Tersedia di https://jtsiskom.undip.ac.id (1 Februari 2018) Jurnal Teknologi dan Sistem Komputer, 6(1), 2018, 37-43
DOI: 10.14710/jtsiskom.6.1.2018.37-43

Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA

Antonius Erick Handoyo, De Rosal Ignatius Moses Setiadi*), Eko Hari Rachmawanto, Christy Atika Sari, Ajib Susanto

Program Studi Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Nakula 5-11, Semarang 50131, 024-3517261

Cara sitasi: A. E. Handoyo, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and A. Susanto, "Teknik Penyembunyian dan Enkripsi Pesan pada Citra Digital dengan Kombinasi Metode LSB dan RSA," Jurnal Teknologi dan Sistem Komputer, vol. 6, no. 1, Jan. 2018. doi: 10.14710/jtsiskom.6.1.2018.37-43, [Online].

Abstract - This study proposed a combination of steganography and cryptography techniques using LSB-RSA method. RSA is a popular cryptographic technique that can be applied to digital imagery. Digital image pixel values range from 0 to 255, making the keys used in RSA limited enough to be less secure. It is proposed to convert pixel image value to 16 bits so that the key used can be more varied. Experimental results prove that there is a steady increase in security and imperceptibility. This is shown by the results of PSNR 57.2258dB, MSE 0.1232dB, this method is also resistant to salt and pepper attacks.
Keyword - *steganography, cryptography, LSB, RSA, image encryption*

Abstrak - Penelitian ini menghasilkan kombinasi teknik steganografi dan kriptografi dengan metode LSB–RSA. RSA merupakan teknik kriptografi yang populer dapat diterapkan pada citra digital. Nilai piksel citra digital hanya berkisar 0 sampai 255, hal ini membuat kunci yang digunakan dalam RSA cukup terbatas sehingga kurang aman. Dalam penelitian ini diusulkan untuk mengkonversi nilai piksel citra menjadi 16 bit sehingga kunci yang digunakan dapat lebih bervariasi. Hasil eksperimen membuktikan adanya peningkatan keamanan serta nilai imperceptibility yang tetap terjaga. Hal ini dibuktikan dengan hasil PSNR 57.2258dB, MSE 0.1232dB, metode ini juga tahan terhadap serangan salt and pepper.
Kata Kunci – *steganografi; kriptografi; LSB; RSA; enkripsi citra*

I. PENDAHULUAN

Kemajuan Internet pada zaman ini sudah menjadi kebutuhan masyarakat umum yang digunakan dalam kehidupan sehari-hari. Internet terus berkembang dalam memberikan layanan baru yang berguna sebagai alat komunikasi, promosi dan media administrasi. Dalam penggunaannya, Internet berdampak positif dalam memberikan data dan informasi yang bermanfaat. Adanya Internet memudahkan pertukaran data dengan cepat dan bebas yang digunakan oleh semua orang [1]. Internet sendiri adalah sekumpulan jaringan komputer yang terhubung dengan berbagai situs pemerintah, grup maupun perorangan guna memberikan informasi terhadap pengguna. Dampak negatifnya adalah kejahatan di dunia maya yang meningkat sehingga perlu adanya perlindungan data dan informasi [2].

Penggunaan keamanan informasi ini ditujukan agar tidak dapat dicuri oleh orang asing yang tidak berkepentingan dalam informasi tersebut. Ada beberapa metode yang dapat dilakukan untuk mengamankan pesan yaitu dengan menggunakan *watermarking*, steganografi, kriptografi dan tanda tangan digital [2]-[5]. Tujuan dari steganografi adalah memanipulasi sebuah objek untuk menyembunyikan pesan ke dalamnya [3]. Terdapat dua macam steganografi menurut domainnya, yaitu domain spasial dan domain frekuensi [6]. Domain frekuensi dapat menggunakan transformasi domain seperti transformasi diskrit *cosine* dan transformasi diskrit *wavelet.* Teknik ini lebih tahan terhadap manipulasi citra [7], [8]. Pada domain spasial banyak digunakan metode *Least Significant Bit* (LSB) [6]. Domain spasial lebih rentan terhahap serang dan informasi pesan mudah hilang ketika terjadi manipulasi citra. Penyembunyian pesan dengan menggunakan metode LSB sangat sederhana karena hanya mengubah nilai bit terakhir dengan bit pesan. Namun, teknik ini dapat menghasilkan citra yang sangat mirip dengan citra aslinya sehingga indra penglihatan manusia tidak dapat mendeteksi perubahan pada citra dan mustahil untuk memersepsikan pesan secara langsung [5], [6].

Namun, cepatnya perkembangan teknologi tidak menutup kemungkinan pihak yang tidak berkepentingan dapat mengekstraksi pesan dari citra *cover*. Oleh karena itu, diperlukan pengamanan lebih pada pesan yang disembunyikan. Pada beberapa penelitian sebelumnya telah banyak diusulkan kombinasi teknik steganografi dan kriptografi, seperti dalam [6]-[9]. Kriptografi sendiri adalah sebuah seni penyandian pesan dengan mengacak sebuah pesan menjadi sedemikian rupa sehingga maksud dari pesan tersebut tidak dimengerti oleh orang lain [10]. Salah satu metode dalam

*) Penulis korespondensi (D. R. I. M. Setiadi)
Email: moses@dsn.dinus.ac.id

Dikirim: 27 November 2017; Direvisi: 4 Desember 2017, 1 Februari 2018; Diterima: 1 Februari 2018

kriptografi yang banyak digunakan yaitu Rivers Shamir Adleman (RSA) [11]. Algoritma kriptografi ini yang memiliki dua macam kunci salah satunya kunci publik dan kunci privat. Kunci publik digunakan untuk melakukan enkripsi, sedangkan kunci privat untuk dekripsi. Skema dari RSA sendiri yaitu *cipher* blok dimana *plaintext* dan c*ipher* teks adalah sebuah bilangan bulat antara 0 sampai dengan n-1 untuk beberapa n. Bilangan bulat ini mewakili nilai-nilai intensitas gambar [9]. Penyembunyian pesan dengan mengombinasikan dengan enkripsi RSA juga dapat telah banyak digunakan pada citra digital, seperti dalam [9]-[12]. Hanya saja terdapat keterbatasan dalam menentukan kunci karena hasil enkripsi piksel citra akan terbatas dengan nilai maksimal 255.

Pada penelitian ini diusulkan kombinasi teknik steganografi dan kriptografi dalam media citra *digital* guna memberikan keamanan ganda pada pesan. Teknik steganografi yang digunakan adalah LSB dan teknik kriptografi menggunakan RSA. Citra *cover* yang digunakan adalah berukuran $256\,px \times 256\,px$ dan $512\,px \times 512\,px$ dengan citra pesan berukuran $64\,px \times 64\,px$ dan $128\,px \times 128\,px$. Peningkatan keamanan dilakukan dengan konversi enkripsi RSA dan memperbanyak variasi kunci, yaitu mengubah ukuran piksel citra pesan yang awalnya berukuran 255 piksel atau setara dengan 8 *bit*, akan dikonversi menjadi 16 *bit*.

II. METODE PENELITIAN

A. Pemrosesan Awal

Dalam pemrosesan awal (*preprocessing*) dilakukan proses *resize* pada citra ukuran $512\,px \times 512\,px$ menjadi beberapa ukuran, yaitu $256\,px \times 256\,px$, $128\,px \times 128\,px$ dan $64\,px \times 64\,px$. Fungsi *resize* ini ditujukan untuk mendapatkan citra yang ukurannya sesuai dengan kebutuhan. Fungsi *resize* ini sendiri hanya mengubah ukuran piksel pada citra tetapi tidak mengubah nilai di tiap – tiap piksel. Citra ukuran $256\,px \times 256\,px$ dan $512\,px \times 512\,px$ ini banyak digunakan sebagai ukuran standar penelitian. Perubahan ukuran ini dilakukan pada citra *cover* dan citra pesan. Ukuran citra *cover* yang dibutuhkan adalah $256\,px \times 256\,px$ dan $512\,px \times 512\,px$, sedangkan untuk ukuran citra pesan $64\,px \times 64\,px$ dan $128\,px \times 128\,px$. Ukuran–ukuran tersebut digunakan untuk memenuhi kebutuhan pada penelitian ini. Skema perubahan ukuran pada citra pesan dan citra *cover* yang digunakan ditunjukkan dalam Gambar 1.

B. Pembuatan Kunci RSA

Pengamanan data yang berisikan suatu informasi penting tidak lain bergantung pada kunci yang digunakan. Semakin bagus kunci yang digunakan, maka semakin susah untuk ditembus keamanannya. Demikian juga kunci yang digunakan dalam algoritma RSA. Pembuatan kunci yang ada pada algoritma ini juga melibatkan pesan itu sendiri. Kunci yang digunakan harus bersifat rahasia. Hanya kunci publik yang tidak dirahasiakan, sedangkan untuk kunci privat harus

(a) (b)

Gambar 1. Sampel citra *cover* yang sudah di-*resize* (a) citra pesan yang sudah di-*resize* (b)

dirahasiakan agar pesan yang disandikan tidak dapat diekstraks kembali tanpa kunci privat ini [13]. Nilai dari kedua kunci lebih baik berbeda agar meningkatkan keamanan yang ada. Dalam pembuatan kunci terdapat rumusan matematis. Langkah-langkah pembuatan kunci adalah sebagai berikut:

1. Langkah pertama adalah memilih dua buah bilangan prima yang acak dengan didefinisikan *p* dan *q*. Bilangan prima yang digunakan harus bilangan besar agar tingkat keamanan semakin tinggi.
2. Menghitung nilai *n* dengan mengalikan *p* dan *q* menggunakan Persamaan 1.

$$n = p \times q \tag{1}$$

3. Menghitung nilai ekuivalen dari *n* menggunakan Persamaan 2.

$$\varnothing(n) = (p-1) \times (q-1) \tag{2}$$

4. Memilih bilangan prima secara random antara 1 sampai $\varnothing(n)$ yang tidak memiliki faktor pembagi dari $\varnothing(n)$ untuk mendapatkan kunci publik *e*.
5. Menghitung kunci privat *d* menggunakan Persamaan 3.

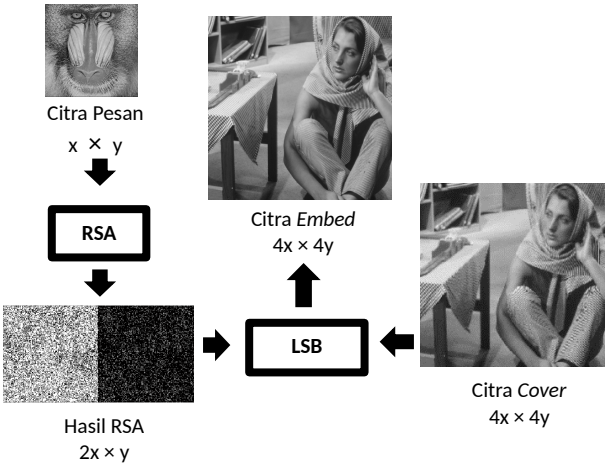
$$(e \times d) mod\ \varnothing(n) = 1 \tag{3}$$

6. Pasangan kunci, yaitu kunci publik (e, n) dan kunci privat (d, n) telah dihasilkan.

C. Penyandian dan Penyembunyian Citra Pesan

Dalam tahap penyembunyian, citra pesan harus melalui beberapa proses untuk mendapatkan citra luaran yang baik. Langkah - langkah penyembunyian citra pesan adalah sebagai berikut (Gambar 2):

1. Langkah awalnya adalah citra pesan yang berukuran x × y piksel dienkripsi menggunakan metode RSA dengan kunci enkripsi yang sudah diperoleh pada langkah sebelumnya.
2. Langkah selanjutnya, proses enkripsi dengan memperbanyak jumlah bit menjadi 16-bit yang membuat ukuran citra pesan berubah menjadi 2x × y piksel.
3. Dalam proses enkripsi RSA, nilai maksimal tiap pikselnya berukuran 255. Jika nilai di dalam sebuah piksel melebihi 255 nilai, maka sisa



Gambar 2. Skema penyandian dan penyembunyian citra pesan

tersebut akan dimasukkan ke dalam bit selanjutnya.

4. Citra hasil enkripsi yang berukuran 2x × y piksel disisipkan ke dalam citra *cover* berukuran 4x × 4y piksel menggunakan metode LSB. Dengan menyisipkan bit citra pesan pada bit terakhir citra *cover*.
5. Hasil akhir adalah berupa citra *embedding* berukuran 4x × 4y piksel yang berisikan pesan rahasia tersandi dengan ukuran 2x × y piksel.

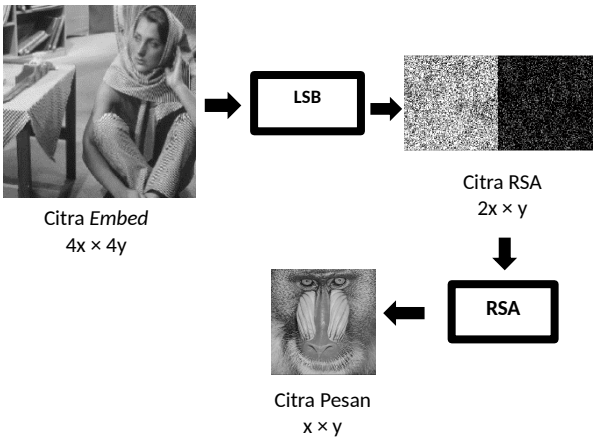
D. Pemisahan dan Dekripsi Citra Pesan

Pada tahap proses pemisahan atau ekstraksi bertujuan untuk mengambil citra pesan tersandi yang disembunyikan di dalam sebuah citra *cover*. Langkah-langkah alur proses ekstraksi adalah sebagai berikut (Gambar 3):

1. Citra hasil *embedding* yang telah diperoleh di-ekstraks menggunakan metode yang sama yaitu LSB dengan mengambil bit terakhir pada citra *cover* yang berisi pesan. Output proses ekstrak tersebut adalah citra RSA yang masih terenkripsi.
2. Citra RSA akan didekripsi dengan melakukan penambahan nilai di tiap bit yang sama.
3. Dengan logika citra yang berukuran 2x × y piksel dipecah menjadi 2 bagian masing-masing dengan ukuran x × y piksel dengan cara memperpendek nilai bit menjadi 8-bit.
4. Nilai yang terdapat pada citra yang sudah dipecah tersebut dijumlahkan dengan hasil citra yang sudah didekripsi menjadi berukuran x × y piksel menggunakan kunci dekripsi yang diperoleh pada langkah sebelumnya.
5. Hasil akhir citra ekstrak adalah berupa citra pesan rahasia yang asli dengan ukuran x × y piksel.

E. Pengujian Metode

Pengujian metode dilakukan sebagai tolak ukur keberhasilan dalam penelitian untuk mengetahui kelebihan serta kekurangan pada sebuah penelitian tersebut. Pengujian kualitas citra untuk mengetahui



Gambar 3. Pemisahan dan dekripsi citra pesan

Tabel 1. Kualitas citra berdasarkan jangkauan PSNR [9]

PSNR (dB)	Kualitas Citra
60	Sangat baik (tanpa derau)
50	Baik (terdapat sejumlah derau tapi kualitas citra masih bagus
40	Cukup baik (terdapat butiran halus atau seperti salju di dalam citra)
30	Kurang baik (terdapat banyak derau)
20	Tidak baik (tidak dapat digunakan)

seberapa bagus kualitas citra tersebut adalah dengan alat ukur *Mean Square Error* (MSE) dan *Peak Signal to Noise Ratio* (PSNR) [8].

MSE digunakan untuk mengetahui nilai sebuah kesalahan kuadrat rata-rata dengan membandingkan selisih nilai piksel pada citra awal dan piksel citra hasil dengan ketentuan posisi piksel yang sama. MSE dihitung menggunakan Persamaan 4.

$$MSE = \frac{1}{mn}\sum_{i}^{m}\sum_{j}^{n}\|I(i,j) - K(i,j)\|^2 \quad (4)$$

Dimana :

MSE = Nilai *Mean Square Error* dari citra tersebut
(i,j) = koordinat masing-masing *pixel*
n = lebar citra tersebut (dalam *pixel*)
m = panjang citra tersebut (dalam *pixel*)

PSNR digunakan untuk menyatakan kualitas citra [9]. PSNR dengan satuan desibel (dB) menunjukkan perbandingan antara nilai maksimum dari sinyal yang diukur dengan besarnya derau yang berpengaruh pada sinyal (Persamaan 5). Kualitas citra berdasarkan nilai PSNR dinyatakan dalam Tabel 1.

$$PSNR = 10 \cdot \log\left(\frac{MAX_I^2}{MSE}\right) \quad (5)$$

Dimana :

PSNR = nilai PSNR citra (dalam dB)
MSE = nilai MSE
MAX_I = nilai maksimum *pixel*

Selain dilakukan uji kualitas, uji ketahanan atau *robustness* juga dilakukan menggunakan *Correlation Coefficient* (CC). Nilai ini didapatkan dengan membandingkan citra pesan asli dengan citra pesan hasil ekstraksi menggunakan Persamaan 6 [2]. Simbol W adalah pesan asli dan W' pesan hasil ekstraksi.

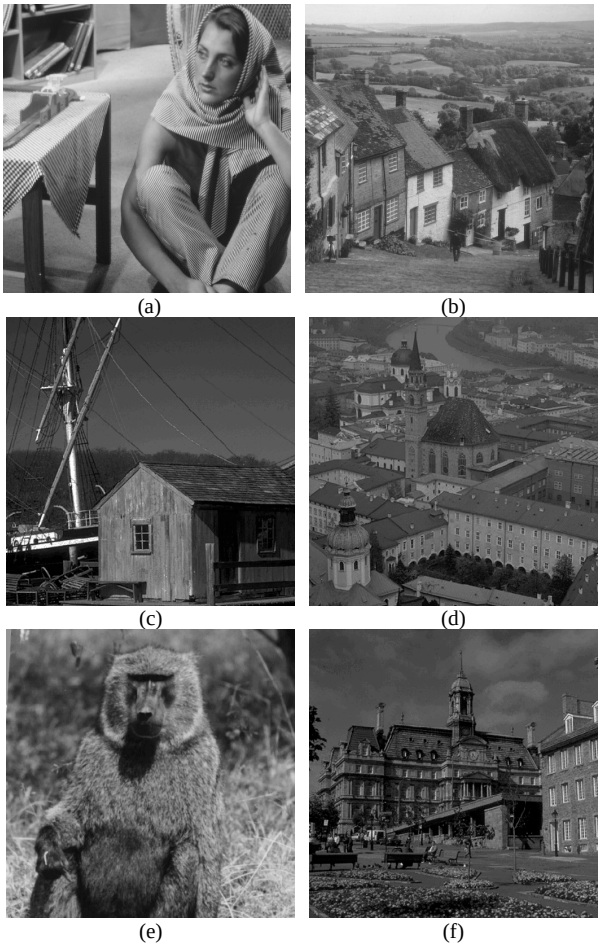
$$CC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}[W(i,j).W'(i,j)]}{\sum_{i=1}^{m}\sum_{j=1}^{n}(W(i,j))^2} \quad (6)$$

Kedua citra tersebut akan dihitung dengan kisaran hasil dari 0 sampai 1. Jika nilai yang dihasilkan semakin dekat dengan 1, maka semakin tinggi pula tingkat kemiripan pesan. Jika nilai CC sama dengan 1, maka pesan terekstraksi dengan sempurna.

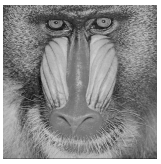
III. HASIL DAN PEMBAHASAN

A. Citra Digital yang Digunakan

Dalam penelitian ini digunakan dua macam ukuran citra *cover*, yaitu dengan ukuran 512 × 512 piksel dan 256 × 256 piksel. Citra *cover* tersebut merupakan citra keabuan standar yang telah banyak digunakan dalam berbagai penelitian pemrosesan citra digital, dengan ini diharapkan memudahkan proses komparasi dengan penelitian berikutnya. Ukuran pesan yang digunakan adalah 128 × 128 piksel untuk *cover* dengan ukuran 512 × 512 dan 64 × 64 piksel untuk *cover* yang berukuran 256 × 256. Citra *cover* yang digunakan pada penelitian ini terdapat pada Gambar 4, sedangkan citra pesan ditunjukkan pada Gambar 5.



Gambar 4. Sampel citra *cover* (a)-(f)

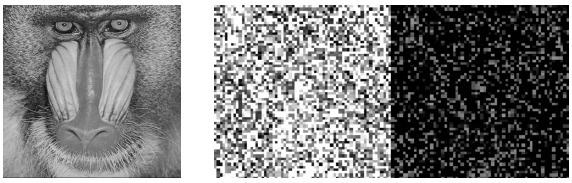


Gambar 5. Citra pesan yang digunakan

B. Enkripsi Citra Pesan

Dengan menggunakan rumus RSA yang diusulkan, maka hasil enkripsi citra pesan menjadi lebih besar, karena bit pada citra pesan diperpanjang menjadi 2 kali 8 bit atau setara 16 bit. Hal ini bertujuan untuk meningkatkan variasi kunci RSA sehingga hasil enkripsi pesan menjadi lebih aman. Hasil enkripsi citra pesan dapat dilihat pada Gambar 6.

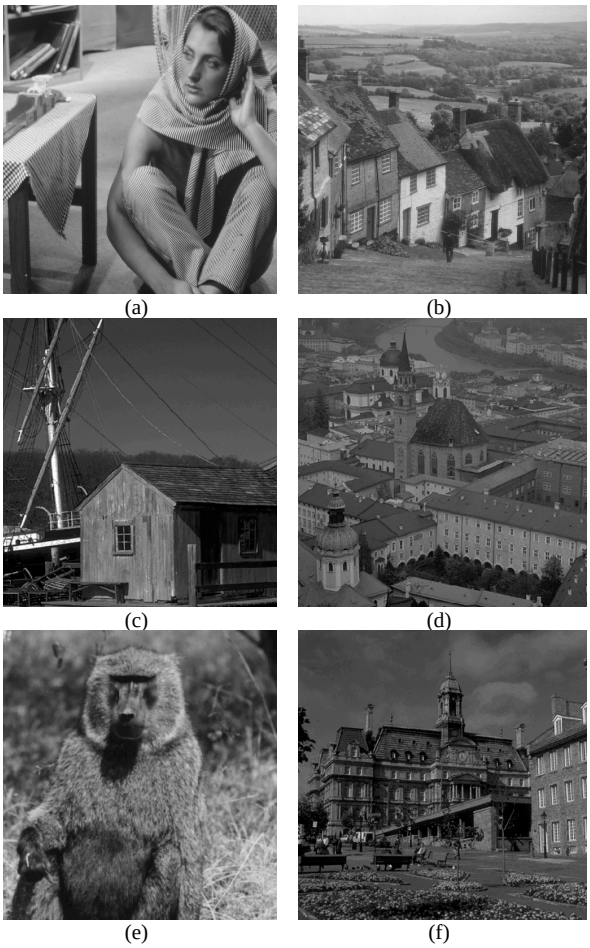
Dari citra pesan hasil enkripsi (Gambar 6) terlihat perbedaan yang sangat mencolok, yaitu dari citra (a) dengan citra (b). Terdapat dua sisi yang berbeda, masing-masing sisi tersebut bernilai 8 bit. Sisi yang berwarna hitam putih tersebut adalah hasil enkripsi yang sudah terproses dengan nilai di bawah 255, sedangkan untuk yang di sisi kanan berwarna hitam adalah nilai sisa yang melebihi 255. Namun karena hasil enkripsi banyak di bawah 255, maka sisi bit selanjutnya berwarna banyak hitam yaitu 0. Enkripsi dengan cara seperti ini akan membuat pesan semakin susah ditebak karena satu piksel citra pesan disimpan dalam dua piksel citra *cover*.



Gambar 6. Citra pesan (a) dan hasil enkripsi pesan (b)

C. Hasil Penyisipan Pesan (Stego Image) dan Uji Kualitas Citra

Bagian ini akan menampilkan hasil penyisipan pesan pada citra stego yang ditunjukkan pada Gambar 7. Jika diamati dan dilihat dengan seksama, tidak terdapat perbedaan saat dilihat secara kasat mata pada citra stego maupun citra *cover*. Hal tersebut merupakan indikasi bahwa kualitas citra stego sangat baik. Tetapi tentunya diperlukan alat ukur standar untuk menentukan kualitas citra stego, maka diukur dengan menggunakan PSNR dan MSE. PSNR untuk membandingkan kualitas citra sebelum dan sesudah disisipkan citra pesan, sedangkan MSE untuk mengetahui nilai kesalahan kuadrat rata-rata antara citra *cover* asli dengan citra *cover* berisi pesan.



Gambar 7. Citra *stego* hasil penyisipan pesan **(**a)-(f)

Dengan adanya pengujian kualitas ini, dapat dianalisis baik buruknya hasil yang diperoleh.

Citra setelah diproses dengan metode ini tidak mengalami perubahan karena besar bit yang dimasukkan ke dalam citra cukup besar, yaitu 65536 bit atau setara dengan 8192 piksel atau karakter untuk citra cover dengan ukuran 256 x 256 piksel dan 2562144 bit atau serata 32768 piksel karakter untuk citra *cover* 512 x 512 piksel. Persentase pesan yang disisipkan adalah sebesar 12,5%. Tabel 2 dan Tabel 3 merupakan hasil pengujian kualitas pada citra stego. Dari hasil tersebut, dapat disimpulkan kualitas citra baik, yaitu nilai PSNR konsisten dan mendekati nilai 60 dB dan nilai MSE yang jauh di bawah 1 sesuai kriteria dalam Tabel 1 [9]. Hal ini menunjukkan tidak banyak derau atau kerusakan pada citra.

D. Hasil Uji Ekstraksi Pesan

Setelah dilakukan proses penyisipan, dilakukan proses ekstraksi dan diukur dengan menggunakan CC sesuai Persamaan 6. Hal ini dilakukan untuk mengetahui kualitas citra hasil ekstraksi. Jangkauan nilai CC berkisar 0-1 dimana jika nilai mendekati 1 maka hasil ekstraksi semakin baik. Tabel 4 menunjukkan hasil ekstraksi dan nilainya. Nilai CC untuk semua citra sama dengan 1 , yang menunjukkan hasil ekstraksi sempurna. Hal ini disimpulkan bahwa hasil ekstraksi dapat dilakukan dengan sempurna karena nilai yang dihasilkan adalah 1.

Tabel 2. Hasil pengukuran PSNR dan MSE pada citra *cover* berukuran 256 x 256 piksel

Citra	PSNR	MSE
(a)	57.2258	0.1232
(b)	57.2506	0.1225
(c)	57.3735	0.1190
(d)	57.3852	0.1187
(e)	57.2609	0.1222
(f)	57.2134	0.1235

Tabel 3. Hasil pengukuran PSNR dan MSE pada citra *cover* berukuran 512 x 512 piksel

Citra	PSNR	MSE
(a)	57.2973	0.1212
(b)	57.2960	0.1212
(c)	57.0847	0.1272
(d)	57.7075	0.1102
(e)	56.0648	0.1609
(f)	57.3619	0.1194

Tabel 4. Hasil pengukuran CC citra pesan pada citra *cover* berukuran 256 x 256 piksel dan 512 x 512 piksel

Citra	CC (256 x 256)	CC (512 x 512)
(a)	1	1
(b)	1	1
(c)	1	1
(d)	1	1
(e)	1	1
(f)	1	1

E. Hasil Uji Ekstraksi Pesan dengan Serangan

Pengujian ini dilakukan dengan menggunakan serangan *salt and paper* untuk mengetahui tingkat ketahanan citra tersebut dari serangan luar. *Salt and paper* merupakan pemberian kebisingan pada citra digital, dimana kebisingan ini akan tampak pada citra seperti butiran bola salju. Dengan adanya pengujian ketahanan ini dapat diketahui seberapa kuat metode ini menghadapi serangan dari luar.

Hasil pengujian ketahanan ditunjukkan dalam Tabel 5, yaitu dengan menggunakan dua ukuran citra pesan yang berbeda sebagai perbandingan tingkat ketahanan dari serangan luar. Saat diserang menggunakan *salt and paper,* hasil nilai CC masih bagus yaitu mendekati nilai 1. Dengan ini membuktikan metode ini tahan terhadap serangan *salt and paper*.

F. Komparasi dengan Metode yang Diusulkan

Implementasi teknik LSB dan teknik steganografi terbukti memberikan keuntungan dalam memberikan kualitas citra stego yang baik dan menjaga aspek *imperceptibility*. Tabel 6 memberikan komparasi dan

Tabel 5. Hasil pengukuran CC citra pesan pada citra cover berukuran 256 x 256 dan 512 x 512 setelah *salt and pepper*

Citra	CC (256 x 256)	CC (512 x 512)
(a)	0.7138	0.7243
(b)	0.7320	0.7315
(c)	0.7098	0.7305
(d)	0.7123	0.7386
(e)	0.6946	0.7245
(f)	0.7246	0.7355

Tabel 6. Komparasi dan hasil implementasi metode steganografi

Metode	Metode yang diusulkan	Metode dalam [7]	Metode dalam [10]
Ukuran citra *cover*	512x512	512x512	512x512
Jenis citra *cover*	*Grayscale* (8 bit)	*Grayscale* (8 bit)	RGB (24 bit)
Jenis pesan	Citra keabuan	Citra B/W,	Teks
Ukuran pesan (bit)	2562144	1024	1360
Metode	LSB-RSA 16 bit	DCT-OTP-PN	LSB-RSA
PSNR (dB)	57	54	69

hasil implementasi metode yang diusulkan dengan penelitian sebelumnya.

Berdasarkan Tabel 6 tersebut dapat disimpulkan bahwa metode yang diusulkan memiliki keamanan yang lebih baik dibandingkan dengan Lahase dan Dhole [10] karena metode RSA yang digunakan telah dimodifikasi dan dikembangkan menggunakan 16 bit. Selain itu, jenis pesan yang dapat disampaikan adalah berupa citra keabuan. Kualitas *imperceptibility* juga lebih baik dibandingkan Najih dkk. [7] karena jumlah pesan yang disisipkan jauh lebih banyak dan nilai PSNR masih lebih baik.

IV. KESIMPULAN

Penggunaan RSA 16 bit pada penyandian citra pesan dapat meningkatkan keamanan karena nilai *p* dan *q* dapat lebih bervariasi. Dengan variasi yang semakin banyak maka enkripsi RSA dapat lebih aman. Metode ini juga berhasil digabungkan dengan steganografi LSB. Selain disandikan, pesan juga disembunyikan dengan metode steganografi LSB sehingga keamanan pesan dapat meningkat. Teknik ini juga terbukti tahan terhadap serangan *salt and paper,* yaitu dengan hasil PSNR 57.2258dB, MSE 0.1232dB dan CC 1.0000 yang lebih baik dari penelitian sebelumnya. Dari hasil tersebut metode ini mampu melindungi dan mengamankan citra pesan *grayscale* dari pencurian pesan.

DAFTAR PUSTAKA

[1] D. R. I. M. Setiadi, E. H. Rachmawanto, and C. A. Sari, "Secure Image Steganography Algorithm Based on DCT with OTP Encryption," *Journal of Applied Intelliegent System*, vol. 2, no. 1, pp. 1-11, 2017.

[2] A. Susanto, D. R. I. M. Setiadi, C. A. Sari, and E. H. Rachmawanto, "Hybrid Method using HWT-DCT for Image Watermarking," in *International Conference on Information Technology for Cyber and IT Service Management (CITSM)*, Denpasar, 2017.

[3] E. H. Rachmawanto, R. S. Amin, D. R. I. M. Setiadi, and C. A. Sari, "A Performance Analysis StegoCrypt Algorithm based on LSB-AES 128 bit in Various Image Size," in *International Seminar on Technology for Technology of Information and Communication (iSemantic)*, Semarang, 2017.

[4] R. D. Ardy, O. R. Indriani, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Digital Image Signature using Triple Protection Cryptosystem (RSA, Vigenere, and MD5)," in *International Conference on Smart Cities, Automation & Intelligent Computing Systems (ICON-SONICS)*, Yogyakarta, 2017.

[5] D. R. I. M. Setiadi, T. Sutojo, E. H. Rachmawanto, and C. A. Sari, "Fast and Efficient Image Watermarking Algorithm using Discrete Tchebichef Transform," in *International Conference on Information Technology for Cyber and IT Service Management (CITSM)*, Denpasar, 2017.

[6] C. Irawan, D. R. I. M. Setiadi, C. A. Sari and E. H. Rachmawanto, "Hiding and Securing Message on Edge Areas of Image using LSB Steganography and OTP Encryption," in *International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, 2017.

[7] M. Najih, D. R. I. M. Setiadi, E. H. Rachmawanto, C. A. Sari, and S. Astuti, "An Improved Secure Image Hiding Technique Using PN-Sequence Based On DCT-OTP," in *International Conference on Informatics and Computational Sciences (ICICoS)*, Semarang, 2017.

[8] A. Setyono, D. R. I. M. Setiadi, and Muljono, "StegoCrypt Method using Wavelet Transform and One-Time Pad for Secret Image Delivery," in *International Conference on Information Technology, Computer and Electrical Engineering (ICITACEE)*, Semarang, 2017.

[9] T. Shahana, "A Secure DCT Image Steganography based on Public-Key Cryptography," *International Journal of Computer Trends and Technology (IJCTT)*, vol. 4, no. 3, pp. 2039-2043, 2013.

[10] M. S. Lahase, and S. A. Dhole, "Hybrid Encryption and Decryption Method using LSB and RSA in Steganography," *International Journal of Advances in Science, Engineering and*

Technology(IJASEAT), vol. 5, no. 3, pp. 68-70, 2015.

[11] M. F. Alamsyah, "Implementasi Metode Steganografi Least Significant Bit dengan Algoritma RSA pada Citra BMP," Skripsi, Universitas Dian Nuswantoro, 2015.

[12] O.R. Arifin, and T. Lucky, "Implementasi Kriptografi dan Steganografi Menggunakan Algoritma RSA dan Metode LSB," Skripsi, Universitas Negeri Malang, 2013.

[13] B. J. Saha, C. Pradhan, K. K. Kabi, and A. K. Bisoi, "Robust Watermarking Technique using Arnold's Transformation and RSA in Discrete Wavets," in *International Conference on Information Systems and Computer Networks (ISCON)*, Mathura, 2014.