REVIEW PAPER

"Steganograpy and Visual Cryptography in Computer Forensics"

Disajikan Sebagai Tugas Mata Kuliah Kriptoanalisis Pada

Program Studi Informatika Universitas Udayana

(Dosen Pengampu: I Komang Ari Mogi, S.Kom., M.Kom)

Disusun Oleh:

I Gusti Ngurah Bagus Pramana Putra (1808561030)

Lalu Muhamad Waisul Kuroni (1808561037)

PROGRAM STUDI INFORMATIKA

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS UDAYANA

2021

Steganografi adalah seni, ilmu, atau praktik di mana pesan, gambar, atau file disimpan tersembunyi di dalam pesan, gambar, atau file lain. Konsep steganografi bukanlah hal baru; itu tanggal kembali ribuan tahun ketika pesan digunakan untuk disembunyikan pada hal-hal penggunaan sehari-hari seperti tanda air pada surat, ukiran di sisi bawah meja, dan benda-benda lainnya. Manfaat utama dari steganografi adalah muatannya tidak diharapkan oleh peneliti yang dapat memeriksa data komputer. Orang yang mengirim data tersembunyi dan orang yang dimaksudkan untuk menerima data adalah satu-satunya orang yang mengetahuinya.

Kriptografi, di sisi lain, adalah penyandian dan penguraian data dan informasi dengan kode rahasia. Kriptografi visual menggunakan konsep yang sama kecuali diterapkan pada gambar. Kriptografi visual juga bisa sedikit menipu mata yang tidak berpengalaman, sedemikian rupa sehingga, jika suatu pembagian gambar jatuh ke tangan yang salah, itu akan terlihat seperti gambar noise acak atau seni buruk tergantung pada pengalaman individu.

Steganografi dan kriptografi visual agak mirip dalam konsep. Pada akhirnya, keduanya adalah cara untuk menyembunyikan data dari mata-mata dan dalam banyak kasus dari penyelidik forensik dan keamanan. Dalam steganografi, hanya pengirim dan penerima yang mengetahui data tersembunyi dan biasanya jika file yang dimuat jatuh ke tangan orang lain, mereka tidak akan mencurigai data tersembunyi tersebut. Sedangkan dalam kriptografi, ketika seseorang menerima data yang dienkripsi, hal pertama yang muncul di benak mereka adalah pertanyaan tentang apa yang dienkripsi dan bagaimana mereka dapat mendekripsi pesan yang disembunyikan.

Ada beberapa metode dan algoritma yang berbeda untuk menyembunyikan data dalam berbagai jenis file.

1. IMAGE STEGANOGRAPHY

Salah satu contoh teknik persembunyian lanjutan pada citra adalah dengan menggunakan **layer citra**. Metode ini membagi citra asli menjadi beberapa blok, kemudian membuat layer untuk setiap blok dari nilai biner piksel sebagai matriks. **Langkah kedua** untuk menyembunyikan bit rahasia adalah mencari di dalam baris dan kolom lapisan ini dan mencoba menemukan kecocokan terbaik antara nilai biner piksel yang disembunyikan dan nilai biner piksel tempat kita ingin menyembunyikannya.

Metode ini menyembunyikan lebih sedikit data per blok, hanya menyembunyikan 1 byte dalam blok 8 x 8 piksel sedangkan metode lain seperti metode revisited pencocokan **LSB (Least Significant Bit)** menyembunyikan 1 bit di setiap piksel. Jadi metode ini menyembunyikan lebih

sedikit data per blok yang meningkatkan kinerja dan mempertahankan kualitas gambar yang lebih baik.

Metode Steganografi LSB Kompensasi Dinamis memberikan ketahanan yang lebih tinggi terhadap steganalisis dan analisis histogram. Metode ini menyembunyikan data dalam LSB dari piksel gambar asli, dan kemudian mengkompensasi secara dinamis pada gambar yang dihasilkan. sehingga metode ini terbukti berhasil dalam menghindari perangkat lunak pendeteksi penyembunyian data bahkan ketika rasio penyematan mendekati **100%**.

Dengan kemajuan dalam metode menyembunyikan data dalam gambar dan berbagai cara baru yang dapat menyembunyikan data dalam gambar, kita dapat memperkirakan bahwa ini adalah tantangan yang berkembang bagi penyidik forensik komputer untuk mendeteksi data tersembunyi. Fakta bahwa penyidik forensik komputer dihadapkan dengan **ribuan file gambar** saat melakukan analisis pada mesin cukup menantang, belum lagi kendala **skema persembunyian** yang tahan perangkat lunak pendeteksi.

2. DETECTION OF STEGANOGRAPHY

Deteksi data tersembunyi menghadirkan tantangan besar bagi penyelidik dan individu yang mencari data tersembunyi. Untuk gambar saja, ada ratusan miliar gambar di web dan melihat semuanya akan menjadi tugas yang sangat memakan waktu dan komputasi yang menantang; apalagi jenis file lain yang mungkin dapat disembunyikan datanya. bagaimana jika beberapa algoritma baru. untuk menyembunyikan data dalam gambar muncul? Apakah aplikasi yang digunakan untuk memindai gambar untuk data tersembunyi cocok dan mampu mengungkap data tersembunyi? Dan apakah layak untuk kembali dan memindai ulang semua gambar lagi dengan perangkat lunak yang sama atau perangkat lunak lain yang diperbarui untuk mendeteksi data tersembunyi dengan algoritme baru?

Jawaban atas pertanyaan di atas adalah hampir tidak mungkin untuk dapat memindai atau mencoba mendeteksi data tersembunyi pada cakupan luas dari gambar yang dicurigai secara akurat. Agak lebih mudah bagi penyelidik untuk memindai data tersembunyi dalam skala yang lebih kecil seperti gambar hard drive, tetapi mereka masih dihadapkan pada ketidakakuratan perangkat lunak yang sama dan kemungkinan menemukan algoritme penyembunyian data yang tidak diketahui.

3. OADA Types OF STEGANOGRAPHY

Metode ini tidak memerlukan perangkat atau sistem operasi yang canggih pada perangkat seluler karena penulis bereksperimen menggunakan bahasa pemrograman **J2ME** yang kompatibel dengan sebagian besar ponsel modern. Jadi jika suatu perangkat mampu mengirim **MMS dan SMS**, algoritma ini dapat diimplementasikan di dalamnya.

4. VISUAL CRYPTOGRAPHY

Visual kriptografi adalah cara lain untuk berbagi data yang disembunyikan, kecuali bahwa itu terbatas pada format gambar. Dalam konsep dasarnya, kriptografi visual bekerja sedemikian rupa sehingga gambar dibagi menjadi beberapa bagian yang terlihat seperti white noise, tetapi ketika bagian tersebut dilapis, mereka mengungkapkan gambar yang tersembunyi. Banyak penelitian telah dilakukan di bidang kriptografi visual dan beberapa algoritma telah dikembangkan. Salah satu metode kriptografi visual yang menarik adalah (t,n) Threshold Image Hiding Scheme. Metode ini menyembunyikan gambar rahasia ke dalam jumlah 'n' gambar sampul, dan dapat dipulihkan jika jumlah gambar sampul tersedia 't'. Gambar tersembunyi dapat mencapai 512 warna dengan ukuran sebesar gambar sampul. Metode ini menggunakan polinomial interpolasi Lagrange, hashing MD5, dan tanda tangan RSA untuk mengenkripsi citra yang akan disembunyikan.

Algoritma kriptografi visual lainnya adalah Image Size Invariant Visual Cryptography [7]. Metode ini menyembunyikan gambar rahasia dua nada dan membaginya menjadi transparansi biner yang terlihat seperti gambar noise acak. Setelah transparansi itu ditumpuk satu sama lain, gambar rahasia terungkap. Citra rahasia juga dapat direkonstruksi dengan komputasi XOR dari transparansi. Algoritma ini didasarkan pada metode VSS (Visual Secret Sharing) konvensional. Hasilnya adalah satu set pembagian gambar seperti warna-noise. Karena enkripsi terjadi pada tingkat vektor, pembagian tidak memiliki korelasi dengan gambar asli, yang membuatnya tahan terhadap serangan brute force yang mencoba mendekripsinya. Dengan metode ini, overlay bagian tidak mengungkapkan data apa pun; modul dekripsi harus mendekripsi bagian untuk data yang akan diungkapkan.

5. CONCLUSION

Dalam tulisan ini, definisi steganografi dan kriptografi visual yang telah dibahas bersama dengan beberapa penelitian yang dilakukan pada berbagai algoritma masing-masing jenis. Steganografi dan kriptografi visual memiliki banyak persamaan dan perbedaan, sehingga memiliki berbagai kegunaan dalam dunia digital dan nyata. Algoritma yang berbeda untuk steganografi dan

kriptografi visual memiliki kelebihan dan kekuatan yang berbeda, serta kekurangan dan kelemahan. Jadi kami perhatikan bahwa metode tertentu lebih mudah dideteksi daripada yang lain. Tetapi secara umum, tugas penyidik forensik dan keamanan tidak mudah. Ketika steganografi dan alat deteksi kriptografi visual digunakan secara eksklusif, hampir tidak mungkin bagi para penyelidik untuk mengungkap data yang tersembunyi atau terenkripsi. Di sisi lain, jika alat deteksi ini digunakan bersama dengan alat dan faktor lain yang mempersempit pencarian ke kumpulan data yang agak lebih kecil, maka itu membuat kehidupan penyelidik jauh lebih mudah dan memberi mereka peluang lebih baik untuk mendeteksi data yang mencurigakan.

Kami melihat bahwa menggunakan algoritme dengan metode rekonstruksi yang solid akan memungkinkan kami untuk merekonstruksi bagian kembali ke gambar asli yang tidak diubah. Algoritma ini akan menghadirkan area yang bagus untuk eksplorasi lebih lanjut yang akan membuka lebih banyak tempat di dunia forensik dan anti-forensik. Akan sangat menarik untuk mempelajari bagaimana data dapat dideteksi setelah menerapkan kriptografi visual dengan rekonstruksi sempurna pada gambar dengan data tersembunyi.

Juga, pertanyaan deteksi yang menarik adalah apakah kita dapat merekonstruksi satu set 'n' bagian menjadi gambar bermakna yang berbeda dari gambar yang digunakan untuk membuat bagian tersebut dengan menghilangkan beberapa n bagian asli dan dengan memasukkan bagian tambahan yang dibuat khusus untuk tujuan seperti itu. Pada dasarnya ini adalah pertanyaan tentang keunikan bagian yang dibuat oleh berbagai algoritma kriptografi visual. Jadi, jika kita mendapatkan satu set bagian dan mencoba untuk merekonstruksinya, dapatkah mereka membuat gambar dengan konten ilegal meskipun mereka mungkin tidak berasal dari gambar dengan konten ilegal? Seberapa unik bagian yang kami peroleh dari algoritma kriptografi visual yang berbeda ini dan seberapa besar pengaruh yang dapat diberikan oleh penyelidik yang tidak etis selama proses dekripsi?