik yang terletak di posisi (X,Y), nilai-nilai komponen *Red*, *Green* dan *Blue* ditambahkan, kemudian hasilnya dibagi 3.

a. $f_o = \frac{155+165+141}{3} = 153{,}67$
b. $f_o = \frac{154+164+140}{3} = 152{,}67$
c. $f_o = \frac{153+163+139}{3} = 151{,}67$
d. $f_o = \frac{154+162+139}{3} = 151{,}67$
e. $f_o = \frac{155+163+140}{3} = 152{,}67$
f. $f_1 = \frac{157+167+143}{3} = 155{,}67$
g. $f_1 = \frac{155+164+143}{3} = 154$
h. $f_1 = \frac{154+164+140}{3} = 152{,}67$
i. $f_1 = \frac{155+163+142}{3} = 153{,}33$
j. $f_1 = \frac{156+164+141}{3} = 153{,}67$
k. $f_o = \frac{158+167+146}{3} = 157$
l. $f_o = \frac{157+166+147}{3} = 156{,}67$
m. $f_o = \frac{157+166+145}{3} = 156$
n. $f_o = \frac{155+164+145}{3} = 154{,}67$
o. $f_o = \frac{151+160+139}{3} = 150$
s. $f_1 = \frac{152+161+142}{3} = 151{,}67$
t. $f_1 = \frac{150+159+140}{3} = 149{,}67$
u. $f_1 = \frac{154+163+144}{3} = 153{,}67$
f. $f_1 = \frac{149+158+139}{3} = 148{,}67$
w. $f_1 = \frac{148+157+138}{3} = 147{,}67$

TIN: Terapan Informatika Nusantara
Vol 1, No 8, Januari 2021, Hal 390-394
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

p. $f_o = \frac{157+166+147}{3} = 156{,}67$
q. $f_o = \frac{154+163+144}{3} = 153{,}67$
r. $f_o = \frac{153+162+143}{3} = 152{,}67$
x. $f_1 = \frac{149+158+139}{3} = 148{,}67$
y. $f_1 = \frac{150+159+140}{3} = 149{,}67$

Maka hasil *pixel* citra warna *Red,Green* dan *Blue* setelah dirubah ke citra *grayscale* maka hasil citra *grayscale* dapat dilihat pada tabel di bawah ini.

Tabel 1. Citra *Grayscale*

153.67	**152.67**	**151.67**	**151.67**	**152.67**
155.67	154.00	152.67	153.33	153.67
157.00	156.67	156.00	154.67	150.00
156.67	153.67	152.67	151.67	149.67
153.67	148.67	147.67	148.67	149.67

Pada proses penerapan algoritma DWT pada citra 2 dimensi di atas setelah mendapatkan nilai R,G,B maka dekomposisi perataan dan pengurangan sama dengan proses pada citra 1 dimensi. Hanya saja proses dekomposisi dilakukan dalam 2 tahap, yaitu tahap pertama proses dekomposisi dilakukan pada seluruh baris, kemudian tahap ke dua pada hasil tahap pertama dilakukan proses dekomposisi dalam arah kolom. Maka dari hasil nilai citra *grayscale* di atas dapat diterapkan untuk algoritma DWT 2 dimensi seperti berikut ini:

153.67	152.67	151.67	151.67
155.67	154.00	152.67	153.33
157.00	156.67	156.00	154.67
156.67	153.67	152.67	151.67
153.67	148.67	147.67	148.67

(a) Citra Asli Grayscale

153,17	151,67	0,50	0,00
154,84	153,00	0,83	-0,33
156,84	155,34	0,17	0,67
155,17	152,17	1,50	0,50
151,17	148,17	2,50	-0,50

(b) Hasil Dekomposisi

Baris 1 : [(153.67+152.67)/2 (151.67+151.67)/2 (153.67-152.67)/2 (151.67-151.67)/2] = [153,17 151,67 0,50 0,00]
Baris 2 : [(155.67+154.00)/2 (152.67+153.33)/2 (155.67-154.00)/2 (152.67-153.33)/2] = [154,84 153,00 0,83 -0,33]
Baris 3 : [(157.00+156.67)/2 (156.00+154.67)/2 (157.00-156.67)/2 (156.00-154.67)/2] = [156,84 155,34 0,17 0,67]
Baris 4 : [(156.67+153.67)/2 (152.67+151.67)/2 (156.67-153.67)/2 (152.67-151.67)/2] = [155,17 148,17 2,50 -0,50]
Baris 5 : [(153.67+148.67)/2 (147.67+148.67)/2 (153.67-148.67)/2 (147.67-148.67)/2] = [151,17 148,17 2,50 -0,50]

Pada proses perhitungan DWT di atas dapat diambil kesimpulan penggeseran setiap *pixel*nya sehingga perubahan gambar tidak terlalu signifikan diakibatkan penggeseran *pixel* yang dirubah hanya sedikit.

3.1. Algoritma Playfair Cipher

Algoritma kriptografi *playfair cipher* merupakan algoritma yang dibuat guna memperbaiki algoritma kriptografi klasik khususnya algoritma *playfair* yang mudah diserang dengan teknik analisis frekuensi untuk *bigram* dan *poligram*.

Algoritma ini melakukan variansi terhadap *Playfair Cipher*, untuk kemudian melakukan super enkripsi dengan melakukan *cipher transposisi* sejumlah panjang kunci terhadap hasil *ciphertext* yang dihasilkan oleh varian *playfair cipher* tersebut.

Playfair menggunakan tabel 5x5. Semua alfabet kecuali J diletakkan ke dalam tabel. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil. Kunci yang digunakan berupa kata dan tidak ada huruf sama yang berulang. Apabila kuncinya "MATAHARI", maka kunci yang digunakan adalah "MATHRI". Selanjutnya, kunci dimasukkan ke dalam tabel 5x5, isian pertama adalah kunci, selanjutnya tulis huruf-huruf berikutnya secara urut dari baris pertama dahulu, bila huruf telah muncul, maka tidak dituliskan kembali.

Tabel 2. Kata Kunci Matahari

M	**A**	**T**	**H**	**R**
I	B	C	D	E
F	G	K	L	N
O	P	Q	S	U
V	W	X	Y	Z

Berikut ini aturan-aturan proses enkripsi pada *Playfair* yaitu:

1. Jika kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan yang sekolom dengan huruf pertama. Contohnya, SA menjadi PH, BU menjadi EP.
2. Jika kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf setelahnya dalam baris yang sama, demikian juga dengan huruf kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya.

TIN: Terapan Informatika Nusantara
Vol 1, No 8, Januari 2021, Hal 390-394
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, AH menjadi TR, LK menjadi KG, BE menjadi CI.

M	**A**	T	**H**	R
I	**B**	C	D	**E**
F	G	**K**	**L**	N
O	P	Q	S	U
V	W	X	Y	Z

3. Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua. Contohnya, DS menjadi LY, PA menjadi GW, ER menjadi RZ.

M	**A**	T	H	**R**
I	B	C	**D**	**E**
F	G	K	L	N
O	**P**	Q	**S**	U
V	W	X	Y	Z

4. Jika kedua huruf sama, maka letakkan sebuah huruf di tengahnya (sesuai kesepakatan).
5. Jika jumlah huruf plainteks ganjil, maka tambahkan satu huruf pada akhirnya, seperti pada aturan ke-4.

Sedangkan proses dekripsinya adalah kebalikan dari proses enkripsi. Contohnya, HR didekripsi menjadi TH, BS didekripsi menjadi DP, ZU didekripsi menjadi RZ.

M	A	T	**H**	**R**
I	**B**	C	D	E
F	G	K	L	N
O	P	Q	**S**	**U**
V	W	X	Y	**Z**

Contoh hasil implementasi *Playfair* dengan menentukan plainteks, baris dan kolom Misalkan kalimat plainteksnya " **NAMA SAYA INDRA**" dengan kata kunci "**MATAHARI**" maka hasilnya dapat dilihat di bawah ini :

X/Y	1	2	3	4	5
1	M	A	T	H	R
2	I	B	C	D	E
3	F	G	K	L	N
4	O	P	Q	S	U
5	V	W	X	Y	Z

Plaintext	:	NA	MA	SA	YA	IN	DR	A
Baris	:	31	11	41	51	23	21	1
Kolom	:	52	12	42	42	15	45	1

Di Enkripsi menjadi :

Chypertext	:	GR	GF	PH	WH	BL	EH	A
Baris	:	31	33	41	51	23	21	1
Kolom	:	25	21	24	51	24	21	1

4. KESIMPULAN

Dari hasil penelitian dapat disimpulkan sistem dapat mendeteksi modifikasi yang bersifat menyebar dan acak yaitu pada modifikasi *noise* dan *sharpening*. Akan tetapi hasil perbaikan yang dihasilkan cukup buruk karena citra ciri mengalami kerusakan yang acak dan menyebar di seluruh bagian citra. Hasil perbaikan yang buruk disebabkan karena metode transformasi yang digunakan dalam pembuatan ciri penting dari suatu citra, karena metode transformasi *DWT* menghasilkan nilai *floating point* sehingga ciri penting tersebut akan merusak gambar pada saat dilakukan proses perbaikan. Pembuatan teknik kriptografi enkripsi dan dekripsi dengan menggunakan metode *playfair* dapat melindungi data di mana program akan melakukan proses enkripsi hanya berupa huruf dengan menggunakan tabel 5 X 5.


TIN: Terapan Informatika Nusantara
Vol 1, No 8, Januari 2021, Hal 390-394
ISSN 2722-7987 (Media Online)
Website https://ejurnal.seminar-id.com/index.php/tin

REFERENCES

Arius, D. (2008). *Pengantar Ilmu Kriptografi dan Implemantasi*. ANDI Yogyakarta.
Ariyus, & Dony. (2006). *Kriptografi Keamanan Data dan Komunikasi*. Yogyakarta: Grahailmu.
Munir, R. (2008). *Belajar Ilmu Kriptografi*. ANDI Yogyakarta.
Putera, A., Siahaan, U., Mesran, M., & Solihin, I. (2018). Implementation of Super Playfair in Messaging. *ICASI 2018*, 109–118.
Setyaningsih, E. (2015). *Kriptografi & Implementasi Menggunakan Matlab*. Yogyakarta: Andi.