TEKNIK STEGANOGRAFI MENGGUNAKAN TRANSFORMASI SLANT DENGAN ALGORITMA ENKRIPSI ELGAMAL

I Gusti Agung Bagus S.1[1], Rismon H. Sianipar2[1], I Ketut Wiryajati3[1]

ABSTRAK

Teknik Steganografi merupakan suatu teknik yang membahas bagaimana suatu pesan disisipkan kedalam sebuah berkas media sehingga pihak ketiga tidak menyadari akan adanya pesan tersebut. Dengan memanfaatkan keterbatasan sistem indra manusia seperti mata dan telinga, metode steganografi ini dapat diterapkan pada berbagai media digital. Hasil keluaran dari steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi ini sebatas oleh kemampuan indra manusia, tetapi tidak oleh komputer atau perangkat pengolah digital lainnya.

Untuk memperkuat keamanan pesan yang akan dikirim, teknik steganogafi dapat dikombinasikan dengan berbagai teknik lain seperti kriptografi dan transformasi. Pada penelitian ini digunakan kriptosistem ElGamal sebagai fungsi untuk mengkodekan pesan sebelum dikirim dan Transformasi Slant sebagai fungsi untuk mengacak gambar sebelum disisipan pesan. Pesan rahasia tersebut awalnya dienkripsi dahulu menggunakan algoritma ElGamal kemudian disisipkan pada gambar yang telah ditransformasi menggunakan transformasi Slant. Hasil dari gambar yang telah tersisipi pesan tersebut kemudian dikembalikan lagi menjadi gambar asli, sehingga pesan yang tersisipkan menjadi tidak terlihat (tersembunyi).

***Kata kunci**: Steganografi, Kriptosistem ElGamal, Enkripsi, Dekripsi, Transformasi Slant.*

ABSTRACT

Steganography Techniques is a technique that discusses how a message is inserted into a media file so that the third party was not aware of the message. By exploiting the limitations of the human sensory systems such as the eyes and ears, steganography method is applicable to a variety of digital media. The output of steganography has a same form perseption of the original, but the perception is limited to the ability of the human senses, not by a computer or other digital processing devices.

To strengthen the security of the message, steganography techniques can be combined with other techniques such as cryptography and transformation. In this study, ElGamal cryptosystem used as a function to encode the message before it is sent and Slant Transformation as a function to scramble the image before the inserted message. The secret message was originally encrypted using ElGamal algorithm then pasted the image that has been transformed using a Slant transformation. The results of the images that have been inserted message, returned again to the original image, so the message has been inserted become invisible (hidden).

***Keywords**: Steganography, ElGamal Cryptosystem, Encryption, Decryption, Slant Transformation.*

PENDAHULUAN

Perkembangan teknologi informasi pada saat ini telah berpengaruh pada hampir seluruh aspek kehidupan manusia, tak terkecuali dalam hal berkomunikasi. Dengan adanya internet komunikasi jarak jauh dapat dilakukan dengan cepat dan mudah. Namun pada kenyataannya internet tidak terlalu aman karena merupakan media komunikasi umum yang dapat digunakan oleh siapa saja, sehingga rawan terhadap penyadapan informasi. Karena penggunaan internet yang sangat luas seperti pada bisnis, perdagangan, industri, dan pemerintahan maka keamanan informasi menjadi faktor utama yang harus dipenuhi. Salah satu metode yang dapat digunakan untuk menjaga kerahasiaan dari suatu informasi tersebut yaitu dengan steganografi.

Steganografi merupakan teknik dan seni menyembunyikan informasi dan data digital dibalik informasi digital lain, sehingga informasi digital yang sesungguhnya tidak terlihat. Namun saat ini telah diketahui ada metode yang dapat melakukan serangan-serangan terhadap steganografi sehingga

[1],Jurusan Teknik Elektro, Fakultas Teknik Universitas Mataram, Nusa Tenggara Barat Indonesia

mengakibatkan keamanan informasi dengan menggunakan teknik steganografi menjadi berkurang. Oleh karena itu, dengan mempertimbangkan keadaan tersebut maka untuk meningkatkan keamanan dari teknik steganografi ini dapat dilakukan kombinasi dengan menggunakan suatu transformasi pada gambar (cover image) dan suatu enkripsi data pada pesan, dimana dalam hal ini digunakan tranformasi Slant dan algoritma enkripsi ElGamal.

Transformasi Slant merupakan suatu tranformasi matriks ortogonal, oleh karena itu nilai matriks inversnya sama dengan nilai matriks transposenya. Dalam hal ini transformasi Slant dapat dimanfaatkan di dalam proses penyisipan pesan rahasia yaitu dengan menyisipkan pesan rahasia tersebut di dalam koefisien-koefisien matriks transformasi Slant. Sedangkan algoritma ElGamal merupakan salah satu dari algoritma asimetris atau sering disebut dengan algoritma kunci publik. Algoritma ElGamal menggunakan dua jenis kunci yaitu kunci publik dan kunci rahasia. Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang tertentu saja yang boleh mengetahuinya.

Pesan rahasia tersebut awalnya dienkripsi dahulu menggunakan algoritma ElGamal kemudian disisipkan pada gambar yang telah ditransformasi menggunakan transformasi Slant. Hasil dari gambar yang telah tersisipi pesan tersebut kemudian dikembalikan lagi menjadi gambar asli, sehingga pesan yang tersisipkan menjadi tidak terlihat (tersembunyi).

Steganografi. Kata steganografi berasal dari bahasa Yunani yaitu *steganos* yang artinya tersembunyi atau terselubung, dan *graphein* yang artinya menulis. Steganografi adalah seni dan ilmu menulis pesan tersembunyi atau menyembunyikan pesan dengan suatu cara sehingga selain si pengirim dan si penerima, tidak ada seorangpun yang mengetahui atau menyadari bahwa ada suatu pesan rahasia.

Steganografi dan kriptografi memiliki hubungan yang erat. Kriptografi menyandikan pesan sehingga tidak dapat dimengerti. Sedangkan steganografi menyembunyikan pesan sehingga tidak akan ada yang mengetahui keberadaan pesan tersebut. Dalam beberapa situasi, mengirim pesan terenkripsi akan menimbulkan kecurigaan sedangkan sebuah pesan tersembunyi tidak menimbulkan kecurigaan, hal inilah yang menjadi kelebihan steganografi dibandingkan kriptografi. Kedua ilmu ini dapat dikombinasikan untuk menghasilkan proteksi terhadap pesan yang lebih baik lagi. Pada kasus ini, ketika steganografi gagal akibat pesan rahasia yang dideteksi, pesan tersebut tetap tidak berarti karena telah dienkripsi menggunakan krtiptografi.

Menyisipkan data yang ingin disembunyi-kan kedalam sebuah media membutuhkan dua buah property yaitu media penampung (citra, suara, text, video) yang terlihat tidak mencurigakan untuk menyimpan pesan rahasia dan pesan rahasia yang ingin disembunyikan.

Steganografi membahas bagaimana se-buah pesan dapat disisipkan kedalam sebuah berkas media sehingga pihak ketiga tidak menyadarinya. Steganografi memanfaatkan keterbatasan sistem indra manusia seperti mata dan telinga. Dengan adanya keter-batasan inilah, metode steganografi ini dapat diterapkan pada berbagai media digital. Hasil keluaran dari steganografi ini memiliki bentuk persepsi yang sama dengan bentuk aslinya, tentunya persepsi ini sebatas oleh kemam-puan indra manusia, tetapi tidak oleh computer atau perangkat pengolah digital lainnya.

Penyembunyian data rahasia ke dalam media digital dapat mengubah kualitas dari media tersebut. Kriteria yang harus diperhatikan dalam penyembunyian data antara lain:

1. Imperceptibility
   Keberadaan pesan rahasia tidak dapat dipersepsi oleh indriawi. Misalnya jika media penampung berupa citra, maka penyisipan pesan membuat stegotext sukar dibedakan oleh mata dengan citra covertext-nya
2. Fidelity
   Mutu citra penampung tidak jauh berubah. Setelah penambahan pesan rahasia, citra hasil steganografi masih terlihat dengan baik. Pengamat tidak mengetahui bila dalam citra tersebut terdapat pesan rahasia.
3. Recovery
   Data yang disembunyikan harus dapat diungkapkan kembali. Karena tujuan steganografi adalah menyembunyikan pesan, maka sewaktu-waktu data rahasia

di dalam citra tersebut harus dapat diambil kembali untuk digunakan lebih lanjut.

Transformasi Slant. Transformasi Slant merupakan suatu transformasi matriks ortogonal, yang memiliki fungsi konstan untuk baris pertama, dan untuk elemen dari baris yang kedua merupakan fungsi linear dari indeks kolom.

Matriks transformasi Slant N x N dapat dinyatakan secara rekursif sebagai berikut [4]:

$$S_n = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & a_n & 0 & 1 & -a_n & 0 \\ b_n & 1 & 0 & b_n & 1 & 0 \\ 0 & 0 & I_{(n/2)-2} & 0 & 0 & I_{(n/2)-2} \\ 0 & 1 & 0 & 0 & -1 & 0 \\ -b_n & a_n & 0 & b_n & a_n & 0 \\ 0 & 0 & I_{(n/2)-2} & 0 & 0 & -I_{(n/2)-2} \end{bmatrix} \begin{bmatrix} S_{n/2} & 0 \\ 0 & S_{n/2} \end{bmatrix} \quad \text{.....(1)}$$

Dimana N = 2^n, I_M merupakan suatu matriks identitas berukuran M x M dan

$$S_1 = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad \text{.....(2)}$$

Parameter a_n dan b_n dapat ditentukan secara rekursif sebagai berikut :

$$\left.\begin{aligned} b_n &= (1 + 4a_{n-1}^2)^{-1/2} \\ a_1 &= 1 \\ a_n &= 2b_n a_{n-1} \end{aligned}\right\} \quad \text{.....(3)}$$

Maka diperoleh :

$$a_{n+1} = \left(\frac{2N^2}{4N^2-1}\right)^{1/2}, b_{n+1} = \left(\frac{N^2-1}{4N^2-1}\right)^{1/2}, N = 2^n \quad \text{.....(4)}$$

Kriptografi. Kriptografi (cryptography) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu kripto dan graphia. Kripto artinya menyembunyikan, sedangkan graphia artinya tulisan. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data, keabsahan data, integritas data, serta autentikasi data. Tetapi tidak semua aspek keamanan informasi dapat diselesaikan dengan kriptografi. Untuk menjaga pesan, maka pesan tersebut dapat diubah menjadi suatu kode yang tidak dapat dimengerti oleh pihak lain.

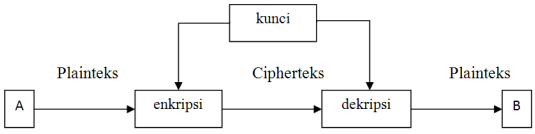
Enkripsi adalah sebuah proses penyandian yang melakukan perubahan sebuah kode (pesan) dari yang bisa dimengerti (plainteks) menjadi sebuah kode yang tidak bisa dimengerti (cipherteks). Sedangkan proses kebalikannya untuk mengubah cipherteks menjadi plainteks disebut dekripsi. Proses enkripsi dan dekripsi memerlukan suatu mekanisme dan kunci tertentu.

Algoritma kriptografi. Ada dua macam algoritma kriptografi, yaitu algoritma simetris (symmetric algorithms) dan algoritma asimetris (asymmetric algorithms).

Algoritma simetri. Algoritma simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Algoritma ini mengharuskan pengirim dan penerima menyetujui suatu kunci tertentu sebelum mereka saling berkomunikasi. Keamanan algoritma simetris tergantung pada kunci, membocorkan kunci berarti bahwa orang lain dapat mengenkripsi dan mendekripsi pesan. Agar komunikasi tetap aman, kunci harus tetap dirahasiakan. Algoritma simetris sering juga disebut dengan algoritma kunci rahasia, algoritma kunci tunggal, atau algoritma satu kunci. Sifat kunci yang seperti ini membuat pengirim harus selalu memastikan bahwa jalur yang digunakan dalam pendistribusian kunci adalah jalur yang aman atau memastikan bahwa seseorang yang ditunjuk membawa kunci untuk dipertukarkan adalah orang yang dapat dipercaya. Masalahnya akan menjadi rumit apabila komunikasi dilakukan secara bersama-sama oleh sebanyak *n* pengguna dan setiap dua pihak yang melakukan pertukaran kunci, maka akan terdapat sebanyak

$$C_2^n = \frac{n!}{(n-2)!.2!} = \frac{n.(n-1)}{2}$$

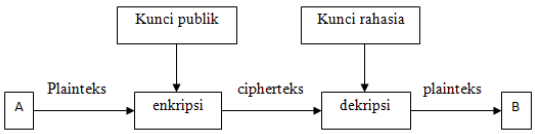
Kunci rahasia yang harus dipertukarkan secara aman



Gambar 1 Skema algoritma simetri

Algoritma Asimetri. Algoritma asime-tris, sering juga disebut dengan *algoritma kunci publik*, menggunakan dua jenis kunci, yaitu *kunci publik* (*public key*) dan *kunci rahasia* (*secret key*). Kunci publik merupakan kunci yang digunakan untuk mengenkripsi pesan. Sedangkan kunci rahasia digunakan untuk mendekripsi pesan. Kunci publik bersifat umum, artinya kunci ini tidak dirahasiakan sehingga dapat dilihat oleh siapa saja. Sedangkan kunci rahasia adalah kunci yang dirahasiakan dan hanya orang-orang

tertentu saja yang boleh mengetahuinya. Keuntungan utama dari algoritma ini adalah memberikan jaminan keamanan kepada siapa saja yang melakukan pertukaran informasi meskipun di antara mereka tidak ada kesepakatan mengenai keamanan pesan terlebih dahulu maupun saling tidak mengenal satu sama lainnya.



Gambar 2 Skema algoritma asimetris

Kriptosistem ElGamal. Algoritma ElGamal pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Sampai saat ini, algoritma ElGamal masih dipercaya sebagai metode penyandian, seperti aplikasi PGP dan GnuPG yang dapat digunakan untuk pengamanan e-mail dan tanda tangan digital. Algoritma ElGamal terdiri dari 3 proses yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks. Kemudian pada blok-blok cipherteks dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk sistem kriptografi ElGamal, dibutuhkan bilangan prima *p* dan elemen primitif.

Prosedur Membuat Pasangan Kunci. Proses pertama adalah pembentukan kunci yang terdiri dari kunci rahasia dan kunci publik. Pada proses ini dibutuhkan sebuah bilangan prima *p*, elemen primitif α dan sebarang x. Kunci publik algoritma ElGamal berupa pasangan 3 bilangan, yaitu (*p*, *α, β*), dengan[1][5]:

$$\beta = \alpha^x \bmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5)$$

Sedangkan kunci rahasianya adalah bilangan x tersebut.

Karena pada algoritma ElGamal menggunakan bilangan bulat dalam proses perhitungannya, maka pesan harus dikonversi kedalam suatu bilangan bulat. Untuk mengubah pesan menjadi bilangan bulat, digunakan kode ASCII (*American Standard for Information Interchange*). Kode ASCII merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Oleh karena itu, berdasarkan sistem kriptografi ElGamal di atas maka harus digunakan bilangan prima yang lebih besar dari 255. Kode ASCII berkorespondensi 1-1 dengan karakter pesan. Berikut ini diberikan suatu algoritma yang dapat digunakan untuk melakukan pembentukan kunci.

1. Pilih sembarang bilangan prima *p* (*p* > 255)
2. Pilih dua buah bilangan acak α dan x, dengan syarat α<*p* dan 1≤ x ≤ *p*-2
3. Hitung $\beta = \alpha^x \bmod p$
4. Publikasikan *p*, *α, β* , dan rahasiakan x

Enkripsi. Pada proses ini pesan dienkripsi menggunakan kunci publik (*p*,*α, β*) dan sebarang bilangan acak rahasia *k* ϵ {0, 1, ..., *p*-1}. Misalkan *m* adalah pesan yang akan dikirim. Selanjutnya, *m* diubah kedalam blok-blok karakter dan setiap karakter dikonversikan kedalam kode ASCII, sehingga diperoleh plainteks *m*1, *m2*, ...,*mn* dengan *mi* ϵ {0, 1, 2,..., p-1}, *i* = 0, 1, 2,..., *n* . Untuk nilai ASCII bilangan 0 digunakan untuk menandai akhir dari suatu teks.

Proses enkripsi pada algoritma ElGamal dilakukan dengan menghitung[1][5] :

$$\gamma = \alpha^k \bmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(6)$$

dan

$$\delta = \beta^k . m \bmod p \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(7)$$

maka diperoleh cipherteks (γ,δ).Bilangan acak *k* ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya, tetapi nilai *k* hanya digunakan saat melakukan enkripsi saja dan tidak perlu disimpan. Algoritma Enkripsi

1. Plainteks disusun menjadi blok-blok *m1, m2, …, mn* sedemikian sehingga setiap blok merepresentasikan nilai di dalam rentang 0 sampai *p*-1.
2. Pilih bilangan acak k dengan syarat 0 < k <*p*-1, sedemikian sehingga k relatif prima dengan *p*-1.
3. Setiap blok m dienkripsi dengan rumus
   $\gamma = \alpha^k \bmod p$
   $\delta = \beta^k . m \bmod p$
4. Diperoleh cipherteks (γ, δ).

Dekripsi. Setelah menerima cipherteks (γ, δ) proses selanjutnya adalah mendekripsi cipherteks menggunakan kunci publik *p* dan kunci rahasia *x*. Diberikan (*p, α, β*) sebagai kunci publik dan x sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (γ, δ) maka[1] [5]:

$$m = \delta . (\gamma^x)^{-1} mod\ p \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(8)$$

Dengan *m* adalah plainteks. Algoritma dekripsi

1. Diketahui cipherteks (γ, δ), i= 1, 2, 3, …, n, kunci publik *p*, dan kunci rahasia x.
2. Untuk i dari 1 sampai n kerjakan
   Hitung $\gamma^{p^{-1-x}} mod\ p$
   Hitung $mi = \delta . (\gamma^{x})^{-1} mod\ p$
3. Diperoleh *m1, m2, …, mn.*
4. Konversikan masing-masing bilangan *m1, m2, …, mn* ke dalam karakter sesuai dengan kode ASCII-nya kemudian hasilnya digabungkan kembali.

METODE PENELITIAN

Alat dan bahan penelitian. Pada penelitian ini, pembuatan program menggunakan komputer core2duo 2.2 GHz, sistem Operasi *Windows XP, Software Microsoft Visual* C++ 6.0 dan *Software Microsoft Visual* C++ 2008.

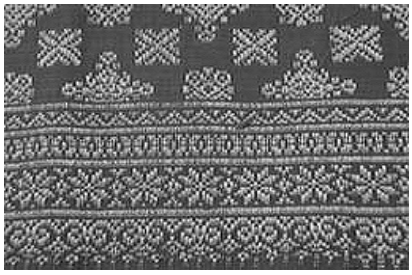
Langkah-langkah penelitian. Rincian proses penelitian yang akan dilakukan antara lain:

1. Penelitian dimulai dengan melakukan studi literatur mengenai topik materi penelitian guna mendapatkan berbagai informasi dan garis besar yang digunakan sebagai acuan dalam menyelesaikan permasalahan.
2. Melakukan perencanaan sistem yang akan digunakan dalam penelitian.
3. Melakukan desain dan coding program.
4. Melakukan pengujian program.
5. Membuat laporan, pembahasan, analisa, dan kesimpulan.

HASIL DAN PEMBAHASAN

Proses Enkripsi. Pada proses enkripsi ini bertujuan untuk menghasilkan gambar yang telah disisipkan suatu cipherteks, adapun tahapan-tahapan dalam proses enkripsi antara lain sebagai berikut :

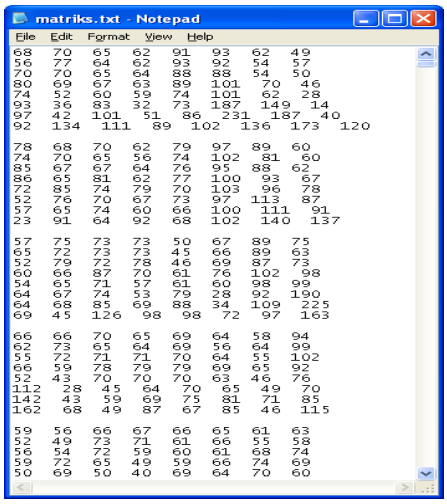
1. Proses pembacaan file gambar (tenun_songket.bmp)
   Pada tahapan ini dilakukan pembacaan *file* gambar, dimana hasil dari pembacaan *file* gambar tersebut akan digunakan sebagai *file* pembawa atau *file* yang akan ditanami *ciphertext*



Gambar 3 tenun_songket.bmp

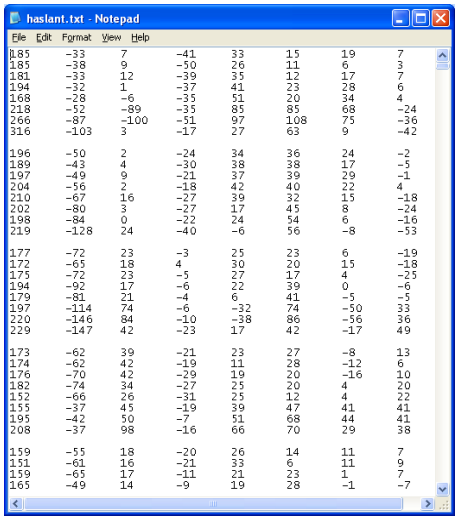
Gambar 4 Hasil pembacaan file gambar tenun_songket.bmp

2. Proses partisi
   Pada tahapan ini dilakukan proses partisi pada file gambar menjadi matriks dengan ukuran 8x8. Hal ini dilakukan dengan tujuan untuk mempermudah di dalam proses pentransformasian, dimana transformasi yang digunakan adalah transformasi Slant 3



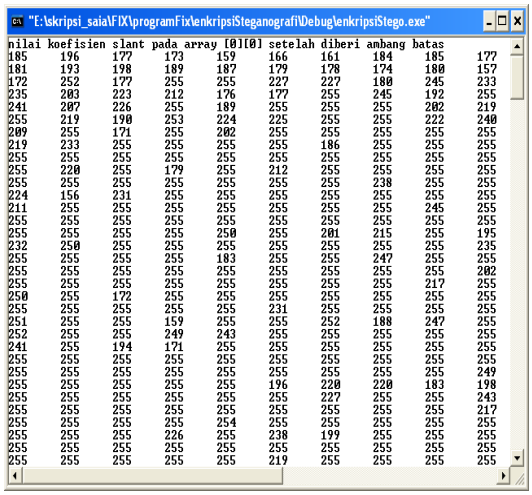
Gambar 5 Hasil pembacaan file gambar dalam matriks 8x8

3. Proses transformasi Slant
   Pada tahapan ini dilakukan transformasi pada nilai dari file gambar yang telah di partisi menjadi matriks 8x8, dengan tujuan untuk mendapatkan nilai koefisien-koefisien matriks Slant.

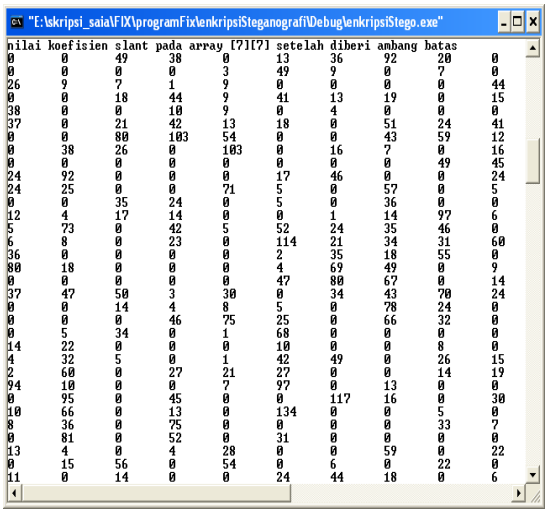


Gambar 6 Koefisien matriks Slant terhadap matriks 8x8

4. Proses pemberian ambang batas pada nilai koefisien matriks Slant
   Pada tahapan ini dilakukan pemberian ambang batas pada nilai ke [0][0] dan nilai ke [7][7] pada koefisien matriks Slant, dengan kondisi apabila nilai lebih besar dari 255 maka nilai menjadi 255 dan apabila nilai lebih kecil dari 255 maka nilai menjadi 0.

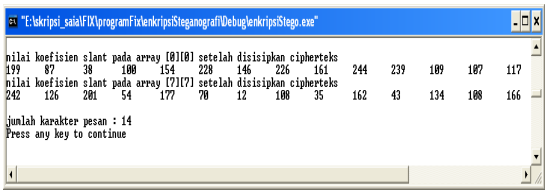


Gambar 7 Nilai ke [0][0] pada koefisien matriks Slant



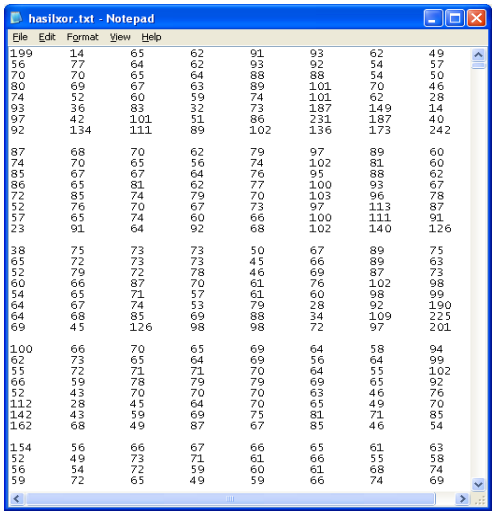
Gambar 8 Nilai ke [7][7] pada koefisien matriks Slant

5. Proses penyisipan nilai cipherteks pada nilai koefisien transformasi Slant
   Pada tahapan ini dilakukan proses penyisipan nilai dari cipherteks ke dalam nilai dari koefisien transformasi Slant yang telah diberikan ambang batas dengan metode XOR.



Gambar 9 Hasil XOR cipherteks

6. Proses menyisipkan nilai XOR ke dalam matriks 8x8 pada file asli
   Pada tahapan ini dilakukan penyisipan nilai XOR ke dalam matriks 8x8 pada file asli yaitu pada nilai ke [0][0] dan nilai ke [7][7] dengan mengganti nilai dari file asli dengan nilai XOR tersebut. Disini juga dilakukan penyisipan jumlah pesan yang dikirim, dimana nilai dari jumlah pesan tersebut diletakkan pada nilai ke [0][1].



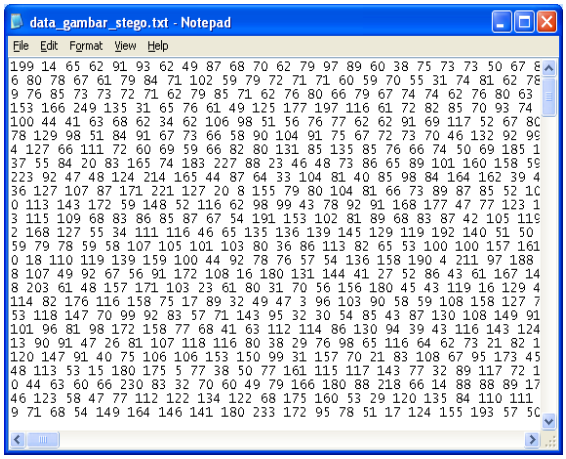
Gambar 10 Hasil penyisipan nilai XOR ke dalam matriks asli 8x8

7. Proses rekonstruksi file gambar
   Pada tahapan ini dilakukan proses rekonstruksi file gambar dari matriks 8x8 menjadi file gambar stego dengan nama gambarStego.bmp.

Gambar 11 gambar Stego.bmp

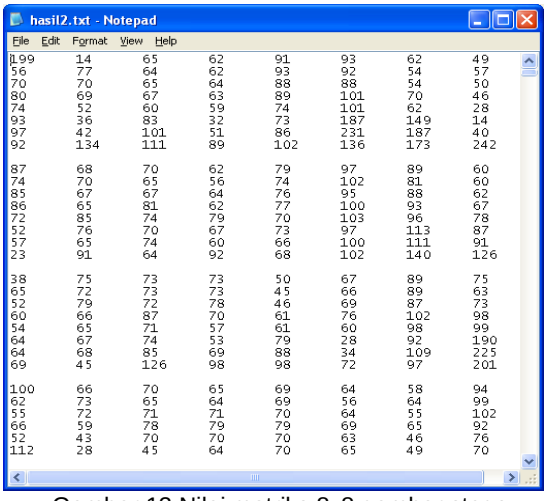
Proses Dekripsi. Pada proses dekripsi ini bertujuan untuk mengambil nilai cipherteks yang telah disisipkan ke dalam gambar kemudian mengkonversikannya kedalam bentuk karakter. Adapun tahapan-tahapan dalam proses dekripsi antara lain sebagai berikut :

1. Proses pembacaan file gambar stego
   Pada tahapan ini dilakukan pembacaan file gambar stego, dimana nilai dari data tersebut akan digunakan untuk menentukan nilai-nilai dari cipherteks.



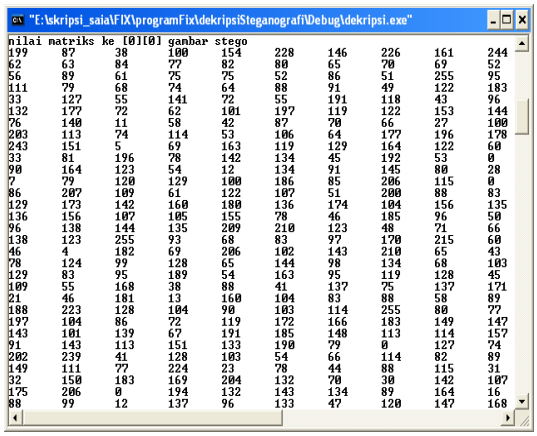
Gambar 12 Hasil pembacaan dari gambar stego

2. Proses partisi gambar stego
   Pada tahapan ini dilakukan proses partisi pada file gambar stego menjadi matriks dengan ukuran 8x8. Hal ini dilakukan dengan tujuan untuk mempermudah dalam menentukan nilai ke [0][0] dan nilai ke [7][7] dari matriks 8x8.

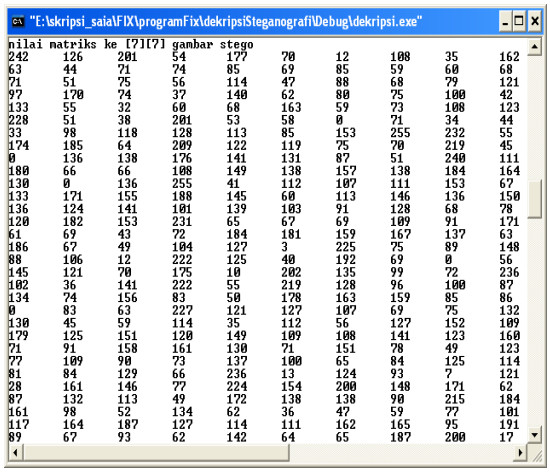


Gambar 13 Nilai matriks 8x8 gambar stego

3. Proses pengambilan nilai matrik
   Pada tahap ini dilakukan pengambilan nilai matriks 8x8 yaitu nilai matriks ke [0][0] dan matriks ke [7][7].

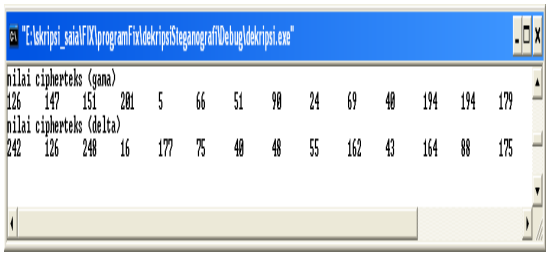


Gambar 14 Nilai matriks ke [0][0]



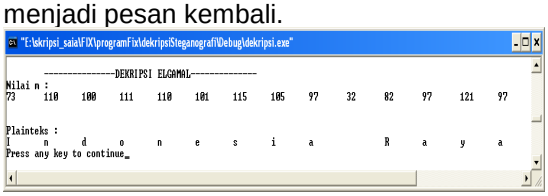
Gambar 15 Nilai matriks ke [7][7]

4. Proses mendapatkan nilai cipherteks
   Pada tahapan ini dilakukan peng-XOR-an nilai, yaitu antara nilai ke[0][0] matriks gambar asli dengan nilai ke [0][0] matriks gambar stego dan antara nilai ke [7][7] matriks gambar asli dengan nilai ke [7][7] matriks gambar stego sesuai dengan jumlah pesan yang dikirim sehingga diperoleh nilai dari cipherteks. Pada program ini di asumsikan bahwa si penerima telah memiliki gambar asli sesuai dengan kesepakatan bersama.



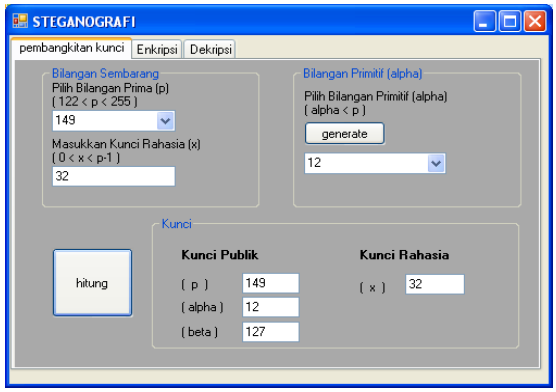
Gambar 16 Nilai cipherteks

5. Proses dekripsi cipherteks
   Pada tahapan ini dilakukan pendekripsian dari nilai cipherteks yang telah diperoleh menjadi pesan kembali.



Gambar 17 Pesan asli

Interface Program. Pembangkitan kunci.

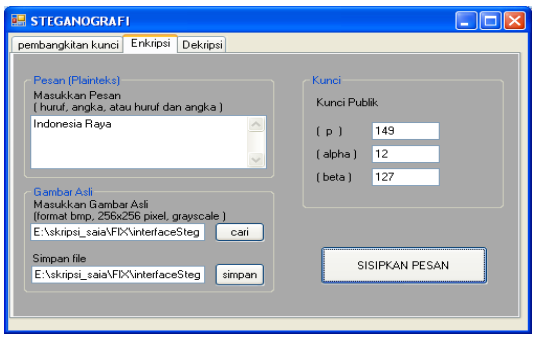


Gambar 18 Interface pembentukan kunci

Pada tahap ini dilakukan pembakitan kunci publik dan kunci rahasia, dengan memasukkan nilai bilangan prima, bilangan rahasia dan bilangan primitif. Kemudian dari nilai-nilai tersebut akan digunakan untuk menghitung nilai beta. Pada program telah diberi batasan bilangan yang memungkinkan untuk dilakukan pembangkitan kunci seperti :

- Pada bilangan prima telah dibatasi nilai yang memungkinkan yaitu dari 122 – 255. Hal ini disebabkan oleh keterbatasan yang timbul akibat adanya kombinasi dengan gambar, dimana pada 1 pixel gambar tersebut hanya mampu menampung nilai hingga 255, sedangkan untuk pemilihan bilangan prima harus lebih besar dari plainteks (batas plainteks = batas ASCII =0 - 255), oleh karena itu diberikan batasan pada plainteks yang akan dikirim yaitu hanya huruf dan angka saja sehingga batas nilai plainteks yang mungkin menjadi 0 - 122.
- Untuk bilangan primitif diperoleh dari men-*generate* dari nilai bilangan prima.
- Untuk kunci rahasia merupakan bilangan sembarang dengan syarat 0<x<p-1.

Proses enkripsi dan penyisipan pesan.



Gambar 19 Interface Enkripsi dan penyisipan pesan

Pada tahap ini dilakukan proses enkripsi dan penyisipan pesan rahasia. Pertama dimasukkan pesan yang akan dikirim berupa huruf, angka, atau gabungan huruf dan angka. Kemudian pilih gambar dengan format BMP dengan ukuran 256x256 yang akan digunakan sebagai media pembawa pesan. Tentukan juga direktori yang akan digunakan sebagai tempat penyimpanan pesan. Terakhir masukkan kunci publik yang akan digunakan dalam proses enkripsi. Dengan menekan tombol “SISIPKAN PESAN” maka akan dilakukan proses enkripsi pesan dengan menggunakan algoritma ElGamal dan penyisipan pesan dalam gambar dengan mengggunakan transformasi Slant. Ketika proses penyisipan selesai maka akan keluar tampilan sebagai berikut

Gambar 20 Pesan ketika proses penyisipan selesai

Proses dekripsi dan pengambilan pesan.

Gambar 21 Interface dekripsi dan pengambilan pesan

Pada tahap ini dilakukan proses dekripsi dan pengambilan pesan rahasia. Pertama pilih gambar asli dan gambar stego yang telah tersisipi pesan rahasia kemudian masukkan kunci yang akan digunakan dalam proses dekripsi yaitu kunci rahasia dan bilangan prima. Dengan menekan tombol “Ambil Pesan” maka akan dilakukan proses pengambilan pesan rahasia yang masih berupa cipherteks pada gambar, kemudian cipherteks tersebut akan di dekripsi untuk mendapatkan pesan asli (plainteks).

Perbandingan gambar sebelum dan sesudah disisipkan pesan dengan gambar berbeda

(a). tenun_songket

(b). tenun_stego

Gambar 22 Perbandingan gambar asli dengan gambar stego

KESIMPULAN

Berdasarkan penelitian yang telah dilakukan, maka dapat disimpulkan bahwa :

1. Penggunaan transformasi Slant pada gambar dapat memperkuat teknik steganografi yakni di dalam proses penyembunyian pesan.
2. Pada proses steganografi ini, hasil dari penyisipan pesan (gambar stego) tidak berubah jauh dari gambar asli.
3. Panjang pesan yang disisipkan dalam gambar mempengaruhi nilai dari SNR, dimana semakin panjang teks yang disisipkan pada gambar maka semakin kecil nilai SNR yang diperoleh.

SARAN

penelitian selanjutnya, diharapkan dapat menggunakan transformasi yang berbeda dalam proses penyisipan pesan, begitu pula pada media pembawanya agar dicoba menggunakan media yang berbeda tidak hanya bergantung pada gambar saja.

DAFTAR PUSTAKA

Menezes, Alfred., Paul van Oorschot and Scott A. 1997. *Handbook of Applied Cryptography*. CRC Press .

Paar, Christof., Jan Pelzl. 2009. *Understanding Cryptography*. Bochum.

Man Young Rhee,*Internet Security :Cryptographic Principles, Algorithms And Protocols*. Seoul, Korea.

Jain, Anil K.1989. *Fundamental Of Digital Image Processing*. Prentice-Hall, Inc.

Widyananta, I Gde Nike.2009. *Perancangan Interface Eksperimen Numeris Dengan Algoritma Enkripsi ElGamal Criptosystem*. Teknik Elektro Universitas Mataram.

Munir, Rinaldi.2006. *Kriptografi.* Informatika Bandung.