

TUGAS BESAR I KRIPTOGRAFI

Aplikasi Steganografi pada Berkas Citra, Video, dan Audio dengan Metode LSB dan Metode BPCS

Oleh

Ignatius Timothy Manullang 13517044

Fatur Rahman 13517056

Didik Supriadi 13517069



**PROGRAM STUDI TEKNIK INFORMATIKA
SEKOLAH TEKNIK ELEKTRO & INFORMATIKA
INSTITUT TEKNOLOGI BANDUNG
OKTOBER 2020**

A. Teori Singkat

Citra terdiri dari sejumlah pixel. Setiap pixel panjangnya n -bit.

1. Citra biner $\rightarrow 1$ bit/pixel
2. Citra grayscale $\rightarrow 8$ bit/pixel
3. Citra true color $\rightarrow 24$ bit/pixel

Nilai pixel pada koordinat (x, y) menyatakan intensitas nilai keabuan pada posisi tersebut. Pada citra grayscale nilai keabuan itu dinyatakan dalam integer berukuran 1 byte sehingga rentang nilainya antara 0 sampai 255. Pada citra berwarna 24-bit setiap pixel terdiri atas kanal red, green, dan blue (RGB) sehingga setiap pixel berukuran 3 byte (24 bit).

Di dalam setiap byte bit-bitnya tersusun dari kanan ke kiri dalam urutan yang paling berarti (most significant bits atau MSB) hingga bit-bit yang kurang berarti (least significant bits atau LSB). Susunan bit pada setiap byte adalah $b_7b_6b_5b_4b_3b_2b_1b_0$.

Jika setiap bit ke- i dari MSB ke LSB pada setiap pixel diekstrak dan di plot ke dalam setiap bitplane image maka diperoleh delapan buah citra biner.

Bitplane LSB, yaitu bitplane 0, terlihat seperti citra acak (random image). Bitplane LSB merupakan bagian yang redundan pada citra. Artinya, perubahan nilai bit pada bagian tersebut tidak mengubah persepsi citra secara keseluruhan. Inilah yang mendasari metode steganografi yang paling sederhana, yaitu metode LSB.

Metode LSB merupakan metode steganografi yang paling populer. Ia memanfaatkan kelemahan indra visual manusia dalam mengamati perubahan sedikit pada gambar. Caranya: Mengganti bit LSB dari pixel dengan bit pesan. Mengubah bit LSB hanya mengubah nilai byte satu lebih tinggi atau satu lebih rendah dari nilai sebelumnya berarti tidak berpengaruh terhadap persepsi visual/auditori.

Secara umum metode LSB sama halnya jika kita berurusan dengan file audio seperti .wav. Intinya adalah kita menyisipkan bit pesan pada *least significant bit* dari file audio yang diberikan.

B. Perancangan dan Implementasi

a. Steganografi Citra

Pada steganografi citra akan dilakukan dengan metode lsb dan metode bpcs. Dimulai dengan lsb, awalnya pesan diubah terlebih dahulu ke bentuk biner. Lalu pesan akan diperiksa apakah citranya cukup untuk menyimpan pesan tersebut. Jika pesan tadi cukup, maka akan disisipkan ke dalam citra. Jika pesan dimasukkan ke image secara pixel yang acak, harusnya pesan di urut secara random.

Kemudian cara bpcs, bagi cover-image menjadi blok 8 x 8 pixel. Lalu bentuk setiap blok 8 x 8 pixel menjadi sistem PBC yang terdiri dari 8 buah bitplane. Ubah sistem PBC menjadi sistem CGC. Tentukan apakah setiap bit-plane merupakan informative region atau noise-like region dengan menggunakan nilai ambang α_0 . Nilai default $\alpha_0 = 0.3$. Jika tergolong noise-like region, maka pesan bisa disisipkan pada bit-plane tersebut, tetapi jika termasuk informative region, maka tidak dapat digunakan untuk menyisipkan pesan. Kemudian bagi pesan menjadi segmen-segmen berukuran 64-bit, lalu nyatakan segmen menjadi blok biner berukuran 8 x 8. Jika blok pesan S tidak lebih kompleks dibandingkan dengan nilai ambang α_0 , dilakukan konjugasi terhadap S untuk mendapatkan S^* yang lebih kompleks. Sisipkan segmen pesan 64-bit ke bit-plane yang merupakan noise-like region dengan cara mengganti seluruh bit pada noise-like region tersebut dengan 64-bit pesan. Sisipkan juga pemetaan konjugasi yang telah dibuat. Dan terakhir, ubah stego-image dari sistem CGC menjadi sistem PBC.

b. Steganografi Video

Steganografi video menggunakan menggunakan metode LSB, dan enkripsi atau dekripsi menggunakan Extended Vigenere Cipher.

Untuk encode, frame dan audio diekstrak terlebih dahulu. Lalu, pesan yang ingin disisipkan dibaca, dienkripsi jika user menginginkan, dan disisipkan dengan method code. Penyisipan method code dilakukan dengan melihat frame order list, yang bisa diacak berdasarkan seed dari key atau tidak, tergantung keinginan pengguna, sehingga dipastikan method code akan disisipkan ke depan pesan yang akan berada di frame 0. Setelah itu, ukuran dari frame 0 diambil, sehingga dapat

mengetahui panjang pesan maksimum dalam 1 frame untuk pembagian pesan. Selanjutnya, pesan dibagi berdasarkan panjang pesan maksimum dalam 1 frame. Terakhir, bagian pesan yang terurut dimasukkan ke dalam frame satu per satu berdasarkan frame order list, yang bisa diacak berdasarkan seed dari key atau tidak, tergantung keinginan pengguna, dengan fungsi encode LSB yang telah ada di Image Steganography, yang juga memungkinkan untuk memasukkan pesan di pixel yang acak, tergantung keinginan pengguna.

Untuk decode, frame dan audio diekstrak terlebih dahulu. Lalu, bagian pesan yang ada di setiap frame didecode menggunakan fungsi decode LSB yang telah ada di Image Steganography, dan diappend secara berurutan ke dalam list. Lalu, method code dari pesan yang ada dalam frame 0 dibaca, lalu dihapus dari pesan. Dari method code itu, program mengetahui apakah pesan diencode dengan frame yang acak atau sequential. Jika sequential, maka bagian pesan yang terdapat di list bagian pesan langsung di join. Jika acak, maka frame order list dishuffle untuk mengetahui urutan pesan di list bagian pesan, dan digunakan untuk mengurutkan bagian pesan di list bagian pesan, baru setelah itu pesan digabungkan. Setelah pesan dijoin atau digabungkan, jika pesan dienkripsi, maka pesan didekripsi, lalu direturn. Jika tidak dienkripsi, maka pesan langsung direturn saja.

c. Steganografi Audio

Pada steganografi audio dengan menggunakan metode lsb, awalnya ingin dilakukan agar bisa menyisipkan bit pesan secara sekuensial atau secara random. Hal ini dibedakan dengan memberikan bit kode pada byte pertama berkas audio. Kode 1 berarti dilakukan secara sekuensial dan kode 0 berarti dilakukan secara random.

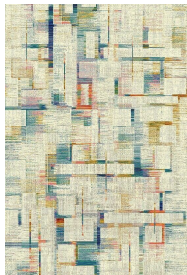
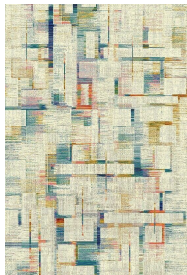
Pada cara sekuensial, bit-bit pesan akan disisipkan pada byte-byte pertama secara terurut dari berkas audio, kecuali byte pertama yang menyimpan kode cara penyisipan pesan. Pemulihan pesan dilakukan dengan mengambil dan mengumpulkan bit-bit pesan secara sekuensial dari byte-byte pertama berkas audio.

Pada cara random, bit-bit pesan akan disisipkan pada byte-byte acak pada berkas audio yang diberikan oleh sekuens nomor acak dengan seed berupa jumlah angka ascii dari tiap huruf dari key Vigenere Cipher. Pemulihan pesan dilakukan dengan mengambil dan mengumpulkan bit-bit pesan sesuai urutan kemunculan bilangan acak sesuai seed dari key Vigenere Cipher pada berkas audio yang telah dilakukan steganografi.

C. Pengujian Program dan Analisis Hasil

a. Steganografi Citra

Pesan & gambar sebelum disisipkan	Pesan & gambar setelah disisipkan	Dienkripsi?	Apakah berkas gambar mengalami perubahan berarti?	Cara penyisipan
Lorem Ipsum "Neque porro quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit..."	Lorem Ipsum "Neque porro quisquam est qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit..."	Tidak	Ya	BPCS, Blok sekuensial
One morning, when Gregor Samsa woke from troubled dreams, he found himself transformed in his bed into a horrible vermin.	11One morning, when Gregor Samsa woke from troubled dreams, he found himself transformed in his bed into a horrible vermin. + stop byte 00000000	Tidak	Tidak	LSB, Pixel Sekuensial

				
---	---	--	--	--

b. Steganografi Video

Pesan sebelum disisipkan	Pesan setelah disisipkan	Video	Dienkripsi ?	Apakah berkas video mengalami perubahan berarti?	Cara penyisipan
One morning, when Gregor Samsa woke from troubled dreams, he found himself transformed in his bed into a horrible vermin.	1133One morning, when Gregor Samsa woke from troubled dreams, he found himself transformed in his bed into a horrible vermin. + stop byte 00000000	https://www.youtube.com/watch?v=wUF9DeWJ0Dk .avi, 3 sec, 640x360, 30fps	Tidak	Tidak	LSB, Frame Sekuensial, Pixel Sekuensial
Lorem ipsum dolor sit amet, consectetur adipiscing elit.	1244Lorem ipsum dolor sit amet, consectetur adipiscing elit.	https://www.youtube.com/watch?v=wUF9DeWJ0Dk .avi,	Tidak	Tidak	LSB, Frame NonSequential, Pixel NonSequential

<p>Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultrices nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu</p>	<p>Aenean commodo ligula eget dolor. Aenean massa. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Donec quam felis, ultrices nec, pellentesque eu, pretium quis, sem. Nulla consequat massa quis enim. Donec pede justo, fringilla vel, aliquet nec, vulputate eget, arcu. In enim justo, rhoncus ut, imperdiet a, venenatis vitae, justo. Nullam dictum felis eu</p>	<p>3 sec, 640x360, 30fps</p>			
--	--	--------------------------------------	--	--	--

pede mollis pretium.	pede mollis pretium. + stop byte 00000000				
----------------------------	---	--	--	--	--

c. Steganografi Audio

Di bawah ini ditampilkan pengujian program hanya untuk cara penyisipan sekuensial.

Pesan Sebelum Disisipkan	Pesan Setelah Dipulihkan	Dienkripsi?	Apakah berkas audio mengalami perubahan yang berarti?	Cara Penyisipan
What happens now determines what happens to the rest of the world	What happens now determines what happens to the rest of the world	Tidak	Tidak	Sekuensial
What happens now determines what happens to the rest of the world	What happens now determines what happens to the rest of the world	Ya	Tidak	Sekuensial
Nothing's gonna change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you	Nothing's gonna change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you	Tidak	Tidak	Sekuensial
Nothing's gonna	Nothing's gonna	Ya	Tidak	Sekuensial

<p>change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you</p>	<p>change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you</p>			
<p>If I had to live my life without you near me The days would all be empty The nights would seem so long With you I see forever, oh, so clearly I might have been in love before But it never felt this strong Our dreams are young and we both know They'll take us where we want to go Hold me now, touch me now I don't want to live without you Nothing's gonna change my love for you You oughta know by now how much I love you</p>	<p>If I had to live my life without you near me The days would all be empty The nights would seem so long With you I see forever, oh, so clearly I might have been in love before But it never felt this strong Our dreams are young and we both know They'll take us where we want to go Hold me now, touch me now I don't want to live without you Nothing's gonna change my love for you You oughta know by now how much I love</p>	Tidak	Tidak	Sekuensial

<p>One thing you can be sure of I'll never ask for more than your love Nothing's gonna change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you</p>	<p>you One thing you can be sure of I'll never ask for more than your love Nothing's gonna change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you</p>			
<p>If I had to live my life without you near me The days would all be empty The nights would seem so long With you I see forever, oh, so clearly I might have been in love before But it never felt this strong Our dreams are young and we both know They'll take us where we want to go Hold me now, touch me now I don't want to live without you</p>	<p>If I had to live my life without you near me The days would all be empty The nights would seem so long With you I see forever, oh, so clearly I might have been in love before But it never felt this strong Our dreams are young and we both know They'll take us where we want to go Hold me now, touch me now I don't want to</p>	Ya	Tidak	Sekuensial

Nothing's gonna change my love for you You oughta know by now how much I love you One thing you can be sure of I'll never ask for more than your love Nothing's gonna change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you	live without you Nothing's gonna change my love for you You oughta know by now how much I love you One thing you can be sure of I'll never ask for more than your love Nothing's gonna change my love for you You oughta know by now how much I love you The world may change my whole life through But nothing's gonna change my love for you			
--	--	--	--	--

D. Kesimpulan dari Hasil Implementasi

Dari hasil implementasi, dapat disimpulkan bahwa data pesan dapat disisipkan pada file gambar, video, atau audio tanpa mengubah tampilan dari file itu sendiri dimata atau ditelinga kita.

Dan pada bpcs sendiri, ukuran $\alpha_0 = 0.3$ sangatlah kecil sehingga gambarnya tampak kabur. Untuk itu kami menyarankan hendaknya ukuran α_0 diubah.

E. Pembagian Tugas

NIM	Nama	Tugas
13517044	Ignatius Timothy Manullang	Image Steganography - LSB

		(Pixel Sequential & Nonsequential) Video Steganography - All Bugfixing bagian lainnya.
13517056	Fatur Rahman	Audio Steganography
13517069	Didik Supriadi	Image Steganography - LSB (Pixel Sequential), BPCS (Pixel Sequential)

Lin