PENGAMANAN PESAN MENGGUNAKAN KOMBINASI METODE KRIPTOGRAFI RSA, VIGENERE CIPHER, DAN HILL CIPHER DENGAN METODE STEGANOGRAFI LEAST SIGNIFICANT BIT

Raynaldi Fatih Amanullah[1], **Bayu Trisna Pratama**[2], **Dony Ariyus**[3]

Magister Teknik Informatika
Fakultas Teknik Informatika
Universitas Amikom Yogyakarta

raynaldi.a@students.amikom.ac.id[1], bayu.pratama@students.amikom.ac.id[2], dony.a@amikom.ac.id[3]

Abstrak

Pengamanan privasi dan kepemilikan informasi telah menjadi isu yang penting dan patut diteliti di era keterbukaan informasi seperti sekarang ini. Keamanan data berfokus pada bagaimana sebuah pesan dapat dijaga kerahasiannya dari pengirim ke penerima. Kriptografi dan Steganografi merupakan salah satu metode yang dapat digunakan untuk mengamankan data. Kombinasi keduanya akan membuat keamanan dalam komunikasi data menjadi lebih kuat. Penelitian ini dilakukan untuk mengembangkan sebuah metode pengamanan pesan dengan menggunakan kombinasi metode kriptografi RSA, Vigenere Cipher, dan Hill Cipher dengan metode steganografi Least Significant Bit (LSB). Metode tersebut kemudian diuji dengan melakukan perubahan warna, ukuran serta pemotongan pada media penyimpan pesan. Hasil pengujian menunjukkan bahwa dalam beberapa kondisi, pesan yang ada dalam media masih dapat dibaca dan didekripsi ke bentuk asalnya.

Kata Kunci: Kriptografi, RSA, Vigenere Cipher, Hill Cipher, LSB, Steganografi.

1. Pendahuluan

Pada saat ini, pengamanan privasi dan kepemilikan informasi selama proses transmisi adalah sebuah pekerjaan penting yang patut dilakukan dan diselesaikan. Mempertahankan konfidentialitas (*confidentiality*) sebuah informasi menjadi faktor penting yang membutuhkan perhatian lebih dalam rangka untuk mempertahankan kerahasiaannya. Kriptografi telah digunakan selama berabad-abad sebagai salah satu metode untuk mengamankan informasi dalam komunikasi. (Sagar dan Kumar, 2015)

Untuk dapat meningkatkan dan memperkuat kemanan data maupun informasi, teknik-teknik seperti kriptografi dan steganografi dapat digunakan. Keduanya memiliki karakteristik yang berbeda, dimana kriptografi bekerja dengan melakukan proses pengacakan data terhadap pesan awal (*plain text*) sehingga menjadi data yang sekilas tidak beraturan yang tidak dapat dibaca tanpa kunci khusus (*key*) untuk membuka atau memecahkan teks tersebut. Sedangkan steganografi berfungsi untuk menyisipkan pesan data asli pada sebuah media

sehingga pihak ketiga (*evil*) tidak menyadari adanya sebuah pesan pada media tersebut. (Irawan, 2015)

Kedua metode tersebut memiliki kelemahannya masing-masing. Steganografi dapat dianggap gagal jika penyerang (*attacker*) mengetahui adanya pesan rahasia dalam media yang ada. Sedangkan kriptografi dianggap gagal jika penyerang mampu meretas dan mengekstraksi pesan rahasia dalam sebuah *cipher text*. Salah satu opsi terbaik untuk mengamankan pesan adalah dengan menggunakan kombinasi keduanya. Steganografi berfungsi untuk menambahkan lapisan keamanan tambahan terhadap kriptogafi. Kombinasi keduanya membuat sebuah komunikasi atau pertukaran data menjadi lebih aman dan kuat. (Imam Rahmani, dkk., 2015)

Beberapa penelitian sebelumnya telah dilakukan untuk mencoba mengombinasikan kriptografi dan steganografi ini. Budi Prasetiyo dkk melakukan penelitian dengan mengombinasikan metode steganografi bit matching dan metode kriptografi DES dan mengujinya dengan penggunaan noise salt dan peper serta diukur nilai *Mean Squared Error* (MSE) nya (Prasetiyo, Gernowo, & Noranita, 2015). Sedangkan Anil Kumar dan Rohini Sharma melakukan penelitian penggabungan metode kriptografi RSA dan metode steganografi Hash-LSB dan mengujinya dengan metode *peak signal to noise ratio* (PSNR) dan MSE (Kumar dan Sharma, 2013). Penelitian lain dilakukan oleh Varsha dan Rajender yang meneliti tentang penggabungan antara metode kriptografi RSA dan metode steganografi *Least Significant Bit* (LSB) dan mengujinya dengan PSNR dan MSE (Chhillar, 2015).

Diantara penelitian-penelitian tersebut masih belum terdapat penelitian yang membahas mengenai kombinasi metode kriptografi RSA, Vigenere Cipher, dan Hill Cipher dengan metode steganografi LSB. Penelitian ini dilakukan untuk meneliti bagaimana mengombinasikan metode-metode tersebut dan mengujinya dengan menggunakan pendekatan perubahan warna (*Coloring*) dan perubahan bentuk (*resize / cropping*).

2. Tinjauan Pustaka

2.1. RSA

Nama algoritma RSA berasal dari tiga orang peneliti MIT (*Massachussets Institute of Technology*) pada tahun 1976, yakni Ron Rivest, Adi Shamir, dan Leonard Adleman (Stallings, 2014). RSA merupakan salah satu teknik penyandiaan yang memiliki kunci berbeda dalam melakukan enkripsi *plain text*

atau pun dekripsi *cipher text*, dimana kunci yang digunakan untuk melakukan enkripsi disebut sebagai *public key* (kunci publik) dan yang digunakan untuk melakukan dekripsi dinamakan *private key* atau kunci privat (Munir, 2004). Dalam hal ini, kunci publik dapat dimiliki oleh sembarang orang, namun untuk kepemilikan kunci privat hanya sebatas oleh orang-orang tertentu yang memiliki kepentingan (Rahajoeningroem dan Aria, 2011).

Adapun langkah-langkah dalam menentukan kunci dalam RSA antara lain, sebagai berikut (Munir, 2004):

1. Menentukan dua buah bilang prima sembarang, sebagai contoh p_1 dan p_2.
2. Menghitung nilai n, yang mana terlihat pada persamaan (1).

$$n = p_1 \times p_2 \quad (1)$$

3. Mencari nilai $\varphi(n)$, diperlihatkan dalam persamaan (2).

$$\varphi(n) = (p_1 - 1) \times (p_2 - 1) \quad (2)$$

4. Memilih sebuah bilangan bulat sebagai kunci publik yang kemudian disebut dengan e, pada umumnya hasil pembagian antara e dan $\varphi(n)$ adalah 1, selain itu apabila ingin melanjutkan pada tahap selanjutnya nilai e tidak boleh menghasilkan bilangan bulat (*integer*).
5. Nilai d merupakan bilangan penyusun kunci privat, yang mana apabila dihitung secara matematis ($d \times e) \, mod \, \varphi(n) = 1$
6. Pembentukan *public key* (kunci publik) berasal dari hasil perhitungan nilai e dan nilai n, sedangkan *private key* (kunci privat) berasal dari perhitungan nilai d dan n.

Keamanan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor primanya, yang dalam hal ini ialah persamaan (1), sekali nilai n berhasil difaktorkan menjadi p_1 dan p_2, maka persamaan (2) dapat dihitung, selain itu karena kunci publik diketahui oleh sembarang orang, maka kunci privat dapat dihitung (Ariyus, 2008).

2.2. Vigenere Cipher

Kode Vigenere termasuk kode abjad-majemuk (*polyalphabetic substitution chiper*). Dipublikasikan oleh diplomat (sekaligus sorang kriptologis) Perancis, Blaise de Vigenere pada abad 16, tepatnya tahun 1586. Algoritma ini baru dikenal luas setelah 200 tahun kemudian dan dinamakan kode Vigenere. Pada teknik substitusi Vigenere setiap teks-kode bisa memiliki banyak kemungkinan teks-asli. Teknik dari substitusi Vigenere bisa dilakukan dengan dua cara, yaitu angka dan huruf (Ariyus, 2008).

1. Angka

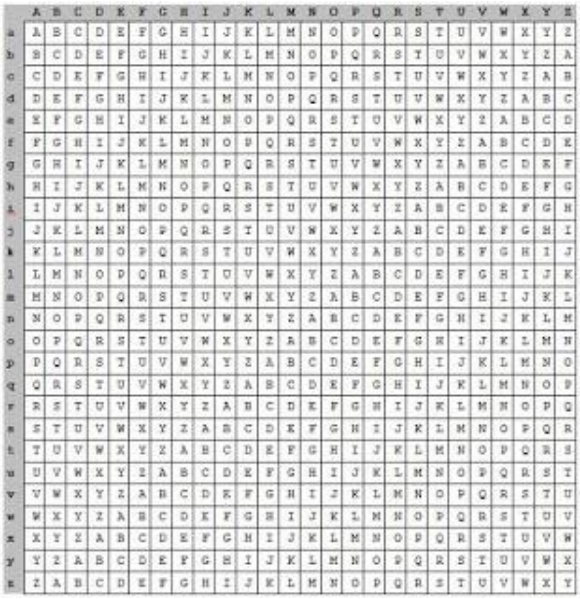
   Teknis substitusi Vigenere dengan menggunakan angka dilakukan dengan menukarkan huruf dengan angka, seperti yang terlihat pada Tabel 1.

Tabel 1 Subtitusi Angka Vigenere Cipher

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
0	1	2	3	4	5	6	7	8	9	10	11	12
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
13	14	15	16	17	18	19	20	21	22	23	24	25

2. Huruf

   Ide dasarnya adalah dengan menggunakan kode Caesar, tetapi jumlah pergeseran hurufnya berbeda-beda untuk setiap hurufnya. Untuk mengenkripsi pesan dengan kode Vegenere digunakanlah *tabula recta*, seperti yang terdapat pada Gambar 1.



Gambar 1: *Tabula Recta*

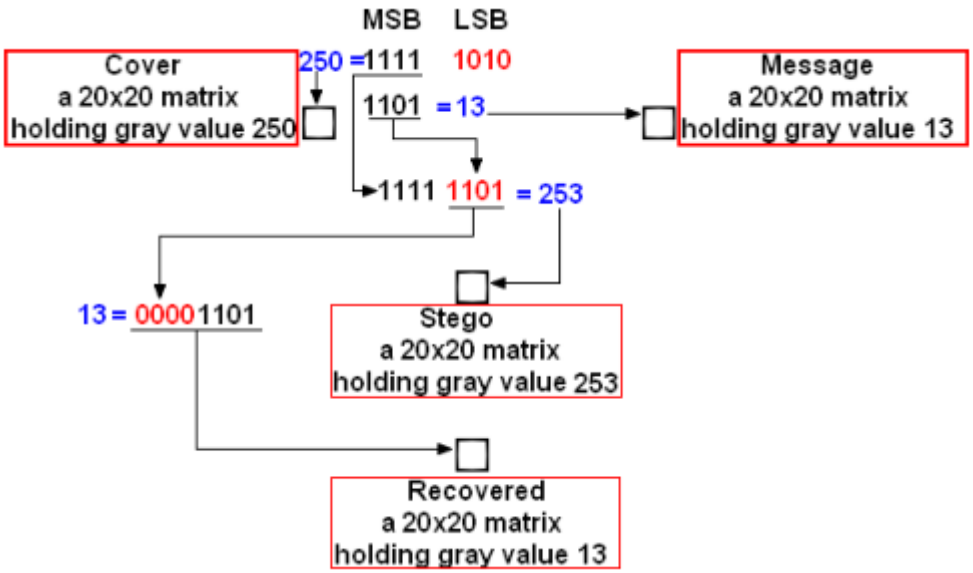
2.3. Hill Cipher

Kode Hill termasuk salah satu sistem kripto polialfabetik, yang berarti setiap karakter alfabet bisa dipetakan ke lebih satu macam karakter. Kode ini ditemukan pada tahun 1929 oleh Lester S. Hill. Ide dari Kode Hill adalah dengan mengambil m kombinasi linear dari m karakter alfabet dalam satu elemen teks-asli sehingga dihasilkan m alfabet karakter dalam satu elemen teks-asli (Ariyus, 2008).

Dasar dari teknik Hill Cipher adalah aritmatika modulo terhadap matriks. Dalam penerapannya, Hill Cipher menggunakan teknik perkalian matriks dan teknik invers terhadap matriks. Kunci pada Hill Cipher adalah matriks n x n dengan n merupakan ukuran blok. Matriks K yang menjadi kunci ini harus merupakan matriks yang invertible, yaitu memiliki inverse K-1 (Forouzan, 2014).

2.4. Least Significant Bit (LSB)

LSB adalah teknik yang umum digunakan dalam enkripsi dan dekripsi informasi rahasia. Cara kerja metode LSB yaitu mengubah bit redundan cover image yang tidak berpengaruh signifikan dengan bit dari pesan rahasia. Gambar 2 berikut ini menunjukkan mekanisme metode LSB pada gambar 8 bit dengan memanfaatkan 4 bit LSB (Cheddad, dkk., 2010).



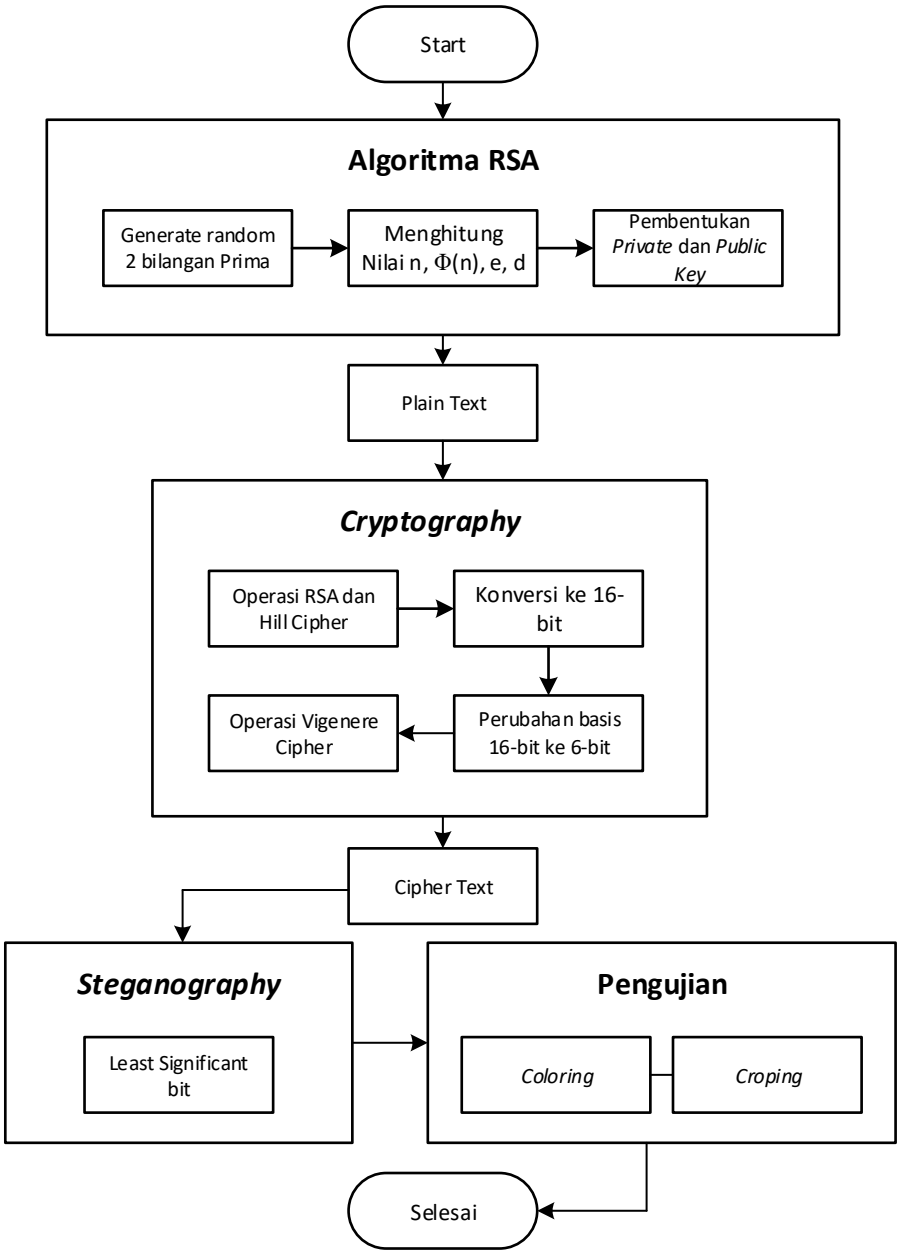
Gambar 2: Mekanisme LSB

Gambar 2 menunjukkan penerapan LSB menggunakan media gambar berbasis pixel dengan nilai 8 bit (gray value). Setiap pixel yang terdiri dari 8 bit dibagi menjadi 2 bagian yaitu, 4 bit MSB (most significant bit) dan 4 bit LSB (least

significat bit). Bagian LSB lah yang diubah menjadi nilai dari pesan yang akan disisipkan. Setelah dibubuhi pesan rahasia, setiap pixel dibangun kembali menjadi gambar yang utuh menyerupai dengan media gambar semula (Cheddad, dkk., 2010).

3. Metode Yang Diusulkan

Metode yang diusulkan dalam penelitian ini memiliki alur sebagaimana yang ditunjukkan oleh Gambar 3 berikut ini.



Gambar 3: Alur Penelitian

Sebagaimana yang terlihat pada Gambar 3, metode yang diusulkan memiliki bagian-bagian atau proses-proses berikut ini:

1. Algoritma RSA. Proses ini dilakukan untuk membuat (*generate*) kunci publik dan kunci pribadi pada RSA. Sebagaimana yang telah dipaparkan pada bagian sebelumnya terdapat proses untuk menggenerasi kunci publik dan pribadi pada RSA.
2. Operasi RSA dan Hill Cipher. Pada proses ini, dilakukan operasi RSA pada plain text. Operasi ini menggunakan persamaan (1) dan (2). Selanjutnya dilakukan operasi Hill Cipher dengan mengalikan matriks kunci dengan matriks plain text hasil operasi dengan RSA.
3. Konversi ke bentuk biner 16 bit dan perubahan basis bit dari 16 bit ke 6 bit. Hasil desimal pada proses sebelumnya diubah ke bentuk biner berbasis 16 bit. Selanjutnya dilakukan penggabungan setiap 3 buah bilangan 16 bit untuk membentuk 8 bilangan berbasis 6 bit.
4. Operasi Vigenere Cipher. Dari hasil sebelumnya, dilakukan operasi vigenere cipher dengan menggunakan kunci berupa matriks kunci publik. Output dari proses ini adalah *cipher text* hasil kombinasi metode kriptografi.
5. Steganografi dengan LSB. Setelah diperoleh *cipher text* dari proses sebelumya, dilakukan penyisipan *cipher text* pada media gambar dengan metode LSB.
6. Pengujian. Pengujian dilakukan untuk menguji keberadaan pesan setelah dikenai proses perubahan warna (*coloring*) dan pemotongan (*croping*) dengan parameter tertentu.

4. Hasil dan Pembahasan

Bagian ini menjelaskan mengenai hasil dan pembahasan antara kombinasi algoritm(a RSA, Vigenere Cipher, Hill Cipher dengan LSB. Terdapat dua skema pengujian, dimana skema yang pertama yakni dilakukannya perubahan warna (*coloring*) dan skema yang kedua dengan dilakukannya perubahan ukuran dan pemotongan dari gambar dengan posisi tertentu. Pada uji coba ini dimisalkan kunci publik dan privat hasil *generate* adalah D-EBIJ dan CHAH-EBIJ, dengan *plain text* berupa kalimat “Selamat Pagi Indonesia”.

4.1. Pengujian Perubahan Warna (*Coloring*)

Dalam proses pengujian ini, dilakukan dengan perubahan skema warna (*coloring*) untuk melihat pengaruhnya terhadap keberadaan pesan yang

tersembunyi dalam gambar uji. Pengujian ini dilakukan seperti yang terlihat pada Tabel 2.

Tabel 2: Pengujian Perubahan Warna (*Coloring*)

Proses	Keterangan	Hasil Dekripsi	Status
Perubahan RGB ke CMYK	Melakukan konversi gambar RGB ke gambar CMYK	selamat pagi indonesia	Berhasil
Perubahan Hue/ Saturation	Mengubah nilai Hue dan Saturation dari 0 menjadi -1	selamat pagi indonesia	Berhasil
Perubahan Brightness	Mengubah pengaturan brightness dari 0 menjadi -1	selamat pagi indonesia	Berhasil
Greyscale	Mengubah gambar menjadi hitam putih	aaaaaaaaaaaaaa aaaaaaaaaaaaaa aaaaaaaaaaaaaa aaaaaaaaaaaaaa aaaaaaaaaaaa	Gagal
Perubahan jumlah bits setiap channel	Mengubah bits/ channel dari 8 ke 16	selamat pagi indonesia	Berhasil
	Mengubah bits/ channel dari 8 ke 32	-	Gagal

Dari Tabel 2, dapat dilihat bahwa dalam pengujian perubahan jenis pewarnaan dari RGB ke CMYK, perubahan Hue/Saturation, perubahan Brightness, dan perubahan jumlah bits setiap channe dari 8 ke 16 bit memberikan status Berhasil yang artinya pesan dalam gambar berhasil didekripsi dengan baik.

Sementara itu, pada pengujian berubahan gambar ke bentuk Grayscale dan perubahan jumlah bits setiap channel dari 8 ke 32 bit ternyata memberikan status Gagal yang artinya pesan tidak berhasil didekripsi setelah dilakukan gambar pembawa pesan dilakukan 2 perubahan tersebut.

4.2. Pengujian Perubahan Ukuran dan Pemotongan Gambar (*Croping*)

Hasil pengujian *steganography* untuk skema yang kedua dapat dilihat pada Tabel 3.

Tabel 3: Pengujian *Resize* dan *Croping*

Proses	Keterangan	Pesan Dekripsi	Status
Perubahan Ukuran (*resize*)	Perubahan pixel dari ukuran 2000 px menjadi 1976 px (*range* pengurangan 1 – 24)	selamat pagi indonesiaa	Berhasil
	Perubahan pixel dari ukuran 2000 px menjadi kurang dari 1976 px (*range* pengurangan lebih 24)	-	Gagal
	Perubahan pixel dari ukuran 2000 px menjadi lebih dari 2032 px (range penambahan lebih dari 32)	-	Gagal
Pemotongan Gambar (*Croping*)	Pemotongan sisi kanan	selamat pagi indonesia	Berhasil
	Pemotongan sisi bawah	selamat pagi indonesia	Berhasil
	Pemotongan sisi kiri	-	Gagal
	Pemotongan sisi atas	-	Gagal

Tabel 3 menunjukkan pengujian perubahan pada gambar pembawa pesan dengan merubah bentuk gambar pembawa pesan melalui proses perubahan ukuran (*resizing*) dan pemotongan gambar (*cropping*). Dari hasil pengujian dengan perubahan ukuran (*resizing*), terlihat pada range pengurangan di bawah 24 px, metode yang diusulkan masih memberikan status Berhasil. Namun, pada range pengurangan di atas 24 px, terlihat metode yang diusulkan gagal. Hal ini menunjukkan bahwa perubahan yang ukuran yang signifikan terhadap gambar membuat pesan yang ada di dalam gambar hilang.

Sementara pada hasil pengujian dengan pemotongan gambar (*croping*), pemotongan gambar pada sisi kanan dan sisi bawah ternyata tidak menghilangkan pesan dalam gambar. Akan tetapi, pemotongan pada sisi kiri dan sisi atas gambar, menghilangkan pesan dalam gambar. Hasil tersebut menunjukkan bahwa metode yang diusulkan belum mampu menangani masalah pada pemotongan gambar.

5. Kesimpulan dan Saran

Pada penelitian ini dilakukan penelitian mengenai kombinasi metode kriptografi RSA, Vigenere Cipher, dan Hill Cipher dengan metode steganografi LSB. Hasil pengujian perubahan warna (coloring) menunjukkan bahwa metode yang diusulkan berhasil pada perubahan RGB ke CMYK, perubahan Hue/Saturation dari 0 menjadi -1, perubahan brightness dari 0 menjadi -1, dan perubahan bits/channel dari 8 ke 16.

Sedangkan pada pengujian perubahan ukuran (*resize*), metode yang diusulkan berhasil pada perubahan ukuran dengan range pengurangan di bawah 24 px. Pada pengujian dengan pemotongan (*croping*) metode yang diusulkan berhasil pada pemotongan sisi kanan dan pemotongan sisi bawah.

Penelitian selanjutnya dapat difokuskan pada penelitian mengenai perubahan pada media setelah diunggah ke media sosial. Hal ini dikarenakan media sosial meruapakan sarana penyebaran media yang tepat dan luas, namun setiap sosial media memiliki kebijakan masing-masing mengenai perubahan pada media yang diupload pada server mereka seperti dilakukan resize, perubahan warna, kompresi ukuran, dll. Penelitian selanjutnya dapat berfokus pada mempertahankan pesan dalam media setelah diunggah pada media sosial tertentu.

Daftar Pustaka

Ariyus, D. (2008). *Pengantar Ilmu Kriptografi: Teori, Analisis dan Implementasi.* Yogyakarta: Penerbit ANDI.

Cheddad, A., Condell, J., Curran, K., & Kevitt, P. M. (2010). Digital Image Steganography: Survey and Analysis of Current Methods. *Signal Processing* (pp. 727 - 754). Brazil: Elsevier.

Chhillar, R. S. (2015). Data Hiding using Advanced LSB with RSA Algorithm. *International Journal of Computer Applications*, *122*(4).

Forouzan, B. A. (2014). *Cryptography and Network Security.* New York: McGraw Hill.

Imam Rahmani, M. K., Goyal, A., & Mudgal, M. (2015). Study of Cryptography and Steganography System. International Journal Of Engineering And Computer Science. https://doi.org/10.18535/ijecs/v4i8.12

Irawan, P. L. T. (2015). Implementasi Teknik Kriptografi Stream Cipher Salsa20 Untuk Pengamanan Basis Data. SMATIKA JURNAL, 5(2), 88–92.

Kumar, A., & Sharma, R. (2013). A secure image steganography based on RSA algorithm and hash-LSB Technique. International Journal of Advanced Research in Computer Science and Software Engineering, 3(7).

Munir, R. (2004). *Algoritma RSA dan ElGamal.* Bandung: Departemen Teknik Informatika Institut Teknologi Bandung.

Prasetiyo, B., Gernowo, R., & Noranita, B. (2015). Kombinasi Steganografi Berbasis Bit Matching dan Kriptografi DES untuk Pengamanan Data. Scientific Journal of Informatics, 1(1), 79–93. https://doi.org/10.15294/sji.v1i1.3643

Rahajoeningroem, T., & Aria, M. (2011). Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa. *Jurnal Majalah Ilmiah Unikom*, 77 - 90.

Sagar, V., & Kumar, K. (2015). A symmetric key cryptography using genetic algorithm and error back propagation neural network. In 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1386–1391).

Stallings, W. (2014). *Cryptography and Network Security Principle and Practice Sixth Edition.* United States of America: Pearsone Education, Inc.