Evolusi Aplikasi Steganografi Dalam Keperluan Militer

Shifa Salsabiila - 13519106
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jalan Ganesha 10 Bandung
E-mail (gmail): 13519106@std.stei.itb.ac.id

***Abstract*—Makalah ini membahas tentang evolusi aplikasi steganografi dalam keperluan militer. Masalah utama keperluan militer yang dapat diselesaikan dengan steganografi adalah sistem transmisi data rahasia. Steganografi sudah ada sejak lama dan masih terus berkembang hingga saat ini. Makalah ini menjelaskan perkembangan steganografi yang terjadi, serta menampilkan hasil simulasi dari *false* dan *multi-level steganography* yang merupakan metode terkini steganografi. *False* dan *multi-level steganography* meningkatkan level keamanan dari sistem transmisi data menggunakan steganografi dengan menggunakan konsep pesan asli (*real message*) dan pesan semu (*false message*). Meski cukup efektif dalam hal keamanan, *false* dan *multi-level steganography* harus mengorbankan ukuran pesan yang dapat disembunyikan dalam proses transmisi.**

Keywords—contribution; steganography; false steganography; multi-level steganography; message transmission

I. Pendahuluan

Salah satu permasalahan terbesar yang penting dalam keperluan militer adalah transmisi data. Seringkali, proses transmisi data yang dilakukan oleh badan militer suatu negara mengandung banyak informasi rahasia yang harus ditangani secara hati-hati. Salah satu metode yang dapat digunakan untuk mengatasi permasalahan ini adalah steganogradi. Steganografi merupakan suatu teknik untuk menyembunyikan pesan dengan membungkusnya ke dalam suatu pesan atau *file* lain sehingga pesan rahasia yang ingini dikirimkan tidak terlihat oleh pihak yang berada di antara pengirim dan penerima. Umumnya, steganografi menggunakan objek pembungkus yang biasa ditemukan pada konteks pengiriman, sehingga tidak menimbulkan kecurigaan.

Konsep steganografi sudah digunakan sejak sebelum masehi dan terus berkembang hingga saat ini. Saat ini, seiring dengan berkembangnya teknologi, pesan dapat disembunyikan ke dalam *file* audio, video, gambar, serta berbagai kanal komunikasi lainnya. Salah satu poin penting dalam steganografi adalah bahwa pesan yang disembunyikan sebisa mungkin tidak mengalami perubahan setelah diekstraksi kembali dari objek pembungkusnya. Dengan mengacu pada kriteria ini, terdapat banyak perkembangan terhadap metode steganografi, khususnya dalam implementasinya pada keperluan transmisi pesan yang digunakan oleh suatu badan militer.

II. Steganografi di Masa Lalu

Salah satu contoh implementasi steganografi paling awal yang diketahui adalah oleh Histiaeus sekitar lima abad sebelum masehi. Histiaeus melakukan transmisi pesan dengan steganografi menggunakan objek pembungkusnya yaitu manusia, tepatnya salah satu pesuruhnya. Pengiriman pesan ini dilakukan dengan cara menuliskan pesan pada kepala pesuruhnya yang seluruh rambutnya telah dipangkas dan membiarkan hingga rabutnya tumbuh kembali. Pada saat inilah proses transmisi akan dilakukan dengan dikirimkannya pesuruh tersebut kepada penerima pesan. Pada sisi penerima, pesan dapat diekstraksi kembali dengan memangkas rambut pesuruh Histiaeus. Pada saat itu, metode ini merupakan metode yang berfungsi dengan baik, namun tentunya sangat tidak efektif, karena proses pengiriman suatu pesan akan memerlukan waktu yang lama, mengingat bahwa proses tersebut harus menunggu hingga rambut pengirimnya tumbuh terlebih dahulu. Akibatnya, jenis pesan yang dapat dikirimkan dengan metode ini terbatas pada pesan-pesasn yang bersifat tidak *urgent*.

Oleh karena itu, sekitar tahun 480 BC, pada *Battle of Thermopylae* antara *Spartans* dan *Xerxes*, Demaratus memberitahukan *Spartans* bahwa *Xerxes* akan menyerang menggunakan steganografi. Proses transmisi pesan ini dilakukan dengan menggunakan sebuah *wax tablet*. *Wax tablet* merupakan sebuah papan tulis yang terbuat dari kayu yang dilapisi lilin. Dengan pendekatan yang mirip dengan yang dilakukan oleh Histiaeus, Demaratus mengkikis seluruh lapisan lilin yang ada pada *wax tablet*, menuliskan pesan peringatan pada *Spartans*, kemudian menuangkan lapisan lilin baru di atas pesan yang telah dituliskan. Dengan demikian, *wax tablet* yang didalamnya telah terdapat pesan peringatan tersebut dapat dengan mudah dikirimkan kepada *Spartans* tanpa menimbulkan kecurigaan apapun, karena yang terlihat oleh pemeriksanya hanyalah sebuah *wax tablet* kosong. Meski serupa dengan metode yang digunakan oleh Histiaeus, metode ini jauh lebih cepat, karena proses persiapan pengirimannya dapat diatur dan dikerjakan oleh manusia.

Meski demikian, metode yang digunakan oleh Demaratus relatif tetap membutuhkan tenaga yang cukup besar dibandingkan dengan metode-metode yang lebih baru. Pada perang dunia ke-2, diketahui bahwa steganografi juga digunakan oleh Nazi dengan menggunakan beberapa metode. Salah satu metode steganografi yang digunakan oleh Nazi

adalah *invisible ink* atau tinta tak terlihat yang hanya bisa dibaca jika diletakkan di bawah sinar UV. Dengan menggunakan tinta tak terlihat ini, pesan dapat dikirimkan tanpa ada yang mencurigainya. Akan tetapi, ketika metode ini sudah mulai tersebar, metode steganografi ini tidak lagi aman, karena menjadi sangat mudah untuk ditemukan.

Metode steganografi lain yang dikembangkan oleh Nazi adalah yang disebut sebagai *Null Cipher*. *Null cipher* menggunakan manipulasi huruf-huruf pada pesan untuk mengirimkan sebuah pesan rahasia di dalam pesan lain yang tidak rahasia. Kedua pesan, baik yang rahasia maupun yang menjadi objeek pembungkusnya berupa teks tidak terenkripsi dan metode penyisipannya dapat divariasikan untuk setiap pesan yang dikirimkan, sehingga akan membutuhkan usaha yang lebih banyak untuk mencari pesannya dibandingkan dengan metode tinta tak terlihat. Salah satu pesan yang cukup populer yang pernah dikirimkan oleh Nazi dengan menggunakan *Null cipher* adalah sebaga berikut:

> *"Apparently neutral's protest is throughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils."*

Pesan ini terlihat sebagai pesan biasa yang tidak mengandung unsur yang patut dicurigai, namun jika dilihat dengan lebih saksama, pesan ini mengandung sebuah pesan tersirat di dalamnya yang dapat diekstraksi dengan mengambil huruf ke-2 dari setiap kata. Dengan menerapkan aturan tersebut, didapatkan pesan tersembunyi:

> *"Pershing sails from NY June I"*

Implementasi steganografi traadisional lainnya telah digunakan oleh tentara Amerika di Vietnam dengan menggunakan pesan yang dikirimkan dalam bentuk kode morse menggunakan kedipan mata yang dibungkus dengan interaksi manusia yang wajar. Metode ini telah berhasil membantu membebaskan banyak tahanan Amerika di Vietnam. Kode morse yang digunakan mengikuti matriks berikut:

	1	2	3	4	5
1	A . -	B - ..	C, K - . -	D - ..	E .
2	F .. - .	G - - ..	H	I	J . - - -
3	L . - ..	M - - ..	N - .	O - - -	P . - - .
4	Q - - . -	R . - . ..	S	T -	U .. -
5	V ... -	W . - - ..	X -	Y - . - -	Z - - ..

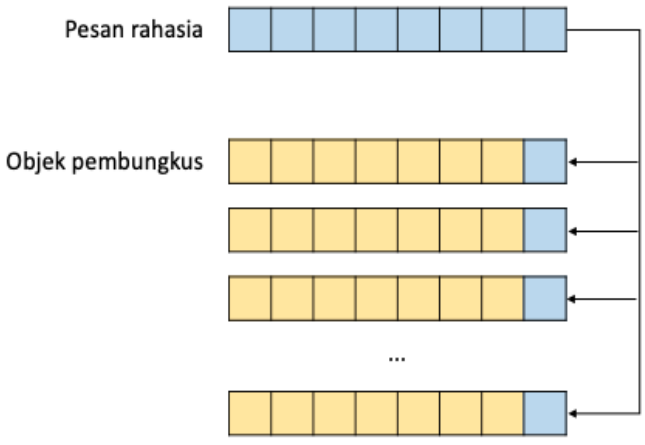
Gambar 1. Matriks kode morse pada perang Vietnam

Sebelumnya telah disebutkan perubahan penggunaan steganografi di masa lampau yang dikategorikan sebagai metode steganografi tradisional. Metode-metode yang telah dijelaskan dianggap sebagai metode tradisional, karena tidak melibatkan teknologi digital. Metode-metode tersebut mungkin memang efektif pada masanya, namun ketika sudah pernah terbongkar rincian metodenya, menjadi sangat mudah untuk kembali dipecahkan. Hal ini menyebabkan metode steganongrafi tradisional sudah tidak lagi aman dan sudah tidak lagi digunakan saat ini. Alasan lain yang menyebabkan metode steganografi tradisional sudah ditinggalkan adalah akibat adanya keterbatasan yang cukup tinggi terkait jenis pesan yang dapat disembunyikannya. Mengingat bahwa metode steganografi tradisional dilakukan secara manual oleh manusia, dibutuhkan usaha yang cukup besar dalam melakukan proses penyembunyian dan penggekstrasikan pesan, sehingga umumnya pesan yang dapat disembunyikan berukuran sangat kecil.

III. Steganografi Saat Ini

Seiring dengan berkembangnya sistem komunikasi digital, hingga saat ini, mayoritas proses komunikasi dilakukan secara digital, steganografi juga berkembang mengikuti *trend* tersebut. Steganografi digital memanfaatkan berbagai jenis media digital seperti *file* text,audio, gambar, serta video sebagai objek pembungkus pesan rahasianya. Steganografi digital telah berhasil meningkatkan kecepatan, keamanan, serta memperluas batasan jenis pesan yang dapat disembunyikan yang sebelumnya terdapat pada steganografi tradisional.

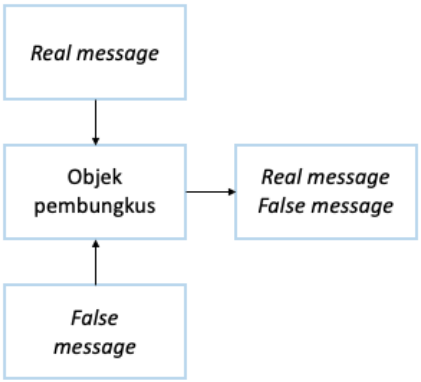
Banyak metode yang digunakan untuk mengimplementasikan steganografi digital. Konsep utama yang biasa digunakan dalam steganografi digital adalah *container modification*, atau melakukan manipulasi terhadap objek pembungkus pesan agar dapat menyimpan pesan rahasia yang tak kasat mata. Salah satu metode yang paling populer dan paling banyak digunakan adalah metode penyisipan *Least Significant Bit* (LSB), yaitu bit paling tidak signifikan pada setiap byte sebuah objek pembungkus akan diubah menjadi potongan bit dari pesan yang ingin dikirmkan. Oleh karena perubahan hanya dilakukan terhadap LSB, objek pembungkus tidak akan menegalami perubahan yang signifikan, bahkan umumnya perubahan yang terjadi tidak akan bisa terdeteksi oleh mata manusia. Metode penyisipan LSB umumnya digunakan bersama objek pembungkus gambar dengan format yang beragam. Pesan yang dapat disembunyikan dengan menggunakan metode penyisipan LSB dapat berupa apapun yang terdiri atas bit-bit, asalkan ukuran pesan yang dikirimkan memenuhi batasan yang dapat ditampung oleh objek pembungkus.



Gambar 2. Diagram metode penyisipan LSB.

Metode ini cukup efektif dalam mengirimkan pesan rahasia dalam konteks yang tidak membutuhkan tingkat kerahasiaan. yang tinggi, karena salah satu masalah yang muncul dengan metode steganografi seperti ini adalah terjadi perubahan terhadap statistika yang dapat diperiksa pada objek pembungkus. Akibatnya, jika sebuah pihak ketiga yang bukan merupakan penerima tujuan memiliki akses terhadap objek pembungkus dan melakukan pemeriksaan terhadap distribusi statistik objek pembungkusnya, pihak tersebut memiliki kemungkinan yang cukup besar untuk menemukan bahwa terdapat pesan tersembunyi di dalam objeke pembungkus. Dengan melakukan steganalisis, maka pihak tersebut dapat juga melakukan ekstraksi terhadap pesan yang tersembunyi. Jika hal ini terjadi, maka steganografi dianggap gagal.

Hal ini perlu menjadi salah satu konsiderasi yang diambil oleh badan militer jika hendak menggunakan steganografi, karena pesan yang ditransmisikan oleh sebuah badan militer memiliki potensi tinggi untuk dicurigai berbagai pihak, sehingga jika hanya menggunakan teknik steganografi sederhana seperti ini, pesan yang dikirim berpotensi tidak aman. Oleh karena itu, saat ini telah dikembangkan steganografi dengan tingkat kedalaman yang lebih dalam untuk keperluan militer. Dua metode yang akan dibahas dan disimulasikan kali ini adalah *false steganography* dan *multi-level steganography*.



Gambar 3. Diagram *false steganography*

A. *False Steganography*

False steganography merupakan modifikasi terhadap steganografi digital yang didesain untuk mempersulit pendeteksian pesan tersembunyi di dalam objek pembungkus. Pada *false steganography*, terdapat dua jenis pesan yang akan disembunyikan di dalam objek pembungkus, yaitu:

- *Real message*, yang merupakan pesan utama yang ingin dikirimkan secara rahasia kepada penerima.
- *False message*, yang merupakan pesan tambahan yang juga disembunyikan di dalam objek pembungkus, tetapi tidak bersifat rahasia. *False message* bertujuan untuk mengelabui pihak ketiga sehingga berpikiran bahwa mereka telah menemuka pesan tersembunyi yang ada di dalam objek pembungkus.

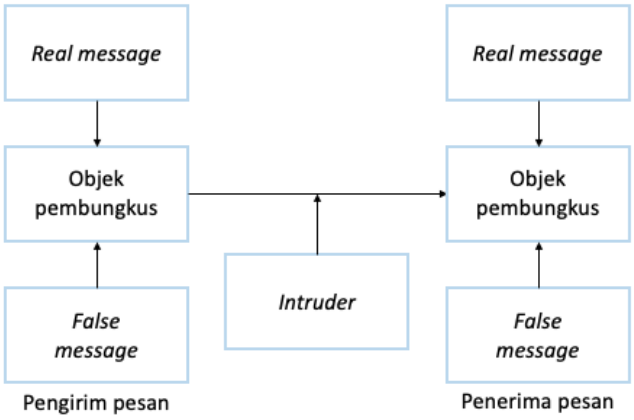
Pada *false steganography*, kedua pesan, *real* dan *false message* akan disembunyikan ke dalam suatu objek pembungkus yang sama. Metode steganografi digital apapun dapat digunakan untuk melakukan *false steganography* ini, dengan catatan bahwa usaha yang dibutuhkan untuk menemukan *real message* harus lebih besar diabndingkan usaha yang dibutuhkan untuk menemukan *false message*. Tentunya, objek pembungkus juga harus lebih besar dan harus dapat menampung kedua pesan, *real* dan *false* dengan baik. Dengan metode ini, kemungkinan besar bahwa jika pesan yang ditransmisikan dicurigai dan dilakukan investigasi oleh suatu pihak yang tidak diinginkan, mereka diharapkan dapat menemukan *false message* terlebih dahulu dan menganggap bahwa mereka sudah berhasil menemukan pesan tersembunyi yang terletak di dalam objek pembungkus. Dengan demikian, diharapkan proses investigasi akan dihentikan dan *real message* tetap aman.

Terdapat tiga kemungkinan hasil dari penggunaan metode *false steganography*, yaitu sebagai berikut:

1. Tidak ada pesan, *real* ataupun *false* yang berhasil terdeteksi – kasus sukses
2. *False message* berhasil terdeteksi, dan *real message* tidak berhasil terdeteksi – kasus sukses
3. *Real message* berhasil terdeteksi, tanpa peduli *false message* terdeteksi atau tidak – kasus gagal.

Pada *false steganography*, baik penerima maupun pengirim tidak mempedulikan apakah *false message* terdeteksi atau tidak, karena fungsi dari *false message* hanya sekedar untuk mengelabui saja. Sama dengan steganografi digital pada umumnya, penerima membutuhkan sebuah kunci untuk dapat mengekstraksi *real message* dari objek pembungkusnya. Umumnya, penerima tidak perlu tahu cara ataupun bahkan keberadaan dari *false message*.

Metode ini dapat menyelesaikan masalah perubahan statistik objek pembungkus yang sebelumnya menjadi masalah pada steganografi digital sederhana, karena meskipun sebuah pihak telah mencurigai adanya pesan tersembunyi di dalam objek pembungkus dan melakukan investigasi lanjutan, kemungkinan besar, pesan yang akan berhasil diekstraksi adalah *false message*. Berikut medupakan gambaran cara kerja *false steganography*:

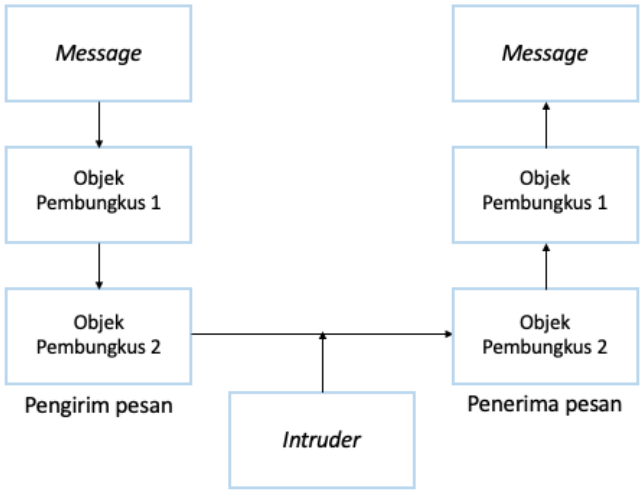


Gambar 4. Diagram *false steganography* dalam proses transmisi

B. *Multi-level Steganography*

Metode penyembunyian *real message* dan *false message* pada *false steganography* saling independen satu sama lain, sehingga meeskipun seharusnya didesain agar *false message* lebih mudah ditemukan dibandingkan *real message*, tetap mungkin bagi suatu pihak untuk menemukan *real message* terlebih dahulu. Hal ini merupakan salah satu kelemahan *false steganography* yang ditangani oleh *multi-level steganography*. Secara umum, *multi-level steganography* menggunakan konsep yang serupa dengan *false stegapnography*, namun dibuat suatu kaitan antara *real message* dan *false message*. Pada *multi-level steganography*, *real message* akan dibungkus ke dalam suatu objek pembungkus yang akan berperan sebagai *false message*. Selanjutnya, *false message* ini akan dibungkus lagi ke dalam suatu objek pembungkus lainnya. Hal ini dapat dilakukan hingga beberapa *level*, sehingga diberikan nama *multi-level steganography*.

Berbeda dengan *false steganography*, *multi-level steganography* tidak memungkinkan suatu pihak untuk mengekstraksi *real message* tanpa mendapatkan *false message* terlebih dahulu. Berikut gambaran alur untuk metode *multi-level steganography*:



Gambar 5. Diagram *multi-level steganography* dalam proses transmisi

IV. SIMULASI

Seperti yang telah disebutkan sebelumnya, *false steganography* ataupun *multi-level steganography* dapat dimplementasikan menggunakan metode steganografi digital apapun. namun untuk simulasi yang akan dibahas pada makalah ini, yang akan digunakan adalah metode penyisipan LSB pada objek pembungkus berupa gambar digital. Seperti yang telah dijelaskan pada bagian sebelumnya, metode penyisipan LSB dilakukan dengan menggantikan LSB dari setiap byte menjadi bit dari pesan yang akan disembunyikan. Oleh karena itu, salah satu hal yang dapat dilakukan untuk menerapkan *false steganography* adalah dengan menyembunyikan *false message* pada LSB dari objek pembungkus, dan menyembunyikan *real message* pada bit ke-2 (ke-2 paling tidak signifikan) pada objek pemebungkus. Oleh karena LSB merupakan metode yang banyak diketahui, secara intuitif, pengecekan terhadap LSB akan lebih mungkin dilakukan seseorang yang ingin mencoba mencari letak pesan rahasianya. Dengan demikian, diharapkan keberadaan *false message* pada LSB dapat menjaga *real message* agar tidak terbongkar.

Proses penyisipannya sendiri akan mengikuti langkah-langkah berikut. Pertama, akan dibangkitkan sebuah kunci yang akan digunakan sebagai *seed* untuk menentukan permutasi bit dari pesan yang akan disisipkan. Proses ini perlu dilakukan untuk mempersulit proses ekstraksi pesan, karena jika pesan hanya disisipkan secara sekuensial, proses ekstraksi oleh pihak luar akan sangat mudah. selanjutnya, dengan mengikuti urutan hasil permutasi, setiap LSB objek pembungkus akan diganti dengan satu bit dari *false message*, dan bit ke-2 paling tidak signifikan dari setiap byte juga akan digantikan dengan satu bit dari *real message*.

Untuk proses ekstraksi di sisi penerima, dibutuhkan juga kunci steganografi yang sebelumnya digunakan pengirim. Kunci ini akan kembali digunakan untuk membangkitkan urutan permutasi. Selanjutnya, dengan mengikuti urutan permutasi dari urutan paling akhir hingga paling awal, penerima dapat menyusun kembali pesan yang tersembunyi sehingga didapatkan pesan asli secara utuh. Berikut merupakan potongan kode dalam bahasa Python dari proses *encoding* dan *decoding* suatu pesan menggunakan metode penyisipan LSB.

Penyisipan dan pengekstraksian pesan:

```
def encode(message, srcFile, destFile, random, *s):
    img = Image.open(srcFile, 'r')
    width, height = img.size
    size = imgSize(img)[0]
    n = imgSize(img)[1]
    array = np.array(list(img.getdata()))

    message = addDelim(message)

    #Encode
    i = 0
    order = generatePxOrder(size, random, s)

    for a in order:
        for b in range(0, 3):
            if i < msgSize:
                array[a][b] =
int(bin(array[a][b])[2:9] + message[i], 2)
                i += 1

    array=array.reshape(height, width, n)
    enc_img = Image.fromarray(array.astype('uint8'),
img.mode)
    enc_img.save(destFile)
    print("Image Encoded Successfully")
```

```
def decode(srcFile, destFile, fileFormat, random,
*s):

    img = Image.open(srcFile, 'r')
    size = imgSize(img)[0]
    array = np.array(list(img.getdata()))

    decoded_bits = ''

    order = generatePxOrder(size, random, s)
    for p in order:
        for q in range(0, 3):
            decoded_bits += (bin(array[p][q])[2:][-
1])
    print(decoded_bits[-40:])
    decoded_bits = [decoded_bits[i:i+8] for i in
range(0, len(decoded_bits), 8)]

    #Cracking the message
    messageChar = ""
    for i in range(len(decoded_bits)):
        if messageChar[-5:] == "!@#$%":
            break
        else:
            messageChar += chr(int(decoded_bits[i],
2))

    if _DELIMITER in messageChar:
        noDelim = messageChar[:-5]
        if fileFormat == "txt":
            print("Hidden Message:", noDelim)
        msgbin = binstr2bin(str2bin(noDelim))
        print(decoded_bits[:-5])
        savefile(msgbin, destFile, fileFormat)

    else:
        print("No Hidden Message Found")
```

Metode ini dapat digunakan dengan efektif, karena penggantian bit paling akhir ataupun kedua paling akhir pada suatu gambar digital tidak mengubah tampilan keseluruhan gambar secara signifikan, sehingga tidak dapat terlihat perbedaannya oleh manusia tanpa melakukan analisis lebih lanjut. Berikut merupakan contoh hasil penyembunyian pesan dengan menggunakan *false steganography*.

Gambar 6. (a) *real message* (b) *false message* yang akan disembunyikan

Gambar 7. (a) Objek pembungkus *original* (b) Objek pembungkus dengan *real message* (c) Objek pembungkus dengan *false message* (d) Objek pembungkus dengan *real* dan *false message*

Pada implementasi *false steganography* di atas, dapat dilihat bahwa hasil akhir objek pembungkus tidak terlihat perbedaannya oleh mata manusia, dengan *false message* diletakkan pada bit paling tidak signifikan dan *real image* diletakkan pada bit kedua paling tidak signifikan. Hasil ini dapat dicapai, karena ukuran gabungan dari *real message* dan *false message* masih jauh lebih kecil dibandingkan ukuran dari objek pembungkus. Dengan menggunakan contoh gambar yang sama, dapat diterapkan juga simulasi untuk *multi-level steganography*. Dalam metode ini, pertama, *real message* akan disisipkan ke dalam *false message* dengan menggunakan metodoe LSB. Di sini, *false message* akan berperan juga sebagai objek pembungkus pertama. Selanjutnya, *false message* akan kembali disisipkan ke dalam objek pembungkus utamanya. Dalam metode ini, ukuran *real* message harus lebih kecil dibandingkan ukuran *false message,* dan ukuran *false message* juga harus lebih kecil dibandingkan ukuran objek pembungkus utamanya. Berikut diberikan hasil simulasi *multi-level steganography*.

Gambar 8. (a) *real message* (b) *false message* yang telah disisipkan *real message*

Gambar 9. (a) Objek pembungkus *original* (b) Objek pembungkus dengan *false message* yang mengandung *real message* di dalamnya

V. KESIMPULAN

Konsep steganografi sudah ada sejak dahulu kala dan sudah banyak juga diterapkan dalam transmisi informasi pada keperluan militer. Steganografi dapat diimplementasikan menggunakan metode-metode tradisional serta digital. Saat ini, salah satu metode terbaru steganografi yang meningkatkan keamanan proses transmisi informasi adalah dengan menggunakan *false* atau *multi-level steganography*. Kedua metode ini bertujuan untuk mengelabui pihak yang tidak diinginkan dengan cara menyisipkan *false message* ke dalam objek pembungkus.

Seiring dengan berkembangnya zaman dan teknologi, steganografi menjadi lebih cepat, aman, dan pilihan untuk pesan yang dapat ditransmisikan juga bertambah semakin banyak. Kedepannya, implementasi steganografi juga dapat digabungkan dengan konsep-konsep lainnya, seperti menggunakan suatu sistem enkripsi sebelum penyisipan pesan. Proses enkripsi bahkan juga dapat diterapkan pada *false message* agar lebih meyakinkan pihak luar. Saat ini, terdapat beragam metode steganografi yang dapat dipilih kecocokannya dengan situasi yang sedang berlangsung. Kedepannya, pilihan metode steganografi berpotensi untuk semakin banyak lagi.

UCAPAN TERIMA KASIH

Penulis ingin mengucapkan puji syukur kepada Tuhan Yang Maha Esa, karena telah diberikan kemudahan dalam menyelesaikan karya tulis ini. Selain itu, penulis juga ingin mengucapkan tereima kasih kepada Bapak Dr. Ir. Rinaldi Munir, M.T. yang telah memberikan wawasan mengenai ilmu kriptografi dengan jelas sehingga penulis dapat menyelesaikan penulisan karya tulis ini.

REFERENSI

[1] Bailey K, Curran K (2005) Steganography—The Art of Hiding Information. Booksurge Publishing

[2] Castiglione A, De Santis A, Soriente C (2007) Taking advantages of a disadvantage: Digital forensics and steganography using document metadata. J Syst Softw 80(5):750–764

[3] Cox IJ, Miller ML, Bloom J, Fridrich J, Kalker J (2008) Digital watermarking and steganography. Morgan Kaufmann Publishers, Burlington

[4] Hachaj T, Ogiela MR (2012) Framework for cognitive analysis of dynamic perfusion computed tomography with visualization of large volumetric data. J Electron Imag 21(4):043017

[5] Nagaraj V, Vijayalakshmi V, Zayaraz G (2013) Color Image Steganography based on Pixel Value Modification Method Using Modulus Function. IERI Procedia 4:17–24

[6] Ogiela L, Ogiela MR (2011) Semantic analysis processes in advanced pattern understanding systems. In: Kim TH et al (eds) Communications in Computer and Information Science, vol. 195. Springer, Berlin, Heidelberg, pp 26–3

[7] Subhedar MS, Mankar VH (2014) Current status and key issues in image
steganography: a survey. Comput Sci Rev 13–14:95–113

[8] Tang M, Hu J, Song W (2014) A high capacity image steganography using multi-layer embedding. Optik 125:3972–3976

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.

Jakarta, 20 Desember 2021

Shifa Salsabiila - 13519106