PERANCANGAN DAN ANALISIS STEGANOGRAFI VIDEO BEBASIS STATIONARY WAVELET TRANSFORM MENGGUNAKAN METODE SINGULAR VALUE DECOMPOSITION DENGAN COMPRESSIVESENSING DAN ALGORITMA KRIPTOGRAFI RSA

DESIGN AND ANALYSIS OF VIDEO STEGANOGRAPHY BASED ON STATIONARY WAVELET TRANSFORM USING SINGULAR VALUE DECOMPOSITION WITH COMPRESSIVE SENSING METHOD AND RSA CRYPTOGRAPHY ALGORITHM

Rifki Husnil Mujalas[1], Rita Magdalena[2], Irma Safitri[3]
[1,2,3] Universitas Telkom, Bandung
rhmujalas@student.telkomuniversity.ac.id[1], ritamagnalena@telkomuniversity.ac.id[2], irmasaf@telkomuniversity.ac.id[3]

Abstrak

Pesatnya perkembangan teknologi, berdampak negatif pada kerahasiaan dan keamanan informasi yang dimiliki pengguna saat melakukan transmisi informasi. Sekiranya diperlukan sistem untuk mencegah bocornya informasi. Salah satu cara menjaga kerahasiaan informasi adalah menggunakan teknik steganografi, dimana informasi disisipkan pada media pembawa dilakukan transmisi. Namun, umumnya penggunaan teknik steganografi saat ini membuat teknik tersebut tidak terlalu efektif. Agar masalah itu dapat diatasi, maka penulis bertujuan melakukan penelitian untuk menggabungkan teknik steganografi dengan teknik kriptografi. Pada penelitian ini akan dilakukan perancangan dan analisis steganografi video berbasis SWT menggunakan teknik SVD dan algoritma kriptografi RSA. Proses steganografi sendiri menggunakan *Stationary Wavelet Transform* (SWT) dan *singular Value Decomposition* (SVD) sebagai ruang penyisipan informasi. Proses kriptografi sendiri menggunakan algoritma RSA untuk *chipering* informasi teks. Sebagai perbandingan, akan disematkan teknik kompresi *Compressive Sensing* (CS) untuk memperkecil ukuran informasi. Berdasarkan hasil pengujian yang telah dilakukan, diperoleh parameter sistem yang paling optimal antara lain P = 13, Q = 17, *layer* RGB merah, *subband* LL, *mother wavelet* db3, dan *frame* ke-11 dengan raihan persentase BER sebesar 0%, persentase CER sebesar 0%, dan nilai PSNR 87,033. Sedangkan raihan untuk sistem dengan kompresi mendapatkan persentase BER sebesar 6,956%, persentase CER sebesar 34,783% dan nilai PSNR sebesar 92,673 dB.
Kata Kunci: Steganografi, Kriftografi, RSA, SVD-CS

Abstract

Technological developments have a negative impact on security of information owned by users when transmitting information. If a system is needed to prevent information leakage. One way to maintain the confidentiality of information is to use steganography technique, where information is inserted into the carrier medium for transmission. However, generally the current use of steganography techniques makes these techniques uneffective. This problem can be overcome, the author aims to conduct research to combine steganography with cryptographic. In this research, SWT-based video steganography will be designed and analyzed using SVD and RSA cryptographic algorithm. Steganography process uses Stationary Wavelet Transform and singular Value Decomposition as information insertion space. Cryptographic process uses the RSA algorithm for ciphering text information. For comparison, Compressive Sensing compression will be embedded to reduce size of information. Based on the results of the tests, the most optimal system parameters obtained P = 13, Q = 17, red RGB layer, LL subband, mother wavelet db3, and 11th frame with BER percentage achievement of 0%, CER percentage of 0 %, and the PSNR value is 87,033. While the achievement for the compressed system gets BER percentage of 6.956%, CER percentage of 34.783% and PSNR value of 92.673 dB.
Keywords: Steganography, Cryptography, RSA, SVD-CS.

1. Pendahuluan

Media internet dewasa ini menjadi media utama dalam pertukaran informasi, baik tulisan, gambar, atau video. Namun tentu ada dampak positif dan dampak negatif dalam pertukaran informasi dalam dunia internet ini. Dampak positifnya adalah informasi dapat sampai ke tujuan dengan kecepatan yang sangat cepat, hanya dalam hitungan detik saja. Adapun salah satu dampak negatifnya adalah rentannya hak cipta sang pemilik asli, dan dengan mudah orang lain bisa mengakui bahwa itu adalah miliknya.

Dalam proses pertukaran informasi ada banyak hal yang bisa membuat informasi cacat atau rusak yang disebabkan pihak ketiga, dikarenakan hal itu diperlukan sebuah cara yang bisa menjaga keamanan sebuah informasi dari pihak ketiga. Salah satu cara yang dapat dilakukan adalah menggunakan teknik steganografi, teknik ini bisa menjadi cara mengamankan informasi [2]. Steganografi yaitu sebuah cara menyembunyikan atau menyisipkan informasi ke dalam sebuah media, baik informasi biasa atau bahkan informasi rahasia .

Pada penelitian ini, metode yang digunakan untuk proses steganografi adalah *Stationary Wavelet Transform* (SWT) yang digabungkan dengan *Singular Value Decomposition* (SVD), sebagai tambahan juga akan digunakan *Compressive Sensing* (CS) yang bisa memperkecil ukuran informasi. Tujuan dari kompresi ini adalah memperkecil ukuran *file* citra sehingga lebih efisien dalam penyimpanan pada *media storage* serta dapat menjaga kualitas citra secara visual manusia setelah proses rekonstruksi citra terkompres dengan memperhatikan nilai *Bit Error Rate* (BER) dan *Peak Signal to Noise Ratio* (PSNR)

2. Konsep Dasar

2.1 Kriptografi RSA

Algoritma RSA merupakan algoritma kriptografi yang paling populer diantara algoritma kriptografi asimetris. Algoritma ini dikembangkan oleh tiga orang peneliti dari *Massachussets Institute of Technology* (MIT) pada tahun 1976 dan mereka adalah Rivest, Shamir, dan Adleman. Sesuai nama penemunya, algoritma ini disebut RSA. Algoritma RSA melakukan enkripsi dengan cara memfaktoran bilangan yang sangat besar menjadi faktor prima, dimana pemfaktoran dilakukan untuk memperoleh kunci yang bersifat privat. Adapun besaran-besaran yang dimiliki Algoritma RSA adalah sebagai berikut:

Tabel 2.1: Besaran Algoritma Kriptografi RSA

Simbol	Keterangan	Sifat	Syarat
p dan q	Bilangan Prima	Rahasia	∞
n	$n = p \times i(q)$	Tidak Rahasia	∞
$i(n)$	$i(n) = (p-1)(q-1)$	Rahasia	∞
E	Kunci Enkripsi	Tidak Rahasia	$PBB(e,i(n)) = 1$
d	Kunci Deskripsi	Rahasia	$d = e^{-1} mod(i(m))$
m	*Plaintext*	Rahasia	ASCII *code*
c	*Chipertext*	Tidak Rahasia	∞

A. Algoritma Pembentukan Kunci
   a. Menentukan dua bilangan prima untuk p dan q (rahasia),
   b. Kalkulasi $n = pq$ dengan nilai dari n tidak perlu dirahasiakan,
   c. Kalkulasi $(n) = (p–1)(q–1)$,
   d. Menentukan sebuah bilangan bulat untuk kunci yang bersifat publik dengan simbol e dengan nilai relatif prima terhadap (n) dan dapat dihitung menggunakan pemfaktoran,
   e. Kalkulasi kunci untuk proses dekripsi d dengan cara $ed \equiv 1 (mod\ m)$ atau $d \equiv e^{-1} mod(i(n))$.

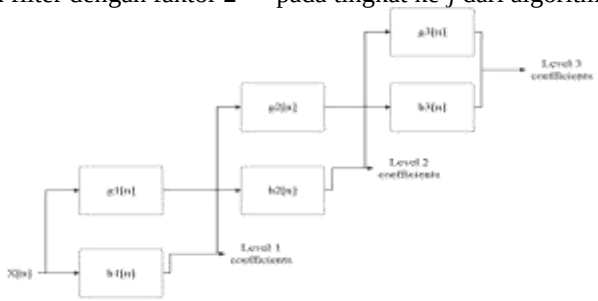
   Hasil dari proses di atas berupa kunci publik dengan pasangan (e,n) dan kunci privat adalah pasangan (d,n).

B. Algoritma Enkripsi
   Menghitung nilai $c = N^e \ mod\ n$ untuk memperoleh *chipertext*. Dari perhitungan tersebut, maka didapatkan *ciphertext* (c) yang siap untuk dikirimkan.

C. Algoritma Dekripsi
   Menghitung $M = c^d \ mod\ n$ untuk mendapatkan pesan kembali dengan d didapatkan dari kunci privat. Dari perhitungan algoritma tersebut menghasilkan pesan hasil dekripsi.

2.2 *Stationary Wavelet Transform*

Transformasi *wavelet* stasioner (SWT) atau transformasi *wavelet Undecimated* adalah modifikasi dari Transformasi *Wavelet* Diskrit untuk menjadikannya sebagai terjemahan-invarian di domain yang tidak menghilangkan koefisien pada setiap tingkat transformasi. *Translation invariance* dicapai dengan menghilangkan *samplers* bawah dan *samplers* sampul di DWT dan up sampling koefisien filter dengan faktor $2^{(j-1)}$ pada tingkat ke-j dari algoritma.



Gambar 2.1: Tiga Fase Dekomposisi menggunakan SWT

Gambar 2.1 merupakan skema inheren redundant karena output dari setiap level mengandung jumlah sampel yang sama dengan input. Jadi untuk dekomposisi level N ada redundansi N pada koefisien wavelet. Algoritma ini, yang diusulkan oleh Holdschneider juga dikenal sebagai ”*algorithmme a trous*``”, mengacu pada memasukkan angka nol pada filter

2.3 *Compressive Sensing*

.*Compressive sensing* (CS) merupakan metoda *sampling* baru dimana akuisisi dan kompresi sinyal dilakukan dalam satu waktu. Idenya adalah memperkenalkan skema sampling dalam jumlah yang lebih rendah dari sample yang diperlukan, dimana sampling tersebut mewakili sinyal *sparse* asli.

Sebuah sinyal $x \in R\ N$ merupakan sinyal *k-sparse* ketika kebanyakan dari elemen *k* dari *x* adalah *non-zero*. Apabila $f \in R\ N$ merupakan sinyal *k-sparse* yang terdapat dalam ruang ψ, dimana ψ merupakan kombinasi linear dari *N*, maka ψ merupakan basis ortonormal dan *f* muncul dengan persamaan

$$f = \psi x \quad (2.1)$$

Lalu sinyal *x* bisa merepresentasikan suatu sinyal *sparse* dengan menggunakan persamaan

$$x=\psi^0 f \quad (2.2)$$

$$y= \varphi f \quad (2.3)$$

dimana $y \in R\ M$ adalah vektor perhitungan dan φ adalah *M*×*N sensing matrix*, lalu persamaan sebelumnya akan diubah menjadi

$$y = \varphi f = \varphi\psi x = \varphi x \quad (2.4)$$

dimana $\varphi \in R\ M \times N$ merepresentasikan *underdetermined matrix* dengan $M \ll N$.

Metode rekonstruksinya memperkirakan jika sinyal $\hat{}x$ yang hampir seluruh nilai *k* adalah *non-zero* dan $k < M \ll N$. Jika matriks φ memenuhi *Restricted Isometry Property* (RIP), maka $\hat{}x$ bisa direkonstruksi sepenuhnya menggunakan algoritma OMP (Orthogonal Matching Pursuit) [5].

Suatu matriks φ dikatakan memenuhi RIP dengan *order k* jika terdapat $\delta k \in$ (0,1) seperti

$$(1-\delta k)|x|\frac{2}{2} \le |\varnothing x|\frac{2}{2} \le (1+\delta k)|x|\frac{2}{2} \quad (2.5)$$

dimana δ*k merupakan Restiricted Isometry Constant* (RIC). Jika φ memenuhi RIP dengan order 2*k* dengan $\delta k < 2-1$, *k* menyebar vektor *x* dan persamaan 2.4 dapat direkonstruksi menggunakan algoritma OMP menjadi

$$\hat{x}= \arg min_x \|x\|_1\ St.y - \emptyset x = 0 \quad (2.6)$$

Pada saat φ merupakan matriks *random gaussian*, maka perhitungan

$$M = O\ (k)\ \log(N/k) \quad (2.7)$$

merepresantasikan baris dari *sensing matrix*.

2.4 Rekonstruksi *Orthogonal Matching Pursuit* (OMP)

Orthogonal Matching Pursuit merupakan *greedy algorithm* yang versi pembaharuan dari *Matching Pursuit* (MP). OMP memperkirakan magnitudo dari koefisien *non-zero* dari x dengan menyelesaikan kesalahan pada kuadrat terkecil antara proyeksi orthogonal dari x yang sudah dikembalikan dan perhitungan vektor y. Perhitungan dari CS *stego-image* y_v termasuk *k*-sparse x dan *L* bit citra yang sudah disisipkan data , kemudian y_v direkonstruksi menggunakan algoritma OMP dari y_v yang dihitung dengan persamaan

$$\hat{x} = \arg min_x \|y - \emptyset x\|_2 \quad (2.8)$$

diubah menjadi

$$\hat{Z} = \arg min_x \|y_v - HZ\|_2 \quad (2.9)$$

dimana $Z = \frac{\hat{x}}{\hat{y}}$ dan $Z = \frac{x}{y}$ merupakan rekonstruksi dari sinyal x.

3. Pengujian dan Analisis

3.1 Analisis Perubahan Nilai P dan Q terhadap BER, CER dan PSNR

Gambar 3.1 Rata-Rata Perolehan BER Pada Setiap Pesan Terhadap Pengaruh Besar P dan Q Tanpa Kompresi

Gambar 3.2 Rata-Rata Perolehan BER Pada Setiap Pesan Terhadap Pengaruh Besar P dan Q Dengan Kompresi

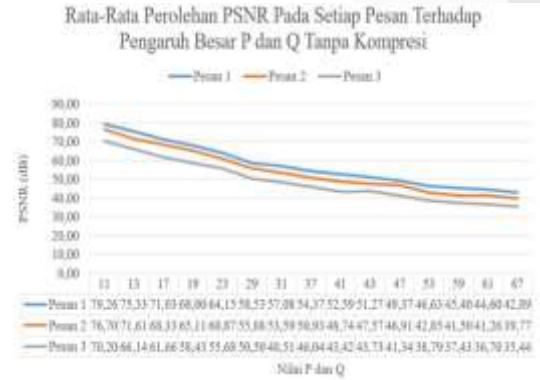
Pada perolehan persentase BER yang didapatkan, terlihat bahwa perolehan BER yang didapatkan semakin besar setelah nilai P dan Q naik. Hal ini disebabkan karena besar nilai P dan Q mempengaruhi besar kunci yang dibangun, semakin besar kunci untuk enkripsi maka semakin rumit dan besar data yang dibangun. Sedangkan jika sebuah pesan disisipkan pada sebuah video, maka kualitas pesan yang akan dikeluarkan akan sedikitnya akan menurun. Pada sistem

tanpa kompresi, persentase BER yang dihasilkan dapat lebih baik jika dibandingkan dengan persentase BER yang didapatkan oleh sistem dengan kompresi. Hal ini disebabkan karena *data loss* pada kompresi pesan mempengaruhi hasil ekstraksi pesan. Teknik rekonstruksi OMP pun merupakan teknik reconstruksi dengan pendekatan pada pesan yang sebenarnya maka hasil ekstraksi yang didapatkan tidak akan 100% sempurna. Setelah melihat perolehan rata-rata persentase BER, maka parameter pengujian yang akan diamati adalah CER untuk mengetahui kualitas pesan yang telah diekstraksi. Adapun rata-rata perolehan persentase CER dapat dilihat pada Gambar 3.3 dan Gambar 3.4.

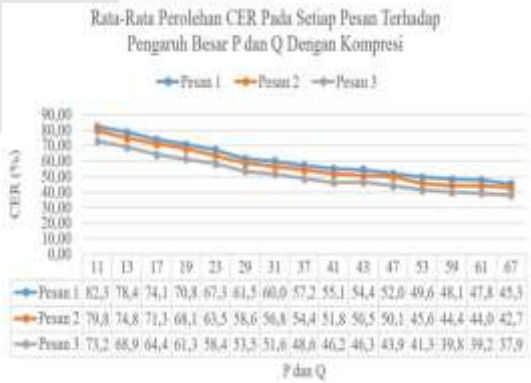
Gambar 3.3: Rata-Rata Perolehan CER Pada Setiap Pesan Terhadap Pengaruh Besar P dan Q Tanpa Kompresi

Gambar 3.4 Rata-Rata Perolehan CER Pada Setiap Pesan Terhadap Pengaruh Besar P dan Q Dengan Kompresi

Kehilangan beberapa bit untuk proses dekripsi menjadi sebuah kekurangan pada sistem kriptografi RSA. Adapun penyebab betapa tinggi nya persentase CER yang didapatkan sistem tanpa kompresi adalah karena CER bertolak ukur pada perubahan karakter dalam suatu teks, sedangkan BER bertolak ukur pada perubahan *bit* setiap karakter dan dijumlahkan setelah semua karakter diperiksa. Maka untuk mengukur kualitas ekstraksi pada teks karakter membutuhkan parameter pengujian CER sebagai penghitung karakter *error*. Pada besar P dan Q sama maka *error rate* yang didapatkan menjadi hampir 100% dan itu disebabkan oleh ketidak unikan sebuah kunci apabila pembangun dari kunci bernilai sama. Karena perhitungan data yang digunakan adalah rata-rata, maka CER yang didapatkan merupakan gabungan dari hasil terbaik dan terburuk. Setelah melakukan analisis parameter BER dan CER, maka parameter PSNR pun harus disertakan untuk menilai faktor *hidden* pada sebuah pesan yang disisipkan.



Gambar 3.5: Rata-Rata Perolehan PSNR Pada Setiap Pesan Terhadap Pengaruh Besar P dan Q Tanpa Kompresi



Gambar 3.6: Rata-Rata Perolehan PSNR Pada Setiap Pesan Terhadap Pengaruh Besar P dan Q Dengan Kompresi

Dari ketiga parameter pengujian yang telah didapatkan, maka akan dipilih parameter sistem yang paling baik untuk pengujian selanjutnya. Untuk nilai P yang akan digunakan adalah angka 13 dan untuk nilai Q yang akan digunakan adalah 17. Alasan penggunaan nilai tersebut adalah memiliki persentase BER, CER, dan PSNR yang cukup stabil dan juga karena nilai P dan Q tidak boleh sama, maka nilai yang diambil pun berbeda. Untuk pesan yang akan digunakan sendiri adalah pesan ke-2 dimana memiliki nilai parameter yang paling stabil, tidak seperti pesan ke-1 yang kurang baik terhadap sistem dengan kompresi dan pesan ke-3 yang selalu memiliki nilai parameter dibawah dua pesan lainnya.

3.2 Analisis Perubahan *Layer*

Pengujian kali ini bertujuan untuk membandingkan performansi dari setiap *layer* yang digunakan dalam sistem untuk dilakukan penyisipan. *Layer* yang digunakan didalam penelitian ini adalah RGB (merah, hijau, dan biru), YCbCr, dan HSV. Sedangkan untuk parameter sistem lainnya yang digunakan antara lain menggunakan pesan 2, P = 13, Q = 17, *subband Low-Low*, *frame* ke-1, dan *mother wavelet* menggunakan db1. Adapun hasil dari pengujian dapat dilihat pada Tabel 3.1.

Tabel 3.1: Perbandingan Persentase BER,CER, dan PSNR terhadap jenis *Layer* Pada Sistem Tanpa Kompresi dan Dengan Kompresi

	Bit Error Rate (%)		*Character Error Rate* (%)		*Peak Signal to Noise Ratio* (dB)	
Layer	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi
Merah	0,000	5,797	0,000	26,087	87,03	87,719
Hijau	4,167	6,667	12,500	26,087	87,06	89,384
Biru	20,833	8,986	75,000	43,478	87,13	90,940
YCbCr	0,000	6,957	0,000	26,087	72,82	76,020
HSV	0,000	6,087	0,000	26,087	80,00	81,961

Dari ketiga parameter pengujian yang telah didapatkan, maka akan dipilih *layer* yang paling baik untuk dijadikan acuan pada pengujian selanjutnya. Untuk *layer* yang digunakan adalah *layer* RGB merah. Alasan pemilihan *layer* RGB merah untuk dijadikan acuan pengujian selanjutnya adalah karena *layer* RGB merah memiliki persentase BER dan CER yang minim pada sistem tanpa kompresi maupun dengan kompresi. Adapun hasil dari parameter PSNR meskipun tidak sebaik *layer* RGB hijau dan biru, namun *layer* RGB merah memiliki kestabilan dalam menyembunyikan pesan dengan baik.

3.5 Analisis Perubahan *Subband*

SWT sebagai metode transformasi untuk disisipi pesan memiliki dua variabel yang diperlukan untuk menampung pesan. Adapun dua variabel yang digunakan tersebut adalah *subband* dan *mother wavelet*. Tujuan dari pengujian ini adalah melihat *subband* mana yang paling baik dalam melakukan penyisipan dan ekstraksi pesan rahasia. *Subband* yang digunakan pada pengujian ini antara lain *Low-Low, Low-High, High-Low,* dan *High-High.* Sedangkan untuk parameter sistem yang lainnya yang digunakan antaralain menggunakan pesan ke-2, P = 13, Q = 17, *layer* RGB merah, dan *mother wavelet* menggunakan db1. Adapun hasil dari pengujian dapat dilihat pada Tabel 3.2.

Tabel 3.2 Perbandingan Persentase BER,CER, dan PSNR terhadap jenis *subband* Pada Sistem Tanpa Kompresi dan Dengan Kompresi

	Bit Error Rate (%)		*Character Error Rate* (%)		*Peak Signal to Noise Ratio* (dB)	
Subband	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi
LL	0,000	5,797	0,000	26,087	87,03	87,719
LH	27,500	27,246	100,000	100,000	104,34	104,955
HL	30,000	26,377	100,000	100,000	101,87	103,717
HH	25,417	25,507	100,000	100,000	94,55	95,748

Dari ketiga parameter pengujian yang telah didapatkan, maka akan dipilih jenis *subband* yang paling baik dalam melakukan ekstraksi dan penyisipan pesan untuk dijadikan sebagai acuan pada pengujian selanjutnya. *Subband* yang akan digunakan merupakan *subband* LL dengan alasan bahwa *subband* LL memiliki persentase BER dan CER yang paling minimum, baik pada sistem tanpa kompresi maupun pada sistem dengan kompresi. Adapun hasil PSNR yang diperlihatkan, meskipun memiliki nilai PSNR paling rendah diantara *subband* yang lain, akan tetapi nilai PSNR yang didapatkan masih tergolong sangat memuaskan dimana PSNR yang didapatkan berada diatas 80 dB.

3.3 Analisis Perubahan Pada *Mother Wavelet*

Sedangkan untuk parameter sistem yang digunakan antaralain menggunakan pesan ke-2, P = 13, Q = 17, *layer* RGB merah, *subband* LL, dan *frame* ke-1. Hasil pengujian dapat dilihat pada Tabel 3.3.

Tabel 3.3 Perbandingan Persentase BER,CER, dan PSNR terhadap jenis *mother wavelet* Pada Sistem Tanpa Kompresi dan Dengan Kompresi

	Bit Error Rate (%)		*Character Error Rate* (%)		*Peak Signal to Noise Ratio* (dB)	
Mother Wavelet	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi
db1	0	10,145	0	47,826	87,0324	90,582
db2	0	15,362	0	56,522	87,0303	88,975
db3	0	10,725	0	43,478	87,0296	91,218
db4	0	13,333	0	56,522	87,0298	89,021
db5	0	11,014	0	47,826	87,0296	89,794

Setelah mendapatkan hasil dari pengujian perubahan *mother wavelet* yang digunakan dalam penyipan, maka akan dipilih *mother wavelet* yang memiliki hasil paling optimal untuk dijadikan sebagai acuan pada pengujian selanjutnya. Untuk *mother wavelet* yang dipilih adalah *mother wavelet* dB3 dengan alasan pada pengujian sistem dengan kompresi

mendapatkan persentase BER dan persentase CER yang paling minimum diantara *mother wavelet* yang lain. Sedangkan untuk peningkatan pada nilai PSNR nya sendiri merupakan yang paling tinggi.

3.4 Analisis Perubahan *Frame* Penyisipan

Adapun *frame* yang akan digunakan dalam penelitian ini adalah *frame* ke-1 hingga ke-30 dengan parameter sistem lainnya yang digunakan antaralain menggunakan pesan ke-2, P = 13, Q = 17, *subband* LL, dan *mother wavelet* db3. Hasil pengujian dapat dilihat pada Gambar 3.7, Gambar 3.8, dan Gambar 3.9.

Gambar 3.7: Perbandingan Persentase BER Terhadap Perubahan *Frame* Pada Sistem Tanpa Kompresi dan Dengan Kompresi

Gambar 3.8: Perbandingan Persentase CER Terhadap Perubahan *Frame* Pada Sistem Tanpa Kompresi dan Dengan Kompresi

Gambar 3.9: Perbandingan Nilai PSNR Terhadap Perubahan *Frame* Pada Sistem Tanpa Kompresi dan Dengan Kompresi

Setelah didapatkan hasil dari seluruh pengujian yang telah dilakukan, maka telah dipilih parameter paling optimal dalam melakukan penyisipan dan ekstraksi pada pesan yang sisipkan. Parameter sistem yang dipilih antara lain P = 13, Q = 17, *layer* RGB merah, *subband* LL, *mother wavelet* db3, dan *frame* ke-11. *frame* ke-11 dipilih dengan alasan memiliki persentase BER dan persentase CER yang paling minimum pada sistem dengan kompresi. Adapun hasil dari parameter pengujian optimal yang didapatkan antaralain persentase BER sebesar 0%, persentase CER sebesar 0%, dan nilai PSNR sebesar 87,034 dB. Sedangkan untuk sistem dengan kompresi memiliki hasil persentase BER sebesar 6,956%, persentase CER sebesar 34,783% dan nilai PSNR sebesar 92,673 dB.

3.5 Pengujian Ketahanan Sistem Terhadap Serangan

Parameter yang digunakan antaralain menggunakan pesan ke-2 P = 13, Q = 17, *layer* RGB merah, *subband* LL, *mother wavelet* db3, dan *frame* ke-11. Adapun serangan yang akan digunakan pada pengujian ini berjumlah empat serangan yakni serangan *Salt & Pepper Noise*, *Gaussian Blur*, *Rescaling*, dan *Cropping*. Pengujian dilakukan terhadap sistem tanpa kompresi dan dengan kompresi. Adapun dari hasil yang didapatkan pada pengujian terhadap serangan dapat dilihat pada Tabel 3.4

Serangan	Parameter	*Bit Error Rate* (%)		*Character Error Rate* (%)		*Peak Signal to Noise Ratio* (dB)	
		Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi	Tanpa Kompresi	Dengan Kompresi
Tanpa Serangan	-	0,000	10,725	0,000	43,478	87,033	91,218
Noise Salt and Pepper	0,01	22,500	21,739	100,000	91,304	87,033	92,855
Noise Gaussian Blur	3×3	9,583	20,870	37,500	78,261	87,033	89,556

Rescaling	50%	0,000	15,362	0,000	47,826	87,033	90,767
Crop	100×100	7,917	27,536	31,250	100,000	87,033	90,385

Setelah dilakukan pengujian ketahanan sistem dengan diberi serangan telah dilakukan, maka akan ditarik kesimpulan bagaimana kualitas sistem setelah diberi serangan. Pada sistem tanpa kompresi, sistem mampu bertahan pada tiga serangan yakni serangan *Gaussian Blur, Rescaling*, dan *Cropping*. Kelemahan sistem tanpa kompresi terdapat pada serangan *Salt & Pepper Noise*. Sedangkan pada sistem dengan kompresi, sistem hanya mampu bertahan pada serangan *Rescaling* dengan masih banyak kesalahan karakter. Sistem dengan kompresi sangat rentan terhadap serangan *Salt & Pepper Noise, Gaussian Blur,* dan *Cropping* karena pada serangan tersebut, data ekstraksi yang dihasilkan mengalami perubahan secara masif.

4. Kesimpulan dan Saran

4.1 Kesimpulan

1. Perancangan simulasi steganografi video berbasis SWT dengan teknik SVD dan algoritma RSA tanpa kompresi CS telah berhasil dilakukan dan memiliki paramater sistem yang paling optimal antaralain menggunakan pesan ke-2, P = 13, Q = 17, *layer* RGB merah, *subband* LL, *mother wavelet* db3, dan *frame* ke-11 dengan raihan persentase BER sebesar 0%, persentase CER sebesar 0%, dan nilai PSNR 87,033.
2. Perancangan simulasi steganografi video berbasis SWT dengan teknik SVD dan algoritma RSA Dengan kompresi CS telah berhasil dilakukan dengan parameter sistem yang paling optimal sama dengan parameter yang digunakan pada sistem tanpa kompresi dengan raihan persentase BER sebesar 6,956%, persentase CER sebesar 34,783% dan nilai PSNR sebesar 92,673 dB.
3. Penggunaan algoritma RSA sebagai metode kriptografi memiliki hasil yang cukup baik dengan nilai P = 13 dan Q = 17 dan menghasilkan parameter pengujian dengan raihan persentase BER sebesar 0%, persentase CER sebesar 0%, dan nilai PSNR sebesar 87 dB.
4. Hasil pengujian ketahanan sistem mendapatkan hasil yang cukup baik dimana sistem tanpa kompresi dapat bertahan pada serangan *Rescaling, Gaussian Blur,* dan *Cropping*, sedangkan untuk sistem dengan kompresi hanya dapat bertahan pada serangan *Rescaling* saja.

4.2 Saran

1. Pemasangan metode steganografi, kriptografi, dan kompresi dirasa tidak terlalu efektif, hendaknya penyandingan dilakukan dengan menerapkan hanya dua metode untuk mengurangi waktu komputasi dan memperbaiki hasil keluaran yang didapatkan.
2. Apabila ingin melakukan dengan ketiga metode tersebut, diharapkan menggunakan data yang lebih besar lagi seperti citra ataupun suara.
3. Penyandingan kompresi dengan steganografi dirasa tidak terlalu efektif karena titik pengamatan utama ada pada pesan yang ingin disisipkan, bukan kualitas dari media penampung. Lebih baik penyandingan dilakukan untuk melakukan *watermarking*.

Referensi

[1] V. K. Yaday and S. Lal, "Desaign and Implementation of Video Steganography System Using Singular Value Decomposition," vol. IV, no. 04, pp. 103-107, 2017.

[2] R. J. Mustafa, K. M. Elleithy and E. Abdelfattah, "A Robust and Secure Video Steganography Method in DWT-DCT Domains Based on Multiple Object Tracking and ECC," IEEE Access, vol. V, pp. 5354-5365, 2017.," vol. V, no. 1, pp. 5354-5365, 2017.

[3] M. B. OULD MEDENI, EL MAMOUN SOUIDI , "A STEGANOGRAPHY SCHEMA AND ERROR-CORRECTING CODES", © JATIT, 2010

[4] Jatinder Kaur, Ira Gabba, "Steganography Using RSA Algorithm", International Journal of Innovative Technology and Exploring Engineering IJITEE) ISSN: 2278-3075, Volume-3, Issue-3, August 2013.

[5] Evgeny Milanov, "The RSA Algorithm", 3 June 2009

[6] C.Gayathri & V.Kalpana ,"Study on Image Steganography Techniques", International Journal of Engineering and Technology (IJET), 2013

[7] Manveer Kaur, Gagandeep Kaur," Review of Various Steganalysis Techniques", International Journal of Computer Science and Information Technologies (IJCSIT), 2014

[8] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, April 2013.

[9] T. Moerland, Steganography and Steganalysis, Leiden Institute of Advance Computing Science.

[10] R. Halder, S. Sengupta, S. Ghosh and D. Kundu, "A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Techniue," vol. 18, no. 1, pp. 39-3, 2016.

[11] R. Apau and C. Adamoko, "Design of Image Steganography based on RSA Algorithm and LSB Insertion for Android Smartphones," vol. 16, no. 1, pp. 13-22, 2017.

[12] P. Chouskey and P. Patel, "Secret Key Steganography Technique Based on Three-Layered DWT and SVD Algorithm," vol. 35, no. 9, pp. 440-445, 2016.

[13] R. Munir, Kriptografi, Bandung: Informatika, 20106.

[14] Tanmay Bhattacharya, Stationary Wavelet Transform Based Audio Authentication Technique, West Bengal, India: Hooghly Engineering & Technology College, 2012.