

Studi Steganografi Pada Citra Digital Menggunakan *Shuffled Singular Value Decomposition* (SSVD)

Ainiya Fahrurrosi Aziza¹, Elly Matul Imah^{2*}

Universitas Negeri Surabaya; Jl. Ketintang, Surabaya, 60231, Indonesia

Jurusan Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam

e-mail: ellymatul@unesa.ac.id

Abstrak

Steganografi merupakan suatu teknik untuk menyisipkan pesan tersembunyi ke dalam suatu citra. Steganografi memiliki peranan penting dalam hal penyembunyian informasi pada suatu komunikasi rahasia. Berbagai penelitian mengenai teknik steganografi telah dikembangkan, salah satu diantaranya menggunakan *Singular Value Decomposition* (SVD). Metode SVD cukup populer diperbincangkan dalam berbagai teknik di antaranya adalah steganografi dan penyisipan *tanda air*. Selain SVD terdapat pula sebuah metode yang dipercaya mampu memberikan hasil yang lebih baik dari SVD pada teknik penyisipan *tanda air* yakni *Shuffled Singular Value Decomposition* (SSVD). Perbedaan antara SSVD dan SVD terletak pada proses rekonstruksi yang diaplikasikan sebelum menerapkan SVD. Kepopuleran SSVD pada teknik penyisipan *tanda air* membuat penulis tertarik untuk mengusulkan studi teknik steganografi menggunakan SSVD. Data yang digunakan berupa dua buah citra RGB dan sebuah pesan berupa citra RGB. Kualitas citra diukur menggunakan PSNR dan Koefisien Korelasi. Dari uji coba diperoleh hasil bahwa kualitas penyisipan pesan yang telah dilakukan untuk kedua metode ini tergolong dalam kategori cukup baik yakni diatas 40 dB, sedangkan proses rekonstruksi pada pesan rahasia pada saat menggunakan metode SSVD mengakibatkan pesan yang disisipkan tidak mudah dibaca sehingga pesan yang disisipkan lebih aman daripada tanpa menggunakan proses rekonstruksi.

Kata Kunci: Steganografi, SVD, SSVD

Abstract

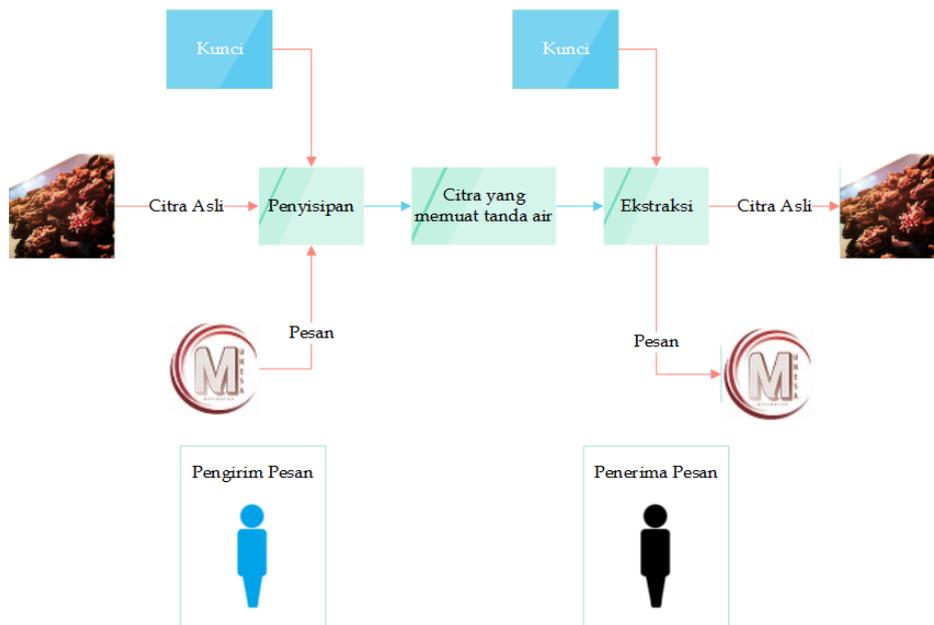
Steganography is a technique of inserting hidden messages into an image. Steganography has an important role, in the field of information hiding for secret communication. Much recent research on it has been developed by, one of them is Singular Value Decomposition (SVD). SVD is quite popular discussed on various techniques including steganography and watermarking. Besides SVD, there is also a method that is believed to be able to provide better results than SVD on watermarking techniques, called Shuffled Singular Value Decomposition (SSVD). The differences between SSVD and SVD is on the shuffle process, which applied before applying the SVD. The popularity of SSVD on the watermarking technique made the writers interested in proposing a study of steganographic techniques using SSVD. The data used are two original RGB images and a message RGB image. Image quality is measured using the PSNR and Correlation Coefficient. The experimental result shows that the quality of insertion message which applied for both of these methods is categorized as quite good which is above 40 dB while shuffling process on the secret message causes the secret message not being easily readable so that the inserted message is securer than without using the shuffle process.

Keywords: Steganography, SVD, SSVD

1 Pendahuluan

Kata steganografi berasal dari bahasa Yunani yakni *steganos* dan *graphein*, *steganos* memiliki makna disembunyikan sedangkan *graphein* bermakna menulis [1]. Steganografi disebut sebagai seni dan ilmu menyembunyikan informasi (pesan) ke dalam sebuah media dengan suatu teknik sehingga tidak ada seorangpun yang mengetahui atau menyadari adanya pesan rahasia di dalam media tersebut, selain pengirim pesan dan penerima pesan yang memiliki kunci yang sama [2]. Catatan pertama tentang steganografi ditulis oleh seorang sejarawan Yunani bernama Herodotus.

Herodotus menyebutkan dua contoh dalam ceritanya, contoh yang pertama yaitu ketika Histaeus menulis pesan dengan cara mentato pesan tersebut pada kulit kepala lalu mengirimkan pesan saat rambut mulai tumbuh, penerima pesan akan mencukur rambut orang tersebut untuk membaca pesan yang telah disembunyikan, contoh yang kedua adalah ketika seorang bangsa Yunani menyampaikan berita kepada Sparta dengan cara menulis pesan pada papan kayu kemudian ditutupi lilin agar tidak diketahui oleh pihak musuh [1][3]. seiring berjalannya waktu pengertian steganografi berkembang menjadi suatu teknik penyembunyian pesan pada suatu media digital seperti gambar, video maupun audio.



Gambar 1. Sistem Steganografi

Teknik steganografi telah banyak dikembangkan seperti steganografi spasial, transformasi steganografi dan steganografi adaptif [4]. Salah satu metode yang sering digunakan dalam penelitian teknik steganografi adalah metode *Singular Value Decomposition* (SVD) [5][6][7]. Berdasarkan hasil penelitian tersebut metode SVD memiliki *robustness* yang baik dari berbagai macam manipulasi seperti kompresi, pemotongan, penambahan *noise impulse*, *noise gaussian*, dan *noise gamma*. SVD memiliki variasi yang disebut dengan *Shuffled Singular Value*

Decomposition (SSVD)[8]. Metode ini sedang hangat diperbincangkan pada tehnik penyisipan *tanda air*.

Pada penelitian SSVD berbasis kekuatan dan keamanan penyisipan *tanda air digital* [8] menunjukkan *robustness* yang baik dari berbagai manipulasi seperti penskalaan, penajaman, penambahan *noise additive gaussian*, *noise multiplicative uniform*, *noise salt & pepper*, *noise speckle*, *noise gamma correction* dan *additive uniform*. Pada penelitian ini akan digunakan teknik steganografi pada citra digital menggunakan metode *Shuffled Singular Value Decomposition* (SSVD) dengan teknik rekonstruksi yang akan diaplikasikan pada pesan.

2 Metode Penelitian

2.1 Steganografi

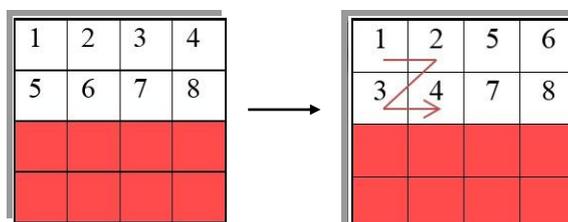
Citra asli (penampung) dinotasikan sebagai citra yang digunakan untuk menerima atau menampung data rahasia atau informasi yang akan disembunyikan. Proses yang digunakan untuk menyembunyikan data rahasia ke dalam citra asli menggunakan algoritma tertentu dan menghasilkan citra yang memuat informasi atau *stego image* (pesan rahasia) disebut dengan proses penyisipan, sedangkan untuk membaca pesan rahasia yang telah disisipkan ke dalam citra asli pembaca harus mengambil pesan tersebut dengan cara ekstraksi. Sistem steganografi dapat dilihat pada Gambar 1. Dalam sistem steganografi yang baik terdapat beberapa hal penting yang perlu diperhatikan diantaranya

a. *Imperceptibility*

Perubahan yang terjadi pada citra asli harus sekecil mungkin sehingga tidak ada perbedaan yang mencolok antara citra asli dan citra yang memuat informasi [9].

b. *Robustness*

Pesan yang disisipkan harus dapat dibaca ketika diekstraksi meskipun telah dilakukan manipulasi [9][10].



Gambar 2. Contoh rekonstruksi

2.2 *Shuffled Singular Value Decomposition* (SSVD)

SVD merupakan salah satu dari sejumlah teknik analisis numerik yang efektif digunakan untuk menganalisis matriks [11]. Misal A adalah sebarang matriks berukuran $N \times N$ dengan rank r didekomposisikan menjadi tiga matriks yaitu U , S dan V seperti pada persamaan (1)

$$A = U \times S \times V^T \quad (1)$$

matriks U berukuran $M \times M$ dan V berukuran $N \times N$ disebut matriks orthogonal. Matriks U dikenal sebagai vektor singular kiri dan V dikenal sebagai vektor singular kanan [11], masing masing merepresentasikan detil horizontal dan vertikal sebuah citra. Matriks S berukuran $M \times N$ disebut matriks diagonal nilai singular. SVD telah digunakan secara luas pada pengolahan citra sehubungan dengan stabilitas nilai singular [11]. Selain SVD terdapat pula *Shuffled singular decomposition* (SSVD) yang merupakan variasi dari SVD [8].

Misal terdapat matriks A sebagai citra asli dengan ukuran $M \times M$ dan matriks W sebagai pesan rahasia dengan ukuran $N \times N$, maka proses penyisipan dan ekstraksi adalah sebagai berikut

1. Proses penyisipan:

- a. Membagi matriks W menjadi blok berukuran $n \times n$, dengan $N = n^2$
- b. Mengambil blok ke- i dalam urutan baris utama kemudian menyusun baris-baris pada blok tersebut menjadi baris ke- i dari X . Secara matematis operator kocok didefinisikan sebagai berikut:

$$X \left[\left[\begin{matrix} i \\ n \end{matrix} \right] n + \left[\begin{matrix} j \\ n \end{matrix} \right], (i \bmod n)n + j \bmod n \right] = A[i, j] \quad (2)$$

- c. Contoh rekonstruksi disajikan pada Gambar 2.
- d. Menerapkan SVD pada A

$$A = USV^T \quad (3)$$

- e. Modifikasi nilai X

$$S_t = S + \alpha X \quad (4)$$

Faktor skala dinotasikan dengan α yang menyatakan kekuatan penyisipan pesan.

- f. Menerapkan SVD pada S_t

$$S_t = U_w S_w V_w^T \quad (5)$$

- g. Merekonstruksi citra yang memuat pesan rahasia.

$$A_w = U S_w V^T \quad (6)$$

2. Proses ekstraksi

- a. Menerapkan SVD pada A_w^* , A_w^* merupakan citra yang memuat pesan rahasia.

$$A_w^* = U^* S_w^* (V^*)^T \quad (7)$$

- b. Menerapkan SVD pada S_t^*

$$S_t^* = U_w S_w V_w^T \quad (8)$$

- c. Merekonstruksi pesan

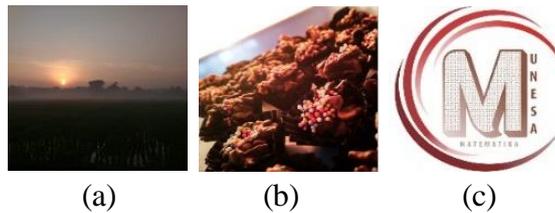
$$W = \frac{1}{\alpha} (S_t - S) \quad (9)$$

d. Menerapkan invers pada operator kocok untuk memperoleh pesan rahasia

$$A[i,j] = X \left[\left\lfloor \frac{i}{n} \right\rfloor n + \left\lfloor \frac{j}{n} \right\rfloor, (i \bmod n)n + j \bmod n \right] \quad (10)$$

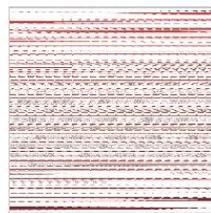
3 Hasil dan Analisis

Data yang digunakan adalah dua buah citra RGB yakni *Scenery* dan *Choco* dengan ukuran 512×512 piksel sebagai citra asli dan sebuah citra “Math” sebagai pesan yang akan mbunyikan. Data yang digunakan disajikan pada Gambar 3. Pada teknik steganografi terdapat dua proses yang harus dilakukan yakni proses *embedding* dan ekstraksi. Proses *embedding* diawali dengan mencocok citra pesan dengan menerapkan operator kocok.



Gambar 3. (a) Citra asli *Scenery*, (b) Citra asli *Choco*, (c) Pesan rahasia “Math”

Hasil dari proses rekonstruksi pesan disajikan pada Gambar 4.



Gambar 4. Hasil proses pencocokan

Setelah dilakukan rekonstruksi maka tahap selanjutnya adalah menyembunyikan pesan rahasia menggunakan metode SSVD. Pada proses *embedding*, pesan yang disisipkan tidak boleh sampai merusak citra penampung [12]. Proses yang kedua adalah ekstraksi. Proses ini diawali dengan menerapkan SSVD pada citra yang memuat pesan lalu menerapkan invers pada operator kocok sehingga diperoleh citra pesan.



Gambar 5. Citra yang memuat pesan (a) “Scenery” disisipkan “Math” (PSNR= 38.8182dB)

(b) “Choco” disisipkan “Math” (PSNR = 48.1531dB) (c) “Scenery” disisipkan “Math”

(PSNR= 38.8818dB) (d) “Choco” disisipkan “Math” (PSNR = 48.2802dB)

Dari hasil uji coba *imperceptibility* diperoleh hasil bahwa metode SSVD dan SVD dapat menyembunyikan pesan rahasia dengan cukup baik hal ini ditandai dengan tidak ada perbedaan yang mencolok antara citra asli dengan citra yang telah disisipi dengan pesan. Hasil uji coba *imperceptibility* disajikan pada Gambar 5a dan 5b untuk metode SSVD dan Gambar 5c dan 5d untuk metode SVD.

Tabel 1. Nilai PSNR Menggunakan Metode SSVD

Faktor skala	Nilai PSNR untuk Citra <i>Scenery</i> (dB)	Nilai PSNR untuk Citra <i>Choco</i> (dB)
0.2	38.8182	48.1531
0.3	34.8293	43.9868
0.4	32.9333	40.6384
0.5	31.2022	37.6669

Pada hasil uji coba terdapat beberapa citra asli yang sulit dibedakan dengan citra yang disisipi dengan pesan sehingga diperlukan PSNR (*Peak Signal to Noise Ratio*) untuk mengetahui nilai perbedaan kualitas antara kedua citra tersebut. PSNR dihitung dalam satuan dB (desibels) [13]. Standar nilai PSNR berkisar antara 30 dB hingga 40 dB, nilai PSNR yang tinggi mengindikasikan kualitas citra yang baik [2] sedangkan nilai PSNR yang kurang dari 30 dB mengindikasikan kualitas penyisipan yang telah dilakukan relatif rendah. Perhitungan nilai PSNR pada citra didefinisikan seperti pada persamaan (10)

$$PSNR = 20 \log\left(\frac{225}{\sqrt{MSE}}\right) \quad (10)$$

Untuk menghitung PSNR diperlukan MSE (*Mean Square Error*). MSE merupakan nilai error kuadrat rata-rata antara citra asli dengan citra manipulasi. MSE pada citra didefinisikan pada persamaan (11).

$$MSE = \frac{1}{M \times N} \sum_i \sum_j [I(i,j) - I_w(i,j)]^2 \quad (11)$$

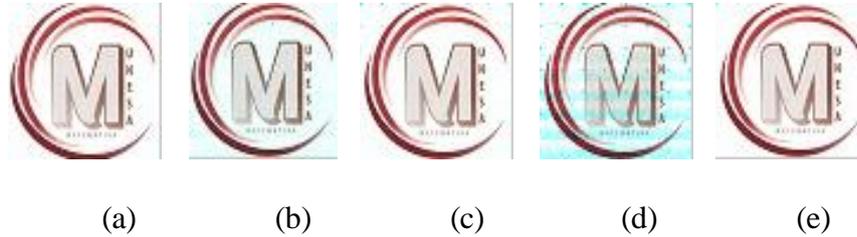
citra asli dinotasikan $I(i,j)$ dan $I_w(i,j)$ menunjukkan citra yang memuat informasi.

Tabel 2. Nilai PSNR menggunakan metode SVD

Faktor skala	Nilai PSNR untuk Citra <i>Scenery</i> (dB)	Nilai PSNR untuk Citra <i>Choco</i> (dB)
0.2	38.8818	48.2802
0.3	34.9172	44.103
0.4	32.9875	40.7472
0.5	31.2431	37.7528

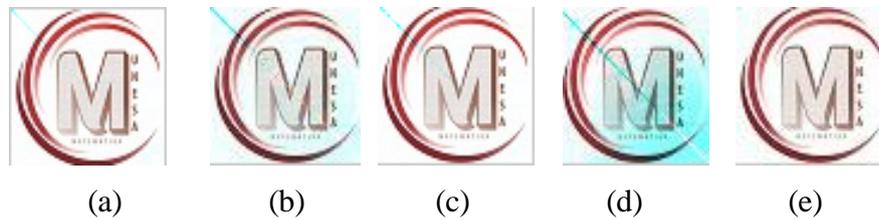
Hasil perhitungan nilai PSNR pada saat menggunakan metode SSVD disajikan pada Tabel 1 dan Tabel 2 untuk metode SVD. Nilai PSNR metode SSVD mencapai 48.1531 dB pada pemilihan faktor skala 0.2 sedangkan pada metode SVD nilai PSNR mencapai 48.2802 dB pada pemilihan faktor skala 0.2. Berdasarkan hasil tersebut dapat dikatakan bahwa nilai PSNR metode

SVD lebih baik dari metode SSVD. Makin kecil faktor skala yang dipilih makin baik nilai PSNR yang diperoleh. Selain uji *imperceptibility*, diperlukan juga uji *robustness*. Pada penelitian ini uji *robustness* dilakukan dengan menambahkan manipulasi berupa *noise*, rotasi dan *blurring*. *Noise* yang digunakan adalah *noise salt & pepper*, *noise gaussian*, *noise speckle*. Hasil ekstraksi citra



Gambar 6. Hasil ekstraksi citra yang memuat pesan menggunakan metode SSVD
(a) *Salt & pepper*, (b) *Gaussian*, (c) *Speckle*, (d) *Blurring*, (e) Rotasi

yang memuat pesan disajikan pada Gambar 6 untuk metode SSVD dan Gambar 7 untuk metode SVD. Untuk mengukur korelasi antara pesan dan hasil ekstraksi citra diperlukan perhitungan koefisien korelasi. Secara matematis koefisien korelasi didefinisikan seperti pada persamaan (12). Pesan dinyatakan dengan W dan W^* menyatakan hasil ekstraksi dari citra yang memuat pesan, μ_w merupakan mean dari penyisipan pesan dan μ_w^* merupakan mean dari hasil ekstraksi.



Gambar 7. Hasil ekstraksi citra yang memuat pesan menggunakan metode SVD
(a) *Salt & pepper*, (b) *Gaussian*, (c) *Speckle*, (d) *Blurring*, (e) Rotasi

Kuat dan tidaknya hubungan antara W dan W^* dapat dinyatakan dengan fungsi linear atau paling tidak mendekati. Nilai koefisien korelasi ini paling sedikit -1 dan paling besar $+1$, makin besar nilai koefisien korelasi maka makin dekat kemiripan antara kedua objek tersebut [14].

$$\rho(W, W^*) = \frac{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \mu_w)(w_{ij}^* - \mu_w^*)}{\sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij} - \mu_w)^2} \sqrt{\sum_{i=1}^N \sum_{j=1}^N (w_{ij}^* - \mu_w^*)^2}} \quad (12)$$

Hasil koefisien korelasi menggunakan metode SSVD pada citra *Scenery* disajikan pada Tabel 3 sedangkan pada citra *Choco* disajikan pada Tabel 4. Untuk hasil perhitungan koefisien korelasi menggunakan metode SVD disajikan pada Tabel 5 untuk citra *Scenery* dan Tabel 6 untuk citra *Choco*.

Tabel 3. Nilai Koefisien Korelasi Menggunakan SSVD untuk citra *Scenery*

Manipulasi	Nilai Koefisien korelasi			
	0.2	0.3	0.4	0.5
<i>Salt & pepper</i>	0.957029	0.945199	0.945701	0.947872
<i>Gaussian</i>	0.773216	0.786458	0.788086	0.7867
<i>Speckle</i>	0.972227	0.971101	0.967885	0.966124
<i>Blurring</i>	0.677928	0.7094	0.71987	0.728779
Rotasi	0.99719	0.993225	0.98685	0.98341

Tabel 4. Nilai Koefisien Korelasi SSVD pada Citra *Choco*

Manipulasi	Nilai Koefisien Korelasi			
	0.2	0.3	0.4	0.5
<i>Salt & pepper</i>	0.99116	0.989676	0.989716	0.98908
<i>Gaussian</i>	0.928847	0.922937	0.923653	0.925485
<i>Speckle</i>	0.980146	0.977477	0.981191	0.978583
<i>Blurring</i>	0.689776	0.646983	0.69163	0.723416
Rotasi	0.995423	0.994208	0.99249	0.990264

Secara umum nilai koefisien korelasi metode SSVD dan SVD cukup tinggi, ini menandakan bahwa pesan yang diperoleh dari hasil ekstraksi citra memiliki kemiripan yang tinggi dengan pesan asli sebelum disembunyikan ke dalam citra asli.

Tabel 5. Nilai Koefisien Korelasi Menggunakan SVD untuk citra *Scenery*

Manipulasi	Nilai Koefisien korelasi			
	0.2	0.3	0.4	0.5
<i>Salt & pepper</i>	0.952172	0.952139	0.948545	0.941626
<i>Gaussian</i>	0.773344	0.789127	0.794649	0.795143
<i>Speckle</i>	0.96748	0.967231	0.964459	0.965547
<i>Blurring</i>	0.681628	0.724003	0.739889	0.747704
Rotasi	0.997144	0.993012	0.98652	0.983082

Tabel 6. Nilai Koefisien Korelasi Menggunakan SVD untuk citra *Choco*

Manipulasi	Nilai Koefisien Korelasi			
	0.2	0.3	0.4	0.5
<i>Salt & pepper</i>	0.990345	0.989381	0.9908	0.989025
<i>Gaussian</i>	0.905719	0.917359	0.923138	0.923644
<i>Speckle</i>	0.972427	0.977976	0.980855	0.979034
<i>Blurring</i>	0.575294	0.655947	0.706328	0.735221
Rotasi	0.995689	0.994348	0.992559	0.990319

Dari hasil uji coba metode SSVD memiliki nilai koefisien korelasi yang lebih tinggi dari pada metode SVD yakni 0.957029 pada manipulasi *salt & pepper*, 0.773216 pada manipulasi *Gaussian*, 0.972227 pada manipulasi *speckle*. Noise yang sering ditemui dalam citra adalah

salt&paper, *Gaussian*, dan *speckle* dan untuk ketiga jenis noise ini SSVD lebih baik performanya untuk diimplementasikan. Sedangkan untuk jenis noise *blurring* dan rotasi, performa SSVD sedikit lebih rendah dari pada SVD dengan selisih nilai yang sangat kecil, yaitu 0.995423 menggunakan SSVD, sedangkan menggunakan SVD sebesar 0.995689, selisih yang tidak terlalu signifikan, yaitu 0.000277. Secara umum SSVD memiliki performa lebih baik daripada SVD.

4 Simpulan

Dari uji coba yang telah dilakukan diperoleh hasil bahwa teknik Steganografi menggunakan metode SSVD mampu membuat pesan menjadi tidak mudah dibaca karena adanya proses rekonstruksi pada citra pesan sebelum menerapkan metode SVD sehingga lebih aman jika dibandingkan dengan metode SVD. Metode SSVD memiliki *robustness* yang lebih baik dari berbagai manipulasi penambahan gangguan seperti *salt & pepper*, *gaussian*, *speckle*. Ketahanan SSVD terhadap noise mengindikasikan bahwa metode ini cukup baik dalam mempertahankan keutuhan pesan.

5 Daftar Pustaka

- [1] R. Bharathipriya, T. Nadu, and T. Nadu, "A Comparative Study on Secured Image Transmission Using Steganography Techniques," *Proc. UGC Spons. Natl. Conf. Adv. Netw. Appl.*, no. March, pp. 3–6, 2015.
- [2] S. Rajkumar and G. Malathi, "A Comparative Analysis on Image Quality Assessment for Real Time Satellite Images," *Indian J. Sci. Technol.*, vol. 9, no. September, 2016.
- [3] R. S. Run, S. J. Horng, J. L. Lai, T. W. Kao, and R. J. Chen, "An improved SVD-based watermarking technique for copyright protection," *Expert Syst. Appl.*, vol. 39, no. 1, pp. 673–689, 2012.
- [4] W. Luo, F. Huang, and J. Huang, "Edge Adaptive Image Steganography Based on LSB Matching Revisited," *IEEE Trans. Inf. FORENSICS Secur.*, vol. 5, no. 2, pp. 201–214, 2010.
- [5] Y. J. Chanu, K. M. Singh, and T. Tuithung, "A Robust Steganographic Method based on Singular Value Decomposition," *Int. J. Inf. Comput. Technol.*, vol. 4, no. 7, pp. 717–726, 2014.
- [6] M. Douglas, K. Bailey, M. Leeney, K. Curran, and M. Douglas, "An overview of steganography techniques applied to the protection of biometric data," *Multimed Tools Appl*, pp. 17333–17373, 2018.

-
- [7] S. Singh, R. Singh, and T. J. Siddiqui, "Singular Value Decomposition Based Image Steganography Using Integer Wavelet Transform," pp. 593–594.
- [8] T. Bhuyan, V. K. Srivastava, and F. Thakkar, "Shuffled SVD based robust and secure digital image watermarking," *Int. Conf. Electr. Electron. Optim. Tech. ICEEOT 2016*, pp. 1229–1233, 2016.
- [9] A. Rashid and M. K. Rahim, "Critical Analysis of Steganography ‘ An Art of Hidden Writing ,’" *Int. J. Secur. Its Appl.*, vol. 10, no. 3, pp. 259–282, 2016.
- [10] N. S. Chavan, "RESEARCH ARTICLE IMAGE STEGANOGRAPHY – AN OVERVIEW," *Int. J. Recent Sci. Res.*, vol. 6, pp. 4800–4804, 2015.
- [11] K. Loukhaoukha, A. Refaey, K. Zebbiche, and M. Nabti, "On the Security of Robust Image Watermarking Algorithm based on Discrete Wavelet Transform , Discrete Cosine Transform and Singular Value Decomposition," *Appl. Math. Inf. Sci.*, vol. 1166, no. 3, pp. 1159–1166, 2015.
- [12] V. Sharma, D. Srivastava, and M. Pratistha, "A Study of Steganography Based Data Hiding Techniques," *Int. J. Emerg. Res. Manag. &Technology*, vol. 9359, no. 4, pp. 145–150, 2017.
- [13] A. Cheddad, J. Condell, K. Curran, and P. M. Kevitt, "Digital Image Steganography: Survey and Analysis of Current Methods," *Signal Processing*, vol. 90, no. 3, pp. 727–752, 2010.
- [14] B. Ratner, "The correlation coefficient : Its values range between $+ 1 / - 1$, or do they?," *J. Targeting, Meas. Anal. Mark.*, vol. 17, pp. 139–142, 2009.