ANALISIS KINERJA SVD-DWT-RSA PADA WATERMARKING CITRA

Ahmad Internaldo[1], Dr. Ida Wahidah, S.T., M.T.[2], Sofiah Sa'idah, S.T., M.T.[3]
[1,2,3] Prodi S1 Teknik Telekomunikasi, Fakultas Teknik, Universitas Telkom
[1]ahmadinternaldo@gmail.com ,[2] @telkomuniversity.ac.id [3]@telkomuniversity.ac.id

Abstrak

Perkembangan teknologi informasi pada masa ini menjadikan internet sebagai salah satu yang dicari dalam pertukaran informasi digital. Oleh karena itu, perlu adanya sistem keamanan yang tidak mudah untuk dibobol dalam pertukaran informasi, salah satunya watermarking. Watermarking citra ditujukan untuk analisis bagaimana pengaruh jenis layer yang digunakan pada DWT, nilai faktor skala SVD terhadap performansi watermarking. Hasil akhir dari tugas akhir ini yaitu untuk mendapatkan konfigurasi optimal terhadap algoritma DWT-SVD-RSA dengan citra sebagai Watermark agar menghasilkan kualitas keamanan yang lebih baik dari sebelumnya. Konfigurasi yang dimaksud adalah bagaimana pengaruh pembagian layer image yang akan digunakan pada DWT dan faktor skala SVD.
Kata kunci : ***Singular Value Decomposition, Discrete Wavelete Transform, RSA*.**

Abstract

Growth the information of technology on this era make the internet to be one of the most searchable in digitial information exchange. Because of that, security system is needed which harder to break, in this case is watermarking. Image watermarking is made to analyse the impact of the layer which is used by DWT, SVD's Scale Factor to watermarking's Performace. The end of this task is to get the most optimal's Configuration with DWT-SVD-RSA using image as watermark to get better quality of security. Configuration mean how the impact of layer's image which using in DWT and SVD's scale factor
Keywords: Singular Value Decomposition, Discrete Wavelete Transform RSA.

1 Pendahuluan

Semakin majunya perkembangan teknologi informasi, menjadikan internet sebagai salah satu yang paling dibutuhkan oleh manusia dalam hal pertukaran informasi digital. Watermarking adalah suatu cara penyembunyian atau penamaan data/informasi tertentu (baik hanya catatan umum ataupun rahasia) kedalam suatu data digital lainnya, tetapi tidak diketahui kehadirannya oleh indera manusia (penglihatan dan pendengaran) dan mampu menghadapi pengolahan sinyal digital sampai tahap tertentu[1].

Proses watermarking yang bersifat nonblind watermarking data yang disisipkan pada citra data menggunakan metode Discrete Wavelet Transform (DWT) dan Singular Value Decomposition (SVD) dan digunakan enkripsi RSA terhadap proses yang akan disisipkan. Metode DWT-SVD-RSA dipilih karena DWT memiliki kelebihan yaitu dapat menghitung kualitas image dimana pesan tersebut disembunyikan didalamnya sedangkan SVD memiliki kelebihan terhadap robustness dan kapasitas data yang disisipkan dan enkripsi RSA sebagai pengacak data untuk keamanan yang lebih tinggi.

2 Dasar Teori

2.1 Citra Digital

Secara umum pengertian citra adalah citra adalah gambar pada bidang dua dimensi. Sedangkan jika ditinjau dari sudut pandang matematis, citra merupakan fungsi kontinu dari intensitas cahaya pada bidang 2 dimensi. Citra juga merupakan kumpulan elemen gambar yang secara keseluruhan merekam suatu adegan melalui media indra visual. Citra sebagai keluaran suatu sistem perekam data dapat bersifat optic yang berupa foto, bersifat analog seperti sinyal-sinyal video pada televisi, ataupun bersifat digital yang dapat disimpan secara langsung pada media penyimpanan bersifat magnetik[2]

2.2 Kriptografi

Watermark muncul pertama pada sekitar tahun 1282 di Italia di sebuah kertas. [2] *Watermarking* adalah proses teknik penyembunyian sebuah informasi berupa teks, gambar, suara, atau video. *Watermarking* merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apa, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta atau *watermark*.

2.3 RSA

Algoritma RSA dibuat oleh tiga orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu Ron Rivest, Adi Shamir dan Leonard Adleman yang menggantikan algoritma National Bureau of Standards (NBS).

Algoritma ini menggunakan algoritma kunci publik, dimana antara enkripsi dan dekripsi menggunakan kunci yang berbeda. Untuk rumus enkripsi:

C= M^e mod(n)

Untuk Dekripsi RSA diberikan rumus sebagai berikut:

$M= C^d \bmod(n)$ (2.2)

dengan C adalah chiper text, M adalah data inputan, e dan d merupakan bilangan bulat

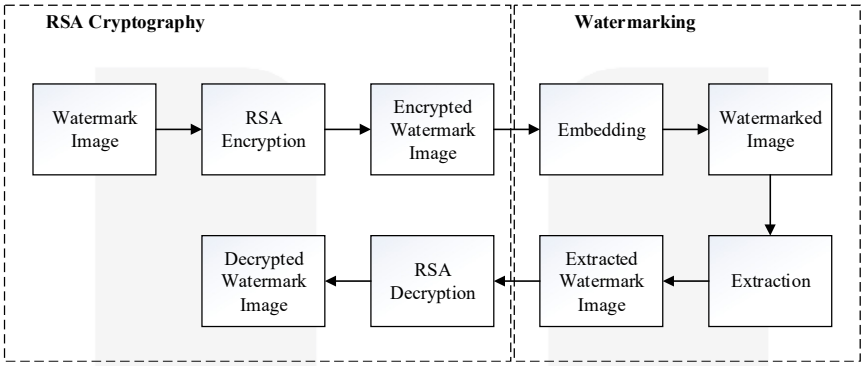
2.4 Watermarking

Suatu citra digital yang direpresentasikan dalam format digital mudah untuk disebarluaskan melalui internet dan dimanipulasi menggunakan *image processing* tools yang tersedia secara bebas.

Watermark bisa berupa teks, logo, atau ekstrasi ciri dari citra digital. Penyisipan yang dilakukan tidak merusak citra digital yang dilindungi dan watermark yang telah disisipi tidak dapat dideteksi oleh indera penglihatan manusia tetapi dapat dideteksi oleh komputer.

3 Desain dan Simulasi Sistem

3.1 Proses penyisipan-ekstraksi

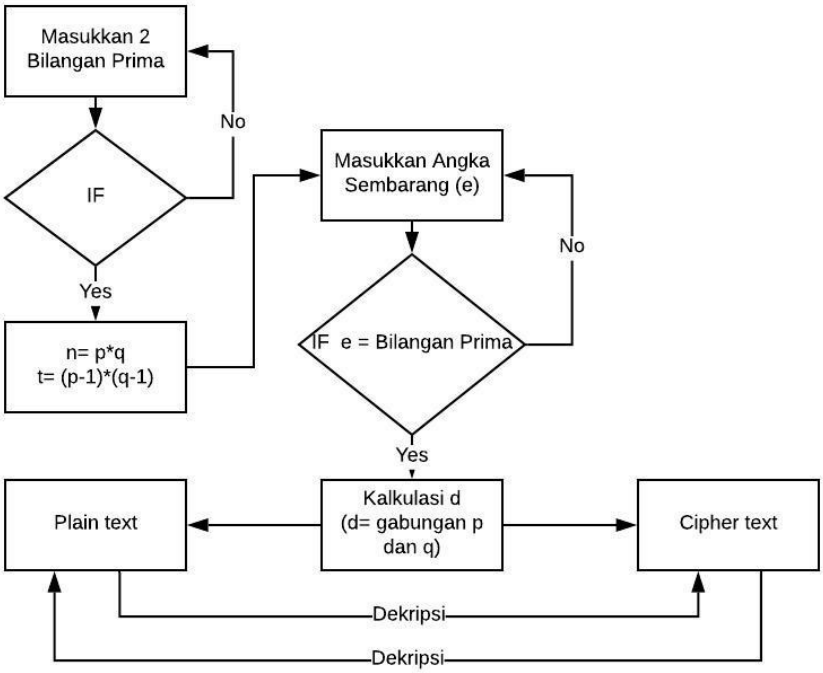


Gambar 1 Desain ekstraksi *watermarking*

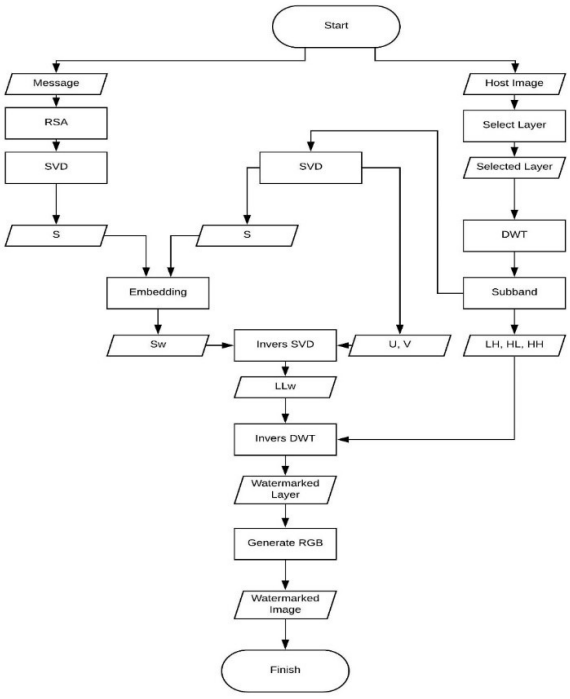
Proses dimulai dengan memilih watermark image yang selanjutnya dilakukan proses enkripsi RSA pada watermark yang terpilih. Hasil dari enkripsi RSA adalah watermark image yang sudah teracak/encrypted watermark image. Proses selanjutnya adalah proses embedding untuk menyisipkan watermark image yang sudah teracak pada host image menggunakan metode DWT-SVD dan menghasilkan watermarked image. Proses Ekstraksi adalah proses untuk mendapatkan kembali image yang sisipkan pada proses embedding. Proses terakhir adalah melakukan proses dekripsi untuk mengembalikan watermark yang teracak menjadi watermark image.

3.2 Diagram Blok

Proses kriptografi RSA bertujuan untuk sisi keamanan ganda pada watermark sehingga apabila seseorang sukses melakukan proses extraction watermark, watermark yang didapat bukan merupakan watermark sesungguhnya. Proses kriptografi terdiri dari dua proses yaitu proses enkripsi dan dekripsi. Proses enkripsi adalah proses pengacakan dan proses dekripsi adalah proses mengembalikan ke data semula dari hasil pengacakan.



3.3 Penyisipan



Proses diawali dengan Image Message yang akan di enkripsi oleh RSA dilain sisi penentuan layer Host untuk penggunaan metode metodenya. Untuk proses RSA, selanjutnya akan dilakukan SVD sehingga menghasilkan S, U dan V.pada bagian matriks ini line S yang akan diambil, tujuannya adalah menggabungkan S yang ada pada Host yang sudah diberi DWT dan SVD menghasilkan S gabungan, dalam konteks ini kita buat hasilnya dengan nama Sw.

Selanjutnya Sw dilakukan invers SVD untuk mendapatkan LLw dan LLw beserta LH, HL, dan HH digunakan untuk melakukan invers transformasi DWT untuk mendapatkan watermarked layer. Proses terkahir adalah menggabungkan watermarked layer menjadi RGB kembali untuk mendapatakan watermarked image.

4 Hasil dan Analisis

4.1 Hasil pengujian jenis layer pada data gambar

Jenis Layer	DWT-SVD				DWT			
	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi
Layer Red RGB	0.80809	49.0708	0	0.034648	0.83877	48.9022	4.06901×10^{-6}	0.034656
Layer Green RGB	0.84053	48.8855	0	0.034648	0.86457	48.7628	8.54492×10^{-5}	0.034831
Layer Blue RGB	0.81405	49.0324	0	0.034648	0.86215	48.7751	8.54492×10^{-5}	0.034831
Layer Y YCbCr	3.75082	42.3934	0	0.034648	3.87515	42.2490	4.06901×10^{-6}	0.034656
Layer V HSV	1.80475	45.7559	0	0.034648	1.67233	45.9825	8.13802×10^{-6}	0.034676

Hasil PSNR terhadap pengujian terhadap jenis layer pada data gambar, bahwa nilai PSNR terbaik yang didapatkan pada proses Embedding berada pada layer Red RGB metode DWT-SVD sdengan nilai PSNR 49,07. nilai BER terbaik yang didapatkan pada proses Dekripsi RSA bernilai sama, dengan nilai terbaik 0.0346

4.2 Hasil pengujian terhadap rasio penyisipan gambar

Rasio	DWT-SVD				DWT			
	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi
0.1	0.53731	50.83064	0	0.034648	0.664609	49.90706	0.000606	0.036572
0.2	0.964636	48.2901	0	0.034648	0.939869	48.40065	0	0.034648
0.3	1.639615	45.98621	0	0.034648	1.736893	45.73423	0.000281	0.035246
0.4	2.572417	44.03049	0	0.034648	2.554907	44.05757	0	0.034648
0.5	3.750828	42.39343	0	0.034648	3.875156	42.24909	4.07E-06	0.034656
0.6	5.181338	40.99159	0	0.034648	5.230695	40.94588	0	0.034648
0.7	6.852787	39.77779	0	0.034648	7.076919	39.6336	0	0.034648
0.8	8.771352	38.70654	0	0.034648	8.968211	38.60455	0	0.034648
0.9	10.91858	37.75664	0	0.034648	11.33568	37.58757	0	0.034648
1	13.30701	36.89816	0	0.034648	13.7675	36.74315	0	0.034648

variasi rasio yang digunakan 0,1 sampai dengan 1. Dapat disimpukan bahwa nilai terbaik yang didapatkan pada skenario pengujian terhadap rasio penyisipan citra gambar pada data gambar ini adalah pada rasio 0,5.

4.3 Hasil pengujian terhadap gangguan AWGN

Sigma	DWT-SVD				DWT			
	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi
1	13.3070	36.89816	0.94230143	0.4710286	13.76749	36.74314	0.4970174	0.4668986
2	13.3070	36.89816	0.9498657	0.4714070	13.76749	36.74314	0.4665730	0.4652547
3	13.3070	36.89816	0.95029296	0.4714599	13.76749	36.74314	0.4561523	0.4634562
4	13.3070	36.89816	0.95032552	0.4714925	13.76749	36.74314	0.4541992	0.4631795
5	13.3070	36.89816	0.95034993	0.4715128	13.76749	36.74314	0.4523152	0.4632812

hasil PSNR pengujian terhadap gangguan AWGN pada data gambar, bahwa nilai PSNR terbaik yang didapatkan pada DWT-SVD dengan nilai PSNR 36,90 dB hasil BER terhadap pengujian terhadap jenis layer pada data gambar, bahwa nilai BER terbaik yang didapatkan pada proses Dekripsi RSA dengan nilai terbaik 0.46

4.5 Hasil pengujian terhadap gangguan Rotation

Sudut dalam derajat	DWT-SVD				DWT			
	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi
5	13.3070	36.89816	2.4414E-05	0.0347371	13.76749	36.74314	0.0470052	0.1751586
15	13.3070	36.89816	0.00091145	0.0377848	13.76749	36.74314	0.1277587	0.3262084
30	13.3070	36.89816	0.00453694	0.0493367	13.76749	36.74314	0.1992228	0.3924316
90	13.3070	36.89816	0	0.0346476	13.76749	36.74314	0	0.0346476

hasil PSNR pengujian terhadap gangguan rotation pada data gambar, bahwa nilai PSNR terbaik yang didapatkan pada DWT-SVD dengan nilai PSNR 36,90 dB hasil BER terhadap pengujian terhadap jenis layer pada data gambar, bahwa nilai BER terbaik yang didapatkan pada proses Dekripsi RSA nilai terbaik 0.035.

4.6 Hasil pengujian terhadap gangguan Translation

Ukuran	DWT-SVD				DWT			
	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi
0.25	13.3070	36.89816	0.95002441	0.471537	13.76749	36.74315	0.5026529	0.4663004
0.5	13.3070	36.89816	0.95002441	0.471537	13.76749	36.74315	0.5026529	0.4663004
0.75	13.3070	36.89816	8.138E-05	0.034908	13.76749	36.74315	0.3396606	0.3622070

hasil PSNR pengujian terhadap gangguan rotation pada data gambar, bahwa nilai PSNR terbaik yang didapatkan pada DWT-SVD dengan nilai PSNR 36,90 dB. hasil BER terhadap pengujian terhadap jenis layer pada data gambar, bahwa nilai BER terbaik yang didapatkan pada proses Dekripsi RSA nilai terbaik 0.03.

4.7 Hasil pengujian terhadap gangguan Rescale

perges eran	DWT-SVD				DWT			
	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi	MSE Embed	PSNR Embed	BER Ekstraksi	BER RSA Dekripsi
5	13.3070	36.89816	0	0.034648	13.76749	36.74314	0.0158081	0.0882975
10	13.3070	36.89816	0.00228271	0.04034	13.76749	36.74314	0.0304321	0.1474609
25	13.3070	36.89816	0.0392985	0.107906	13.76749	36.74314	0.0833862	0.2750732
50	13.3070	36.89816	0.28048095	0.339221	13.76749	36.74314	0.1945841	0.4028930

hasil PSNR pengujian terhadap gangguan translation pada data gambar, bahwa nilai PSNR terbaik yang didapatkan pada DWT-SVD dengan nilai PSNR 36,90 dB. hasil BER terhadap pengujian terhadap jenis layer pada data gambar, bahwa nilai BER terbaik yang didapatkan pada proses Dekripsi RSA nilai terbaik 0.03.

5 Kesimpulan

Terdapat beberapa intisari yang dihasilkan dari analisi pada pengujian sistem dan skenario yang telah dilakukan pada Tugas Akhir ini. Berikut adalah beberapa kesimpulan sebagai berikut

1. Implementasi penyisipan watermark pada data gambar dengan menggunakan enkripsi RSA dan teknik penyisipan DWT-SVD telah berhasil dilakukan dan didapatkan hasil terbaik yaitu DWT-SVD dengan menggunakan enkripsi RSA untuk hampir keseluruhan data lebih baik daripada DWT yang menggunakan enkripsi RSA.
2. Semakin besar resolusi image host yang digunakan maka hasilnya akan semakin baik. Dapat dianalisa dengan melihat hasil dari pengujian dengan rata-rata BER sebesar 0,03.
3. Semakin besar rasio yang digunakan maka nilai PSNR yang didapatkan semakin kecil atau bias dikatakan semakin besar rasio yang digunakan maka kualitas dari watermark akan semakin jelek.
4. Untuk scenario gangguan, gangguan yang paling berpengaruh pada proses watermark ini adalah Rescaling dikarenakan nilai BER yang didapatkan mendapatkan nilai yang cukup tinggi dibandingkan serangan menggunakan AWGN

5.2 Saran

Terdapat beberapa kesalahan yang dilakukan oleh peneliti saat menyelesaikan penelitian Tugas Akhir. Maka dari itu beberapa saran yang dapat dituliskan sebagai berikut:

1. Lakukan penelitian penyisipan watermark dengan menggunakan metode penyisipan pada citra lainnya agar dapat diperoleh hasil yang lebih baik.
2. Lakukan penelitian menggunakan teknik enkripsi lainnya.
3. Lakukan dengan menggunakan file host lain seperti audio dan video.
4. Lakukan dengan menggunakan file citra sisip lain seperti audio dan video

DAFTAR PUSTAKA

[1] F. Hartung, S. Member, and M. Kutter, “Multimedia Watermarking Techniques,” IEEE Access, vol. 87, no. 7, pp. 1079–1107, 1999.
[2] N.S enthilkumaran and S. Abinaya, “DIGITAL IMAGE WATERMARKIN G USING DFT ALGORITHM,” vol. 7, no. 1, pp. 9–17, 2016.
[3] P. Patil, P. Narayankar, D. G. Narayan, and S. M. Meena, “A Comprehensive Evaluation of Cryptographic Algorithms : DES ,” Procedia - Procedia Comput. Sci., vol. 78, no. December 2015, pp. 617–624, 2016.
[4] J. Coron, “(12) Patent Application Publication (10) Pub . No .: US 2017 / 0207918 A1,” vol. 1, no. 19, 2017.
[5] A. Shehab et al., “Secure and Robust Fragile Watermarking Scheme for Medical Images,” IEEE Access, vol. 6, pp. 10269–10278, 2018.
[6] Y. Li, M. Wei, F. Zhang, and J. Zhao, “A New Double Color Image Water marking Algorithm Based on the SVD and Arnold Scrambling,” Hindawi - Hindawi Corp., vol. 2016, no. 2, 2016.
[7] S. Hemalatha, U. D. Acharya, and A. Renuka, “Wavelet transform based st eganography technique to hide audio signals in image .,” Procedia - Proced ia Comput. Sci., vol. 47, pp. 272–281, 2015.
[8] D. Gupta and S. Choubey, “Discrete Wavelet Transform for Image Processi ng,” IJETAE Access, vol. 4, no. 3, pp. 598–602, 2008.
[9] J. Cesar et al., “Data Compression in Smart Distribution Systems via Singu lar Value Decomposition,” IEEE Trans. Smart Grid, vol. 8, no. 1, pp. 275–284, 2017.
[10] F. Fioranelli, M. Ritchie, and H. Griffiths, “Classification of Unarmed / Armed Personnel Using the NetRAD Multistatic Radar for Micro - Doppler and Singular Value Decomposition Features,” IEEE Geoscience, vol. 12, no. April, pp. 1933–1937, 2016.
[11] C. Musco and C. Musco, “Randomized Block Krylov Methods for Stronger and Faster Approximate Singular Value Decomposition,” Massachusetts Institute of Technology - EECS, pp. 1–9.