Paper

Perancangan Aplikasi Steganografi Dengan Algoritma Twelve Square Substitution Cipher dan Metode Indeks Variabel

Author: **Yessi Fitri Annisah Lubis, Imran Lubis**

SNASTIKOM 10
Seminar Nasional Teknologi Informasi dan Komunikasi
UNIVERSITAS HARAPAN MEDAN 2012-2023
Program Studi Teknik Informatika
TEMA : DUNIA AKADEMIK DI ERA SOCIETY 5.0 : TANTANGAN DAN PELUANG
ISSN : 2964-1950

SNASTIKOM Ke 10 Tahun 2023
ISBN: 2964-1950

Perancangan Aplikasi Steganografi Dengan Algoritma Twelve Square Substitution Cipher dan Metode Indeks Variabel

Yessi Fitri Annisah Lubis[1], Imran Lubis[2]
[1,2]Universitas Harapan Medan, Indonesia
[1]yessifitriannisahlubis@unhar.ac.id, [2]imranlubis@unhar.ac.id

Abstrak

Penggunaan internet telah meningkat secara signifikan dan semua orang dengan mudah dapat mengaksesnya. Tetapi tidak seharusnya semua orang berhak mendapatkan informasi yang rahasia, sehingga tidak ada rasa aman dan nyaman dalam berkomunikasi. Ketidaknyamanan itu dapat timbul karena adanya orang ketiga yang ingin mengetahui, mengubah, dan bahkan mencuri informasi rahasia. Ada banyak metode Steganografi yang telah dibuat untuk dapat mengamankan informasi rahasia di dalam sebuah citra, sehingga pihak yang tidak berhak tidak menyadari adanya pesan rahasia didalamnya. Masing-masing algoritma memiliki kelebihan maupun kekurangan sendiri. Algoritma *Twelve Square Substitution Cipher* dan *LSB* didasarkan pada konsep Steganografi, dimana informasi terlebih dahulu dienkripsi dengan algoritma *Twelve Square Substitution Cipher* dan digunakan posisi *LSB* untuk menghasilkan pola yang menyembunyikan bit data ke dalam *LSB* pada nilai pixel RGB gambar. Sehingga dihasilkan pesan rahasia didalam gambar tersebut dan orang ketiga tidak menyadari adanya pesan tersembunyi didalamnya.
.

Kata Kunci: algoritma *Twelve Square Substitution Cipher*, *LSB*, citra digital, pesan rahasia, steganografi

Abstract

Internet usage has improved significantly, and everyone can easily access it. But it should not be everyone's right to get confidential information, so there is no sense of security and comfort in communicating. The discomfort can arise because of a third person who wants to know, change, and even steal confidential information. There are many methods of Steganography that have been made to secure confidential information in an image, so that unauthorized parties are not aware of any secret messages in it. Each algorithm has its own advantages and disadvantages. The Twelve Square Substitution Cipher and LSB algorithms are based on the concept of Steganography, where information is first encrypted with the Twelve Square Substitution Cipher algorithm and used the LSB position to generate patterns that hide the data bits into the LSB on the image pixel RGB value. So that generated a secret message in the picture and the third person is not aware of any hidden messages in it.

Keywords: *Twelve Square Substitution Cipher, LSB algorithm, digital image, secret message, steganography*

1. PENDAHULUAN

Saat ini, teknologi komputer sudah berkembang sangat pesat dan telah menjadi salah satu media yang sering digunakan untuk membantu manusia dalam menyelesaikan pekerjaan dalam kehidupan sehari-hari. Dalam pemanfaatan teknologi ini, terkadang perlu untuk melakukan pengawasan secara rahasia, namun tidak menarik perhatian dari pihak lain, yang berarti pihak lain tidak mengetahui bahwa telah diawasi. Penerapan konsep ini dapat dilihat pada penyisipan *secret code* pada hasil cetakan *printer* berwarna. Sebuah tim peneliti yang dipimpin oleh *Electronic Frontier Foundation* (EFF) berhasil memecahkan kode yang disembunyikan di titik *track* sangat kecil yang dilakukan oleh beberapa *printer laser* berwarna. Kode ini disembunyikan secara rahasia pada setiap dokumen yang dicetak keluar. Agen rahasia Amerika Serikat (US *Secret Service*) mengakui bahwa informasi *tracking* adalah bagian dari

perjanjian dengan beberapa perusahaan *printer laser* berwarna yang digunakan untuk mengidentifikasi pemalsuan. Staf EFF menyatakan bahwa kumpulan titik dari satu baris yang dicetak keluar oleh *printer* tersebut berisi tanggal dan waktu dokumen dicetak dan juga nomor seri dari *printer* (Beberapa *printer* yang menerapkan konsep steganografi ini adalah Xerox dan Canon. Steganografi dapat menyamarkan pesan ke dalam suatu media tanpa orang lain menyadari bahwa media tersebut telah disisipi suatu pesan, karena hasil keluaran steganografi adalah data yang memiliki bentuk persepsi yang sama dengan data aslinya apabila dilihat menggunakan indera manusia [1].

Metode steganografi citra yang paling populer adalah metode *LSB substitution*. Namun, metode *LSB* ini tidak tahan terhadap penyerangan dengan menggunakan operasi pengolahan citra. Untuk itu, maka dapat dilakukan modifikasi terhadap metode *LSB* dimana bit tidak hanya disisipkan pada bit ke-8, namun juga dapat disisipkan pada bit ke-6 dan bit-7. Metode ini dinamakan metode Indeks Variabel. Sementara itu, untuk meningkatkan keamanan informasi yang dikirimkan, maka dapat digabungkan penggunaan steganografi dan kriptografi untuk melindungi informasi rahasia, sehingga sulit untuk diubah dan dideteksi. Penggabungan Algoritma *Twelve Square Substitution Cipher* dan metode indeks variabel ini ditemukan oleh Parimal Autade dan Katariya S. S pada tahun 2013 [2]. Pesan terlebih dahulu dienkripsi dengan menggunakan algoritma *Twelve Square Substitution Cipher* kemudian menyisipkan *ciphertext*-nya dengan metode indeks variabel, sehingga pesan rahasia menjadi lebih aman [3].

Citra mempunyai karakteristik yang tidak dimiliki oleh data teks, yaitu citra kaya dengan informasi. Ada sebuah peribahasa yang berbunyi "sebuah gambar bermakna lebih dari seribu kata" (*a picture is more than a thousand words*). Maksudnya tentu sebuah gambar dapat memberikan informasi yang lebih banyak daripada informasi tersebut disajikan dalam bentuk kata-kata (tekstual) [4].

Istilah *encryption of data in motion* mengacu pada enkripsi pesan yang ditransmisikan melalui saluran komunikasi, sedangkan istilah *encryption of data at-rest* mengacu pada enkripsi dokumen yang disimpan di dalam *storage*. Contoh *encryption of data in motion* adalah pengiriman nomor PIN dari mesin ATM ke komputer *server* di kantor bank pusat. Contoh *encryption of data at-rest* adalah enkripsi *file* basis data di dalam *hard disk* [5].

Steganografi dapat dipandang sebagai kelanjutan kriptografi. Jika pada kriptografi, data yang telah disandikan (*ciphertext*) tetap tersedia, maka dengan steganografi cipherteks dapat disembunyikan sehingga pihak ketiga tidak mengetahui keberadaannya. Di negara-negara yang melakukan penyensoran informasi, steganografi sering digunakan untuk menyembunyikan pesan-pesan melalui gambar (*images*), video, atau suara (*audio*) [6].

2. METODE PENELITIAN

2.1 Prosedur Metode

Prosedur kerja dari metode steganografi yang menggunakan algoritma *Twelve Square Substitution Cipher* dan Indeks Variabel ini dapat dibagi menjadi 2 tahapan besar, yaitu:

1. Proses penyisipan

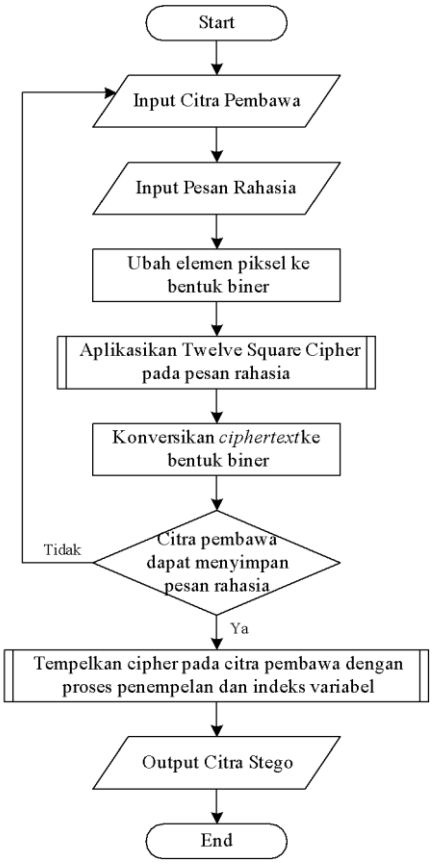
   Proses ini berfungsi untuk melakukan penyisipan pesan rahasia ke dalam sebuah citra pembawa. Proses ini memerlukan dua jenis data input, yaitu:

   a. Citra pembawa yang akan digunakan sebagai tempat penyisipan pesan rahasia.
   b. Pesan rahasia yang akan disisipkan ke dalam citra pembawa.

ISBN: 2964-1950

Prosedur kerja dari proses penyisipan ini dapat dirincikan sebagai berikut:

Langkah 1: Transformasikan citra pembawa ke bentuk deretan biner.
Langkah 2: Aplikasikan *Twelve Square Substitution Cipher* untuk memperoleh *ciphertext* pada pesan rahasia.
Langkah 3: Konversikan *ciphertext* ke bentuk biner.
Langkah 4: Pastikan bahwa panjang dari citra pembawa cukup untuk menyembunyikan pesan rahasia.
Langkah 5: Tempelkan *cipher* pada citra pembawa dengan menggunakan proses penempelan dengan metode Indeks Variabel yang dimodifikasi.
Langkah 6: Kirimkan citra hasil kepada penerima.

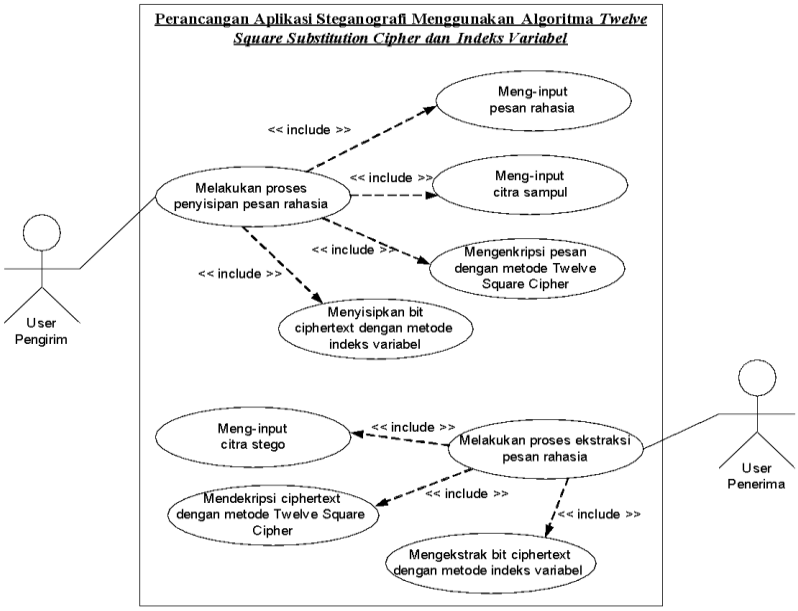


Gambar 1. *Flowchart* Proses Penyisipan

2.2 Perancangan Sistem

Aplikasi steganografi menggunakan algoritma *Twelve Square Substitution Cipher* dan Indeks Variabel ini dapat dimodelkan dengan menggunakan *use case diagram* seperti terlihat pada gambar berikut:

ISBN: 2964-1950



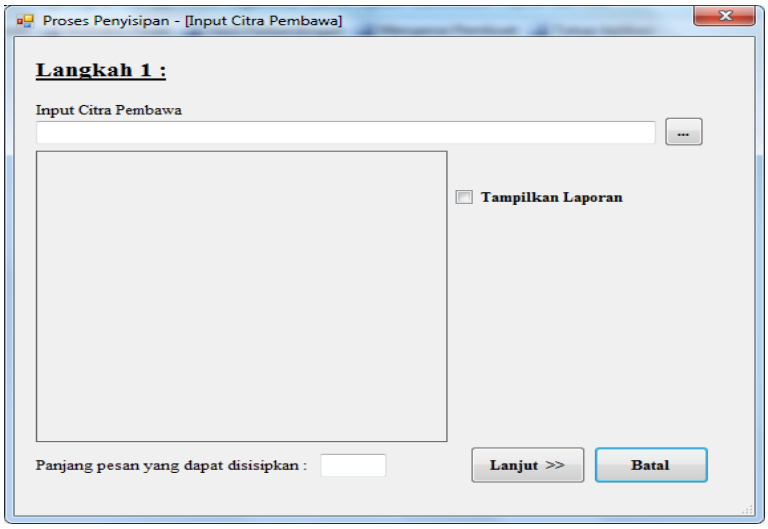
Gambar 2. *Use Case* Diagram dari Sistem

3. HASIL DAN PEMBAHASAN

3.1 Hasil

Pada tampilan utama ini terdapat beberapa link utama yang berfungsi untuk mengakses form-form yang terdapat dalam sistem. Berikut perincian dari link yang terdapat dalam sistem:

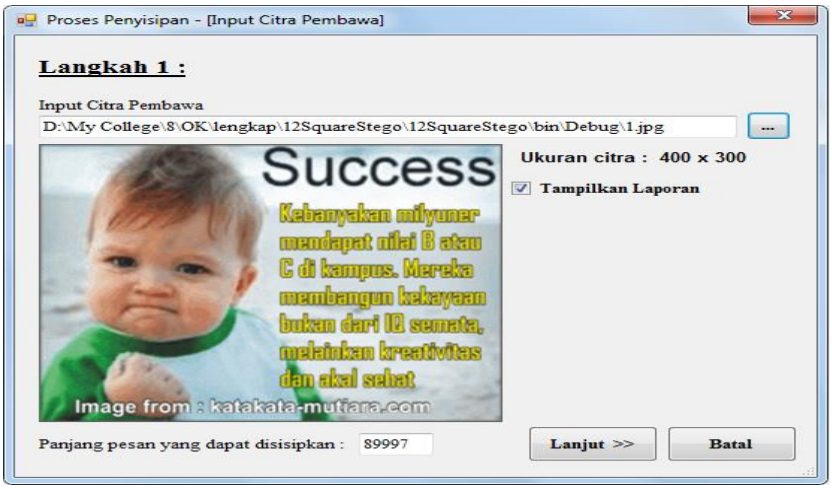
a. Link ‘Penyisipan Pesan’ digunakan untuk melakukan proses penyisipan pesan. Tampilan form ‘Penyisipan Pesan’ dapat dilihat pada gambar berikut:



Gambar 3. Tampilan Form Penyisipan Pesan

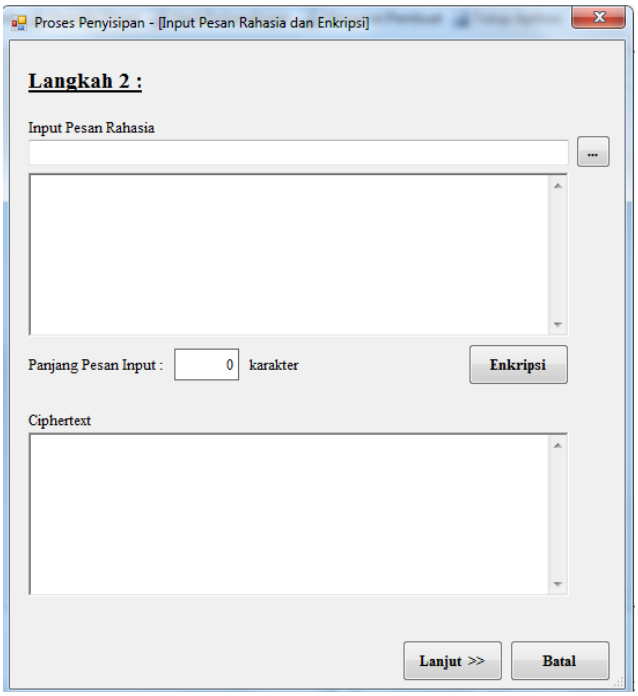
b. Pilihlah file citra yang diinginkan. Setelah itu, klik tombol ‘Open’. Sedangkan, untuk membatalkan proses pemilihan file citra, maka klik tombol ‘Cancel’. Tampilan form Tempel Pesan Rahasia dapat dilihat pada gambar berikut:

ISBN: 2964-1950



Gambar 4. Tampilan Tempel Pesan Rahasia Setelah Input Data

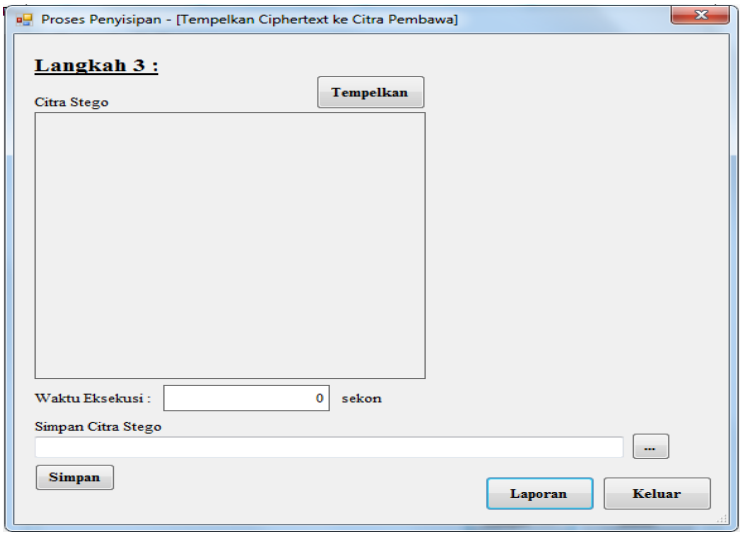
c. Setelah semua data dimasukkan, kliklah link ‘Lanjut >>>’ sehingga sistem akan menampilkan langkah selanjutnya dari proses penyisipan yaitu proses pengisian pesan rahasia dan enkripsi. Tampilan sistem dapat dilihat pada gambar berikut:



Gambar 5. Tampilan Form Input Pesan Rahasia

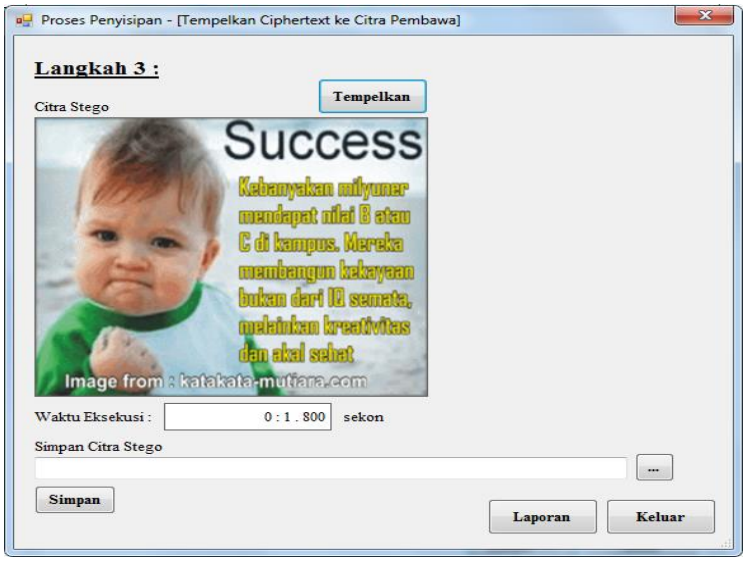
d. Setelah itu, klik tombol ‘Lanjut’ sehingga sistem akan menampilkan proses penempelan pesan rahasia ke citra sampul. Tampilan form Tempelkan Ciphertext ke Citra Pembawa dapat dilihat pada gambar berikut:

ISBN: 2964-1950



Gambar 6. Tampilan Form Tempelkan Ciphertext ke Citra Pembawa

e. Klik tombol ‘Tempelkan’ untuk melakukan proses penyisipan pesan rahasia ke citra sampul. Tampilan form Tempelkan Ciphertext ke Citra Pembawa setelah proses penempelan dapat dilihat pada gambar berikut:



Gambar 7. Tampilan Form Tempelkan Ciphertext ke Citra Pembawa Setelah Proses Penempelan

f. Pilihlah file citra pertama dan kedua yang ingin dibandingkan. Setelah itu, klik tombol ‘Proses’ sehingga sistem akan menampilkan hasil perbandingan, seperti terlihat pada gambar berikut:

ISBN: 2964-1950

Gambar 8. Tampilan Form Hasil Perbandingan Setelah Proses

KESIMPULAN

Setelah menyelesaikan pembuatan perangkat lunak ini, penulis dapat menarik beberapa kesimpulan sebagai berikut:

1. Berdasarkan hasil pengujian, tidak tampak adanya perbedaan antara citra asli dengan citra stego secara kasat mata. Hal ini dapat dilihat pada nilai MSE yang relatif kecil, dimana semakin kecil nilai MSE antara dua buah citra digital berarti bahwa kedua citra tersebut semakin mirip.
2. Proses perubahan / penghapusan bagian tertentu pada citra tidak berdampak pada pesan yang disisipkan, dengan kemungkinan terjadinya perubahan terhadap isi pesan relatif kecil.

DAFTAR PUSTAKA

[1] J. Ilmiah and W. Pendidikan, “2 1,2,3,” vol. 9, no. June, pp. 486–503, 2023.

[2] R. N. Nugraha, S. Remilenita, and N. Hidayah, “Model Perencanaan Metaverse Ar Di Taman Literasi Dalam Mengakses Buku Online,” *J. Inov. Penelit.*, vol. 3, no. 9, pp. 7531– 7538, 2023.

[3] R. Roedavan and B. Pudjoatmodjo, “Implementasi Metaverse Untuk Jagad Creative Sebagai Media Promosi Digital,” vol. 1, no. November, pp. 188–192, 2022, [Online].
Available: https://doi.org/10.26760/rekakarya.v1i3.188-192

[4] R. Wijaya, G. Kosala, and T. Waluyo, “Dunia Baru Pendidikan Di Era Metaverse Untuk Guru Sma Muhammadiyah Cileungsi,” *Pros. COSECANT Community Serv. Engagem. Semin.*, vol. 2, no. 2, 2023, doi: 10.25124/cosecant.v2i2.18681.

[5] A. K. Sari, P. R. Ningsih, W. Ramansyah, A. Kurniawati, I. A. Siradjuddin, and M. K. Sophan, “Pengembangan Kompetensi Guru Smkn 1 Labang Bangkalan Melalui

ISBN: 2964-1950

Pembuatan Media Pembelajaran Augmented Reality Dengan Metaverse," *Panrita Abdi -J. Pengabdi. pada Masy.*, vol. 4, no. 1, p. 52, 2020, doi: 10.20956/pa.v4i1.7620.

[6] R. Gusman and M. E. Apriyani, "Analisis Pemanfaatan Metode Markerless User Defined Target Pada Augmented Reality Sholat Shubuh," *J. INFOTEL - Inform. Telekomun. Elektron.*, vol. 8, no. 1, p. 64, 2016, doi: 10.20895/infotel.v8i1.53.