IMPLEMENTASI PENGAMANAN TEXT FILE PADA HYBRID SISTEM MENGGUNAKAN ALGORITMA VIGENERE DAN ALGORITMA ADAPTIVE MINIMUM ERROR LEAST SIGNIFICANT BIT REPLACEMENT(AMELSBR)

¹Wamiliana, ²Tryo Romadhoni Pujakusuma, ³Febi Eka Febriansyah, dan ⁴Dwi Sakethi

^{1,2,3,4}Jurusan Matematika FMIPA Unila

Abstract

The development of technology and the internet allows everyone to exchange data and information. Problems arise when the information is confidential, especially for a company, institution and also individuals who have important documents and data. Therefore, the security of the data is a must. In this case cryptography plays a role of encrypting secret messages into the form of unreadable messages and steganography that hides the irregular messages into the image media, resulting in double security in the delivery of secret messages. In this research we develop a hybrid system using Vigenere and AMELSBR with cover media in the form of (.jpg) format as input (cover), file type (.png) as output (stegoimage) and data be inserted as a file with text format. The conclusion of this research is that the hybrid system can be used to encrypt the secret message and hide it into the cover media to make it more secure in data transmission. Therefore, the use of AMELSBR method is good used in steganography. Stegoimage can withstand the process of manipulating the brightness and contrast with the image record must have the dominant black color value (rgb (0,0,0)) or white (rgb (255,255,255)) and not many color variants, in other words the image can restore the file without experiencing excessive reduction of meaning after the manipulation of brightness and contrast is an image with binary image quality and grayscale image.

Key word: Hybrid, Cryptography, Steganography, Vigenere, AMELSBR.

1. Pendahuluan

Teknologi informasi dan komunikasi telah berkembang pesat, memberikan pengaruh yang besar bagi kehidupan manusia. Perkembangan teknologi jaringan dan internet memungkinkan setiap orang untuk saling bertukar data, informasi, atau pesan kepada orang lain tanpa batasan jarak dan waktu. Masalah yang muncul ketika informasi tersebut bersifat rahasia, terutama bagi suatu perusahaan, institusi atau organisasi dan juga individu yang mempunyai dokumen-dokumen rahasia dan data-data yang penting, sehingga, perlu dijaga keamanan dari dokumen-dokumen tersebut agar terhindar dari gangguan orang lain. Salah satu cara untuk mengamankan data atau informasi dari tindak kejahatan tersebut adalah menggunakan teknik kriptografi dan steganografi.

Pada penelitian ini akan dikembangkan perangkat lunak metode hibridkriptografi dan steganografi menggunakan algoritma vigenere dan algoritma AMELSBR(*Adaptive Minimum Error Least Significant Bit Replacement*) yang mana pesan dienkripsi sehingga menjadi pesan acak (*ciphertext*) yang akan dikeluarkan dalam bentuk *file* (*.txt), kemudian *file* (*.txt) akan disisipkan kedalam media penampung (*cover image*) yang berupa gambar (*.jpg/.jpeg) sehingga menghasilkan output (*stegoimage*) berupa gambar (*.png) yang didalamnya mengandung *ciphertext*

2 Metodologi

Penelitian ini menggunakan metode kriptografi Vigenere dan steganografi AMELSB. Berdasarkan penelitian yang dilakukan oleh Lee dan Chen digunakan gambar dengan citra biner sebagai media penampung [1], selanjutnya penelitian yang dilakukan oleh Mark David Gan adalah dengan menggunakan citra warna dengan format gambar bitmap sebagai media penampung [2]. Sedangkan pada penelitian ini digunakan citra warna untuk dijadikan media penampung dengan format gambar .jpg/.jpeg. sedangkan pada *stegoimage* digunakan format gambar .png.

Metode pengembangan sistem yang digunakan adalah metode *waterfall*. Tahap-tahap pada metode *waterfall* adalah perencanaan sistem, analisis kebutuhan, desain dan implementasi [3]. Tahap penelitian dan pengembangan sistem disajikan pada Gambar 1.

Gambar 3.1 Tahap Penelitian dan Pengembangan Sistem.

Tahapan melakukan enkripsi dan penyisipan berkas adalah sebagai berikut:

1. Memasukkan Plaintext (.txt)
2. Memasukkan kunci
3. Proses Enkripsi menggunakan Vigenere
4. Mendapat ciphertext

5. Memasukkan Gambar (.jpg/.jpeg)
6. Verifikasi gambar
7. Memasukkan ciphertext
8. Verifikasi Berkas
9. Proses penyisipan gambar menggunakan AMELSBR

Tahapan melakukan ekstraksi dan dekripsi:

1. Memasukkan gambar (.jpg/.jpeg)
2. Verifikasi gambar
3. Proses Ekstraksi menggunakan AMELSBR
4. Mendapat Ciphertext
5. Memasukkan Berkas Ciphertext
6. Memasukan kunci
7. Proses Dekripsi menggunakan Vigenere

Pada penelitian ini alasan digunakannya gambar dengan format *file .jpg/.jpeg* sebagai media penampung adalah:

1. Berdasarkan situs resmi www.jpeg.org menegaskan bahwa setiap hari terdapat jutaan gambar diambil dengan kamera digital dan kamera ponsel dengan format .jpg. dengan demikian gambar dengan format ini mudah untuk didapatkan.
2. Gambar dengan format .jpg/.jpeg telah tergabung dalam *International Standardization Organization* (ISO).
3. Gambar dengan format .jpg/.jpeg telah tergabung dalam *International Electrotechnical Commission* (IEC).

Selain itu, alasan digunakannya gambar dengan format *file .png* sebagai output *stegoimage* adalah:

1. Format gambar .png termasuk dalam *lossy compression*[4].
 2. Gambar dengan format .png telah tergabung dalam *International Standardization Organization* (ISO).
- Gambar dengan format .png telah tergabung dalam *International Electrotechnical Commission* (IEC).

3. Hasil dan Pembahasan

Pada penelitian ini telah disiapkan pesan yang akan digunakan dalam percobaan ini, yang pesan tersebut berisikan “*The Quick Brown Fox Jumps Over the Lazy Dog*,;'[<>?:''}]|=/_+)(*&^%\$#@!/~`1234567890”. Alasan digunakannya pesan tersebut dikarenakan pesan tersebut mencakup seluruh alfabet dan diikuti dengan seluruh tanda baca serta angka. Selain itu juga pada pengujian ini menggunakan kunci “ilmukomputer11”.

3.1 Pengujian Enkripsi dan Dekripsi

Pada pengujian enkripsi pesan tersebut berhasil ter-enkripsi menjadi sekumpulan angka yang berisikan “2(&t1<.*+sf<CK=kr<:nv>}<[q%J#/B*(11-G/q4C%ZbgXYXaqqcmvtcfVcbgTVZXHTbaHJKS?DCGMM?MWX”, dan dengan begitu pesan asli dapat terjaga keamanannya dari pihak yang ingin mencuri data. Sedangkan pada dekripsi

sekumpulan angka tersebut berhasil dikembalikan menjadi pesan asli yaitu “*The Quick Brown Fox Jumps Over the Lazy Dog*,, '[/]\<?:''{}/=-_+)(*&^%\$#@!~`1234567890”.

3.2 Pengujian Perubahan *Brightness* dan *Contrast*

Penelitian selanjutnya digunakan 8 *file* gambar yang berbeda-beda dengan format (.jpg) sebagai *input* atau sebagai media penampung dengan perbedaan ukuran disetiap *file* gambarnya. Pengujian ini dilakukan dengan cara memanipulasi *stegoimage* dengan perubahan *brightness* dan *contrast*. Interval perubahan *brightness* yaitu -150, -120, -90, -60, -30, 30, 60, 90, 120, 150, sedangkan interval perubahan *contrast* yaitu -50, -30, 30, 60, 90, sebagai contoh file gambar 1 dilakukan perubahan *brightness* sebesar -150, lalu akan diuji oleh sistem apakah berkas dapat kembali atau tidak, hal yang sama dilakukan pada perubahan *contrast*. 8 *file* gambar (.jpg) disajikan pada Tabel 1.

Tabel 1. 8 File Gambar (.jpg)

No Gambar	Gambar (.jpg)	Ukuran (cm)	Ukuran (pixel)	Ukuran (kb)
Gambar 1		45.16 x 28.22	1280 x 800	278
Gambar 2		57.33 x 38.1	1625 x 1080	202
Gambar 3		35.98 x 29.99	1020 x 850	104
Gambar 4		36.12 x 27.09	1024 x 768	77
Gambar 5		50.8 x 31.75	1440 x 900	396
Gambar 6		56.44 x 35.28	1600 x 1000	237
Gambar 7		56.44 x 35.28	1600 x 1000	57
Gambar 8		36.12 x 27.09	1024 x 768	136

Sebelum melakukan manipulasi *file* citra gambar, telah dilakukan penyisipan berkas terhadap 8 gambar tersebut dengan berkas *ciphertext* yang sebelumnya telah didapatkan dari proses enkripsi, yang berisi “2(&t1<.*+sf<CK=kr<:nv>}<[q%J#/B*(11-G/q4C%ZbgXYXaqqcmvtcfVcbgTVZXHTbaHJKS?DCGMM?MWX”, dan yang mempunyai makna yaitu “*The Quick Brown Fox Jumps Over the Lazy Dog*,;’/|<>?:’”{/=+_+)(*^%\$#@!~`1234567890”. Pengujian 8 *file* gambar dengan berkas *ciphertext* disajikan pada Tabel 2.

Tabel 2. Pengujian 8 File Gambar Dengan Berkas *Ciphertext*

No Gambar	Gambar (.jpg)	Stegoimage (.png)
Gambar 1	278 kb	379 kb
Gambar 2	202 kb	840 kb
Gambar 3	104 kb	596 kb
Gambar 4	77 kb	431 kb
Gambar 5	396 kb	2.033 kb
Gambar 6	237 kb	1.925 kb
Gambar 7	57 kb	504 kb
Gambar 8	136 kb	1.039 kb

Dari Tabel 2 dapat dilihat bahwa terjadi perubahan ukuran pada setiap gambar sebelum disisipi dan sesudah disisipi berkas *ciphertext*. Perubahan terjadi dikarenakan gambar menampung pesan yang berasal dari *ciphertext* tersebut. Namun pada gambar sebelum dan sesudah disisipi tidak terlihat perbedaan secara kasat mata, sehingga *stegoimage* yang dihasilkan tidak tampak mencurigakan.

3.2.1 Pengujian Perubahan *Brightness*

Pada percobaan ini dilakukan dengan cara melakukan perubahan *brightness* dengan interval -150, -120, -90, -60, -30, 30, 60, 90, 120, 150 di masing-masing citra *stegoimage*. Contoh manipulasi *stegoimage* dengan perubahan *brightness* disajikan pada Tabel 3.

Tabel 3. Contoh Perubahan *Brightness*

Setelah dilakukan perubahan *brightness* pada seluruh *stegoimage*, gambar yang tahan terhadap perubahan *brightness* adalah gambar yang mempunyai nilai warna dominan hitam ($\text{rgb}(0,0,0)$) atau putih ($\text{rgb}(255,255,255)$) dan tidak banyak memiliki varian warna.

3.2.2 Pengujian Perubahan *Contrast*

Pada percobaan ini dilakukan dengan cara melakukan perubahan *contrast* dengan interval -50, -30, 30, 60, 90 di masing-masing citra *stegoimage*. Contoh manipulasi *stegoimage* dengan perubahan *contrast* disajikan pada Tabel 4.

Tabel 4. Contoh Perubahan *Contrast*

Setelah dilakukan perubahan *contrast* pada seluruh *stegoimage*, gambar yang mempunyai nilai warna dominan hitam ($\text{rgb}(0,0,0)$) atau putih ($\text{rgb}(255,255,255)$) dan tidak banyak memiliki varian warna cenderung akan tahan terhadap perubahan *contrast*.

3.3 Pengujian Pemotongan Gambar (*Cropping*)

Pada pengujian ini dilakukan pemotongan gambar pada masing-masing *stegoimage* disetiap area atas, bawah, kanan, dan kiri dengan skala pemotongan $1/3$ dan $3/8$ dari ukuran asli. Contoh pemotongan gambar *stegoimage* disajikan pada Tabel 5.

Tabel 5. Contoh Pemotongan Gambar *Stegoimage*

Pada pengujian pemotongan gambar (*cropping*), berkas yang berhasil dikembalikan cenderung berada pada area pemotongan kanan dan bawah, sedangkan pemotongan pada area kiri dan atas cenderung tidak dapat mengembalikan berkas.

4. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan sebagai berikut.

1. Sistem *hybrid* dengan menggabungkan algoritma Vigenere dan metode AMELSBK ini berhasil untuk menyandikan pesan rahasia serta menyembunyikannya ke dalam media penampung gambar sehingga memperoleh keamanan ganda dalam pengiriman data.
2. Tidak terlihat perbedaan yang signifikan antara *stegoimage* dengan gambar aslinya setelah dilakukan penyisipan. Dengan demikian penggunaan metode AMELSBK baik digunakan dalam steganografi.
3. *Stegoimage* dapat tahan terhadap proses manipulasi *brightness* dan *contrast* dengan catatan gambar harus mempunyai nilai warna dominan hitam (rgb(0,0,0)) atau putih (rgb(255,255,255)) dan tidak banyak varian warna, dengan kata lain gambar yang dapat mengembalikan berkas tanpa mengalami pengurangan makna secara berlebihan setelah dilakukannya manipulasi *brightness* dan *contrast* adalah gambar dengan kualitas citra *biner* dan citra *grayscale*.

5. Referensi

- [1] Lee, Y. K., dan Chen, L. H. 1999. *An Adaptive Image Steganographic Model Based on Minimum-Error LSB Replacement*. National Science Council, ROC. NSC87-2213-E-009-006.
- [2] Gan, M. D. 2003. Chameleon Image Steganography, http://chameleonstego.tripod.com/downloads/Chameleon_Technical_Paper.pdf
- [3] Satzinger, John W. Robert Jackson. and Stephen D. Burd. 2010. *Systems analysis and design in a changing world, Five Edition* . Course Technology, Cengage Learning, Boston, Massachusetts. Canada.
- [4] Widhiartha, Putu. 2008. *Pengantar Kompresi Data*, http://nyoman.staf.narotama.ac.id/files/2012/01/widhiartha_kompresidata.pdf