ISSN: 2477-5126
e-ISSN: 2548-9356

Implementasi Algoritma *Hybrid* dan Metode *Least Significant Bit* Untuk Keamanan Data

Ibnu Sulistyo[1*)], Eko Aribowo[2]
[1,2]JProgram Studi Teknik Informatika, Fakultas Teknologi Industro, Universitas Ahmad Dahlan, Yogyakart
[1,2]Jl. A.Yani(Ring Road Selatan) Kragilan, Tamanan, Banguntapan, Bantul,,Yogyakarta 55191, Indonesia
email: [1]ibnusulistyo16@gmail.com, [2]ekoab@tif.uad.ac.id

Abstract – Computer networks can improve the quality of communication; however, it also allows accessing data illegally. Unauthorized access to people's data can cause harm. In order for the data to remain safe, the cryptographic algorithm encryption process is needed. Nevertheless, there is also a disadvantage of encryption which can lead to suspicions. To get rid of unnecessary suspicion, there is a need for steganography algorithms, and one way of making sure that it is hidden is by using the least significant bit method. This research uses a hybrid algorithm and the least significant bit technique. Hybrid algorithm models are used for better security before being concealed under the image, and the only way of doing that is by using least significant bit method. The types of image files used are PNG and JPG or JPEG. The success rate of this experiment is 100%, with eight tests that have been done with a maximum insertion of 5000 characters.

Abstrak – Jaringan komputer dapat meningkatkan kualitas komunikasi namun memungkinkan akses yang ilegal terhadap data. Akses tidak sah kesuatu data dapat merugikan pemilik data. Supaya data tetap aman diperlu proses enkripsi algoritma kriptografi. Namun, memiliki kekurangan yaitu keunikan hasil enkripsi mampu menimbulkan kecurigaan terhadap data tersebut. Untuk menutupi itu diperlukannya algoritma steganografi, salah satunya metode *least significant bit*. Penelitian ini menerapkan algoritma *hybrid* dan *least significant bit*. Penggunaan model algortima *hybrid* untuk keamanan berlapis yang lebih baik sebelum disembunyikankan ke dalam gambar menggunakan metode *least significant bit*. Jenis *file* gambar yang digunakan yaitu PNG dan JPG/JPEG. Tingkat keberhasilan sebesar 100% dengan pengujian yang telah dilakukan sebanyak 8 percobaan dengan masimal penyisipan 5000 karakter.

***Kata Kunci* – Hybrid, Least Significant Bit, Kriptografi, Steganografi**

I. PENDAHULUAN

Jaringan komputer dapat meningkatkan kualitas komunikasi namun memungkinkan suatu akses yang ilegal terhadap data. Oleh karena itu, keamanan informasi saat pertukaran data perlu diperhatikan untuk menghindari para hacker atau pelaku yang merugikan melalui layanan email, media sosial[1][2]. Berbagai pihak yang tidak berkepentingan tersebut menyalahgunakan teknologi untuk mencuri data yang dapat menimbulkan kerugian bagi pemilik data[3][4][5][6]. Menghadapi ancaman keamanan tersebut, diperlukanlah teknik keamanan untuk menjaga kerahasiaan pesan menggunakan Algoritma kriptografi[1]. Algoritma kriptografi terbagi menjadi algoritma simetri, asimetri dan *hybrid*.

Algortima simetri terdapat kelebihan diantaranya proses enkripsi lebih ringan, sedangkan algoritma asimetri saat pengenkripsiannya lebih lambat. Tetapi algoritma simetri lemah dalam penyebaran kunci, namun algoritma asimeri unggul dalam penyebaran kunci. Algoritma simetri terdiri dari *Caesar Ciphertext*, *Vigenere Cipher, Hill Cipher*, IDEA, AES, dan sebagainya. Algoritma asimetri terdiri dari *Rivest-Shamir-Adleman* (RSA), *ElGamal, McEliece*, LUC dan DSA (*Digital Signature Algorith*) [7]

Menutupi kelemahan masing-masing algoritma, maka digunakanlah Algoritma *hybrid*. Algoritma *hybrid* merupakan cara memperkuat keamanan jadi lebih aman dengan menggabungkan berbagai algoritma [8]. Namun, algoritma kriptografi memiliki kelemahan yang mampu membuat curiga pihak lain dengan dokumen yang susah baca atau tidak berarti, karena dokumen tersebut telah mengalami perubahan karakter acak bisa berupa simbol dan lainnya, yang membuat dokumen tersebut memiliki informasi yang berarti [9]. Selain menggunakan kriptografi untuk mengamankan data, terdapat algoritma steganografi.

Steganografi adalah cara supaya pesan dapat disembunyikan ke dalam pesan atau data lain, sehingga pesan tersebut tidak diketahui oleh orang lain[2][10]. Metode *Least Significant Bit*(LSB) ialah metode steganografi yang sering digunakan. Metode ini memiliki kelebihan pada proses penyembunyian dan pengungkapan yang cepat daripada metode yang lain. Metode ini mengganti nilai *byte* yang sedikit tidak signifikan menjadi lebih tinggi atau lebih rendah[11].

Berdasarkan penjabaran tersebut maka penelitian ini akan menerapkan algoritma *hybrid* dengan menggabungkan metode LSB yang diharapkan mampu mengamankan data atau informasi.

II. PENELITIAN YANG TERKAIT

Penelitian ini, peneliti menggunakan penelitian terdahulu sebagai acuan untuk menyelesaikannya. Adapun penelitian terdahulu yang digunakan yaitu penelitian yang dilakukan oleh Mara Husein. Permasalahan dalam penelitian tersebut, yaitu bagaimana menyisipan pesan teks kedalam suatu citra

*) **penulis korespondensi**: Ibnu Sulistyo
Email: ibnusulistyo16@gmail.com

gambar dengan menggunakan metode *Caesar Cipher* dan *Least Significant Bit*(LSB). Hasil penelitian tersebut ialah sebuah sistem yang digunakan untuk mengamankan dan menyembunyikan pesan teks kedalam suatu *file* gambar berformat *.bmp, *.jpg, dan * .tiff sehingga tidak akan muncul kecurigaan pihak lain sehingga kerahasiaan pesan terjaga yang berjalan di *platform desktop* [3].

Penelitian selanjutnya tentang perancangan aplikasi steganografi dengan teknik *Least Significant Bit*(LSB) dan algoritma RC4 dan *base64 encoding* yang dilakukan Soleh dan kawan-kawan. Permasalahan yang diangkat dalam penelitian tersebut adalah banyaknya ancaman serangan kejahatan dunia maya terhadap transaksi data seperti layanan email, peer to peer maupun lainnya. Hasil penelitiannya berupa sebuah aplikasi mobile yang digunakan untuk pengamanan data. Metode yang digunakan ialah algoritma kriptografi RC4 dan *Base64 Encoding* yang menjadikan pesan rahasia terlihat acak, kemudian dilakukan penyisipan menggunakan metode *Least Significant Bit*(LSB).[2]

Penelitian lain yang dilakukan oleh Rahimah tentang penyembunyian dan penyandian pesan di citra. Penelitian ini menghasilkan sebuah sistem untuk melakukan penyembunyian dan penyandian pesan di citra yang menggunakan algoritma *Affine Cipher* dan metode LSB yang berjalan di *platform desktop*. *File* citra yang digunakan sebagai media penyembunyian pesan berformat *.bmp, *.png dan *.gif dengan ukuran maksimal 400 x400 piksel[5].

Penelitian selanjutnya dilakukan oleh Alim Muadzani, dan kawan-kawan tentang penyisipan suatu data berupa teks maupun citra digital pesan ke dalam citra digital pembawa. Penelitian ini menghasilkan sistem penyisipan data, berupa teks maupun citra digital pesan ke dalam media citra pembawa menggunakan metode Least Significant Bit(LSB). Media citra digital yang digunakan berformat *.png[4].

Selain itu, Kemal Ade Sekarwati dan Ariep Budiman(2017) melakukan penelitian tentang keamanan *file* dan dokumen. Penelitian ini menggunakan algoritma *Rivest-Shamir Adleman*(RSA) dan metode *Least Significant Bit*(LSB). *File* dokumen yang digunakan berformat *.txt, dan *.doc. Sedangkan media citra yang digunakan dengan format *.bmp, *.jpg dan *.png. Sistem ini berjalan di *platform desktop*[9].

Berbeda dengan penelitian-penelitian sebelumnya, penelitian yang akan dilakukan menggunakan algoritma *hybrid* dan metode *Least Significant Bit*(LSB) untuk mengamankan data. Pengamanan data dilakukan dengan mengenkripsikan data terlebih dahulu dengan algoritma hybrid yaitu algoritma *Caesar Ciphertext* dan *Rivest-Shamir Adleman*(RSA) , kemudian hasil enkripsi akan disisipkan ke dalam citra digital dengan metode *Least Significant Bit*(LSB) sehingga data rahasia tidak diketahui oleh pihak yang tidak berkepentingan dan keamanan data tetap terjaga sampai di tangan penerima. Data yang digunakan berupa data text atau pesan, sedangkan citra digital yang digunakan sebagai media penyisipan berupa gambar berformat *.png, dan *.jpg.

III. METODE PENELITIAN

Subjek penelitian ini adalah bagaimana mengimplementasikan metode *Least Significant Bit*(LSB) dan algoritma *hybrid* untuk keamanan data dengan menyisipkan data yang telah dienkripsikan ke dalam citra digital berformat JPEG dan PNG.

Pengumpulan data digunakan sebagai landasan penyelesaian masalah. Adapun metode pengumpulan data yang digunakan yaitu metode kepustakaan atau studi litelatur.

Adapun tahapan-tahapan implemntasi algoritma *hybrid* dan metode *least significant bit* menjadi sistem ialah melakukan analisis kebutuhan, perancangan *flowchart*, implementasi dan pengujian .

Tahapan pengujian menggunakan beberapa cara yaitu melakukan pengujian sistem terhadap proses enkripsi penyembunyian, pengungkapan dan dekripsi. Kemudian, melakukan pengujian histogram

IV. HASIL DAN PEMBAHASAN

A. Analisi Kebutuhan

Tahapan ini Berdasarkan hasil pengumpulan data maka diketahui bahwa kebutuhan sistem dapat dideskripsikan sebagai berikut.

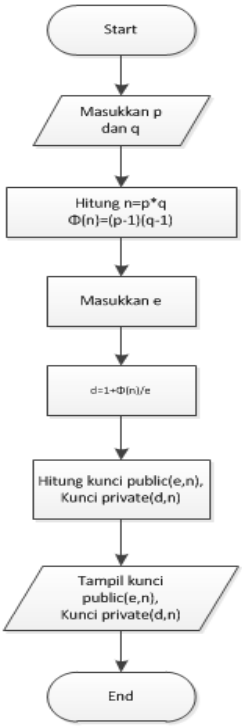
- Sistem dapat melakukan proses pembuatan kunci RSA (*Rivest Shamir Adleman*).
- Sistem dapat melakukan proses enkripsi, dekripsi, penyembunyian, dan pengungkapan
- Sistem dapat menampilkan perbedaan hasil *file* gambar yang belum dan sesudah dilakukan proses penyembunyian

B. Perancangan

Perancangan yang dilakukan ialah merancang alur kerja(*flowchart*) algoritma *hybrid* dan metode L*east Significant Bit(*LSB*)* saat melakukan pembuatan kunci, pengenkripsian data teks, penyembunyian data teks, pengungkapan dan pendekripsian..

1. *Flowchart* Pembuatan Kunci

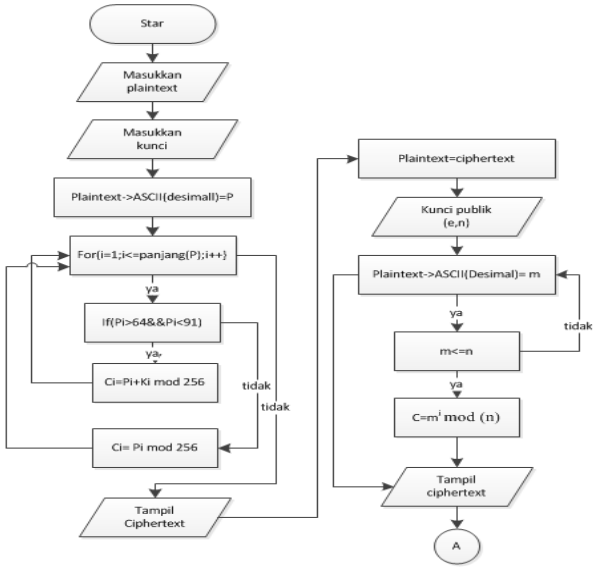
Flowchart pembuatan kunci merupakan alur pembuatan kunci RSA yang digunakan saat melakukan pengenkripsian dan pendekripsian algoritma RSA, kunci RSA terdiri dari kunci private dan kunci public. Adapun flowchart pembuatan kunci ditunjukkan dalam Gbr 1.



Gbr 1. *Flowchart* pembuatan kunci

2. Flowchart Enkripsi

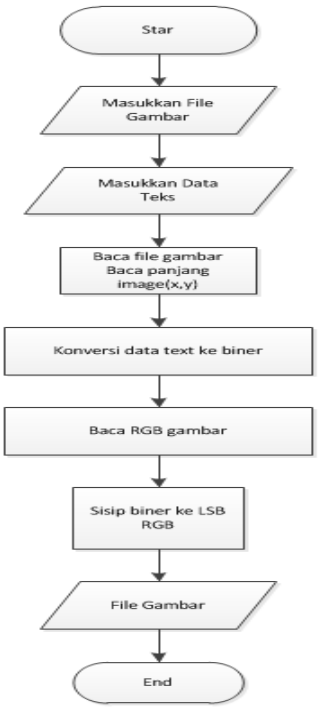
Flowchart enkripsi ini ialah alur kerja algoritma hybrid yang merupakan gabungan algoritma kriptograifi *caesar ciphertext* dengan RSA (*Rivest Shamir Adleman*). *Flowchart* enkripsi ditunjukkan dalam Gbr 2.



Gbr 2. *Flowchart* Enkripsi

3. Flowchart Penyembunyian

Flowchart penyembunyian merupakan alur penyisipan data teks ke dalam file gambar menggunakan metode *Least Significant Bit(*LSB*)*. Adapun alur penyembunyian ditunjukkan dalam Gbr 3.



Gbr 3. *Flowchart* Penyembunyian

C. Implementasi

1. Halaman Menu Kunci

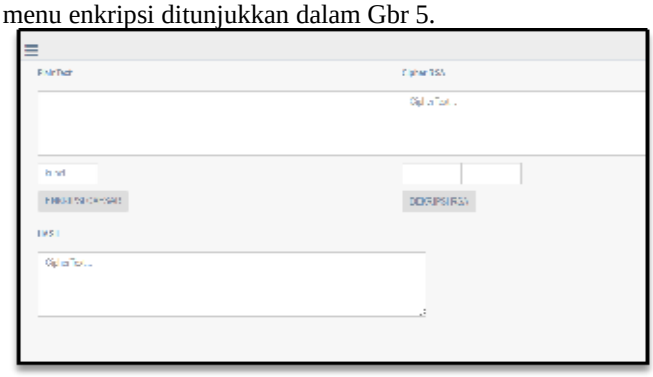
Halaman menu kunci merupakan halaman pembuatan kunci RSA yang digunakan dalam proses pengenkripsian maupun pendekripsian data teks. Halaman ini memerlukan proses inputan nilai p dan q, yang mana nilai p dan q berupa bilangan prima. Adapun tampilan menu kunci ditunjutkkan dalam Gbr 4.

Gbr 4. Halaman menu kunci

2. Halaman Menu Enkripsi

Halaman menu enkripsi merupakan halaman penyandian atau pengenkripsian data teks menjadi data yang tidak berarti berupa bilangan acak. Pengenkrisian ini menggunakan algoritma *caecar ciphertext* dan algoritma RSA beserta

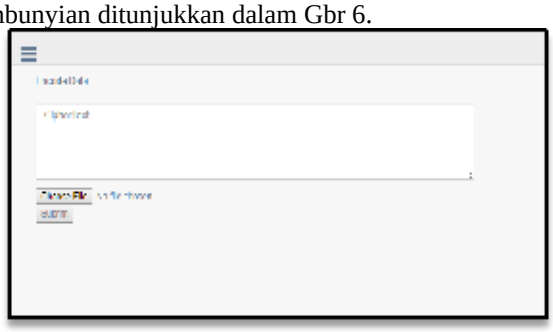
hasilnya dilakukan pengkodean *base64*. Adapun tampilan menu enkripsi ditunjukkan dalam Gbr 5.



Gbr 5. Halaman menu enkripsi

3. Halaman menu penyembunyian

Halaman menu penyembunyian digunakan untuk menyembunyikan data teks ke dalam *file* gambar sehingga tidak dapat diketahui secara visual, penyembunyian ini menggukan metode LSB. Adapun tampilan menu penyembunyian ditunjukkan dalam Gbr 6.



Gbr 6. Halaman menu penyembunyian

D. Pengujian

1. Pengujian Sistem

TABEL I
MEDIA PENYIMPAN

No	Nama *File*	Ukuran *File*	Tipe	Gambar
1.	Australia. jpg	768x512 (470,8KB)	*Jpeg*	
2.	Nature. jpeg	1280x720 (214,5KB)	*Jpeg*	
3.	Sonic.png	1200x675 (715,1KB)	PNG	
4.	Monalisa. png	2403x3591 (9,2 MB)	PNG	

Pengujian dilakukan dengan memanfaatkan beberapa *file* gambar sebagai media penyimpan teks yang akan disimpan. *File* gambar yang digunakan berupa PNG dan JPEG. Adapun *file* gambarnya yang digunakan untuk media penyimpan ditunjukkan dalam Tabel I.

TABEL II
DATA TEKS

No	Jumlah Karakter
1	200
2	5000

Seperti yang ditunjukkan Tabel II, tabel tersebut merupakan jumlah karakter data teks yang akan digunakan dalam pengujian sistem. Tabel I dan Tabel II digunakan untuk pengujian terhadap kemampuan sistem dalam melakukan pengenkripsian, penyembunyian, pengungkapan dan pendekripsian terhadap data yang banyak

TABEL IIII
HASIL PENGUJIAN PENYEMBUNYIAN

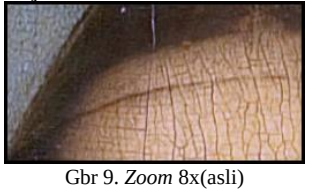
No	Media Penyimpan	Data Teks	Status Pengujian	Keluaran
1.	1	1	Berhasil	Australia.png
2.	1	2	Berhasil	Australia(1).png
3.	2	1	Berhasil	Nature.png
4.	2	2	Berhasil	Nature(1).png
5.	3	1	Berhasil	Sonic.png
6.	3	2	Berhasil	Sonic(1).png
7.	4	1	Berhasil	Monalisa.png
8.	4	2	Berhasil	Monalisa(1).png

Tabel III menunjukkan pengujian penyembunyian sebanyak 8 percobaan yang dilakukan dengan tingkat persentase keberhasilan 100%. Data teks berhasil disisipkan ke dalam *file* gambar dengan syarat data teks tidak melebihi batas penyisipan karakter di media penyimpan. Perbandingan tampilan antara *file* gambar sebelum penyisipan dan sesudah penyisipan ditunjukkan dalam Gbr 7 dan Gbr 8.

Gbr 7. Monalisa(asli)

Gbr 8. Monalisa(hasil penyisipan)

Secara visual, gambar tersebut tidak memiliki perbedaan. Apabila gambar tersebut diperbesar sampai 8x di area yang sama maka hasilnya masih sulit dikenali secara visual, seperti ditunjukkan dalam Gbr 9 dan Gbr 10.



Gbr 9. *Zoom* 8x(asli)

Gbr 10. *Zoom* 8x(hasil penyisipan)

Namun, kedua gambar tersebut memiliki perbedaan nilai piksel. Perbedaan tersebut ditunjukkan dalam Gbr 11 dan Gbr 12.

R	G	B
42	29	30
30	24	21
30	31	30
37	33	35
28	20	17
39	32	31
46	39	40
39	33	30
54	47	50
38	30	28
71	68	78
49	44	47
62	61	70
49	48	51

Gbr 11. Nilai RGB(asli)

R	G	B
42	29	30
30	25	21
31	31	30
37	32	34
28	21	16
38	32	31
46	39	40
38	32	31
54	47	51
39	31	28
71	68	78
49	44	46
63	61	70
49	48	51

Gbr 12. Nilai RGB(hasil penyisipan)

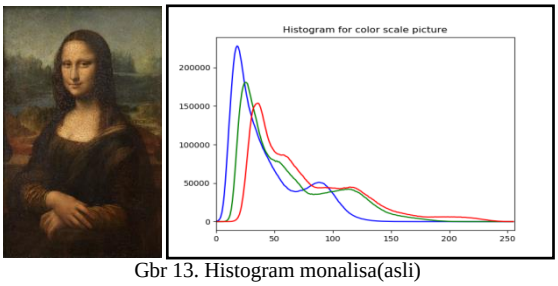
Perbedaan tersebut berupa perubahan nilai komponen warna sedikit tidak signifikan karena perubahan nilai tidak lebih ±1. Itu dikarenakan perubahan yang terjadi hanya bit terakhir LSB. Sedangkan dari segi ukuran *file*, *file* gambar sebelum disisipi dan setelah disisipi akan mengalami perubahan ukuran, ini ditunjukkan dalam Tabel IV.

TABEL IV
PERBANDINGAN FILE GAMBAR

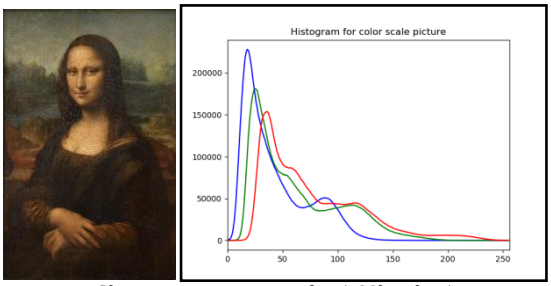
No	Media Penyimpan	Data Teks	Ukuran *File* Gambar	Ukuran *File Stegano*
1.	1	1	768x512 (470,8KB)	768x512 (743,7KB)
2.	1	2	768x512 (470,8KB)	768x512 (773,3KB)
3.	2	1	1280x720 (214,5KB)	1280x720 (1,5MB)
4.	2	2	1280x720 (214,5KB)	1280x720 (1,5MB)
5.	3	1	1200x675 (715,1KB)	1200x675 (624,7KB)
6.	3	2	1200x675 (715,1KB)	1200x675 (651KB)
7.	4	1	2403x3591 (9,2MB)	2403x3591 (9,6MB)
8.	4	2	2403x3591 (9,2MB)	2403x3591 (9,6MB)

2. Histogram

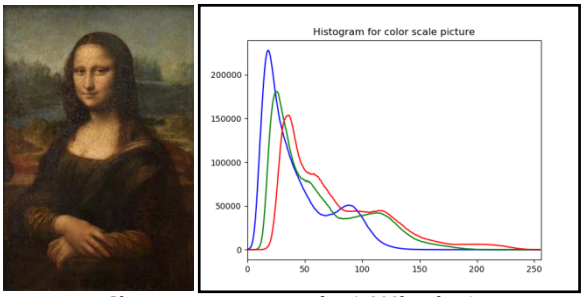
Pengujian histogram dilakukan dengan menggunakan *opencv*. Tujuan dilakukan untuk melihat perubahan dan perbedaan frekuensi warna *file* gambar sebelum disisipi dan sesudah disisipi. Pengujian histogram dilakukan terhadap tiga *file* gambar yaitu *file* gambar asli, gambar yang disisipi 200 karakter dan gambar yang disisipi 5000 karakter. Histogram *file* gambar asli ditunjukkan dalam Gbr 13, *file* gambar yang telah disisipi 200 karakter ditunjukkan dalam Gbr 14, sedangkan *file* gambar yang telah disisipi 5000 karakter ditunjukkan dalam Gbr 15. Berdasarkan hasil histogram, setiap gambarnya menunjukan tingkat kontras cahaya histogram yang *underexposed*(gelap)



Gbr 13. Histogram monalisa(asli)



Gbr 14. Histogram Monalisa(200karakter)

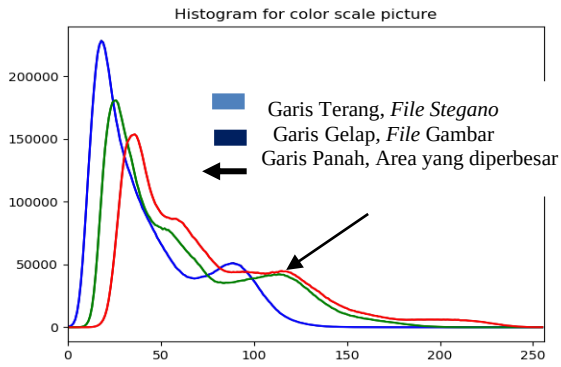


Gbr 15. Histogram Monalisa(5000karakter)

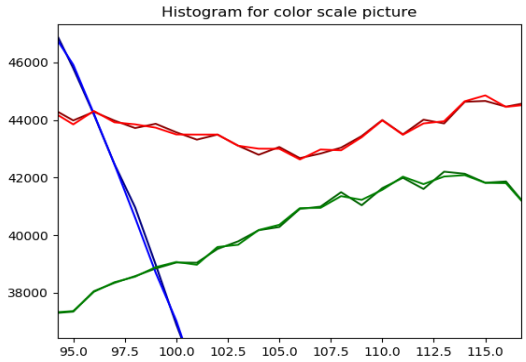
Perbandingan hasil histogram *file* gambar asli dengan *file* yang telah disisipkan data teks antara lain:

a) Perbandingan histogram(200 karakter)

Berdasarkan Gbr 13, *file* gambar asli dengan *file* gambar yang disisipi 200 karakter tidak terlihat ada perbedaan. Jika histigram tersebut diperbesar, maka hasilnya seperti ditunjukkan dalam Gbr 14 yang menunjukkan bahwa ada perbedaan namun sedikit tidak signifikan.

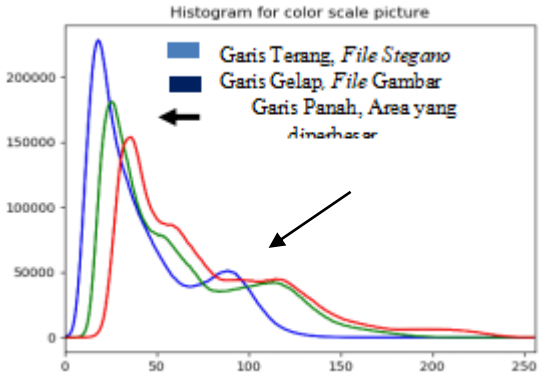


Gbr 13. Perbandingan histogram 200 karakter

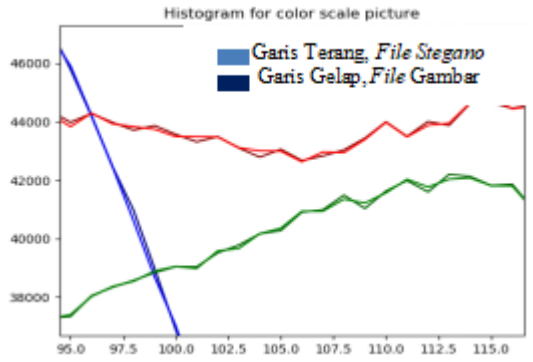


Gbr 14. Perbandingan Histogram 200 karakter(Diperbesar)

b) Perbandingan histogram(5000 karakter)



Gbr 15. Perbandingan histogram 5000 karakter



Gbr 16. Perbandingan histogram 5000 karakter(diperbesar)

Perbandingan dengan gambar yang disisipi 5000 karakter juga tidak terlihat perbedaan, hal ini ditunjukkan dalam Gbr 15. Jika histogram perbandingan *file* gambar asli dengan file gambar yangelah disisipi 5000 karakter diperbesar, perbedaan grafik dapat dilihat namun tidak terlalu signifikan, seperti ditunjukkan dalam Gbr 16.

V. KESIMPULAN

Model kombinasi dalam algoritma *hybrid* antara *Caecar Ciphertext* dan *Rivest Shamir Adleman* (RSA) dapat digunakan untuk meningkatkan kemananan karena dilakukan pengamanan 2 lapis dengan menggunakan kunci yang berbeda yaitu *private* dan *public*. Selain itu, hasil enkripsi yang berupa *ciphertext* akan disembunyikan ke dalam suatu *file* gambar berformat PNG dan JPEG/JPG. Serta berdasarkan hasil uji histogram, metode *least significant bit* yang melakukan penyisipkan satu bit pesan (bernilai 0 atau 1) di satu komponen warna menunjukkan kualitas citra tidak mengalami perubah yang berarti.

Adapun saran kedepannya ialah perlu adanya penambahan jenis file digital lainnya yang digunakan sebagai media penyimpan atau sebagai file yang akan disisipkan ke file digital lainnya, melakukan pengujian sebuah file berukuran yang lebih besar atau file yang banyak, atau mempertimbangkan faktor keamanan data dengan melakukan *cryptanalysis* dan *steganalysis* secara lebih pasti.

DAFTAR PUSTAKA

[1] M.H.Arif, and A.Z.Fanani, "Kriptografi Hill Cipher dan Least Significant Bit untuk Keamanan Pesan pada Citra," *Computer Science Research and Its Development Journal(CSRID)*, vol. 8, no. 1, pp. 60-72, 2016.

[2] Soleh, F. Alfiah, and B. Yusuf, "Perancangan Aplikasi Steganografi Dengan Teknik LSB dan AlgoritmaRC4 & Base64 Encoding," *Technomedia Journal (TMJ)*, vol.3, no.1, 2018.

[3] M. Husein, "Implementasi Caesar Cipher untuk Penyembunyian Pesan Text Rahasia Pada Citra dengan Menggunakan Metode Least Significant Bit," *Pelita Informatika Budi Darma*, vol.VII, no.2, 2014.

[4] A. Muadzani, O.D. Nurhayati, and I.P. Windasari, "Penyisipan Media Teks dan Citra Menggunkan Teknik Stganografi pada Media Pembawa Citra Digital," *Jurnal Teknologi dan Sistem Komputer*, vol.4, no.3, 2016.

[5] Rahimah, "Implementasi Penyembunyian dan Penyandian Pesan Pada Citra Menggunakan Algoritma Affine Cipher dan Metode Least Significant Bit," *Pelita Informatika Budi Darma*, vol.VI, no.1, 2014.

[6] M. Yunus, and A. Harjoko, "Penyembunyian Data pada File Video Menggunakan Metode LSB dan DCT," *IJCCS*, vol.8, no.1, 2014

[7] H.A.Siregar, "Implementasi Metode Hybrid Cryptosystem untuk Pengamanan Transminsi Data Pajak Studi Kasus Pajak RSUD Bangkinang," UIN SUSKA RIAU, 2014

ISSN: 2477-5126
e-ISSN: 2548-9356

[8] M. Jain, and A. Agrawal, "Implementation of hybrid cryptography algorithm," *International Journal Of Core Engineering & Management(IJCEM),* vol.1, no.3, 2014
[9] K.A. Sekarwati, and A. Budiman, "Implementasi Algoritma Rivest-Shamir-Adleman (RSA) dan Metode Least Significant Bit(LSB) Untuk Keamanan File Teks dan Dokumen Menggunakan Visual C#," *Jurnal Teknologi Rekayasa,* vol.22, no.1, 2017
[10] A. Arief and R. Saputra, "Implementasi Kriptografi Kunci Publik dengan Algoritma RSA-CRT pada Aplikasi Instant Messaging", *Scientific Journal of Informatics,* vol. 3, no. 1, pp. 46-54. 2016
[11] R.S. Basuki, and E.N. Maranggi, "Embedding Pesan Rahasia Dengan Metode LSB," *in Seminar Nasional Teknologi Informasi & Komunikasi Terapan 2011 (Semantik 2011),* 2011