pISSN: 2442-3386 eISSN: 2442-4293
Vol 6 No 1 Januari 2020, 33 - 40
Melek IT
INFORMATION TECHNOLOGY JOURNAL

STEGANOGRAFI LSB DENGAN MODIFIKASI KRIPTOGRAFI: CAESAR, VIGENERE, HILL CIPHER DAN PLAYFAIR PADA IMAGE

Arvin Claudy Frobenius[1], Eko Rachmat Hidayat S. H. S [2]
[1] Universitas Amikom Yogyakarta, arvinclaudy@amikom.ac.id
[2]Universitas Amikom Yogyakarta, erachmat@amikom.ac.id

Abstrak

Pada era modern ini, teknologi informasi berkembang dan menjadi salah satu media yang bertujuan membentuk sistem dengan cara pengelolahan, pengumpulan, penyimpanan, sampai pengiriman. Keamanan informasi harus diperhatikan, dikarenakan terdapat kejahatan dimana oleh banyak pihak yang ingin mengakses informasi dan menyalagunakan informasi yang bukan pemiliknya. Oleh karena itu, diperlukan teknologi informasi dan pengamanan informasi untuk memiliki informasi bersifat pribadi. Penggabungan teknik kriptografi dan steganografi dapat digunakan untuk pengamanan informasi. Teknik kriptografi menggabungkan empat metode yaitu Caesar cipher, vigenere, hill cipher, dan playfair. Pada teknik steganografi LSB (least Significant Bit) untuk menyisipkan informasi berupa teks didalam gambar. Metode pengujian dilakukan dengan menggunakan beberapa cara yaitu kapasitas penyisipan, histogram, pemotongan gambar dan pengubahan ekstensi. Hasilnya menunjukan bahwa penyisipan data yang terdapat pada gambar mengalami penambahan ukuran file yaitu menggunakan 17 karekter menghasilkan nilai 192 KB dan 13 karakter menadapatkan nilai 170 KB. Selain itu, hasil pada pengujian histogram juga mengalami perbedaan yaitu pada nilai mean pada file gambar enkripsi mengalami peningkatan 220.87. Pada pengukian selanjutnya adalah standard deviation yang mengalami penurunan pada file gambar enkripsi yaitu dengan nilai 72.35 dari nilai 72.45.
Kata Kunci: Caesar Cipher, Vigenere, Hill Cipher, Playfair, SLB (Least Significant Bit).

Abstract

In this modern era, information technology is developing and becoming one of the media that aims to form a system by way of management, collection, storage, until delivery. Information security must be considered, because there is a crime by many parties who want to access information and misuse information that is not the owner. Therefore, information technology and information security are needed to have personal information. The combination of cryptography and steganography techniques can be used for information security. Cryptography techniques combine four methods such as caesar cipher, vigenere, hill cipher, and playfair. In the LSB steganography technique (least Significant Bit) to insert information in the form of text in the image. The testing method is done by using several methods namely insertion capacity, histogram, cropping and changing the extension. The results show that the insertion of data contained in the image has increased file size using 17 characters producing a value of 192 KB and 13 characters getting a value of 170 KB. In addition, the results of the histogram test also experienced a difference, namely the mean value of the encrypted image file increased by 220.87. In the next test, the standard deviation has decreased in the encrypted image file with a value of 72.35 from a value of 72.45
Keywords: Caesar Cipher, Vigenere, Hill Cipher, Playfair, SLB (Least Significant Bit)

PENDAHULUAN

Pada masa lalu pos adalah media konvensional satu-satunya yang digunakan untuk mengirimkan suatu barang. Selain itu, pos juga berfungsi sebagai tempat untuk pengiriman dan pertukaran informasi seperti surat-menyurat. Adapun selain pos yaitu agen rahasia yang digunakan institusi khusus untuk menjadi pengirim rahasia. tetapi yang membedakan adalah informasi yang dibawa. Seorang agen harus mengirimkan pesan yang bersifat rahasia kepada penerima langsung dan tidak boleh ada pembocoran informasi. Menjadi pengirim baik pada kantor pos ataupun agen rahasia, mereka harus menjaga rahasia sebuah informasi yang akan dikirim. Tetapi pada pengiriman baik menggunakan pos ataupun agen juga harus memerlukan waktu berhari-hari untuk pesan tersebut sampai pada tujuan penerima. Selain itu, terdapat resiko akan informasi tidak sampai pada penerima secara langsung.

Pada era modern ini, teknologi informasi berkembang dan menjadi salah satu media yang bertujuan membentuk sistem dengan cara

pengelolahan, pengumpulan, penyimpanan, sampai pengiriman. Bertambah Kemajuan teknologi informasi yang pesat membuat permasalahan baru lagi yaitu tentang keamanan informasi. Keamanan data merupakan cara melindungi informasi dari ancaman baik sengaja maupun tidak disengaja. Informasi dapat berupa dokumen, gambar, email, audio, pesan teks dan lainnya. Permasalahan keamanan informasi harus diprioritaskan dalam membangun sebuah sistem sistem informasi, ini dikarenakan terdapat kejahatan dimana oleh banyak pihak yang ingin mengakses informasi dan menyalagunakan informasi yang bukan kepemilikannya. Oleh karena itu, diperlukan teknologi informasi dan pengamanan informasi yang berfungsi untuk memiliki data informasi bersifat pribadi, dimana pengirim dan penerima yang hanya mengetahui isi informasi tanpa menimbulkan rasa curiga oleh orang lain.
Pada penelitian [1] menggunakan metode Hill Cipher dan Least Significant Bit (LSB) untuk mengenkripsi pesan yang dimasukan dalam gambar dan mengembalikan kembali pada pesan original. Pada hasil metode yang disampaikan selanjutnya diimplementasikan dengan mebuat sebuah website. Penelitian yang dilakukan [2] menggunakan metode vigenere cipher dan metode LSB yang digunakan untuk menyisipkan pesan yang sudah terenkripsi dengan vigenere kemudian disisipkan kedalam gambar, tetapi kata yang disediakan untuk kata tidak terlalu banyak dan tidak dapat menggunakan spasi.

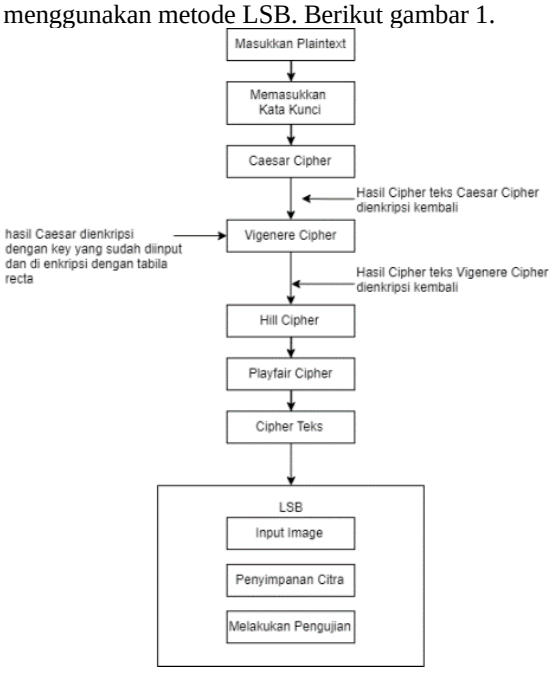
Pada penelitian selanjutnya pada [3] menggunakan metode playfair chipper untuk penyembunyian teks terenkripsi pada citra dengan metode end of file dengan menggunakan pengacakan matrik 7x5 terdiri dari 25 huruf capital alphabet dan 10 angka. Pengujian yang dilakukan adalah membandingan nilai pixel yang menghasilkan tidak terdapat perubahan. Pengujian selanjutnya menggunakan brightness dan darkness yang menghasilkan terdapat pengurangan nilai brightness dan darkness. Selanjutnya pengujuan menggunakan MSE dan PSNR dengan gambar asli dan embedding menghasilkan nilai MSE odB dan PSNR 99dB.

Pada latar belakang yang disampaikan, penelitian melakukan penggunaan metode teknik subtitusi yaitu mengombinasikan empat teknik yaitu caesar, vigenere, hill cipher, dan playfair. Selain itu, mengkombinasikan teknik subtitusi dengan menggunakan teknik steganografi dengan metode LSB (*least significant bit*) berbasis *mobile* untuk memberikan proteksi ganda pada pesan rahasia.

I. METODE

2.1 Tahapan Penelitian

Dalam tahapan penelitian pengembangan kriptografi yang melibatkan empat algoritma (Caesar, vigenere, hill dan playfair) yang dikombinasi LSB. Pada proses enkripsi plaintext akan dieksekusi dengan pertama yaitu Caesar, vigenere, hill, dan playfair dengan kata kunci yang diinputkan. Kata kunci ini akan digunakan sebagai kunci di setiap enkripsi. Selanjutnya terdapat proses memasukan chipper teks kedalam citra menggunakan metode LSB. Berikut gambar 1.



Gambar 1. Tahapan Penelitian

2.2 Kriptografi

Kriptografi adalah sebuah ilmu atau seni dimana digunakan untuk menjaga keamanan sebuah pesan ketika pesan dikirim dari pengirim ke penerima. Dalam bahasa Yunani, kriptografi memiliki arti dimana berasal dari kata *crypto* berarti *secret* (rahasia) dan *graphia* berarti *writing* (menulis). Algoritma pada kriptografi memiliki tiga fungsi dasar yaitu [4]:

- Enkripsi: merupakan pengaman data yang akan dikirim tetap terjaga kerahasiaannya. Istilah *plaintext* adalah pesan asli, sedangkan enkripsi dapat disebut dengan cipher atau kode.
- Deskripsi: merupakan kebalikan dari enkripsi. Dimana sebuah pesan yang telah dienkripsi dikembalikan ke bentuk awalnya. Algoritma enksripsi berbeda dengan algoritma yang digunakan untuk deskripsi.
- Kunci: merupakan yang dipakai untuk melakukan enkripsi dan deskripsi. Kunci dibagi menjadi dua yaitu kunci rahasia dan kunci umum.

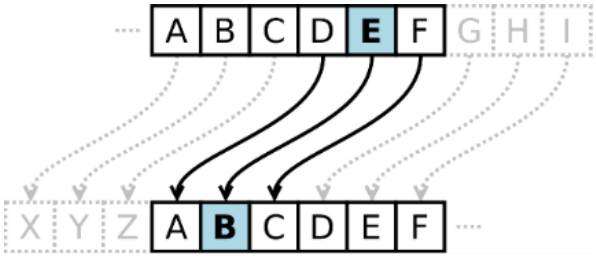
pISSN: 2442-3386 eISSN: 2442-4293
Vol 6 No 1 Januari 2020, 35 - 40
Melek IT
INFORMATION TECHNOLOGY JOURNAL

Kriptografi memiliki dua macam jenis yaitu kriptografi klasik dan kriptografi modern. Berikut penjelasannya [4]:

- Kriptografi klasik merupakan sebuah algoritma yang menggunakan satu kunci untuk sebagai pengaman dari sebuah data. Pada kriptografi klasik terdapat dua teknik dasar algoritma yaitu teknik subtitusi dan teknik transposisi.
- Kriptografi Modern merupakan sebuah algoritma yang memiliki kerumitan komplek dimana algoritma ini dioperasikan menggunakan komputer.

2.3 Caesar Cipher

Caesar cipher merupakan enkripsi yang sering digunakan karena sederhana untuk digunakan. Teknik caesar ini termasuk algoritma kriptografi klasik dengan teknik subtitusi. Teknik ini dapat dilakukan dengan cara melakukan aturan pergeseran kunci kekanan atau kekiri sesuai yang ditentukan. Teknik pada enkripsi caesar cipher teradapat pada Gambar 2



Gambar 2. Teknik Caesar Cipher

Berikut contoh dalam melakukan enkripsi menggunakan Caesar cipher, sebagai contoh dengan jumlah pergeseran 2.

Plaintext:
ABCDEFGHIJKLMNOPQRSTUVWXYZ

Ciphertext:
CDEFGHIJKLMNOPQRSTUVWXYZAB

Caesar cipher dapat dapat dinyatakan dalam matematis dalam proses enkripsi dan deskripsinya, berikut rumus matematis Caesar cipher

Rumus enkripsi Caesar Cipher dapat dilihat pada persamaan (1).

$$E_n(x) = (x + n)\ mod\ 26 \quad (1)$$

Rumus enkripsi Caesar Cipher dapat dilihat pada persamaan (2).

$$D_n(x) = (x - n)\ mod\ 26 \quad (2)$$

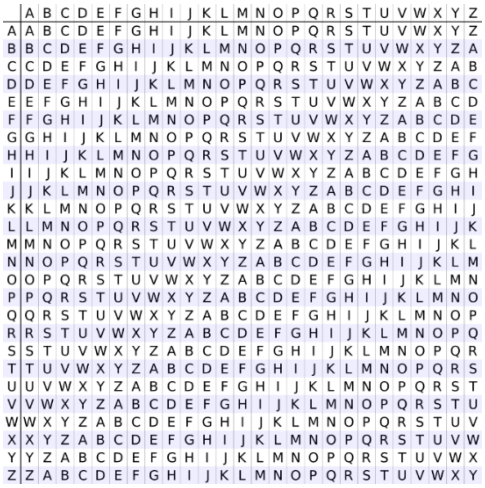
Kelemahan Caesar cipher adalah *brute foce attact* ataupun dapat dipecahkan dengan menggunakan *exhaustive key search*

2.4 Vigenere

Vigenere merupakan bentuk sederhana dari sandi polialfabetik. Kelebihan dari metode vigenere dibanding metode caesar. Metode vigenere tidak memiliki kerentanan terhadap pemecahan sandi yang bisa disebut juga dengan analisis frekuensi [5]. Pada vigenere terbagi menjadi dua teknik subtitusi yaitu angka dan huruf.

- Angka yaitu teknik subtitusi dilakukan dengan menggantikan huruf alphabet dengan angka, proses ini seperti pada metode Caesar.

Huruf merupakan pengembangan dari Caesar cipher, tetapi jumlah pergeseran hurufnya berbeda-bedauntuk setiap periode. Untuk mengenkripsi pesan dengan kode vigenere menggunakan *tabila recta*. Tabila recta digunakan untuk memperoleh teks-kode dengan menggunakan kunci tertentu. Berikut contoh gambar pada teknik huruf dan angka dilihat pada Gambar 3 dan Gambar 4



Gambar 3. teknik Vigenere Pada Huruf.

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

Gambar 4. Teknik Vigenere Pada Angka

2.5 Hill Cipher

Hill cipher merupakan algoritma menggunakan matriks berukuran ordo m x m sebagai kunci dan deskripsi. Dasar teori menggunakan perkalian matrik dalam membuat enkripsi dan

melakukan invers pada matrik untuk melakukan proses deskripsi. berikut matematis perkalian matrik untuk enkripsi dan invers untuk deskripsi.

Rumus Perkalian matrik 2x2 ditunjukan pada persamaan(3)

$$\begin{bmatrix} a & b \\ d & c \end{bmatrix} x \begin{bmatrix} p & q \\ s & r \end{bmatrix} = \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix} \quad (3)$$

Rumus Perkalian matrik 2x2 ditunjukan pada persamaan (4).

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} x \begin{bmatrix} p & q & r \\ s & t & u \\ v & w & x \end{bmatrix} = \begin{bmatrix} ap + bs + cv & aq + bt + cw & ar + bu + cx \\ dp + es + fv & dq + et + fw & dr + eu + fx \\ gp + hs + iv & gq + ht + iw & gr + hu + ix \end{bmatrix} \quad (4)$$

Rumus Invers Matrik untuk Deskripsi ditunjukkan pada persamaan (5)

$$\begin{bmatrix} a & b \\ d & c \end{bmatrix}^{-1} = \frac{1}{ad - bc} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} \quad (5)$$

Hill cipher merupakan polyalphabetic cipher yang dapat dikategorikan sebagai block cipher ini dikarenakan teks akan diproses akan dibagi menjadi block dengan ukuran tertentu. Setiap karakter yang ada dalam sebuah blok dapat saling mempengaruhi karakter lainnya dalam proses enkripsi dan deskripsi. Sehingga, karakter sama tidak dipetakan menjadi karakter yang sama pula [6].

2.6 Kode Playfair

Kode playfair ditemukan oleh Sir Charles dan Baron lyon Playfair pada tahun 1854. Kunci dari cipher playfair menggunakan matriks 5 x 5 (dengan masukan terdiri dari 25 karakter dan membuang J yang ada di dalam alphabet) [4]. Playfair cipher adalah bagian dari sebuah algoritma kriptografi klasik. Metode playfair ini juga masuk didalam polygram chipher, yaitu sebuah plainteks diubah menjadi bentuk poligram dan proses dari enkripsi dan deksripsi dilakukan untuk poligram [7].

2.7 Steganografi

Steganografi (*steganography*) yaitu *steganos* artinya adalah "tersembunyi" dan graphien "menulis" yang di ambil dari Bahasa yunani. Steganografi merupakan seni untuk menyembunyikan pesan di dalam media digital teks, audio, ataupun gambar. Stegnografi memerlukan dua atribut utama, yaitu media penampung (covertext) dan pesan rahasia (hiddentext). Manfaat dari Steganografi juga dapat mengamankan sebuah tanda hak cipta dalam suatu media digital. Teknik ini disebut *Watermarking* [8]. Teknik steganografi dapat dengan mudah deskrisi sebuah pesan. Kinerja dari macam-macam metode steganografi dapat dinilai dari tiga parameter yaitu: keamanan, kapasitas, dan imperceptibility [9].

2.8 LSB Based Image Steganography

Semua file yang terdapat dalam komputer dapat digunakan sebagai media, seperti file gambar berformat jpeg, gif, bmp, atau music dalam format mp3, bahakan video dengan format wav atau avi. Semua media ini dapat dijadikan tempat untuk menyembunyikan sebuah pesan tanpa menghilangi fungsi dan kualitas tidak jauh beda dengan yang aslinya [6].

Sebuah teknik yang popular pada teknik steganografi, LSB (The least Significant Bits) perlindungan data media digital digunakan untuk menyembunyikan sebuah pesan. Paling sederhana teknik LSB adalah LSB replacement. Steganografi LSB replacement membalik bit terakhir pada setiap nilai data untuk mencerminkan pesan yang membutuhkan untuk disembunyikan [1]. Untuk penyembunyian suatu gambar didalam LSB yaitu di setiap byte dari sebuah gambar yaitu 24-bit, dapat menyimpan 3 byte di setiap pixel pada gambar.

2.9 Metode Uji Coba

Pada tahap ini peneliti akan melakukan uji pada gambar untuk ketahanan, keamanan, dan kapasitas. Selain itu, menggunakan testing method untuk mengetahui perbandingan data original dengan data yang sudah mengalami enkripsi. Berikut metode yang akan digunakan oleh peneliti:

- Histogram

Sebuah grafik dimana menunjukan sebuah frekuensi kemunculan setiap nilai gradasi warna. Histogram digunakan untuk menguji kehandalan sebuah gambar. Hasil dari test histogram dapat mengetahui seberapa besar perbandingan histogram pada file gambar asli dengan file gambar yang telah terenkripsi.

- Kapasitas penyisipan

Pada metode ini akan menguji seberapa besar perubahan besar ukuran file pada file gambar antara file gambar original dan file gambar terenkripsi.

pISSN: 2442-3386 eISSN: 2442-4293
Vol 6 No 1 Januari 2020, 37 - 40
Melek IT
INFORMATION TECHNOLOGY JOURNAL

- Pengubahan ekstensi file

Ekstensi file adalah jenis sebuah file yang meliputi nama dan dan nama ekstensi “Namafile.ekstensi”. pada metode ini bertujuan untuk mengetahui ketahanan dan keamanan pada file rahasia dengan merubah-merubah ekstensi file.

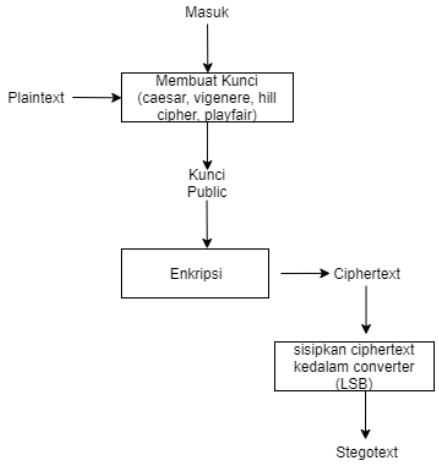
- Pemotongan gambar

Pada metode ini akan melakukan pemotongan pada gambar. tujuan pada metode ini adalah untuk mengetahui width dan length pixel gambar yang tersimpan untuk text enkripsi.

II. HASIL DAN PEMBAHASAN

3.1 Skema Sistem Enkripsi

Pada penelitian ini para peneliti mengembangkan sistem menggunakan aplikasi berbasis mobile. Proses utama pada sistem ini adalah menggabungkan steganografi LSB pada citra digital gambar dengan empat metode kriptografi klasik yaitu Caesar, vigenere, hill cipher dan playfair. Skema proses enskripsi ditunjukkan pada Gambar 5.

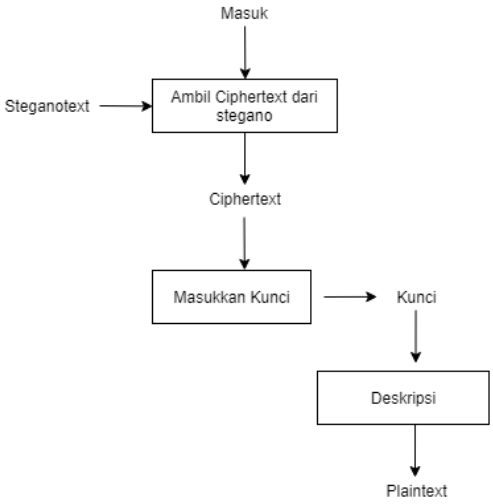


Gambar 5. Skema Proses Enkripsi

Gambar 5 merupakan proses enkripsi pesan, proses ini dilakukan oleh orang yang akan mengirim pesan rahasia. Pada proses enkripsi akan dibuat terlebih dahulu beberapa kunci untuk yang meliputi Caesar, Vigerene, Hill Cipher, dan playfair. Setelah membuat kunci akan melakukan proses menjadi enkripsi dan menghasilkan ciphertext. Ciphertext yang sudah didapatkan disisipkan dalam media berupa file gambar png dengan metode LSB. Hasil dari proses sisip pesan ini adalah file gambar yang sudah berisi pesan rahasia.

3.2 Skema Sistem Deskripsi

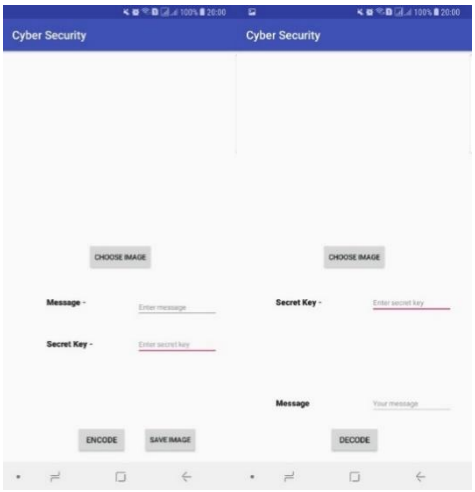
Pada schema system description adalah proses mengembalikan data pesan rahasia menjadi pesan asli. Proses ini dilakukan oleh orang yang menerima pesan rahasia. Langkah Proses description merupakan kebalikan proses encryption yaitu pertama Pesan yang masih berupa ciphertext diambil dari file gambar dengan menggunakan metode LSB, kedua ciphertext harus dideskripsi untuk mendapatkan pesan rahasia. Pada proses ini untuk mendeskripsi harus melakukan proses kebalikan dari proses enksripsi dengan menggunakan kunci. Dengan demikian pesan rahasia yang sebenarnya dapat dibaca, gambar 6.



Gambar 7. Skema Proses Deskripsi

3.3 Tampilan Aplikasi

Pada implementasi penelitian ini peneliti menggunakan aplikasi berbasis mobile. Berikut user interface aplikasi, gambar 7.



Gambar 7. Tampilan Aplikasi

Terdapat dua interface, pertama interface untuk membuat pesan rahasia (ciphertext), dan interface lainnya digunakan untuk mengembalikan pesan rahasia menjadi pesan deskripsi (plaintext).

3.4 Uji Metode

- Penyisipan Kapasitas

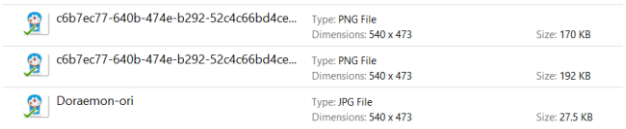
Pada tahap proses pengujian kapasitas penyisipan, dilakukan sebanyak tiga kali untuk mengetahui seberapa besar ukuran kapasitas file gambar. File gambar menggunakan gambar PNG dengan kapasitas file original adalah 27.5 KB dengan ukuran dimensi (pixel) 540 x 473. *File image original* pada Gambar 8.

Gambar 8. File Image Original

Setelah dilakukan proses enkripsi dengan teknik kombinasi kriptografi: Caesar, vigenere, hill dan playfair dan disisipkan pada file gambar menggunakan metode LSB dengan file gambar PNG dihasilkan dengan tiga kali uji coba dengan jumlah karakter berbeda. Hasil ditunjukan pada Tabel 1 dan Gambar 9.

Tabel 1. Hasil pengujian kapasitas penyisipan

Nama	Kata	Karakter	Ukuran (KB)	Dimensi
Ori	0	null	27.5	540x473
Enkrip 1	17	ujianakhirsemester	192	540x473
Enkrip 2	13	Ujiansemester	170	540x473

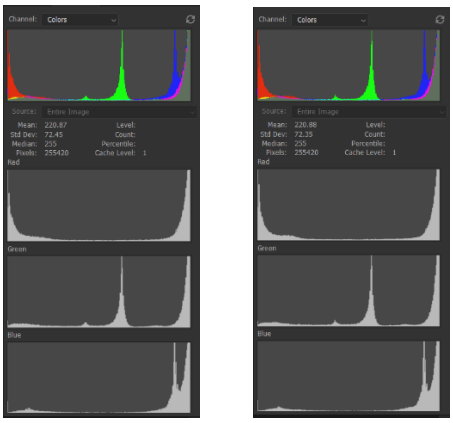


Gambar 9. Hasil Pengujian Kapasitas Penyisipan

Dari hasil ini menunjukan bahwa kapasitas ukuran file mengalami perubahan dari tiga kali uji coba. Pada data pengujian dapat diperhatikan jika semakin besar karakter kata yang dimasukan semakin besar ukuran yang akan disimpan tetapi dengan ukuran dimensi sama seperti original. Seperti data "Enkrip1" dan "Enkrip2" dengan jumlah kata 17 huruf dan 13 huruf menghasilkan ukuran 192 KB dan 170 KB denngan dimensi tetap sama yaitu 540x473.

- Histogram

Dalam pengujian Histogram penelitian ini menggunakan tools dari aplikasi photoshop CC 2018 versi 19.1.6. pengujian dilakukan untuk mengetahui perubahan dan perbedaan frequensi warna pada gambar sebelum disisipi pesan rahasia kecil ataupun besar. Perbandingan histogram dilakukan pada file gambar original dan file gambar yang telah di enkripsi. Hasil dari pengujian histogram pada file gambar PNG ditunjukkan pada Gambar 10



Original Enkripsi 1

Gambar 10. Hasil Pengujian Histogram

Pada tahap hasil pengujian histogram dihasilkan bahwa terdapat perbedaan pada hasil instogram file gambar original dengan file gambar yang terenkripsi. Hasil perbedaan histogram terletak pada bagian standard deviation dan mean. Hasil pengujian menggunakan histogram ditunjukkan pada tabel 2.

Tabel 2. Hasil Histogram

	Original	Enkripsi1
Mean	220.87	220.88
Std Dev	72.45	72.35
Median	255	255
Pixels	255420	255420
Dimensi	540x473	540x473

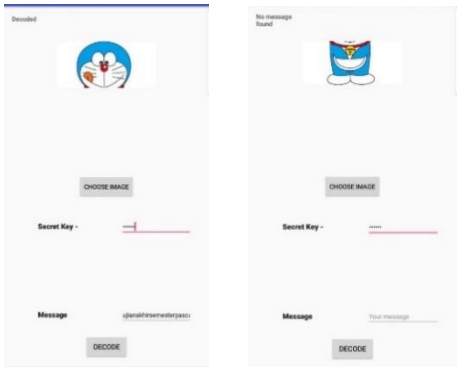
Data menunjukan nilai pada mean antara file gambar original dengan enkripsi1 mengalami perbedaan dengan nilai masih-masing adalah 220.87 dan 220.88, ini mununjukan mengalami peningkatan pada nilai mean. Pada nilai standar deviation file gamabr original memiliki nilai 72.45 dan pada file gambar enkripsi1 memiliki nilai 72.35, ini menunjukan mengalami penurunan pada bagian standard deviation.

- Pemotongan Gambar

Dalam pengujian pemotongan file gamabr pada penelitian ini digunakan untuk mengetahui isi

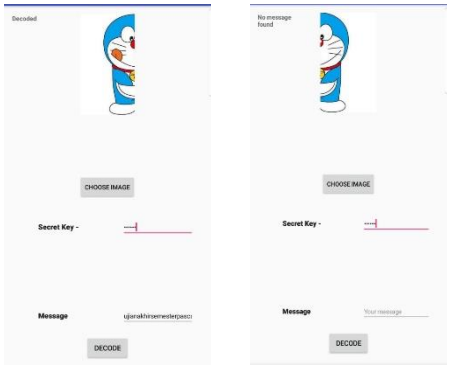
pISSN: 2442-3386 eISSN: 2442-4293
Vol 6 No 1 Januari 2020, 39 - 40
Melek IT
INFORMATION TECHNOLOGY JOURNAL

pesan rahasia yang disisipkan pada gambar mengalami kerusakan atau tidak. Dari hasil pemotongan selanjutnya ingin diketahui letak penyisipan pesan rahasia pada pixel gambar. Pada pengujian pemotongan file gambar dibagi menjadi empat bagian yaitu atas, bawah, kanan dan kiri. Dalam pengujian gambar ini file gambar berformat PNG. Hasil dari uji pemotongan pada gambar 10



Gambar 11. Pemotongan Gambar Bagian Atas dan Bawah

Pada hasil pengujian pemotongan file gambar bagian atas didapatkan hasil bahwa pesan rahasia yang disisipkan pada gambar tidak memiliki kerusakan dan pesan rahasia masih dapat untuk di akses. Selanjutnya, pada pengujian pemotongan file gambar bagian bawah yang sudah mengalami enkripsi. Pada hasil pemotongan gambar file bawah menghasilkan bahwa file mengalami kerusakan yaitu tidak adanya file rahasia yang ditemukan. Pada tahap ketiga dan keempat melakukan pemotongan file gambar bagian kanan dan kiri. Hasil dapat dilihat pada Gambar 12.



Gambar 12. Pemotongan File Gambar Bagian Kanan dan Kiri

Pada hasil pemotongan file gambar kanan dan kiri dihasilkan bahwa pada pemotongan file gambar kiri bagian kiri menunjukan bahwa pesan rahasia tidak mengalami kerusakan dan pada file gambar bagian kanan mengalami kerusakan dan file rahasia tidak ditemukan. Dari hasil uji coba pemotongan file gambar pada beberapa bagian dapat ditemukan letak Sehingga dapat disimpulkan bahwa pesan rahasia dapat ditemukan di posisi mana pesan rahasia disisipkan pada file gambar. Gambar 13 dimana posisi pesan rahasia disisipkan pada pixel gambar.

Gambar 13. Posisi Pesan Rahasia pada Pixel Gambar

- Ekstensi file

Pada pengujian yang dilakukan pada tahap ini adalah perubahan file gambar dari PNG menjadi JPEG. Pada pengujian ini ingin mengetahui apakah terdapat kerusakan pada pesan rahasia pada gambar. Hasil menunjukan bahwa perubahan file ekstensi dari PNG ke JPEG mengalami kerusakan yaitu pesan rahasia tidak ditemukan dan diketahui ukuran kapasitas file dari file gambar yang sudah di enkripsi dan di ubah pada bentuk JPEG mengalami penyusutan dimana hasilnya ditunjukkan pada table 3.

Table 3. Penyusutan File Enkripsi PNG ke JPEG

PNG Original	PNG Enkripsi	JPEG
27.5 KB	192 KB	42.3 KB

III. PENUTUP

4.1. Kesimpulan

Kesimpulan pada penelitian berhasil mengkombinasikan empat metode teknik kriptografi yaitu Caesar, vigenere, hill, playfair dan least significant bit (LSB) berbasis aplikasi *mobile* Android. Aplikasi ini dapat digunakan untuk menyembunyikan pesan yang telah di enkripsi dan disimpan kedalam gambar berformat PNG. Berdasarkan uji coba yang dilakukan menghasilkan bahwa penyisipan data yang terdapat pada gambar mengalami penambahan ukuran file yaitu 192 KB dan 170 KB dengan karakter 17 dan 13 huruf. Sehingga dapat disimpulkan yaitu semakin banyak jumlah karakter huruf yang disisipkan pada gambar, semakin besar pula ukuran file pada gambar. Selain itu, pada hasil uji coba menggunakan histogram mengalami perbedaan yaitu pada nilai mean pada file gambar jpeg enkripsi mengalami peningkatan 220.87. pada pengujian terakhir adalah pada nilai standard deviation mengalami penurunan nilai, yaitu

pada file gambar enkripsi dengan nilai 72.35 dari nilai 72.45.

DAFTAR PUSTAKA

[1] Wamiliana, R. Adrian and E. F. Jayanti, "Implementasi Kriptografi Dan Steganografi Pada Media Gambar Menggunakan Hill Cipher Dan Least Significant Bit (LSB)," *Jurnal Komputasi*, vol. 5, 2017.

[2] S. M. F, "Implementasi Teknik Steganografi Menggunakan Algoritma Vigenere Cipher dan Metode LSB," *Jurnal TICOM* , vol. Vol 4, 2016.

[3] D. P. Donnar, Implementasi Teknik Playfair Cipher untuk Penyembunyian Teks Terenkripsi pada Citra dengan Metode End of File, Jember: Teknik Elektro Universitas Jember, 2018.

[4] D. Ariyus, Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi, Yogyakarta: Penerbit Andi, 2008.

[5] T. Cahyadi, "Implementasi Steganografi LSB Dengan Enkripsi Vigenere Cipher Pada Citra JPEG," *Transient*, no. 1, pp. 281-288, 2012.

[6] I. J. Sari and H. T. Sihotang, "Implementasi Penyembunyian Pesan Pada Citra Digital Dengan Menggabungkan Algoritma HILL Cipher Dan Metode Least Significant BIT (LSB)," *Jurnal Mantik Penusa*, vol. 1, pp. 1-8, 2017.

[7] I. Solihin, Mesran and A. P. U. Siahaan, "Implementasi Algoritma Super Playfair Chiper dan Two Square Cipher Dalam Pengamanan Pesan Teks," *Konferensi Nasional Teknologi Informasi dan Komputer*, vol. 1, no. 1, pp. 195-201, 2017.

[8] E. S. Rusman, "Steganalisis Dalam Pengujuan Citra DIgital Dengan Pengguna Crystalize Dan Histogram Pada Image BMP," Issuu, Tasikmalaya, 2016.

[9] D. Debnath, S. Deb and N. Kar, "An Advanced Image Encryption Standard Providing Dual Security: Encryption Using Hill Cipher & RGB Image Steganography," *International Conference on Computational Intelligence and Networks*, pp. 178-183, 2015.