Coding: Jurnal Komputer dan Aplikasi
Volume 08, No. 01 (2020), hal 11-22 ISSN 2338-493X

ANALISA PERBANDINGAN METODE VERNAM CIPHER DAN STEGANOGRAFI LSB UNTUK TANDA TANGAN DIGITAL PADA *E-DOCUMENT*

[1]**Abi Mabrur Ansharullah,** [2]**Sampe Hotlan Sitorus**
[1][2]Jurusan Rekayasa Sistem Komputer, Fakultas MIPA Universitas Tanjungpura
Jalan Prof Dr. H. Hadari Nawawi Pontianak
Telp./Fax: (0561) 577963
e-mail: [1]sayeabi46@gmail.com, [2]sitorus.hotland@gmail.com

ABSTRAK

Fungsi tanda tangan adalah untuk memastikan keaslian identitas dari penanda tangan pada suatu surat atau dokumen. Tanda tangan juga digunakan untuk menjaga keaslian dan legalitas dari suatu dokumen. Namun tanda tangan tersebut haruslah terjaga keamanan dan keasliannya dari pihak ketiga. Dengan menggunakan dua metode yaitu metode Vernam Cipher dan Steganografi LSB tanda tangan akan dirahasiakan. Menggunakan metode Vernam Cipher citra tanda tangan di XOR dengan citra yang berfungsi sebagai kunci. Dan dengan menggunakan metode Steganografi LSB bit terakhir dari citra tanda tangan disisipkan bit bit dari citra pesan. Pada metode kriptografi Vernam Cipher tanda tangan nantinya tampak berbeda. Sedangkan dengan metode Steganografi LSB tanda tangan akan tampak sama (dengan kasat mata). Sehingga pihak ketiga tidak curiga melihat tanda tangan tersebut. Penelitian yang dilakukan yaitu melihat selisih ukuran file pada citra yang sudah di enkripsi dan dekripsi. Dari hasil penelitian diperoleh nilai rata-rata dengan menggunakan metode Vernam Cipher memiliki selisih untuk enkripsi rata-rata sebesar 17.3 Kb dan selisih untuk dekripsi rata-rata sebesar 20.4 Kb. Sedangkan menggunakan metode Vernam Cipher memiliki selisih untuk enkripsi rata-rata sebesar 5.5 Kb dan selisih untuk dekripsi rata-rata sebesar 8.5 Kb.

Kata Kunci: Vernam Cipher, Steganografi LSB, Tanda Tangan Digital

1. PENDAHULUAN

Perkembangan teknologi informasi pada saat ini telah memungkinkan manusia melakukan pertukaran dokumen dengan cepat. Pada suatu dokumen yang menjadi sebuah penanda atau identitas adalah tanda tangan. Tanda tangan juga digunakan untuk menjaga keaslian dan legalitas dari suatu dokumen. Dengan kecanggihan teknologi pada saat ini tanda tangan yang tadinya menggunakan tanda tangan basah berganti menjadi tanda tangan digital. Namun tanda tangan tersebut haruslah terjaga keamanan dan keasliannya dari pihak ketiga. Metode yang pernah digunakan untuk menjaga keamanan dan keaslian tanda tangan yaitu metode kriptografi Vernam Cipher dan metode Steganografi LSB. Pada metode kriptografi Vernam Cipher tanda tangan nantinya tampak berbeda. Sedangkan dengan metode Steganografi LSB tanda tangan tampak sama (dengan kasat mata).

Penelitian lainnya yang berjudul Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher. Penelitian tersebut menyajikan hasil pengujian kinerja metode Vernam Cipher dengan mengacak pesan citra digital menggunakan kunci yang berbeda di setiap karakternya. Citra baru yang dihasilkan melalui enkripsi diperoleh karena adanya perubahan pada interaksi warna citra menggunkan 12 gambar yang berukuran kurang dari 100 Kb tingkat keberhasilannya 100% [1].

Penelitian berikutnya adalah berjudul Image Steganography Dengan Metode Least Significant Bit (LSB). Pada penelitian tersebut bertujuan menyembunyikan pesan berupa teks rahasia ke dalam citra true colour 24 bit dalam format RGB. Metode Least Significant Bit (LSB) digunakan untuk menyisipkan pesan rahasia dengan mengganti bit terakhir atau bit ke-8 dalam setiap komponen warna RGB. Hasil yang diperoleh yaitu pesan yang disembunyi kan ke dalam citra digital tidak mengurangi kualitas citra digital secara signifikan, dan pesan yang telah disembunyi kan dapat diekstrak kembali, sehingga pesan yang dikirimkan dapat sampai dengan aman kepada penerima [2].

Penelitian berikutnya adalah berjudul Aplikasi Kriptografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner. Pada penelitian ini diterapkan metode kriptografi Vernam Cipher dengan melakukan proses pengacakan data sehingga file yang asli tidak mudah untuk di baca oleh pihak yang tidak berkepentingan. Metode Vernam Cipher merupakan algoritma berjenis symmetric key kunci yang digunakan untuk melakukan enkripsi dan dekripsi yang menggunakan kunci yang sama [3].

Penelitian selanjutnya berjudul Penerapan Steganografi Pada File Gambar (Jpg) Menggunakan Metode LSB Dengan Aplikasi Matlab. Penelitiam tersebut menggunakan metode LSB untuk menyamarkan data rahasia sehingga sulit untuk dideteksi, dengan menyisipkan pesan teks kedalam citra. Cara yang digunakan untuk menyembunyikan pesan rahasia pada aplikasi ini adalah dengan cara menyisipkan pesan kedalam bit rendah (LSB-*Least Significant Bit*) yaitu dengan mengganti tiap-tiap bit pixel pada file citra yang disisipkan. Tujuan yang diharapkan antara lain membangun perangkat lunak Steganografi pada citra digital file gambar bitmap dengan menggunakan aplikasi Matlab dan menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi dan menghasilkan file gambar yang mempunyai kualitas tidak jauh berbeda dengan citra digital file gambar aslinya [4].

Penelitian yang dilakukan yaitu membuat aplikasi untuk mengamankan dan menjaga keaslian tanda tangan. Dari hasilnya nanti dibandingkan metode mana yang lebih baik. Penelitian yang dilakukan berjudul "Analisa Perbandingan Metode Vernam Cipher dan Steganografi LSB pada Tanda Tangan Digital untuk *E-Document*".

2. LANDASAN TEORI

2.1. Tanda Tangan Digital

Tanda tangan digital adalah suatu mekanisme otentikasi yang mengijinkan pemilik pesan membubuhkan sebuah sandi pada pesannya yang bertindak sebagai tanda tangan. Jadi tanda tangan disini bukanlah tanda tangan yang di digitalisasi menggunakan alat scanner, namun suatu nilai kriptogratos yang bergantung pada pesan dan pengirim pesan [5].

2.2. Citra

Citra adalah suatu representasi (gambaran), kemiripan, atau imitasi dari suatu objek. Citra sebagai keluaran suatu sistem perekaman data dapat bersifat optik berupa foto, bersifat analog, berupa sinyal-sinyal video seperti gambar pada monitor televisi, atau bersifat digital yang langsung disimpan pada suatu media penyimpanan [6].

Pengolahan citra adalah salah satu cabang dari ilmu informatika. Pengolahan citra berkutat pada usaha untuk melakukan transformasi suatu citra/gambar menjadi citra lain dengan menggunakan teknik tertentu. Pengolahan citra merupakan bidang yang bersifat multidisiplin, yang terdiri dari banyak aspek, antara lain fisika, elektronika, matematika, seni dan teknologi computer [6].

2.3. Kriptografi

Kriptografi adalah ilmu untuk menyandikan pesan asli (*plaintext*) menjadi pesan rahasia (*ciphertext*) dengan sebuah kunci (*key*) enkripsi sehingga pesan sulit dibaca oleh seseorang. Sebaliknya, dekripsi adalah proses mengubah pesan tersandi (*ciphertext*) menjadi pesan semula (*plaintext*) dengan menggunakan kunci (*key*) [7]. Maka fungsi enkripsi dan dekripsi dapat ditulis dengan Persamaan 1.

$$E_K(P) = C \text{ dan } D_K C = P \quad (1)$$

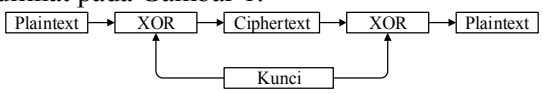
Dan kedua fungsi ini memenuhi Persamaan 2.

$$D_K(C) = P \quad (2)$$

Dengan E adalah Enkripsi, D adalah Dekripsi, K adalah Kunci, C adalah Ciphertext, P adalah Plaintext.

2.4. Vernam Cipher

Algoritma Vernam Cipher merupakan algoritma berjenis symetric key yang artinya bahwa kunci yang digunakan untuk melakukan enkripsi dan dekripsi merupakan kunci yang sama. Dalam proses enkripsi, algoritma ini menggunakan stream cipher yang berasal dari hasi XOR antara bit plaintext dan bit key. Pada metode ini plaintext diubah kedalam kode ASCII dan kemudian dikenakan operasi XOR terhadap kunci yang sudah diubah ke dalam kode ASCII [3]. Proses Vernam Cipher dapat dilihat pada Gambar 1.



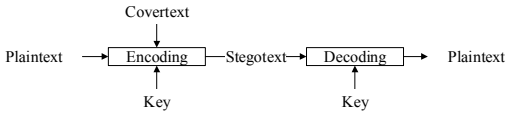
Gambar 1 Proses Vernam Cipher

2.5. Operasi Logika XOR

Operasi logika XOR dengan dua masukan memiliki keluaran bernilai logika 0(*false*), jika dan hanya jika kedua masukannya memiliki nilai logika sama. Sebaliknya, memiliki keluaran bernilai logika 1(*true*) jika dan hanya jika kedua masukannya memiliki nilai logika yang tidak sama [8].

2.6. Steganografi

Steganografi (*Steganography*) berasal dari bahasa Yunani *steganos* (*hidden*) dan *gráphein* (*writing*). Jadi, *steganografi* berarti *hidden writing* (tulisan tersembunyi). Steganografi merupakan seni menyembunyi kan data rahasia didalam wadah (media) digital sehingga keberadaan dan rahasia tersebut tidak diketahui atau tidak disadari orang lain. Steganografi membutuhkan dua properti yaitu media digital sebagai wadah penampungan dan data rahasia yang akan disembunyikan. Wadah penampung dan data rahasia tersebut dapat berupa citra, suara (audio), teks, atau video [9]. Proses kerja Steganografi dapat di lihat pada Gambar 2.



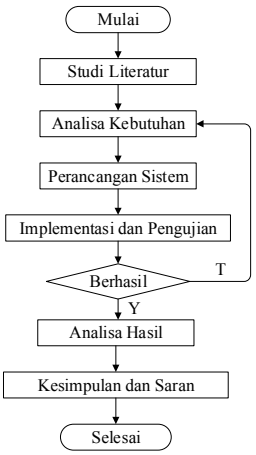
Gambar 2 Proses Kerja Steganografi

2.4. LSB (*Least Significant Bit*)

Metode LSB merupakan metode yang cukup sederhana dalam melakukan proses Steganografi. Selain itu, proses penyisipan dan ekstraksi dari metode ini juga relatif cukup cepat. Metode LSB menyisipkan pesan ke dalam *cover image* pada bit yang paling kurang berarti atau bi yang paling kanan. Untuk LSB 1 bit, bit yang disisipi adalah bit ke-8 untuk setiap byte, perubahan nilai desimal dari satu byte menjadi satu nilai lebih tinggi, atau satu nilai lebih rendah, atau sama dari nilai desimal dari satu byte sebelum terjadi penyisipan.

3. METODE PENELITIAN

Studi literatur adalah tahapan pertama dalam proses penelitian yang dilakukan. Studi literatur berguna untuk untuk mendapatkan teori-teori penunjang yang berkaitan dengan pembuatan aplikasi. Setelah teori teori didapatkan tahapan berikutnya mengumpulkan data yang diperlukan. Data yang digunakan adaalah 10 tanda tangan. Selanjutnya analisa kebutuhan yang terbagi menjadi dua yaitu analisa kebutuhan perangkat keras dan analisa kebutuhan perangkat lunak. Berdasarkan analisa kebutuhan perangkat dilakukanlah proses perancangan database dan antarmuka aplikasi. Dan kemudian melakukan implementasi untuk nantinya dilakukan pengujian. Pada tahapan terakhir yaitu menarik kesimpulan dari hasil penelitian yang telah dilakukan. Tahapan penelitian dapat dilihat pada Gambar 3.

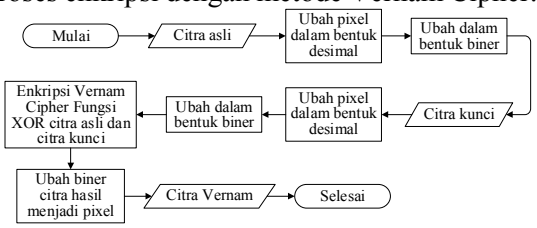


Gambar 3 Tahapan Penelitian

4. PERANCANGAN

4.1. Rancangan Sistem

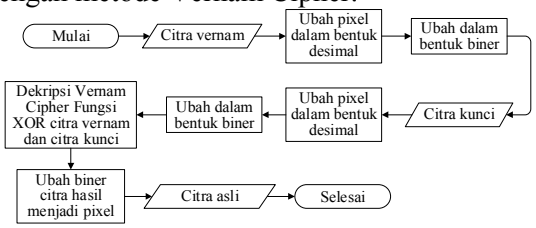
Alur enkripsi metode Vernam Cipher dengan operasi XOR diawali dengan menginput citra asli (tanda tangan) dan citra kunci. Selanjutnya kedua citra diubah ke desimal dan juga ke biner. Kemudian setiap bit citra asli dan bit citra kunci di proses menggunakan metode vernam cipher fungsi XOR. Setelah itu hasil yang di dapat diubah binernya menjadi pixel, maka menjadi citra vernam. Pada Gambar 4 menunjukan alur dari proses enkripsi dengan metode Vernam Cipher.



Gambar 4 *Flowchart* Enkripsi Vernam Cipher

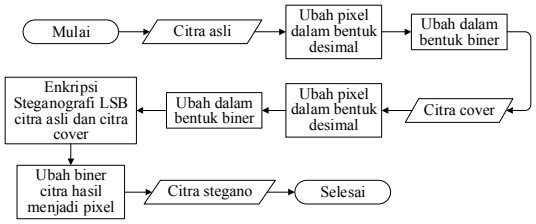
Alur dekripsi metode Vernam Cipher dengan operasi XOR diawali dengan menginput citra vernam dan citra kunci. Selanjutnya kedua citra tersebut di ubah kedalam bentuk desimal dan juga kedalam bentuk biner. Kemudian setiap bit citra vernam dan bit citra kunci di proses menggunakan metode vernam cipher fungsi XOR. Setelah itu hasil yang di dapat diubah binernya menjadi

pixel, maka menjadi citra asli kemabali. Pada Gambar 5 menunjukan alur dari proses dekripsi dengan metode Vernam Cipher.



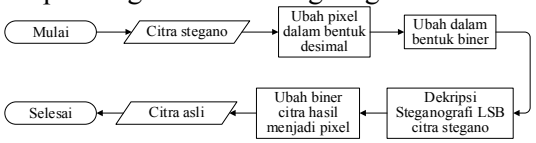
Gambar 5 *Flowchart* Dekripsi Vernam Cipher

Alur enkripsi metode Steganografi LSB diawali dengan menginput citra asli (tanda tangan) dan citra cover. Selanjutnya kedua citra tersebut di ubah pixelnya menjadi desimal dan juga biner. Kemudian setip bit terakhir biner citra diubah dengan bit cover. Setelah mendapatkan hasilnya, ubah biner hasil menjadi pixel. Selanjutnya pixel diubah menjadi citra, maka menghasilkan citra stegano. Pada Gambar 6 menunjukan alur dari proses enkripsi dengan metode Steganografi LSB.



Gambar 6 *Flowchart* Enkripsi Steganografi LSB

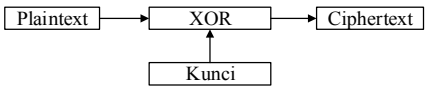
Alur dekirpsi metode Steganografi LSB diawali dengan menginput citra stegano dan selanjutnya diproses dengan menggunakan metode Steganografi LSB. Setelah diproses maka menghasilkan citra asli (tanda tangan). Pada Gambar 7 menunjukan alur dari proses dekripsi dengan metode Steganografi LSB.



Gambar 7 *Flowchart* Dekripsi Steganografi LSB

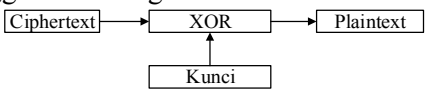
4.2. Perancangan Prosedural

Perancangan prosedur pada penelitian ini digunakan untuk mengambarkan secara umum proses yang terjadi pada sistem yang dibuat. Untuk melakukan enkripsi metode Vernam Cipher dibutuhkan plaintext (pesan asli) dan juga kunci sehingga menghasilkan ciphertext (pesan rahasia). Pada Gambar 8 menjelaskan proses enkripsi dengan menggunakan fungsi XOR.



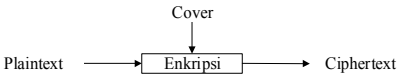
Gambar 8 Proses Enkripsi Metode Vernam Cipher

Untuk melakukan dekripsi metode Vernam Cipher dibutuhkan ciphertext (pesan rahasia) dan juga kunci sehingga menghasilkan plaintext (pesan asli). Pada Gambar 9 menjelaskan proses dekripsi dengan menggunakan fungsi XOR.



Gambar 9 Proses Dekripsi Metode Vernam Cipher

Proses enkripsi metode Steganografi LSB dibutuhkan plaintext (pesan asli) dan juga cover sehingga menghasilkan ciphertext (pesan rahasia). Proses enkripsi dapat dilihat pada Gambar 10.



Gambar 10 Proses Enkripsi Metode Steganogarfi LSB

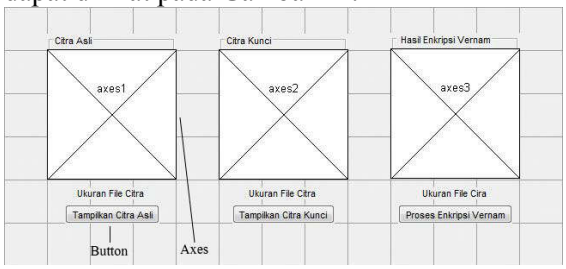
Proses dekripsi metode Steganografi LSB dibutuhkan ciphertext (pesan rahasia) dan juga cover, sehingga menghasilkan plaintext (pesan asli). Proses dekripsi dapat dilihat pada Gambar 11.

Gambar 11 Proses Dekripsi Metode Steganogarfi LSB

4.3. Perancangan Tampilan

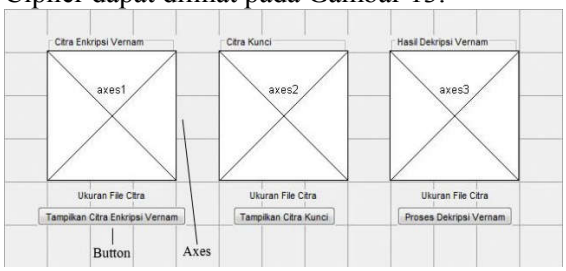
Terdapat beberapa rancangan tampilan aplikasi pada penelitian ini, rancangan tersebut digunakan sebagai media untuk pengguna. Untuk membuat rancangan tenkripsi metode Vernam Cipher menggunakan 3 axes, 3 text dan 3 button. Axes1 digunakan untuk menampilkan citra asli (tanda tangan). Axes2 digunakan untuk menampilkan citra kunci. Axes3 digunakan untuk menampilkan hasil XOR antara citra asli dan citra kunci. Text1 digunakan untuk menampilkan ukuran citra asli. Text2 digunakan untuk menampilkan ukuran citra kunci. Text3 digunakan untuk menampilkan ukuran hasil enkripsi Vernam Cipher. Button1 digunakan untuk memanggil citra asli. Button2 digunakan untuk memanggil citra kunci. Button3 untuk proses enkripsi menggunakan metode Vernam Cipher. Rancangan tampilan untuk melakukan enkripsi

dengan menggunakan metode Vernam Cipher dapat dilihat pada Gambar 12.



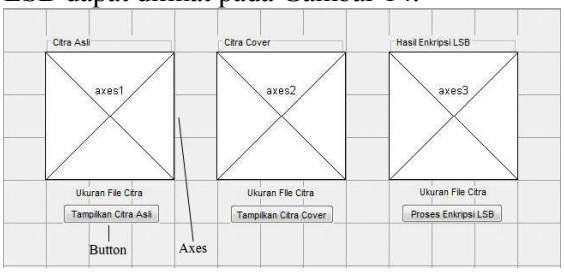
Gambar 12 Tampilan Rancangan Enkripsi Metode Vernam Cipher

Untuk merancang tampilan dekripsi mentode Vernam Cipher menggunakan 3 axes, 3 text dan 3 button. Axes1 digunakan untuk menampilkan hasil citra dari metode Vernam Cipher. Axes2 digunakan untuk menampilkan citra kunci. Axes3 digunakan untuk menampilkan hasil dari XOR antara hasil citra vernam cipher dan citra kunci. Button1 digunakan untuk memanggil citra vernam cipher. Text1 digunakan untuk menampilkan ukuran citra enkripsi vernam. Text2 digunakan untuk menampilkan ukuran citra kunci. Text3 digunakan untuk menampilkan ukuran hasil dekripsi vernam cipher. Button2 digunakan untuk memanggil citra kunci. Button3 untuk proses dekripsi menggunakan metode Vernam Cipher. Rancangan tampilan untuk melakukan dekripsi dengan menggunakan metode Vernam Cipher dapat dilihat pada Gambar 13.



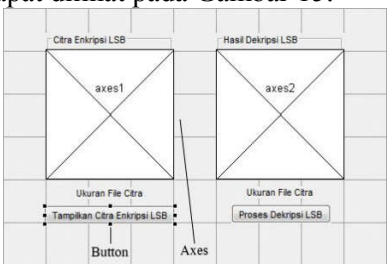
Gambar 13 Tampilan Rancangan Dekripsi Metode Vernam Cipher

Rancangan enkripsi metode Steganografi LSB menggunakan 3 axes, 3 text dan 3 button. Axes1 digunakan untuk menampilkan citra pesan. Axes2 digunakan untuk menampilkan citra asli. Axes3 digunakan untuk menampilkan hasil dari proses Steganografi LSB. Button1 digunakan untuk memanggil citra asli. Button2 digunakan untuk memanggil citra cover. Button3 untuk proses enkripsi menggunakan metode Steganografi LSB. Text1 digunakan untuk menampilkan ukuran citra asli. Text2 digunakan untuk menampilkan ukuran citra cover. Text3 digunakan untuk menampilkan ukuran hasil enkripsi Steganografi LSB. Rancangan tampilan untuk melakukan enkripsi dengan menggunakan metode Steganografi LSB dapat dilihat pada Gambar 14.



Gambar 14 Tampilan Rancangan Enkripsi Metode Steganografi LSB

Rancangan dekripsi metode Steganografi LSB menggunakan 2 axes, 2 text dan 2 button. Axes1 digunakan untuk menampilkan citra hasil enkrispi metode Steganografi LSB. Axes2 digunakan untuk menampilkan hasil dekripsi metode Steganografi LSB. Button1 digunakan untuk memanggil citra enkripsi LSB. Button2 digunakan untuk melakukan proses dekripsi. Rancangan tampilan untuk melakukan dekripsi dengan menggunakan metode Steganografi LSB dapat dilihat pada Gambar 15.



Gambar 15 Tampilan Rancangan Dekripsi Metode Steganografi LSB

5. IMPLEMENTASI DAN PENGUJIAN

5.1. Tampilan Enkripsi Metode Vernam Cipher

Pada tahapan ini dijalankan aplikasi untuk enkripsi metode Vernam Cipher. Pada Gambar 16 merupakan tampilan setelah tombol tampilkan citra asli, tombol tampilkan citra kunci dan tombol proses enkripsi vernam diklik. Setelah tombol proses enkripsi vernam diklik maka proses enkripsi Vernam Cipher dilakukan dengan fungsi XOR terhadap citra asli dan citra kunci. Hasil dari proses tersebut ditampilkan pada label hasil enkripsi vernam dan juga menampilkan ukuran citranya.

Gambar 16 Hasil Metode Vernam Cipher

5.2. Tampilan Dekripsi Metode Vernam Cipher

Pada tahapan ini dijalankan aplikasi untuk dekripsi metode Vernam Cipher. Pada Gambar 17 merupakan tampilan setelah tombol citra enkripsi vernam, tombol tampilkan citra kunci dan tombol proses dekripsi vernam diklik. Setelah tombol proses dekripsi vernam diklik maka proses vernam cipher dilakukan dengan fungsi XOR terhadap citra enkrispi vernam dan citra kunci. Hasil dari proses tersebut ditampilkan pada label hasil dan juga menampilkan ukuran citranya.

Gambar 17 Hasil Metode Vernam Cipher

5.3. Tampilan Enkripsi Metode Steganografi LSB

Pada tahapan ini dijalankan aplikasi untuk enkripsi metode Steganografi LSB. Pada Gambar 18 merupakan tampilan pada saat tombol citra asli, tombol citra cover dan tombol proses enkripsi LSB diklik. Setelah diklik maka proses Steganografi LSB dilakukan dan menampilkan nya pada label hasil enkrispi LSB beserta ukurannya.

Gambar 18 Hasil Enkripsi Steganografi LSB

5.4. Tampilan Dekripsi Metode Steganografi LSB

Pada tahapan ini dijalankan aplikasi untuk dekripsi menggunakan metode Steganografi LSB. Pada Gambar 19 merupakan hasil setelah tombol tampilkan citra enkripsi dan tombol proses dekripsi LSB diklik. Setelah diklik maka dilakukanlah proses dekripsi menggunakan metode Steganografi LSB. Hasil dari proses tersebut ditampilkan pada label hasil dekrispi LSB beserta ukurannya.

Gambar 19 Hasil Dekripsi

5.5. Implementasi Vernam Cipher dan Steganografi LSB pada Citra Tanda Tangan Digital

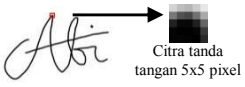
Pada tahap ini pengujian terhadap aplikasi untuk melakukan tanda tangan digital pada *e-document* dengan menggunakan kedua metode tersebut dilihat keberhasilannya. Setalah berhasil dilihat perbandingan terhadap tampilan dan kerahasian pesan kedua metode tersebut.

5.5.1. Pengujian Enkripsi dengan Metode Vernam Cipher

Pada pengujian ini tanda tangan digital diproses dengan metode Vernam Cipher yang menggunakan operasi XOR. Citra tanda tangan digital dilakukan perhitungan nilai RGB. Selanjutnya diubah menjadi bilangan desimal dan setelah itu diubah dalam bentuk biner. Sebelum dilakukan pengujian dengan menggunkan metode Vernam Cipher dilakukan perhitungan dan pencarian nilai citra tanda tangan. Sebagai contoh digunakan citra berukuran 512x512 yang ditunjukan pada Gambar 20.

Gambar 20 Citra Tanda Tangan Digital

Citra tanda tangan tersebut dihitung nilai RGB pada *pixel* yang lebih kecil misalnya dengan citra berukuran 5x5 *pixel*. Tampilan citra berukuran 5x5 *pixel* yang diambil dapat dilihat pada Gambar 21.



Gambar 21 Citra tanda tangan 512x512 pixel

Pada citra berukuran 5x5 *pixel* diperoleh nilai dalam bentuk desimal. Nilai desimal tersebut nantinya diubah dalam bentuk biner. Nilai desimal dari citra 5x5 *pixel* dapat dilihat pada Tabel 1.

Tabel 1 Nilai ASCII Desimal Citra Tanda Tangan 5x5 Pixel

		x				
		220	221	222	223	224
y	158	246	240	239	244	249
	159	211	190	182	203	231
	160	121	82	72	114	169
	161	34	9	8	33	102
	162	6	2	2	7	58

Nilai citra 5x5 *pixel* dalam bentuk desimal diubah dalam bentuk biner 8 bit sesuai kode ASCII. Nilai biner citra 5x5 *pixel* tersebut dapat dilihat pada Tabel 2.

Tabel 2 Nilai Biner Citra Tanda Tangan

		x				
		220	221	222	223	224
y	158	11110110	11110000	11101111	11110100	11111001
	159	11010011	10111110	10110110	11001011	11100111
	160	01111001	01010010	01001000	01110001	10101001
	161	00100010	00001001	00001000	00100001	01100110
	162	00000110	00000010	00000010	00000111	00111010

Sebagai citra cover dihitung nilai RGB pada *pixel* yang lebih kecil misalnya dengan citra berukuran 5x5 *pixel*. Nilai Citra cover yang berupa nilai desimal diubah dalam bentuk nilai biner juga. Nilai desimal citra cover dapat dilihat pada Tabel 3.

Tabel 3 Nilai ASCII Desimal Citra Kunci 5x5 Pixel

		x				
		220	221	222	223	224
y	158	255	255	255	255	255
	159	255	255	255	255	255
	160	255	255	255	255	255
	161	255	255	255	255	255
	162	255	255	255	255	255

Representasikan dalam bentuk biner citra kunci 5x5 pixel yang dilihat pada Tabel 4.

Tabel 4 Representasi Nilai Biner Citra Kunci

		x				
		220	221	222	223	224
y	158	11111111	11111111	11111111	11111111	11111111
	159	11111111	11111111	11111111	11111111	11111111
	160	11111111	11111111	11111111	11111111	11111111
	161	11111111	11111111	11111111	11111111	11111111
	162	11111111	11111111	11111111	11111111	11111111

Pada tahapan ini nilai biner citra tanda tangan di XOR dengan nilai biner citra kunci. Pada tabel 5 berikut menunjukan nilai yang berada di atas adalah nilai biner citra tanda tangan dan nilai yang berada di bawah adalah nilai biner citra kunci.

Tabel 5 Operasi Vernam Cipher XOR

		x				
		220	221	222	223	224
y	158	11110110 11111111	11110000 11111111	11101111 11111111	11110100 11111111	11111001 11111111
	159	11010011 11111111	10111110 11111111	10110110 11111111	11001011 11111111	11100111 11111111
	160	01111001 11111111	01010010 11111111	01001000 11111111	01110001 11111111	10101001 11111111
	161	00100010 11111111	00001001 11111111	00001000 11111111	00100001 11111111	01100110 11111111
	162	00000110 11111111	00000010 11111111	00000010 11111111	00000111 11111111	00111010 11111111

Setelah nilai dari kedua citra didapat maka dilakukan perhitungan menggunakan metode Vernam Cipher dengan operasi XOR. Setiap nilai bit citra tanda tangan di XOR dengan nilai biner dari citra cover. Hasil dari perhitungan menggunakan metode Vernam Cipher dengan operasi XOR tersebut dapat dilihat pada Tabel 6.

Tabel 6 Hasil Vernam Cipher XOR

		x				
		220	221	222	223	224
y	158	00001001	00001111	00010000	00000100	00000110
	159	00101100	01000001	01001001	00110100	00011000
	160	10000110	10101101	10110111	10001110	01010110
	161	11011101	11110110	11110111	11011110	10011001
	162	11111001	11111101	11111101	11111000	11000101

Pengujian pertama yaitu menggunakan citra tanda tangan pertama dengan nama ttd1 yang berukuran file 37 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 17 Kb. Selisih ukuran file sebelum dan setelah proses enkripsi adalah 20 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 14 Kb. Selisih citra ttd1 dengan citra proses dekripsi adalah 23 Kb.

Pada pengujian kedua yaitu menggunakan cita tanda tangan kedua dengan nama ttd2 yang berukuran file 36 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 17 Kb. Selisih ukuran file sebelum dan sesudah proses penkripsi adalah 19 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 14 Kb. Dan selisih citra ttd2 dengan citra proses dekripsi adalah 22 Kb.

Pengujian ketiga yaitu menggunakan citra tanda tangan ketiga dengan nama ttd3 yang berukuran file 30 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 15 Kb. Selisih ukuran file sebelum dan sesudah proses enkripsi adalah sebesar 15 Kb. Setelah dilakukan proses dekripsi berubah menjadi ukuran 12 Kb. Dan selisih citra ttd3 dengan citra proses dekripsi adalah 18 Kb.

Pengujian selanjutnya keempat yaitu menggunakan citra tanda tangan keempat dengan nama ttd4 yang berukuran file 34 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 16 Kb. Selisih ukuran file sebelum dan sesudah ekripsi adalah sebesar 18 Kb. Dan setelah dilakukan proses berubah menjadi ukuran 13 Kb. Selisih citra ttd4 dengan citra proses dekripsi adalah 22 Kb.

Pengujian kelima yaitu menggunakan citra tanda tangan kelima dengan nama ttd5 yang berukuran file 35 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 17 Kb. Selisih ukuran file sebelum dan sesudah proses enkripsi adalah sebesar 18 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi

ukuran 14 Kb. Dan selisih citra ttd5 dengan citra proses dekripsi adalah 21 Kb.

Pengujian keenam yaitu menggunakan citra tanda tangan keenam dengan nama ttd6 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 15 Kb. Selisih ukuran file sebelum dan sesudah proses enkripsi adalah sebesar 17 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 12 Kb. Selisih citra ttd6 dengan citra proses dekripsi adalah 20 Kb.

Pengujian ketujuh yaitu menggunakan citra tanda tangan ketujuh dengan nama ttd7 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 15 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 17 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 12 Kb. Selisih citra ttd7 dengan citra proses dekripsi adalah 20 Kb.

Pengujian kedelapan yaitu menggunakan citra tanda tangan kedelapan dengan nama ttd8 yang berukuran file 34 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 17 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 17 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 14 kb. Selisih citra ttd8 dengan citra proses dekripsi adalah 22 Kb.

Dan pengujian kesembilan yaitu menggunakan citra tanda tangan kesembilan dengan nama ttd9 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 16 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 16 Kb. Dan setelah dilakukan proses berubah menjadi ukuran 13 Kb. Selisih citra ttd9 dengan citra proses dekripsi adalah 19 Kb.

Pengujian yang terakhir kesepuluh yaitu menggunakan citra tanda tangan kesepuluh dengan nama ttd10 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 16 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 16 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 12 Kb. Selisih citra ttd10 dengan citra proses dekripsi adalah 20 Kb. Tanda tangan, hasil pengujian enkripsi metode vernam cipher dan hasil pengujian dekripsi metode vernam cipher dapat di lihat pada Tabel 7, Tabel 8 dan Tabel 9.

Tabel 7 Hasil Pengujian

No	Nama Tanda Tangan	Citra Asli	Dimensi Citra (pixel)	Ukuran File Citra (Kb)
1	Ttd1		512x512	37
2	Ttd2		512x512	36
3	Ttd3		512x512	30
4	Ttd4		512x512	34
5	Ttd5		512x512	35
6	Ttd6		512x512	32
7	Ttd7		512x512	32
8	Ttd8		512x512	34
9	Ttd9		512x512	32
10	Ttd10		512x512	32

Tabel 8 Hasil Pengujian Enkripsi Metode Vernam Cipher

No	Citra Asli	Citra Kunci	Hasil XOR	Ukuran File Citra (Kb)
1				17
2				17
3				15
4				16
5				17
6				15
7				15
8				17
9				16
10				16

Tabel 9 Hasil Pengujian Dekripsi Metode Vernam Cipher

No	Citra XOR	Citra Kunci	Hasil XOR	Ukuran File Citra (Kb)
1				14
2				14
3				12

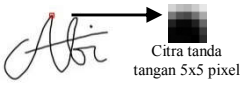
4				13
5				14
6				12
7				12
8				14
9				13
10				12

5.5.2. Pengujian Enkripsi dengan Metode Steganografi LSB

Cara yang digunakan yaitu menyisipkan cover kedalam bit rendah atau bit yang paling kanan (LSB). Caranya mengganti tiap-tiap bit pixel pada file citra tanda tangan yang disisipkan. Untuk menyisipkan citra cover ke dalam citra tanda tangan dicari nilai citra tanda tangan terlebih dahulu. Sebagai contoh digunakan citra berukuran 512x512 *pixel* yang ditunjukan pada Gambar 22.

Gambar 22 Citra Tanda Tangan Digital

Citra tanda tangan tersebut dihitung nilai RGB pada *pixel* yang lebih kecil misalnya dengan citra berukuran 5x5 *pixel*. Tampilan citra berukuran 5x5 *pixel* yang diambil dapat dilihat pada Gambar 23.



Gambar 23 Citra Tanda Tangan 512x512 *pixel*

Pada citra berukuran 5x5 *pixel* diperoleh nilai dalam bentuk desimal. Nilai tersebut nantinya diubah dalam bentuk biner. Nilai desimal citra 5x5 *pixel* seperti pada Tabel 10.

Tabel 10 Nilai ASCII Desimal Citra 5x5 Pixel

		x				
		220	221	222	223	224
y	158	246	240	239	244	249
	159	211	190	182	203	231
	160	121	82	72	114	169
	161	34	9	8	33	102
	162	6	2	2	7	58

Nilai citra 5x5 *pixel* dalam bentuk desimal diubah dalam bentuk biner 8 bit sesuai kode ASCII. Nilai biner tersebut dapat dilihat pada Tabel 11.

Tabel 11 Nilai Biner Citra 5x5 *pixel*

		x				
		220	221	222	223	224
y	158	11110110	11110000	11101111	11110100	11111001
	159	11010011	10111110	10110110	11001011	11100111
	160	01111001	01010010	01001000	01110001	10101001
	161	00100010	00001001	00001000	00100001	01100110
	162	00000110	00000010	00000010	00000111	00111010

Sebagai citra cover dihitung nilai RGB pada *pixel* yang lebih kecil misalnya dengan citra berukuran 5x5 *pixel*. Nilai Citra cover yang berupa nilai desimal diubah dalam bentuk nilai biner juga. Nilai desimal citra cover dapat dilihat pada Tabel 12.

Tabel 12 Nilai ASCII Desimal Citra Kunci 5x5 Pixel

		x				
		220	221	222	223	224
y	158	255	255	255	255	255
	159	255	255	255	255	255
	160	255	255	255	255	255
	161	255	255	255	255	255
	162	255	255	255	255	255

Selanjutnya nilai desimal citra cover berukuran 5x5 *pixel* diubah dalam bentuk nilai biner. Nilai biner dapat dilihat pada Tabel 13.

Tabel 13 Representasi Nilai Biner Citra Kunci

		x				
		220	221	222	223	224
y	158	11111111	11111111	11111111	11111111	11111111
	159	11111111	11111111	11111111	11111111	11111111
	160	11111111	11111111	11111111	11111111	11111111
	161	11111111	11111111	11111111	11111111	11111111
	162	11111111	11111111	11111111	11111111	11111111

Setelah nilai dari kedua citra didapat maka dilakukan perhitungan menggunakan metode Steganografi LSB. Setiap nilai bit terakhir citra tanda tangan digantikan dengan nilai biner dari citra cover. Hasil dari perhitungan menggunkan metode Steganografi LSB tersebut dapat dilihat pada Tabel 14.

Tabel 14 Hasil Steganografi LSB

		x				
		220	221	222	223	224
y	158	11110111	11110001	11101111	11110101	11111001
	159	11010011	10111111	10110111	11001011	11100111
	160	01111001	01010011	01001001	01110001	10101001
	161	00100011	00001001	00001001	00100001	01100111
	162	00000111	00000011	00000011	00000111	00111011

Pengujian pertama yaitu menggunakan citra tanda tangan pertama dengan nama ttd1 yang berukuran file 37 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 34 Kb. Selisih ukuran file sebelum dan setelah proses enkripsi adalah 3 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 32 Kb. Selisih citra ttd1 dengan citra proses dekripsi adalah 5 Kb.

Pada pengujian kedua yaitu menggunakan cita tanda tangan kedua dengan nama ttd2 yang berukuran file 36 Kb. Setelah dilakukan proses enkripsi berubah menjadi

ukuran 33 Kb. Selisih ukuran file sebelum dan sesudah proses penkripsi adalah 3 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 30 Kb. Dan selisih citra ttd2 dengan citra proses dekripsi adalah 6 Kb.

Pengujian ketiga yaitu menggunakan citra tanda tangan ketiga dengan nama ttd3 yang berukuran file 30 Kb Setelah dilakukan proses enkripsi berubah menjadi ukuran 21 Kb. Selisih ukuran file sebelum dan sesudah proses enkripsi adalah sebesar 9 Kb. Setelah dilakukan proses dekripsi berubah menjadi ukuran 18 Kb. Dan selisih citra ttd3 dengan citra proses dekripsi adalah 12 Kb

Pengujian selanjutnya keempat yaitu menggunakan citra tanda tangan keempat dengan nama ttd4 yang berukuran file 34 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 29 Kb. Selisih ukuran file sebelum dan sesudah ekripsi adalah sebesar 5 Kb. Dan setelah dilakukan proses berubah menjadi ukuran 26 Kb. Selisih citra ttd4 dengan citra proses dekripsi adalah 8 Kb.

Pengujian kelima yaitu menggunakan citra tanda tangan kelima dengan nama ttd5 yang berukuran file 35 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 33 Kb Selisih ukuran file sebelum dan sesudah proses enkripsi adalah sebesar 5 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 29 Kb. Dan selisih citra ttd5 dengan citra proses dekripsi adalah 6 Kb.

Pengujian keenam yaitu menggunakan citra tanda tangan keenam dengan nama ttd6 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 27 Kb. Selisih ukuran file sebelum dan sesudah proses enkripsi adalah sebesar 5 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 23 Kb. Selisih citra ttd6 dengan citra proses dekripsi adalah 9 Kb.

Pengujian ketujuh yaitu menggunakan citra tanda tangan ketujuh dengan nama ttd7 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 24 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 8 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 21 Kb. Selisih citra ttd7 dengan citra proses dekripsi adalah 11 Kb.

Pengujian kedelapan yaitu menggunakan citra tanda tangan kedelapan dengan nama ttd8 yang berukuran file 34 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 30 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 4 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 27 Kb. Selisih citra ttd8 dengan citra proses dekripsi adalah 7 Kb.

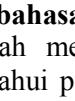
Dan pengujian kesembilan yaitu menggunakan citra tanda tangan kesembilan dengan nama ttd9 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 24 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 8 Kb. Dan setelah dilakukan proses berubah menjadi ukuran 21 Kb. Selisih citra ttd9 dengan citra proses dekripsi adalah 11 Kb.

Pengujian yang terakhir kesepuluh yaitu menggunakan citra tanda tangan kesepuluh dengan nama ttd10 yang berukuran file 32 Kb. Setelah dilakukan proses enkripsi berubah menjadi ukuran 24 Kb. Selisih ukuran file sebelum dan sesudah enkripsi adalah sebesar 8 Kb. Dan setelah dilakukan proses dekripsi berubah menjadi ukuran 22 Kb. Selisih citra ttd10 dengan citra proses dekripsi adalah 10 Kb. Hasil pengujian enkripsi metode Steganografi LSB dan hasli pengujian dekripsi metode Steganografi LSB dapat di lihat pada Tabel 15 dan Tabel 16.

Tabel 15 Hasil Pengujian Enkripsi Metode Steganografi LSB

No	Citra Asli	Citra Cover	Hasil	Ukuran File Citra (Kb)
1				34
2				33
3				21
4				29
5				33
6				27
7				24
8				24
9				24
10				24

Tabel 16 Hasil Pengujian Dekripsi Metode Steganografi LSB

No	Citra Asli	Citra Cover	Hasil	Ukuran File Citra (Kb)
1				32
2				30
3				18
4				26
5				29
6				23
7				21
8				27
9				21
10				22

5.6. Pembahasan

Setelah melakukan perhitungan maka dapat diketahui perbandingan serta perbedaan nilai pada citra yang telah dienkripsi dan dekripsi. Analisa yang dilakukan berupa perubahan pada ukuran file citra enkripsi dan dekripsi. Untuk metode Vernam Cipher memiliki selisih rata-rata untuk enkripsi sebesar 17.3 Kb dan dekripsi rata-rata 20.4 Kb. Sedangkan dengan metode Steganografi LSB memiliki selisih rata rata untuk enkripsi sebesar 3.5 Kb dan dekrispi rata-rata 8.5 Kb.

5.7. PEMBAHASAN

Setelah melakukan perhitungan maka dapat diketahui perbandingan serta perbedaan nilai pada citra yang telah dienkripsi dan dekripsi. Analisa yang dilakukan berupa perubahan pada ukuran file citra enkripsi dan dekripsi. Untuk metode vernam cipher memiliki selisih rata-rata untuk enkripsi sebesar 17.3 Kb dan dekripsi rata-rata 20.4 Kb. Sedangkan dengan metode steganografi LSB memiliki selisih rata rata untuk enkripsi sebesar 3.5 Kb dan dekrispi rata-rata 8.5 Kb.

Tabel 17 Hasil Selisih Dan Rata-rata Enkripsi dan Dekripsi Metode Vernam Cipher

Nama Tanda Tangan	Selisih Enkripsi	Selisih Dekirpsi
Ttd1	20 Kb	23 Kb
Ttd2	19 Kb	22 Kb
Ttd3	15 Kb	18 Kb
Ttd4	18 Kb	21 Kb
Ttd5	18 Kb	21 Kb
Ttd6	17 Kb	20 Kb
Ttd7	17 Kb	20 Kb
Ttd8	17 Kb	20 Kb
Ttd9	16 Kb	19 Kb
Ttd10	16 Kb	20 Kb
Rata-Rata	17.3	20.4

Tabel 18 Hasil Selisih Dan Rata-Rata Enkripsi dan Dekripsi Metode Steganografi LSB

Nama Tanda Tangan	Selisih Enkripsi	Selisih Dekirpsi
Ttd1	3 Kb	5 Kb
Ttd2	3 Kb	6 Kb
Ttd3	9 Kb	12 Kb
Ttd4	5 Kb	8 Kb
Ttd5	2 Kb	6 Kb
Ttd6	5 Kb	9 Kb
Ttd7	8 Kb	11 Kb
Ttd8	4 Kb	7 Kb
Ttd9	8 Kb	11 Kb
Ttd10	8 Kb	10 Kb
Rata-rata	5.5 Kb	8.5 Kb

6. KESIMPULAN DAN SARAN

6.1. Kesimpulan

Berdasarkan dari penelitan yang dilakukan yaitu analisa perbandingan metode Vernam Cipher dan Steganografi LSB maka kesimpulan yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

1. Perbandingan yang didapat menggunakan metode Vernam Cipher memiliki selisih untuk enkripsi rata-rata sebesar 17.3 Kb dan selisih untuk dekripsi rata-rata sebesar 20.4 Kb.
2. Perbandingan yang didapat menggunakan metode Steganografi LSB memiliki selisih untuk enkripsi rata-rata sebesar 5.5 Kb dan selisih untuk dekripsi rata-rata sebesar 8.5 Kb.
3. Dari rata-rata selisih kedua metode yakni metode Vernam Cipher dan Steganografi LSB membuktikan bahwa metode Steganogarfi LSB memiliki hasil enkripsi dan dekripsi yang lebih baik karena selisihnya yang kecil sebesar rata-rata sebesar 5.5 Kb untuk enkripsi dan rata-rata sebesar 8.5 Kb untuk dekripsi. Semakin kecil selisih ukurannya maka semakin mirip antara citra asli denan metode Vernam Cipher atau Steganografi LSB.

6.2. Saran

Saran yang dapat disampaikan dalam penelitian ini kedepannya menjadi lebih baik, terutama berkaitan dengan pengembangan sistem. Saran dari penulis yaitu metode ini bisa menggunakan media lain yaitu seperti audio atau video.

7. DAFTAR PUSTAKA

[1] T. S. Permana, C. A. Sari, E. H. Rachmawanto, D. R. Ignatius, M. Setiadi and E. R. Subhiyakto, "Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher," *Techno.com,* pp. 337-347, 2017.

[2] M. M. Amin, "Image Steganography Dengan Metode Least Significant Bit (LSB)," *CSRID Journal,* vol. 6, pp. 53-64, 2014.

[3] M. Sholeh and J. Hamokwarong, "Aplikasi Kriptografi Dengan Metode Vernam Cipher Dan Metode Permutasi Biner," *Momentum,* vol. 7, pp. 8-13, 2011.

[4] D. Nugroho and Maftuhin, "Penerapan Steganografi Pada File Gambar (Jpg) Menggunakan Metode LSB Dengan Aplikasi Matlab," *Jurnal Visualika – STMIK Muhammadiyah Jakarta,* pp. 53-58, 2016.

[5] F. Nurhasanah and R. Sulaiman, "Pembuatan Tanda Tangan Digital Menggunakan Digital Signature Algorithm," 2013.

[6] T. Sutoyo, E. Mulyanto, V. Suhartono, O. D. Nurhayati and W. , Teori Pengolahan Citra Digital, Yogyakarta: Andi, 2009.

[7] D. Ariyus, Kriptografi Keamanan Data Dan Komunikasi, Yogyakarta: Graha Ilmu, 2006.

[8] A. Kadir, Dasar Pemograman WEB dengan ASP, Yogyakarta: Andi, 2005.

[9] Sutoyo, E. Mulyanto, V. Suhartono, D. N. and W. , Pengolahan Citra Digital, 2009.

[10] M. Nasrun, G. Dwi and R. , "Implementasi kriptografi dan steganografi pada media gambar menggunakan algoritma blowfish dan metode least signifikan bit," 2016.

[11] A. Wahyuni, "Aplikasi Kriptografi Untuk Pengamanan E-Dokument dengan Metode Hybrid : Biometrik Tandatangan Dan DSA (Digital Signature Algorithm)," 2011.

[12] Sutoyo, E. Mulyanto, V. Suhartono, O. D. Nurhayati and W. , Teori Pengolahan Citra Digital, Yogyakarta: Andi, 2009.