SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Publikasi Jurnal & Penelitian Teknik Informatika
Volume 2 Nomor 2, April 2018
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Penyisipan Audio Terenkripsi pada Citra dengan *Discrete Wavelet Transform*

Mohammad Iqbal Maulana
Universitas Jember
Jln. Kalimantan 37, Jember 68121
iqbal3496m@gmail.com

Abduh Riski
Universitas Jember
Jln. Kalimantan 37, Jember 68121
riski.fmipa@unej.ac.id

Ahmad Kamsyakawuni
Universitas Jember
Jln. Kalimantan 37, Jember 68121

***Abstract*—**Pengamanan suatu pesan audio dapat menggunakan teknik kriptografi dan steganografi. Kriptografi merupakan teknik untuk merahasiakan informasi penting dalam suatu pesandengan cara mengenkripsi pesan tersebut sehingga tidak dapat diketahui informasinya oleh orang lain (*attacker*). Selanjutnya pesan audio terenkripsi diamankan kembali menggunakan teknik steganografi. Steganografi merupakan teknik menyisipkan suatu pesan ke dalam media lain sehingga keberadaan pesan tersebut tidak terdeteksi oleh manusia. Pada penelitian ini *International Data Encryption Algorithm* (IDEA) digunakan sebagai algoritma pada kriptografi dan *Discrete Wavelet Transform* (DWT)digunakan pada proses steganografi. Pesan audio terenkripsi IDEA akan disisipkan ke dalam citra menggunakan DWT. *Signal to Noise Ratio* (SNR), *Peak Signal to Noise Ratio* (PSNR) dan analisis sensitivitas kunci digunakan untuk menganalisis kemanan dari metode yang diajukan. Dari hasil penelitian didapatkan teknik enkripsi menggunakan algoritma IDEA pada sebuah pesan audio dapat dikatakan baik karena IDEA memiliki kunci yang sensitif walaupun hasil dari proses enkripsi akan menimbulkan kecurigaan *attacker* karena menghasilkan *cipher audio* yang tidak jelas, oleh karena itu dapat dilakukan teknik pengamanan selanjutnya yaitu steganografi.*Cipher audio* dari proses enkripsi akan disisipkan ke dalam suatu citra menggunakan metode DWT, dimana dari penelitian ini didapatkan sebuah hasil jika proses penyisipan *cipher audio* ke dalam citra menggunakan DWT baik, karena citra hasil penyisipan tidak mengalami perubahan yang signifikan dengan ditunjukkan dari nilai PSNR yang lebih dari 40dB. Oleh karena itu pengamanan pesan audio menggunakan teknik kriptografi IDEA dan dilanjutkan dengan teknik steganografi DWT sangatlah baik karena suatu audio akan memiliki tingkat keamanan ganda dari proses kriptografi dan steganografi.

Keywords—kriptografi; steganografi; *international data encryption algorithm*; *discrete wavelet transform*;*sound' image*.

I. LATAR BELAKANG

Pengiriman pesan pada era sekarang sering sekali menggunakan media digital. Hal tersebut dilakukan karena efisiensi waktu serta tempat saat berkirim pesan sangatlah cepat dan mudah. Pesan audio sering digunakan seseorang untuk saling bertukar atau mengirim pesan. Namun pengiriman pesan melalui media digital juga memiliki sisi negatif dimana *attacker* atau orang yang tidak berhak atas pesan dapat mengambil suatu pesan yang bersifat rahasia dengan mudah. Oleh karena itu pesan dapat diamankan dengan beberapa teknik sebelum dikirimkan. Teknik yang digunakan yaitu kriptografi dan steganografi.

Teknik kriptografi digunakan dengan cara mengenkripsi suatu pesan audio menggunakan algortima yang tersedia. Enkripsi sendiri merupakan teknik untuk merahasiakan suatu informasi penting (pesan) kedalam suatu bentuk yang tidak dapat dibaca oleh siapapun. Algortima yang digunakan pada teknik kriptografi yaitu IDEA (*International Data Encryption Algorithm*) karena IDEA aman untuk mengenkripsi pesan berupa teks [1]. Selain itu steganografi digunakan sebagai pengamanan tingkat lanjut setelah proses kriptografi. Steganografi sendiri merupakan teknik untuk menyembunyikan suatu pesan ke dalam media lain sehingga keberadaan pesan tidak terdeteksi indera manusia.

Metode DWT (*Discrete Wavelet Transform*) digunakan pada steganografi untuk meyembunyikan pesan kedalam suatu citra digital. DWT digunakan karena DWT memiliki keamanan yang baik sebagai metode dalam penyisipan suatu pesan ke dalam media lain[2].

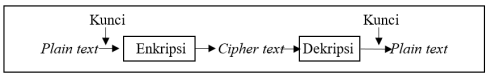
Pengamanan suatu pesan audio dilakukan dengan cara mengenkripsi pesan menggunakan IDEA dan selanjutnya disisipkan kedalam suatu citra menggunakan DWT. Hal tersebut dilakukan karena audio hasil enkripsi akan menghasilkan *output* yang tidak jelas, sehingga dapat menimbulkan kecurigaan bagi *attacker* saat mendapatkan pesan tersebut, oleh karena itu pengamanan pesan dapat dilanjutkan dengan teknik steganografi dimana bertujuan agar pesan audio terenkripsi dapat tersembunyi di dalam sebuah citra sehingga tidak akan menimbulkan kecurigaan *attacker*.

Pada penelitian ini audio berformat **.wav* yang digunakan sebagi tempat suatu pesan rahasia, serta citra digital yang berformat *.bmp dan *.jpg sebagai citra penyisipan.

II. TINJAUAN PUSTAKA

A. Kriptografi

Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimanamerahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapatdibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semuladengan menggunakan berbagai macam teknik yang telah ada, sehingga informasitersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau tidakberkepentingan [3].



Gambar 1. Proses kriptografi

. *Plain text* merupakan informasi awal yang bisa dibaca. *Cipher text* merupakan informasi hasil pesan *plain text* yang sudah disandikan. Enkripsi adalah teknik untuk menjadikan data *plain text* agar tidak dapat dibaca. Dekripsi adalah teknik untuk mengembalikan *cipher text* menjadi *plain text* kembali. Kunci (*key*) berfungsi untuk mengatur dan menjalankan suatu algoritma. Sedangkan, algoritma adalah suatu metode untuk melalukan proses enkripsi dan dekripsi tersebut.

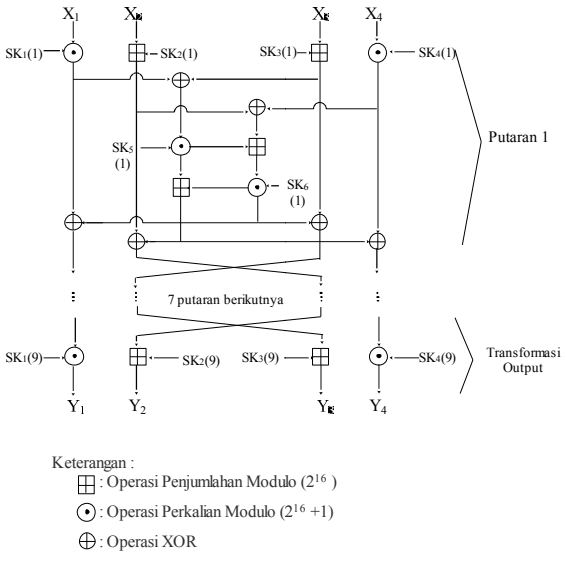
B. Steganografi

Secara garis besar metode steganografi terdiri dari 2 bagian utama, yaitu proses penyembunyian data (*hidden message*) atau biasa disebut penyisipan data (*embedding message*) dan proses pengembalian data kebentuk semula (*reveal message*) atau juga dapat disebut *extraction* [4].

. Steganografi (*steganography*) adalah ilmu dan seni menyembunyikan pesan rahasia sedemikian sehingga keberadaan pesan tidak terdeteksi oleh indera manusia. Kata steganografi berasal dari bahasa yunani yang berarti "tulisan tersembunyi" (*covered writing*). Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah diproses enkripsi (*cipher text*) tetap tersedia atau dengan kata lain dapat terlihat, maka dengan steganografi, *cipher text* dapat disembunyikan sehingga *attacker* tidak mengetahui keberadaannya.

C. *International Data Encryption Algorithm*

IDEA merupakan salah satu algoritma kriptografi yang beroperasi pada blok *plain text* 64 bit dengan panjang kuncinya 128 bit dan menggunakan operasi XOR, penambahan modulo 2^{16} dan juga perkalian modulo $2^{16}+1$.IDEA memiliki 8 putaran ditambah dengan 1 Transformasi *Output* (TO). Adapun proses algoritma enkripsi dan dekripsi yang digunakan dalam IDEA seperti pada gambar 2, dimana algoritma dari proses enkripsi dan dekripsi menggunakan algoritma yang sama.

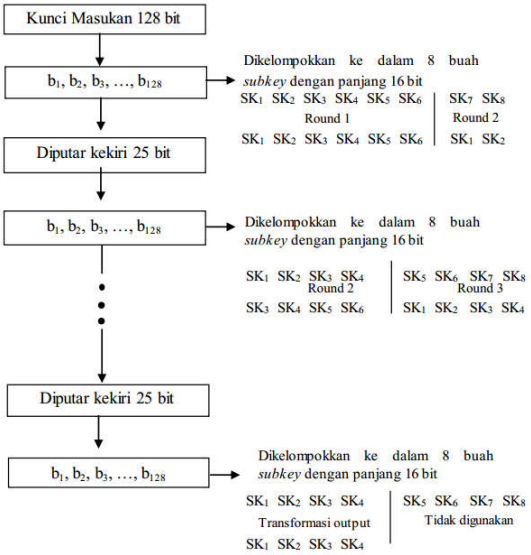


Gambar 2. Proses IDEA

Selain itu IDEA memiliki pembangkitan kunci. Kunci yang memiliki panjang 128bit akan mengalami proses pembangkitan kunci, yang mana proses dari pembangkitan kunci pada IDEA seperti pada gambar 3.

Pada proses pembentukan kunci dalam enkripsi dan dekripsi memiliki algoritma yang sama, yang membedakan pada dekripsi setelah didapatkan *subkey* dari proses pembangkitan kunci, *subkey* mengalami permutasi atau perpindahan posisi dan juga mengalami invers, dapat berupa invers penjumlahan yang disimbolkan dengan –SK atau invers perkalian

yang disimbolkan menjadi SK^{-1}. Adapun *Subkey* untuk enkripsi pada Tabel 1 dan dekripsi pada Tabel 2.



Gambar 3. Pembangkit Kunci IDEA

Tabel 1. *Subkey* Enkripsi IDEA

Putaran	Enkripsi					
1	$SK_1(1)$	$SK_2(1)$	$SK_3(1)$	$SK_4(1)$	$SK_5(1)$	$SK_6(1)$
2	$SK_1(2)$	$SK_3(2)$	$SK_2(2)$	$SK_4(2)$	$SK_5(2)$	$SK_6(2)$
3	$SK_1(3)$	$SK_3(3)$	$SK_2(3)$	$SK_4(3)$	$SK_5(3)$	$SK_6(3)$
4	$SK_1(4)$	$SK_3(4)$	$SK_2(4)$	$SK_4(4)$	$SK_5(4)$	$SK_6(4)$
5	$SK_1(5)$	$SK_3(5)$	$SK_2(5)$	$SK_4(5)$	$SK_5(5)$	$SK_6(5)$
6	$SK_1(6)$	$SK_3(6)$	$SK_2(6)$	$SK_4(6)$	$SK_5(6)$	$SK_6(6)$
7	$SK_1(7)$	$SK_3(7)$	$SK_2(7)$	$SK_4(7)$	$SK_5(7)$	$SK_6(7)$
8	$SK_1(8)$	$SK_3(8)$	$SK_2(8)$	$SK_4(8)$	$SK_5(8)$	$SK_6(8)$
TO		$SK_1(9)$	$SK_2(9)$	$SK_3(9)$	$SK_4(9)$	

Tabel 2. *Subkey* Dekripsi IDEA

Putaran	*Subkey*					
1	$SK_1(9)^{-1}$	$-SK_2(9)$	$-SK_3(9)$	$SK_4(9)^{-1}$	$SK_5(8)$	$SK_6(8)$
2	$SK_1(8)^{-1}$	$-SK_3(8)$	$-SK_2(8)$	$SK_4(8)^{-1}$	$SK_5(7)$	$SK_6(7)$
3	$SK_1(7)^{-1}$	$-SK_3(7)$	$-SK_2(7)$	$SK_4(7)^{-1}$	$SK_5(6)$	$SK_6(6)$
4	$SK_1(6)^{-1}$	$-SK_3(6)$	$-SK_2(6)$	$SK_4(6)^{-1}$	$SK_5(5)$	$SK_6(5)$
5	$SK_1(5)^{-1}$	$-SK_3(5)$	$-SK_2(5)$	$SK_4(5)^{-1}$	$SK_5(4)$	$SK_6(4)$
6	$SK_1(4)^{-1}$	$-SK_3(4)$	$-SK_2(4)$	$SK_4(4)^{-1}$	$SK_5(3)$	$SK_6(3)$
7	$SK_1(3)^{-1}$	$-SK_3(3)$	$-SK_2(3)$	$SK_4(3)^{-1}$	$SK_5(2)$	$SK_6(2)$
8	$SK_1(2)^{-1}$	$-SK_3(2)$	$-SK_2(2)$	$SK_4(2)^{-1}$	$SK_5(1)$	$SK_6(1)$
TO		$SK_1(1)^{-1}$	$-SK_2(1)$	$-SK_3(1)$	$SK_4(1)^{-1}$	

D. *Discrete Wavelet Transform*

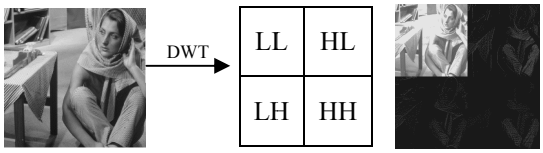
Salah satu dari jenis dari transformasi *wavelet* adalah *Discrete Wavelet Transform* (DWT). Transformasi wavelet merupakan suatu proses pengubahan data dalam bentuk lain agar lebih mudah dianalisis. Wavelet merupakan gelombang mini (*small wave*) yang mempunyai kemampuan mengelompokkan energi citra dan terkonsentrasi pada sekelompok kecil koefisien, sedangkan kelompok koefisien lainnya hanya mengandung sedikit energi yang dapat dihilangkan tanpa mengurangi nilai informasinya [5].

Pada penilitian kali ini akan menggunakan dekomposisi Haar Wavelet. Haar wavelet mengubah citra dengan domain spasial ke domain frekuensi dengan persamaan berikut ini:

$$H_0: f(n) = \frac{X_n + X_{n+1}}{2} (1)$$

$$H_1: f(n) = \frac{X_n - X_{n+1}}{2} (2)$$

Persamaan (1) merupakan *high pass filter* dan persamaan (2) merupakan *low pass filter* dengan $X=\{X_n\}$, n= 1, 2, 3, …, N merupakan *pixel-pixel*dari citra. Proses dekomposisi akan menghasilkan *sub band* LL, LH, HL dam HH (Gambar 4).



Citra asli

Citra hasil dekmposisi

Gambar 4. Dekomposisi Citra

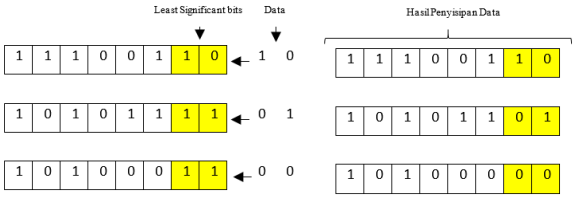
Selanjutnya untuk mengembalikan hasil dekomposisi kebentuk semula digunakan IDWT (*Inverse Discrete Wavelet Transform*) menggunakan persamaan (3) dan (4).

$$Y_{2n-1} = X_n + X_{n+m} \quad (3)$$

$$Y_{2n} = X_n - X_{n+m} \quad (4)$$

E. *Least Significant Bit*

LSB (Least Significant Bist) merupakan salah satu metode dalam steganografi. LSB dilakukan dengan mengambil bit–bit terakhir warna pada citra dan menggantinya dengan bit – bit data.Misalkan kita memiliki data 100100 akan disisipkan pada 3 *pixel* citra yaitu 11100110, 10101111, 10100011 sehingga proses LSB dapat dilihat pada Gambar 5.



Gambar 5. *Least Significant Bit*

Pada penelitian ini LSB akan sedikit dimodifikasi, modifikasi LSB dilakukan pada *pixel-pixel* yang memiliki nilai riil. Pada bilangan yang bernilai negatif akan dimutlakan dahulu setelah itu apabila nilainya berbentuk pecahan maka akan dibagi 2 kelompok yaitu kelompok bilangan bulat dan bilangan setelah koma. Bilangan bulat yang akan diproses proses penyisipan dilakukan seperti biasanya yang nantinya akan dikembalikan lagi nilai setiap *pixel* serta penambahan nilai bilangan pecahanya (bilangan bulat setelah koma). Misalkan nilai sebuah *pixel* gambar -89,5 $_{(10)}$ akan disipkan biner $10_{(2)}$, nilai |-89,5| = 89,5 dan biner dari 89 (1011001) maka penyisipan biner 10 akan dilakukan pada biner 1011001 sehingga didapatkan biner baru 1011010 sehingga didapatkan bilangan desimal 90 karena menyimpan nilai 0,5 sebelumnya maka 90 akan ditambahkan dengan nilai 0,5 sehingga nilainya menjadi 90,5 setelah itu akan dikembalikan pada nilai nya. Karena nilai awal bernilai negatif maka nilai *pixel* akan menjadi -90,5.

F. *Signal to Noise Ratio* (SNR)

SNR(*Signal to Noise Ratio*) didefinisikan sebagai *ratio* antara daya sinyal yang diingkan dengan daya derau (*noise*). Derau pada sinyal menyebabkan gangguan pada sinyal sehingga menyebabkan rusaknya sinyal informasi tersebut, dengan satuan dari SNR adalah dB (*decibel*). Semakin besar nilai SNR semakin baik kualitas sinyal yang dihasilkan atau dengan kata lain semakin kecil deraunya. Sinyal dikatakan baik apabila nilai SNR lebih besar dari atau sama dengan 25dB sedangkan untuk nilai kurang dari atau sama dengan 13dB dimana terdapat derau atau *noise* yang besar dalam sinyal [6]. Perhitungan SNR dapat dilakukan dengan metode korelasi. Metode korelasi dilakukan dengan membandingkan dua runtun data (sinyal) yang masing-masing nilai sampelnya diambil secara serempak [7]. Perhitungan SNR menggunakan persamaan berikut:

$$\rho = \frac{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\frac{1}{n}\sum_{i=1}^{n}(x_i-\bar{x})^2}.\sqrt{\frac{1}{n}\sum_{i=1}^{n}(y_i-\bar{y})^2}}$$

$$\text{SNR} = \frac{\text{sinyal}}{\text{derau}} = \left(\frac{\rho}{1-\rho}\right)$$

$$\text{SNR}_{dB} = 10 \times \log_{10}\left(\frac{\rho}{1-\rho}\right) \quad (5)$$

Persamaan 5 untuk mencari nilai SNR dari data audio uji.

G. *Peak Signal to Noise Ratio* (PSNR)

PSNR adalah sebuah istilah dalam bidang teknik yang menyatakan perbandingan antara kekuatan sinyal maksimum yang mungkin dari suatu sinyal digital dengan kekuatan derau yang mempengaruhi kebenaran sinyal tersebut. Sama halnya dengan SNR hanya saja penggunaan PSNR digunakan pada suatu citra. Nilai PSNR dikatakan memiliki kemiripan yang tinggi jika nilai PSNR lebih besar atau sama dengan 40dB [8]. Perhitungan PSNR dilakukan dengan menghitung nilai MSE pertama kali. *Mean Square Eror* (MSE) dihitung untuk seluruh pixel dalam citra.

$$\text{MSE} = \frac{\sum_{i=1,j=1}^{i=n,j=m}(f(i,\ j) - F(i,j))^{\ 2}}{M \times N} \quad (7)$$

$$\text{PSNR} = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \quad (8)$$

H. Analisis Sensitivitas Kunci

Analisis sensitivitas kunci digunakan untuk mengetahui sensitivitas kunci dari suatu algoritma. Dua hal yang menjadi tolak ukur yaitu, (i) ketika kunci yang digunakan untuk mengenkripsi citra tersebut sedikit berbeda maka akan menghasilkan *cipher image* yang sangat berbeda, (ii) jika ada perbedaan kunci antara proses enkripsi dan dekripsi maka tidak akan memperoleh *plain image* yang diinginkan. Tolak ukur tersebut didapatkan dengan menggunakan *Signal to Noise Ratio*[9]

III. PEMBAHASAN

A. Desain Eksperimen

Penelitian ini dilakukan dalam beberapa tahap, meliputi tahap *input* dan mengubah selang data audio, *input* kunci dan pembangkitan, enkripsi audio, *input* citra dan DWT proses, *embedding*data audio terenkripsi pada citra DWT serta tahap pengungkapan data. Prosedur penyelesaian masalah di atas dapat dijelaskan pada langkah-langkah berikut:

Langkah 1:*input* data atau pesan audio. Audio memiliki data atau *sample* yang memiliki rentang -1 hingga 1, oleh karena itu harus dirubah menjadi nilai yang berada diantara selang 0-255. Konversi *sample* menggunakan persamaan (9) dan dilanjutkan konversi desimal menjadi biner.

$$f(x) = \left\lfloor\frac{255x+255}{2}\right\rfloor \quad (9)$$

Langkah 2: *input* kunci 16 karakter dan dikonversi kedalam biner. Setelah itu dilakukan pembangkitan kunci sesuai Gambar 3.

Langkah 3: pengelompokan data biner audio menjadi 64 bit, yang mana setiap *sub blok*ini akan menjadi *plain text* pada proses IDEA.

Langkah 4: proses enkripsi IDEA sesuai tahapan pada Gambar 2 sehingga didapatkan data berbentuk biner 64 bit.

Langkah 5: *input* Citra t penyisipan. Citra sebelum disisipi nkripsi, akan mengalami proses DWT 4.

Langkah 6: penyisipa o terenkripsi pada citra hasil DWT m

Langkah 7: proses pengembalian citra menjadi citra semula menngunakan IDWT.

Langkah 8: proses pengungkapan data diawali dengan memecah citra yang memiliki data terenkripsi di dalamnya menggunakan DWT sehingga didapatkan data biner.

Langkah 9: Data biner dikelompokkan menjadi 64bit perkelompok (sub blok).

Langkah 10: *input* kunci, dan lakukan pembentukan kunci (*subkey* dekripsi)

Langkah 11: proses tiap sub blokdengan proses IDEA menggunakan kunci dari *subkey* dekripsi.

Langkah 12: didapatkan *plain text* (biner) dan bagi menjadi 8 bit per sub blok, dan konversi menjadi desimal.

Langkah 13: Ubah desimal dengan rentang 0-255 menjadi rentang -1 hingga 1 menggunakan persamaan (10)

$$f(y) = \frac{2y}{255} - 1 \qquad (10)$$

Data yang digunakan sebagai data uji yaitu "*not-a-dream-whats-happening-to-place.wav*", dengan kunci "KRIPTOGRAFI IDEA".

Tabel 3. Sampel Awal Data Audio Uji

Baris	*Sample*	*Plainaudio*	Biner
1	-0,0010	127	01111111
2	-0,0012	127	01111111
3	-0,0008	127	01111111
4	0,0002	128	10000000
5	0,0008	128	10000000
6	0,0007	128	10000000
7	0,0002	128	10000000
8	-0,0009	127	01111111

Tabel 4. Kunci "KRIPTOGRAFI IDEA"

Karakter	Biner
K	01001011
R	01010010
I	01001001
P	01010000
T	01010100
O	01001111
G	01000111

Karakter	Biner
A	01000001
F	01000110
I	01001001
"spasi"	00100000
I	01001001
D	01000100
E	01000101

R	01010010

A	01000001

Pada proses penyisipan penguji menggunakan citra *barbara.png* (Gambar 6) yang digunakan sebagai tempat penyisipan data audio terenkripsi.

Gambar 6. *barbara.png*

B. Hasil Penelitian

Metode usulan diatas dengan menggunakan pemrograman Matlab 2015b. Dari sampel uji didapatkan beberapa hasil dari proses enkripsi, proses *embedding* dan juga hasil dari pengunkapan data. Hasil dari kriptografi akan diuji sentivitas kuncinya dimana hal tersebut bertujuan menentukan apakah IDEA baik digunkaan untuk mengenkripsi data berupa audio.

1) Enkripsi Pesan Audio dan *Embedding*

Dari proses enkripsi didapatkan hasil seperti pada Tabel 4.

Tabel 4. Hasil Enkripsi IDEA kunci "KRIPTOGRAFI IDEA"

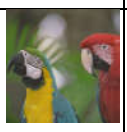
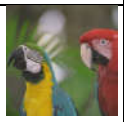
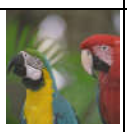
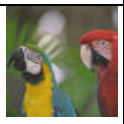
Data ke-	*Plain audio*	*Cipher audio*	Biner
1	-0,0010	0,3098	10100111
2	-0,0012	-0,9294	00001001
3	-0,0008	0,2863	10100100
4	0,0002	0,7882	11100100
5	0,0008	0,7882	11100100
6	0,0007	0,3020	10100110
7	0,0002	-0,1294	01101111
8	-0,0009	0,7412	11011110

Pada proses penysipan data audio terenkripsi dalam citra *barbara.png* menghasilkan PSNR 40,7 dB dengan kata lain dari kedua citra (asli dan hasil penyisipan) tidak menunjukkan perbedaan (Gambar 7).

Gambar 7. *Barbara.png* berisi data audio terenkripsi

Adapun beberapa uji sampel yang digunakan pada penelitian ini (Tabel 5).

Tabel 5. Uji Beberapa Data Uji

No	Data	Citra	Citra Hasil	PSNR
1	Audio: not-a-dream-whats-happening-to-place.wav Durasi:± 4 detik Kunci: KRIPTOGRAFI IDEA Citra: barbara.png DWT: tingkat 1			45,44
2	Audio: not-a-dream-whats-happening-to-place.wav Durasi:± 4 detik Kunci: KRIPTOGRAFI IDEA Citra: barbara.png DWT: tingkat 2			42,55
3	Audio: Recording 1.wav Kunci: KRIPTOGRAFI IDEA Durasi:± 19 detik Citra: barbara.png DWT: tingkat 1			40
4	Audio: Recording 1.wav Durasi:± 19 detik Kunci: kriptografi idea Citra: parrots.png DWT: tingkat 1			40,98
5	Audio: Recording 2.wav Durasi:± 26 detik Kunci: kriptografi idea Citra: parrots.png DWT: tingkat 1			42,71

2) *Extraction* dan Dekripsi

Dari proses ekstraksi citra beirisi data audio terenkripsi (Gambar 7) dan dilanjutkan dengan proses dekripsi didaptakan hasil *plain audio* kembali yang telah mendapatkan penambahan noise. Penambahan noise akan dihitung apakah noise menyebabkan hilangnya informasi didalam audio atau tidak.

Proses ekstraksi dan dekripsi dari citra *barbara.png* berisis pesan audio terenkripsi didapatkan plain audio pada Tabel 6.

Tabel 6. Hasil Pengungkapan Citra

No	Biner Data	Desimal	*Plainaudio*
1	01111111	127	-0,0039
2	01111111	127	-0,0039
3	01111111	127	-0,0039
4	10000000	128	0,0039
5	10000000	128	0,0039
6	10000000	128	0,0039
7	10000000	128	0,0039
8	01111111	127	-0,0039

Didapatkan *plain audio* kembali, dari proses ekstraksi dan dekripsi. Data audio berbeda dengan plain audio asli, karena penambahan noise, namun setelah dilakukan perhitungan menggunakan SNRdB didapatkan hasil 40,7 dB dimana menunjukkan adanya penambahan noise pada audio hasil dekripsi namun tidak menyebabkan hilangnya informasi dididalamnya. Dengan menggunakan beberapa sampel uji (Tabel 7) didapatkan nilai jika proses ekstraksi dan dekripsi menggunakan metode yang diajukan tidak menyebabkan hilangnya informasi rahasia didalamnya.

Tabel 7. Data Uji Sampel Berbeda

Nama (Audio)	Durasi	Kunci	*Size* (kb)		SNR_{dB}
			Sebelum	Dekripsi	
not-a-dream-whats-happening-to-place.wav	4 detik	KRIPTOGRAFI IDEA	88	88	40,7
Recording 1.wav	19 detik	KRIPTOGRAFI IDEA	305	305	35,24
Recording 2.wav	26 detik	kriptografi idea	204	204	37,5
human_voice.wav	2 detik	kriptografi idea	38	38	*Inf*

3) Analisis sensitivitas kunci

Serta saat menggunakan kunci yang sedikit berbeda (1 karakter) yaitu KRIPTOGRAFI IDEC pada proses enkripsi plain audio yang sama menunjukkan hasil yang berbeda singnifikan (Tabel 8). Pemilihan perbedaan satu karakter A ke C karena A dan C memiliki perbedaan biner hanya 1 karakter saja. Oleh karena itu sesuai syarat kunci yang sensitif yaitu perubahan 1 bit pada kunci.

Tabel 8. Hasil Enkripsi IDEA kunci "KRIPTOGRAFI IDEC"

Data ke-	*Plain audio*	*Cipher audio*
1	-0,0010	0,6706
2	-0,0012	-0,9059
3	-0,0008	-0,1608
4	0,0002	0,4980

5	0,0008	0,7255
6	0,0007	-0,7333
7	0,0002	0,1451
8	-0,0009	0,5059

Perbedaan dari keduanya dapat dilihat dari nilai SNR_{dB} dari kedua *cipher audio* yang menunjukkan nilai -16,296dB, dengan kata lain saat perubahan sediki pada kunci akan menyebabkan berbedanya *cipher nya.*

Pada proses dekripsi saat menggunakan kunci yang sedikit berbeda ("KRIPTOGRAFI IDEC") dari proses enkripsi juga akan menyebabkan tidak didapatkan *plain audio* kembali (Tabel 6).

Tabel 8. Dekripsi dengan Kunci Beda

Data ke-	*Plain audio*	*Plain audio*
1	-0,0010	-0,765
2	-0,0012	0,882
3	-0,0008	-0,642
4	0,0002	0,043
5	0,0008	-0,875
6	0,0007	-0,122
7	0,0002	0,576
8	-0,0009	-0,020

Dari penjelasan diatas didapatkan jika algoritma IDEA memiliki syarat sensitivitas kunci, oleh karena itu IDEA baik digunakan untuk mengenkripsi data berupa audio.

IV. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Proses pengamanan pada data audio berformat *.wav dapat dilakukan dengan melakukan enkripsi menggunakan algoritma IDEA yang selanjutnya melakukan embedding data audio terenkripsi ke dalam sebuah citra menggunakan DWT dan LSB. Proses enkripsi dapat memberikan keamanan bagi data audio karena hasil dari enkripsi (cipher audio) sangatlah berbeda dengan plain audio-nya. Serta proses embedding pada citra dapat meningkatkan keamanan bagi data audio terenkripsi karena data audio terenkripsi yang berada di dalam sebuah citra tidak akan menimbulkan kecurigaan sebab citra hasil proses embedding tidak memiliki perbedaan dengan citra sebelum proses embedding karena PSNR dari beberapa data uji menunjukkan nilai lebih dari 40dB.
2. Proses pengungkapan data dilakukan dengan melakukan proses ekstraksi pada citra sehingga didapatkan data audio terenkripsi, kemudian dilakukan proses dekripsi dengan algortima IDEA. Proses pengungkapan data mampu mengembalikan sebuah citra berisi data rahasia menjadi plain audio kembali, dengan nilai dari data audio asli dengan data audio setelah proses pengamanan data menunjukkan nilai SNR_{dB} lebih dari 25dB, sehingga data audio dapat dikatakan bagus (derau tidak merusak audio asli).
3. Berdasarkan analisis keamanan, algoritma yang diajukan dalam proses enkripsi aman untuk proses perlindungan data audio karena memiliki kunci yang sensitif, serta memiliki keamanan ganda yang baik setelah melewati proses embedding data audio kedalam sebuah citra karena memiliki nilai PNSR lebih besar dari 40dB maka dapat dikatakan sangat bagus (tidak memiliki perbedaan yang signifikan dengan citra asli).

REFERENSI

[1] Hanan, A. 2013. *Metode Enkripsi Dan Deskripsi Datamenggunakan Kriptografi Idea. Skripsi.* Aceh: Teknik Informatika Sekolah Tinggi Manajemen InformatikaDan KomputerStmik U'budiyah Indonesia.

[2] Goel, S., A. Rana., M. Kaur. 2013. A Review of Comparison Techniques of Image Steganography. *Global Journals of Computer Science and Technology*. 17(4-F)

[3] Munir, R. 2006. *Diktat Kuliah IF504 Kriptografi*. Jakarta: Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika..

[4] Munir, R. 2004. *Pengolahan Citra digital dengan Pendekatan Algoritmik*. Bandung:Informatika Bandung.

[5] Sydney, B. C., A. G. Remesg, G. Haito. 1998. Introduction to Wavelets and Wavelet Transform. New Jersey: *Prentice-Hall International, Inc*.

[6] Haq, A. D., Santoso, I., Macrina, A. A. 2012. *Estimasi Signal to Noise Ratio (SNR) Menggunakan Metode Korelasi.* Semarang: Universitas Diponegoro.

[7] Fitri, N. A., Srihendayana, H., Dasril. 2014. *Analisis Kualitas Jaringan Useetv Cable menggunakan kabel tembaga pada PT Telkom Pontianak*. Pontianak: Jurusan Teknik Elektro Fakultas Teknik Universitas Tanjungpura.

[8] Hakim, A. R. 2012. *Analisa Perbandingan Watermarking Image Menggunakan Discrete Wavelet Transform*. Skripsi. Depok: Fakultas Teknik Universitas Indonesia

[9] Song, C., & Y. Qiao. 2015. A Novel Image Encryption Algortithm Based on DNA encoding and Spatiotempral Chaos. *Entropy*. 17: 6954-6968.