Alternatif Penerapan Steganografi dalam Kriptografi Visual

Gloryanson Ginting 13516060
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
13516060@std.stei.itb.ac.id

***Abstrak*—Pada makalah ini akan dibahas sebuah teknik untuk melakukan kriptografi visual dengan hasil share yang dapat menyembunyikan pesan aslinya, dan sekaligus menghasilkan hasil share yang merupakan gambar - gambar lain. Selain itu akan dibahas analisis dan cara kerja kriptografi visual yang telah dibuat.**

***Keywords*—kriptografi visual, steganografi.**

I. PENDAHULUAN

Kriptografi visual merupakan salah satu teknik kriptografi yang dapat menyembunyikan pesan atau gambar dengan cara membagi-bagi pesan atau gambar menjadi beberapa bagian (*share*) sehingga pesan atau gambar aslinya tidak dapat lagi dibaca atau dikenali secara visual menggunakan mata manusia.

Namun hasil pembagian gambar oleh algoritma kriptografi visual ini menjadi sangat tidak jelas dan seperti tidak berarti apa-apa. Hal ini mungkin akan menimbulkan kecurigaan akan adanya pesan penting dalam kumpulan gambar tak berarti tesebut dan mengundang perhatian para penyadap untuk mencari tahu isi pesan tersebut.

Salah satu solusi untuk mengurangi kecurigaan tersebut akan diberikan dalam makalah ini. Teknik yang digunakan adalah dengan membagi pesan atau gambar asli menjadi *share* yang tidak terlalu acak, melainkan menjadi beberapa *share* yang menyerupai gambar atau tulisan yang dapat dibaca atau dikenali secara visual oleh mata manusia.

Dengan demikian, kumpulan *share* yang dihasilkan hanyalah kumpulan gambar – gambar biasa yang tidak terlalu mencurigakan dibandingkan dengan gambar yang berupa noise acak yang dihasilkan oleh kriptografi visual dasar.

II. TEORI PENDUKUNG

1. Kriptografi Visual

Kriptografi visual adalah Teknik kriptografi yang memungkinkan informasi visual seperti gambar, teks, dll. dapat dienkripsi dengan cara tertentu sehingga hasil dekripsi dapat ditampilkan ke dalam gambar visual.

Salah satu teknik yang paling dikenal adalah milik Moni Naor dan Adi Shamir yang dikembangkan pada tahun 1994. Mereka mendemonstrasikan skema *secret sharing* visual, di mana sebuah gambar dipecah menjadi n *shares* sehingga hanya orang – orang yang memiliki semua *shares* dapat mendekripsi gambar tersebut, karena memiliki n-1 *share* saja tidak dapat memungkinkan untuk mendekripsi gambar asli.

2. Skema (k, n)

Satu gambar dibagi menjadi n buah *share*. Untuk mendekripsi, diperlukan paling sedikit k buah *share.* Jika jumlah *share* yang ditumpuk kurang dari k, maka tidak dapat menghasilkan gambar semula.

3. Kriptografi Visual untuk citra biner

Berikut beberapa cara kerja kriptografi visual untuk gambar biner.

1. Tiap pixel muncul pada n buah share
2. Tiap share terdiri dari m buah sub-pixel berwarna hitam dan putih.
3. Dideskripsikan sebagai matriks S berukuran n x m, dimana S[i,j] = 1 jika sub-pixel ke-j pada share ke-i berwarna hitam dan S[i,j] = 0 jika sub-pixel ke-j pada share ke-i bnerwarna putih
4. Penumpukan dua atau lebih share dapat dipandang sebagai operasi “OR”
5. Bobot Hamming (H(V)): Jumlah simbol tidak-nol dalam sebuah vektor dengan m-elemen.
6. Level abu-abu hasil penumpukan share sebanding H(V) dianggap hitam jika $H(V) \geq d$ dan dianggap putih jika $H(V) < d - \alpha m$ dimana d adalah threshold, $1 \leq d \leq m$ dan α adalah level kontras, $\alpha > 0$

4. Steganografi

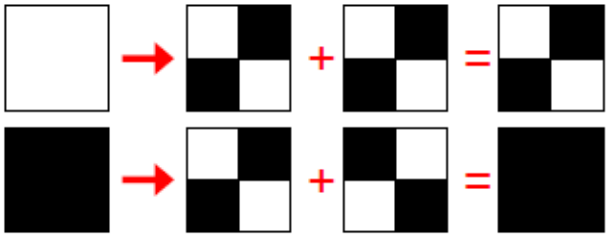
Steganografi merupakan Teknik menyembunyikan pesan ke dalam pesan lain atau sebuah objek fisik. Dalam konteks komputasi/elektronik, sebuah file computer seperti teks, gambar, atau video disembunyikan ke dalam file teks, gambar, atau video lain.

Keuntungan steganografi dibandingkan kriptografi biasa adalah hasil penyisipan pesan rahasia tidak menarik perhatian untuk ditelusuri atau dipecahkan oleh orang yang tidak berkepentingan. Serumit apapun sebuah pesan yang dienkripsi, apabila pesan tersebut dapat dikenali sebagai pesan yang telah dienkripsi, maka akan selalu mengundang perhatian pihak – pihak lain untuk memecahkan pesan tersebut.

III. PEMBAHASAN

1. Implementasi Algoritma

Teknik yang digunakan dalam makalah ini dimodifikasi dari algoritma kriptografi visual untuk citra biner. Pada kriptografi visual biasanya, Gambar atau pesan aslinya akan dibagi menjadi 2 share dengan cara mengkonversi berdasarkan pixel hitam atau putih.

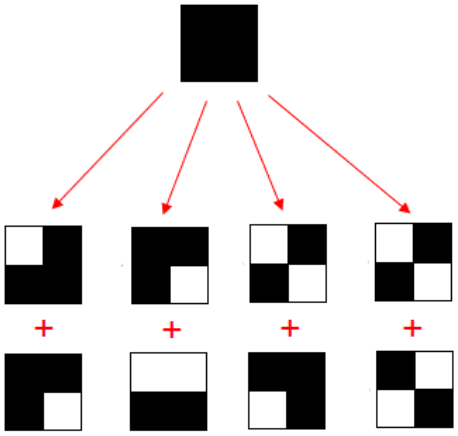


Gambar 3.1. Contoh kombinasi hasil pembagian share 1 dan share 2 untuk masing- masing pixel hitam dan putih pada kriptografi visual biasa

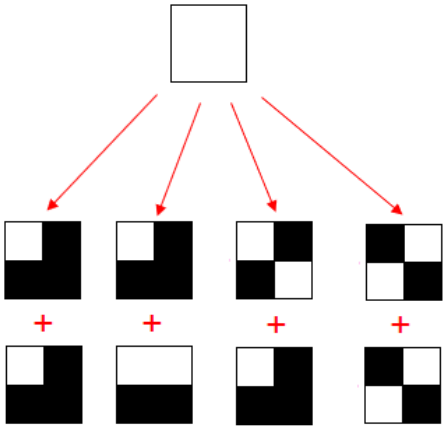
Dalam makalah ini, kombinasi hasil pembagian share 1 dan share 2 akan dimodifikasi. Satu pixel putih yang pada awalnya dibagi menjadi 2 pixel hitam dan 2 pixel hitam diganti menjadi 3 pixel hitam dan 1 pixel putih, sedangkan untuk pixel hitam tetap sama. Hal ini memungkinkan lebih banyaknya kombinasi share 1 dan share 2. Selain itu, kelebihan utama dari teknik ini adalah memungkinkan kita untuk menghasilkan share yang bukan hanya gambar noise yang tidak berarti, melainkan suatu gambar atau teks tertentu yang tidak ada kaitannya dengan gambar atau pesan aslinya.

Pendekatan ini mirip dengan metode steganografi dalam hal mencegah pesan sangat tampak sebagai pesan yang dienkripsi. Namun pada steganografi, hasil share disisipkan ke dalam gambar lain yang sama untuk kedua share, sedangkan pada teknik ini, hasil share itu sendiri yang akan dijadikan menyerupai gambar lain.

Pada dasarnya, teknik ini seolah-olah menambahkan satu level kriptografi visual dari kriptografi visual biasanya. Pada level pertama, yaitu gambar atau pesan asli, pixel putih direpresentasikan dengan 3 pixel hitam dan 1 pixel putih, sedangkan pixel hitam direpresentasikan dengan 4 pixel hitam. Pada level kedua, yaitu hasil share yang juga merupakan gambar, pixel putih akan direpresentasikan dengan 2 pixel putih dan 2 pixel hitam, sedangkan pixel hitam direpresentasikan dengan 3 pixel hitam dan 1 pixel putih.



Gambar 3.2. Contoh kombinasi hasil pembagian share 1 dan share 2 untuk masing- masing pixel hitam



Gambar 3.3. Contoh kombinasi hasil pembagian share 1 dan share 2 untuk masing- masing pixel putih

Pada gambar 3.2 dan 3.3, panah pertama dari kiri menunjukkan salah satu kombinasi pembagian gambar jika pixel pada share 1 dan share 2 keduanya hitam, panah kedua menunjukkan share 1 memiliki pixel hitam dan share 2 pixel putih, panah ketiga menunjukkan share 1 memiliki pixel putih dan share 2 memiliki pixel hitam, dan yang terakhir menunjukkan pixel kedua share berupa pixel putih.

Berikut beberapa kasus yang terdapat dalam pemilihan pixel untuk kedua share:

1. Saat gambar yang disembunyikan memiliki pixel hitam
    a. Saat kedua pixel share hitam, maka untuk share 1 akan dipilih secara acak subpixel yang terdiri dari 3 pixel hitam dan 1 putih, dan untuk share 2 akan dipilih secara acak subpixel yang juga terdiri atas 3 pixel

hitam, namun tidak boleh sama persis dengan share 1 agar tidak menghasilkan pixel putih saat kedua share digabungkan

b. Saat pixel share 1 hitam dan share 2 putih, untuk share 1 akan dipilih secara acak subpixel yang terdiri atas 3 pixel hitam, dan untuk share 2 dipilih subpixel yang terdiri atas 2 pixel hitan dan 2 putih, dengan syarat salah satu pixel hitam pada share 2 harus berada pada posisi yang sama dengan pixel putih share 1.

c. Saat pixel share 1 putih dan share 2 hitam, mirip dengan poin b namun kebalikannya

d. Saat kedua pixel putih, maka share 1 akan dipilih pixel yang terdiri dari 2 hitam dan 2 putih, dan untuk share 2 subpixel yang sama namun harus posisi yang berkebalikan

2. Saat gambar yang disembunyikan memiliki pixel putih
   a. Saat kedua pixel share hitam, maka untuk share 1 akan dipilih secara acak subpixel yang terdiri dari 3 pixel hitam dan 1 putih, dan untuk share 2 akan dipilih secara acak subpixel sama persis dengan share 1 agar menghasilkan satu pixel putih saat kedua share digabungkan

   b. Saat pixel share 1 hitam dan share 2 putih, untuk share 1 akan dipilih secara acak subpixel yang terdiri atas 3 pixel hitam, dan untuk share 2 dipilih subpixel yang terdiri atas 2 pixel hitam dan 2 putih, dengan syarat salah satu pixel putih pada share 2 harus berada pada posisi yang sama dengan pixel putih share 1.

   c. Saat pixel share 1 putih dan share 2 hitam, mirip dengan poin b namun kebalikannya

   d. Saat kedua pixel putih, maka share 1 akan dipilih pixel yang terdiri dari 2 hitam dan 2 putih, dan untuk share 2 subpixel yang sama namun satu pixel putih pada share 1 dan share 2 harus di posisi yang sama (tidak boleh dua pixel)

2. Kode Program

Kode program diimplementasikan dalam bahasa Python. Potongan kode berikut merupakan proses pembagian subpixel ke masing-masing share. Variabel *height* dan *width* adalah tinggi dan panjang gambar asli. Angka “0” merupakan bit untuk pixel hitam dan “255” bit untuk pixel putih.

Fungsi Bb1b2() mengembalikan array yang terdiri atas kombinasi subpixel yang dipilih secara acak, untuk pixel pesan asli hitam (Black), share 1 hitam, dan share 2 hitam. Fungsi Wb1w1() mengembalikan array kombinasi subpixel untuk pixel pesan asli putih (White), share 1 hitam, dan share 2 putih. Dst.

```
for i in range(height):

    for j in range(width):

        if (array[i,j] == 0):

            if (s1[i,j] == 0 and s2[i,j] == 0):
                input = Bb1b2()

            elif (s1[i,j] == 255 and s2[i,j] == 0):
                input = Bw1b2()

            elif (s1[i,j] == 0 and s2[i,j] == 255):
                input = Bb1w2()

            elif (s1[i,j] == 255 and s2[i,j] == 255):
                input = Bw1w2()

        elif (array[i,j] == 255):

            if (s1[i,j] == 0 and s2[i,j] == 0):
                input = Wb1b2()

            elif (s1[i,j] == 255 and s2[i,j] == 0):
                input = Ww1b2()

            elif (s1[i,j] == 0 and s2[i,j] == 255):
                input = Wb1w2()

            elif (s1[i,j] == 255 and s2[i,j] == 255):
                input = Ww1w2()

    share1[i*2][j*2] = input[0]
    share1[i*2][j*2+1] = input[1]
    share1[i*2+1][j*2] = input[2]
    share1[i*2+1][j*2+1] = input[3]

    share2[i*2][j*2] = input[4]
    share2[i*2][j*2+1] = input[5]
    share2[i*2+1][j*2] = input[6]
    share2[i*2+1][j*2+1] = input[7]
```

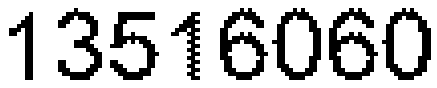
Berikut kode program untuk menyatukan kedua share

```
    for i in range(height*2):

        for j in range(width*2):

            if (share1[i,j] == 255 and share2[i,j] == 255):
                result[i,j] = 255

            else:
                result[i,j] = 0
```

```
result_image = Image.fromarray(result)
result_image.save(result.png')
```

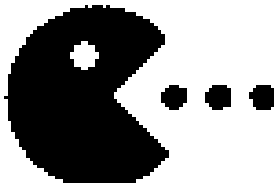
3. Hasil Percobaan

Uji coba sederhana dilakukan pada sebuah gambar citra biner berukuran 100 x 300 pixel



Gambar 3.4. citra asli yang akan di enkripsi

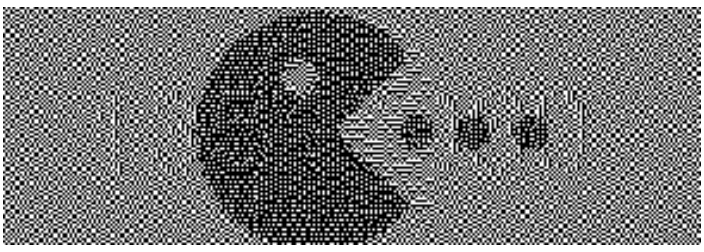
Untuk mendukung teknik ini, digunakan dua buah gambar berukuran 100 x 300 pixel yang tidak ada kaitannya dengan gambar asli pada Gambar 3.4.



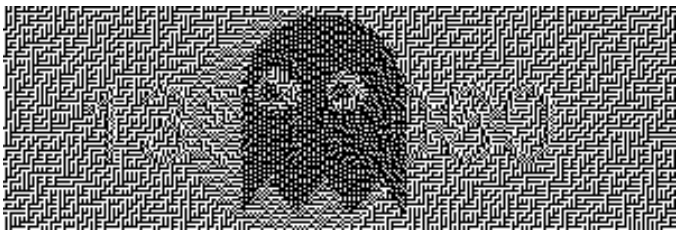
Gambar 3.5. citra pendukung untuk share 1

Gambar 3.6. citra pendukung untuk share 2

Dari proses enkripsi diperoleh kedua share yang masing-masing berukuran 200 x 600 pixel berikut ini

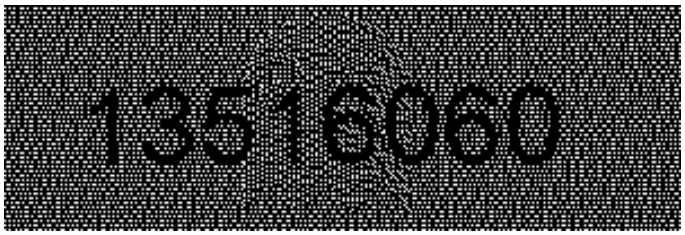


Gambar 3.7. share 1



Gambar 3.8. share 2

Berikut hasil penggabungan kedua share yang berukuran 200 x 600 pixel.



Gambar 3.9. Penggabungan share 1 dan share 2

Pada percobaan ini, kedua share masih terlihat tidak natural dan masih kelihatan pesan asli secara samar-samar jika dilihat dengan teliti. Hal ini diakibatkan pada percobaan, teknik randomisasi untuk pola pembagian share 1 dan share 2 masih terbatas dan belum maksimal.

4. Kelebihan dan Kekurangan

Dibandingkan dengan kriptografi visual biasa, kriptografi visual dengan cara ini dapat menyembunyikan fakta bahwa gambar – gambar yang dikirim bukanlah pesan terenkripsi. Teknik ini menerapkan steganografi, tanpa menggunakan gambar tambahan untuk cover, sehingga ukuran file share yang dikirim lebih kecil dan lebih efisien.

Kekurangan dari teknik ini adalah dengan memilih subpixel dengan tiga pixel hitam dan satu pixel putih sebagai representasi pixel putih mengakibatkan hasil penambahan share 1 dan share 2 menjadi lebih gelap dan sulit dibaca.

VI. KESIMPULAN

Kriptografi visual merupakan cara yang efektif dalam mengenkripsi gambar atau pesan menjadi beberapa share yang tidak dapat dipahami isinya. Namun dengan demikian, hasil share tersebut akan mudah untuk dicurigai dan mengundang perhatian para penyadap.

Teknik ini dapat mengatasi hal tersebut, sekaligus menjadi alternatif yang baik untuk penggunaan steganografi dalam kriptografi visual karena memiliki algoritma yang sederhana namun cukup efektif dan efisien.

REFERENSI

[1] Naor, Moni; Shamir, Adi (1995). "Visual cryptography". Advances in Cryptology — EUROCRYPT'94. Lecture Notes in Computer Science. 950. pp. 1–12. doi:10.1007/BFb0053419. ISBN 978-3-540-60176-0.

[2] Pahati, OJ (2001-11-29). "Confounding Carnivore: How to Protect Your Online Privacy". AlterNet. Archived from the original on 2007-07-16. Retrieved 2008-09-02.

[3] Munir, Rinaldi. Kriptografi Visual, Teori dan Aplikasinya

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 21 Desember 2020

Gloryanson Ginting, 13516060