 http://dx.doi.org/10.29313/.v6i2.23418

Keamanan Citra Digital Dengan Menggunakan Metode Kriptografi Kunci Publik dan Steganografi

Romzi Farhan Ghozi*, Yurika Permanasari

Prodi Matematika, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Islam Bandung, Indonesia.

*romzifarhan29@gmail.com

Abstract. Cryptography as part of Mathematical science, facilitates data and information security. Cryptography has the power for confusion and diffusion. The purpose of cryptography is to maintain data confidentiality, authentication, data integrity, and non-repudiation. Based on its purpose, cryptography is often used to secure the delivery of messages in the form of text or images (digital images) via Internet channels. One of the cryptographic methods commonly used is public key cryptography. Public key cryptography is a method of securing messages using two keys, namely the public key and the private key. The Rivest Shamir Adleman (RSA) method is a public key cryptographic method that is commonly used in information security. The advantage of the cryptographic method is the speed of the encryption and decryption of messages. Therefore, cryptography is often used to secure realtime messages. The results of cryptographic encryption are in the form of ciphertext that is difficult to read so that it easily raises public suspicion which indicates an important hidden message. Therefore we need a method that can hide messages without seeing the original message, namely steganography. The encrypted message image consists of 2 variations, namely, a color image with many objects and a greyscale image with one object. The process of embedding a color message image takes longer than a black and white image. Based on testing, the different message images and cover images show that the image quality level is influenced by the color variations in the cover image. The results of the second test obtained values ranging from 26 dB - 55 dB. The less color variations in the cover image, the smaller the error or MSE value in the embedding image will result in a larger PSNR value.

Keywords: cryptography, steganography, public key, RSA algorithm, LSB method.

Abstrak. Kriptografi sebagai bagian dari ilmu Matematika, memfasilitasi keamanan data dan informasi. Kriptografi memiliki kekuatan untuk confusion (pembingungan) dan diffusion (peleburan). Tujuan dari kriptografi adalah menjaga kerahasiaan data, autentikasi, integritas data, dan non repudiansi. Berdasarkan tujuannya, kriptografi sering digunakan untuk mengamankan pengiriman pesan baik berupa teks maupun gambar (citra digital) melalui saluran Internet. Salah satu metode kriptografi yang umum digunakan yaitu kriptografi kunci publik. Kriptografi kunci publik merupakan metode pengamanan pesan dengan menggunakan dua kunci yaitu kunci publik dan kunci privat. Metode Rivest Shamir Adleman (RSA) merupakan sebuah metode kriptografi kunci publik yang umum digunakan pada keamana informasi. Kelebihan dari metode kriptografi adalah kecepatan proses enkripsi dan dekripsi

pesan. Oleh karena itu kriptografi sering digunakan untuk mengamankan pesan realtime. Hasil enkripsi kriptografi berupa cipherteks yang sulit dibaca sehingga dengan mudah menimbulkan kecurigaan awam yang menandakan adanya pesan penting yang tersembunyi. Maka dari itu dibutuhkan suatu metode yang dapat menyembunyikan pesan tanpa terlihat pesan aslinya yaitu dengan steganografi. Citra pesan yang dienkripsi terdiri dari 2 variasi yaitu, citra berwarna dengan banyak objek dan citra greyscale dengan satu objek. Proses embedding citra pesan berwarna memakan waktu lebih lama dibandingkan dengan citra hitam putih. Berdasarkan pengujian, pada citra pesan dan citra cover yang berbeda didapatkan hasil bahwa tingkat kualitas citra dipengaruhi pada variasi warna pada citra cover. Hasil dari pengujian kedua diperoleh nilai dengan range 26 dB – 55 dB. Semakin sedikit variasi warna pada citra cover maka error atau nilai MSE pada citra embedding akan semakin kecil dan mengakibatkan nilai PSNR semakin besar.

Kata Kunci: kriptografi, steganografi, kunci public, algoritma RSA, Metode LSB.

1. Pendahuluan

Kemajuan teknologi semakin hari mengalami perkembangan yang sangat pesat. Perkembangan teknologi, terutama yang berkaitan dengan teknologi informasi dan komunikasi bukan hanya dalam hitungan tahun, bahkan bisa dalam hitungan bulan, hari, ataupun jam. Salah satu hal yang mengalami perkembangan sangat pesat diseluruh dunia adalah Internet. Masyarakat dunia tidak dapat terlepas dari Internet dalam berbagai kegiatan kesehariannya. Semua informasi multimedia di Internet dapat diakses dengan sangat mudah. Salah satu objek yang sering diakses adalah gambar digital (Citra Digital).

Dengan semakin mudahnya mengakses internet maka kerahasiaan suatu informasi sulit untuk dijaga termasuk informasi pada citra digital. Citra Digital merupakan sebuah representasi numerik dari sebuah gambar dua-dimensi. Citra Digital dapat mengandung sebuah informasi yang tidak semua orang dapat mengakses informasi tersebut. Pada skripsi ini citra digital dibagi menjadi dua yaitu citra pesan dan citra cover. Citra pesan merupakan citra yang menggandung suatu informasi didalamnya sedangkan citra cover merupakan citra yang digunakan sebagai media penyisipan citra pesan.

Dampak negatif kemajuan teknologi yaitu meningkatnya kejahatan dunia maya dimana keamanan suatu informasi menjadi ancaman nyata. Cepatnya perkembangan teknologi tidak menutup kemungkinan pihak yang tidak berkepentingan dapat dengan mudah mendapatkan suatu informasi yang rahasia

meskipun informasi tersebut sudah diamankan. Dengan kata lain dibutuhkan suatu hal yang baru agar masyarakat dapat mengamankan suatu informasi yang mereka miliki dari berbagai macam serangan peretas (hacker) atau orang yang tidak mempunyai hak mengetahui informasi tersebut.

Kriptografi sebagai bagian dari ilmu Matematika, memfasilitasi keamanan data dan informasi [1]. Kriptografi adalah ilmu dan seni dalam menyandikan suatu data/informasi yang biasa disebut sebagai pesan (message) melalui proses enkripsi [2]. Kriptografi memiliki kekuatan untuk confusion (pembingungan) dan diffusion (peleburan). Tujuan dari kriptografi adalah menjaga kerahasiaan data, autentikasi, integritas data, dan non repudiansi. Berdasarkan tujuannya, kriptografi sering digunakan untuk mengamankan pengiriman pesan baik berupa teks maupun gambar (citra digital) melalui saluran Internet.

Metode lain yang dapat digunakan untuk mengamankan pengiriman pesan adalah steganografi. Steganografi berasal dari bahasa Yunani yang berarti tulisan tersembunyi [3]. Steganografi merupakan ilmu yang mempelajari, meneliti, dan mengembangkan seni

menyembunyikan suatu informasi atau pesan [3]. Teknik Steganografi menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhmya tidak terlihat. Proses ini disebut dengan proses embeding.

Kelebihan dari metode kriptografi adalah kecepatan proses enkripsi dan dekripsi pesan. Oleh karena itu kriptografi sering digunakan untuk mengamankan pesan realtime seperti saluran telepon selular, Whatsapp, Line dan lain-lain. Akan tetapi hasil enkripsi kriptografi berupa cipherteks yang sulit dibaca sehingga dengan mudah menimbulkan kecurigaan awam yang menandakan adanya pesan penting yang tersembunyi. Maka dari itu dibutuhkan suatu metode yang dapat menyembunyikan pesan tanpa terlihat pesan aslinya yaitu dengan steganografi.

Beberapa peneliti telah mempelajari mengenai metode kriptografi RSA dan steganografi LSB. Berdasarkan kesimpulan dari penelitian sebelumnya, Niswati mengatakan bahwa metode LSB pada pengamanan pesan teks harus mempunyai ukuran yang sama dengan besaran citra cover [3]. Menurut A.E Handoyo mengatakan bahwa kombinasi metode RSA dan LSB mampu mengamankan citra pesan grayscale dari pencurian pesan [4]. Oleh karena itu skripsi ini akan meneliti mengenai keamanan citra digital menggunakan metode kriptografi kunci publik dan steganografi dengan citra pesan dan citra cover yang berbeda.

Berdasarkan latar belakang yang telah diuraikan, maka perumusan masalah dalam penelitian ini sebagai berikut: “Bagaimana proses enkripsi RSA dan embedding LSB pada citra pesan ?”, “Apa perbedaan citra yang dihasilkan dari proses kombinasi kriptografi kunci publik RSA dan steganografi LSB dengan memperhatikan variasi citra pesan dan citra cover ?”, “Bagaimana kualitas citra yang dihasilkan dari kombinasi metode RSA dan LSB ?”. Selanjutnya, tujuan dalam penelitian ini diuraikan dalam pokok-pokok sbb.

1. Mengetahui bagaimana proses enkripsi RSA dan embedding LSB pada citra pesan.
2. Mengetahui perbandingan gambar dari hasil proses kombinasi metode RSA dan LSB berdasarkan variasi objek yang berbeda.
3. Mengetahui kualitas citra yang dihasilkan dari proses kombinasi metode RSA dan LSB.

2. Landasan Teori

Citra merupakan suatu gambaran, kemiripan, atau imitasi dari sebuah objek. Pada penelitian ini citra dibagi menjadi dua yaitu citra yang mengandung informasi atau disebut citra pesan, dan citra cover yaitu citra yang tidak memiliki arti atau dengan kata lain hanya berupa gambar saja.

Pada proses pengamanan citra digital dibutuhkan dua metode pengamanan yaitu kriptografi dan steganografi. Kriptografi (cryptography) berasal dari Bahasa Yunani: “cryptos” artinya “secret” (tersembunyi atau rahasia), sedangkan “graphein” artinya “writing” (tulisan). Sehingga kriptografi artinya ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan keamanan informasi, seperti kerahasian data, keabsahan data, integritas data dan autentikasi data (Menezes, Oorshot and Vanstone 1996).

Kriptografi kunci publik merupakan metode pada kriptografi yang pada penelitian ini digunakan untuk mengamankan citra. Pada kriptografi kunci publik dibutuhkan dua kunci untuk melakukan pengamanannya yaitu kunci publik untuk mengamankan pesan dan kunci privat untuk menterjemahkan pesan. Metode kriptografi kunci publik yang digunakan pada penelitian ini yaitu metode Rivest Shamir Adleman (RSA).

Sedangkan steganografi adalah ilmu dan seni menulis atau menyembunyikan pesan ke dalam sebuah media sedemikian rupa sehingga keberadaan pesan tidak diketahui atau tidak disadari oleh orang selain pengirim dan penerima pesan tersebut. Least Significant Bit (LSB) adalah Teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode Least Significant Bit (LSB) yaitu merubah bit redundan cover image yang tidak berpengaruh signifikan dengan bit dari pesan rahasia [8].

Pada penelitian ini, hasil dari proses RSA dan LSB akan diuji menggunakan metode *Mean Square Error* (MSE) dan *Peak Signal to Noise Ration* (PSNR) untuk mendapatkan nilai error dan kualitas citra yang dihasilkan.

3. Hasil Penelitian dan Pembahasan

Proses Enkripsi dan Dekripsi Citra Digital

Proses pengamanan citra digital dilakukan sebanyak dua kali yaitu dengan menggunakan metode Rivest Shamir Adleman (RSA) dan Least Significant Bit (LSB). Langkah awal dalam proses pengamanan citra digital yaitu dibutuhkan kunci publik dan kunci privat untuk melakukan proses enkripsi dan dekripsi dengan metode Rivest Shamir Adleman (RSA). Citra pesan akan dienkripsi menggunakan metode RSA dengan menggunakan kunci publik sehingga dihasilkan citra terenkripsi. Citra yang digunakan dalam penelitian ini memiliki format JPG.

Gambar 1. Citra Pesan

Gambar 2. Citra Terenkripsi

Gambar 1. merupakan citra pesan sebelum dilakukan proses enkripsi menggunakan metode RSA dan Gambar 2. merupakan gambar citra yang sudah dienkripsi (Citra Terenkripsi). Citra terenkripsi akan digunakan pada proses *embedding* LSB. Proses pada metode LSB yaitu merubah nilai bit akhir pada citra cover dengan nilai biat pada citra terenkripsi. Proses LSB dapat digambarkan sebagai berikut:

Tabel 1. Nilai Biner Citra Cover

00000000	00010010	00011011	00000000	…
00011101	00000000	00001011	00000000	…
00000000	00011000	00010010	00100011	…
…	…	…	…	…

Tabel 1. Nilai Biner Citra Pesan

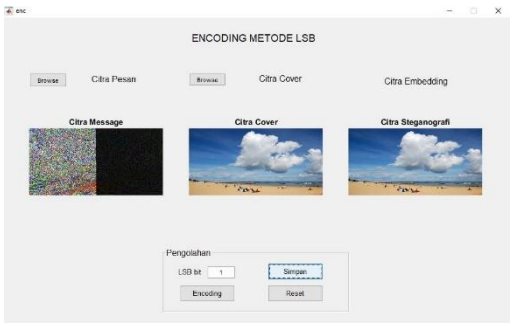
00000011	…
00100001	…
00100001	…
…	…

Tabel 1. dan Tabel 2. merupakan sebuah contoh nilai biner dari citra cover dan citra pesan. Dalam hal ini nilai biner pada citra cover akan disisipkan sebuah pesan yang berasal dari citra pesan dengan mengubah bit akhir pada citra cover dengan bit citra pesan. Besaran bit yang terdapat pada citra cover maupun citra pesan yaitu 8 bit.

Tabel 3. Citra Embedding

00000000	00010010	00011010	00000000	…
00011100	00000000	00001011	00000000	…
00000000	00011000	00010011	00100010	…
…	…	…	…	…

Dengan menggunakan metode LSB dapat dilihat pada Tabel 3., nilai yang dicetak tebal merupakan nilai baru hasil dari penyisipan pesan kedalam citra cover. Sehingga akan diperoleh sebuah nilai baru pada tiap elemen matriksnya dan citra pesan yang dihasilkan akan tersamarkan dengan citra cover dan diperoleh citra embedding. Hasil dari proses embedding akan diperoleh gambar seperti berikut :



Gambar 3. Proses LSB

Setelah melakukan proses RSA dan LSB, citra embedding akan diuji menggunakan metode *Mean Square Error* (MSE) dan *Peak Signal to Noise Ration* (PSNR). Uji kualitas bertujuan untuk melihat seberapa baik kualitas citra embedding yang dihasilkan. Pada penelitian ini akan dilakukan 2 pengujian yaitu :

1. Pengujian pada citra embedding berdasarkan variasi citra pesan dan satu citra cover.
2. Pengujian pada citra embedding berdasarkan variasi citra cover dan satu citra pesan.

Hasil dari dua pengujian akan diperoleh nilai sebagai berikut :

Tabel 2. Uji Kualitas Pada Variasi Citra Pesan

Citra	MSE	PSNR
Citra Embedding 1	21.318	26.1433 dB
Citra Embedding 2	21.2294	26.1934 dB

Tabel 3. Uji Kualitas Pada Variasi Citra Cover

Citra Cover	MSE	PSNR
Cover 1	18.6583	26.1714 dB
Cover 2	4.57008	40.2173 dB
Cover 3	11.9923	32.5992 dB
Cover 4	0.998848	55.4242 dB

4. Kesimpulan

Berdasarkan pembahasan dalam penelitian ini, peneliti menyimpulkan beberapa hasil penelitian sebagai berikut:

1. Teknik pengamanan citra digital menggunakan kriptografi RSA dan steganografi LSB dilakukan dengan mengenkripsi terlebih dahulu citra pesan menggunakan RSA kemudian mengganti bit terakhir kode biner dari masing-masing piksel citra terenkripsi menggunakan metode LSB.
2. Hasil proses RSA pada citra pesan menghasilkan 2 layer citra terenkripsi. 2 layer tersebut akan menjadi input proses embedding pada steganografi LSB.
3. Keamanan pada citra ditunjukan pada tingkat derau yang dimiliki citra. Kualitas embedding pada citra dikatakan baik apabila nilai MSE kecil dan nilai PSNR diatas 30 dB. Pada kasus yang diteliti, terdapat beberapa pengujian terhadap citra pesan dan citra cover yang berbeda. Hasil pengujian pada citra pesan dan citra cover yang berbeda menghasilkan nilai yang bervariasi. Pengujian pada citra pesan yang berbeda dan citra cover yang sama diperoleh nilai MSE yang tinggi dan nilai PSNR dibawah 30 dB. Sedangkan pada pengujian citra pesan yang sama dan citra cover yang berbeda diperoleh hasil yang bervariasi berdasarkan banyaknya kombinasi warna pada citra cover. Hasil dari pengujian kedua diperoleh nilai dengan range 26 dB – 55 dB. Berdasarkan kedua pengujian dapat dikatakan bahwa tingkat kualitas embedding ditentukan dari citra cover yang digunakan. Semakin sedikit variasi warna pada citra cover maka semakin kecil nilai MSE yang menyebabkan nilai PSNR semakin tinggi.

Daftar Pustaka

[1] R. W. Lumbangaol, "Aplikasi Pengamanan Gambar Dengan Algoritma Rivest Shamir Adleman (RSA)".
[2] R. Munir, Kriptografi Edisi Kedua, Bandung: Informatika, 2019.
[3] Z. Niswati, "Steganografi Berbasis Least SIgnificant Bit (LSB)," Faktor Exacta, pp. 181-191, 2010.
[4] 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," Teknologi dan Sistem Komputer, p. 6, 2018.
[5] T. Sutoyo, Teori Pengolahan Citra Digital, Yogyakarta: Andi Offset, 2009.
[6] S. Kromodimeoljo, "Teori dan Aplikasi Kriptografi," SPK IT Consulting, 2009.
[7] A. A. Rakhman and A. W. Kurniawan, "Implementasi Algoritma Kriptografi Rivest Shamir Adleman (RSA) dan Vigenre Cipher Pada Gambar Bitmap 8 Bit".
[8] K. Imam, Penyembunyian Pesan Rahasia Pada Citra Digital Dengan Teknik Steganografi Menggunakan Metode Least SIgnificant Bit (LSB), Jakarta: Universitas Budi Luhur, 2013.
[9] A. Kadir and A. Susanto, Teori dan Aplikasi Pengolahan Citra, Yogyakarta: Publisher, 2013.
[10] S. and M. Rezqy, "Implementasi Teknik Visible Watermarking Dengan Metode One-To-One Mapping Pada Citra Digital," Jurnal Ilmiah Teknik Mesin, vol. VII, no. 1, pp. 43-44, November 2015.
[11] G. M. Male, W. and E. Setijadi, "Analisis Kualitas Citra Pada Steganografi Untuk Aplikasi e-Government," in Prosiding Seminar Nasional Teknologi XV, Surabaya, 2012.