

APLIKASI KRIPTOGRAFI VISUAL PADA DOKUMEN KEUANGAN

Dion Jogi Parlinggoman (13509045)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganessa 10 Bandung 40132, Indonesia
13509045@std.stei.itb.ac.id

Abstract—Kriptografi visual adalah teknik untuk memudahkan pengamanan dalam pengiriman data. Algoritma pada kriptografi visual sederhana dan tidak kompleks dibandingkan dengan komputasi pada algoritma lainnya. Namun, dibutuhkan suatu kondisi untuk memecahkan daerah “abu-abu” pada suatu dokumen. Kriptografi visual membutuhkan kondisi fisik penglihatan yang prima pada seseorang. Jadi, apabila kriptografi visual diterapkan pada dokumen keuangan, manusia akan mengalami kesulitan dalam membedakan digit secara akurat. Dengan bantuan *threshold technique*, dokumen yang menggunakan kriptografi visual akan dapat dilihat jelas dan hampir identik. Meskipun kriptografi visual membutuhkan penyimpanan yang besar, algoritma yang sederhana, keamanan, dan transmisi yang cepat adalah keunggulan dari kriptografi visual yang membuat hal ini layak sebagai alternatif dalam mengirim dokumen penting.

Index Terms—Kriptografi visual, *Threshold Technique*, Dokumen Keuangan.

I. PENDAHULUAN

Pada bab ini akan dibahas mengenai latar belakang, rumusan masalah dan batasan masalah dalam pembuatan makalah ini.

A. Latar Belakang

Dengan penggunaan internet dalam bisnis saat ini yang universal, kebutuhan untuk berbagi dokumen keuangan melalui media ini meningkat. Sebuah kriptografi visual yang sederhana dan cepat dalam memberikan perlindungan privasi ketika terjadi transmisi data yang sensitif/rahasia antar ruangan maupun perusahaan. Kriptografi visual juga membuat sulit bagi penerima untuk mengubah data asli, sehingga teknik ini dapat mempertahankan keaslian dokumen. Selain itu, gambar akhir yang terlihat dapat diperoleh hanya dengan sistem visual dari manusia. Namun, teknik ini mempunyai kekurangan terkait dengan biaya penyimpanan yang meningkat. Namun, jika dilihat terkait biaya penyimpanan disk yang terus menurun, masalah ini menjadi kurang berarti.

Kriptografi visual mengambil salah satu dokumen keuangan, lalu direpresentasikan sebagai sebuah file peta bit, dan dipecah menjadi dua atau lebih file peta bit yang disandikan. File tersebut dapat ditransfer ke penerima

melalui surat elektronik. Untuk melihat isi yang identik dengan dokumen asli, penerima hanya perlu memiliki bagian yang diinginkan dari beberapa file dan urutan pemecahan file tersebut.

B. Rumusan Masalah

Sistem pada kriptografi visual memberikan efek “abu-abu” atau gambar yang didekode menjadi kabur dan jauh lebih gelap dari gambar asli. Hal inilah adalah salah satu alasan bagi pendekatan ini untuk tidak menjadi teknik yang kompetitif pada keamanan aplikasi/data.

C. Batasan Masalah

Pada makalah ini akan dibahas hal-hal mengenai teori kriptografi visual, beserta keuntungan dan masalah. Di dalam tulisan ini juga akan dilampirkan notasi matematika dan contoh-contoh terkait dengan kriptografi visual.

II. DASAR TEORI

Pada bab ini akan dibahas mengenai kriptografi visual.

A. Kriptografi Visual

Pada tahun 1994, Naor dan Shamir menyajikan buah pikiran terkait dengan dunia kriptografi berdasarkan level pixel. Hal ini disebut kriptografi visual dan diperkenalkan sebagai metode untuk mengenkripsi hal-hal seperti catatan dari tulisan tangan, gambar, serta teks yang diketik dan disimpan sebagai gambar.

Model Dasar

Ada 2 model kriptografi visual yang sebagai pesan rahasia dikodekan menjadi dua transparansi, satu transparansi mewakili cipherteks dan potongan yang lain sebagai kunci rahasia. Kedua transparansi tampak sebagai titik-titik yang acak ketika diperiksa oleh masing-masing individu dan tidak memberikan informasi tentang data pada file yang asli. Namun, dengan menyelaraskan beberapa potongan gambar, pesan rahasia yang asli dapat direproduksi. Proses memecahkan pesan yang sebenarnya dilakukan dengan sistem visual manusia.

Naor dan Shamir memaparkan skema kriptografi visual adalah hal yang terlibat pada pembagian data menjadi pesan rahasia yang dapat dilihat sebagai kumpulan pixel hitam dan putih. Setiap pixel dalam gambar asli diwakili oleh setidaknya satu sub-pixel di setiap n transparansi /

potongan yang dihasilkan. Setiap potongan gambar (transparansi) terdiri dari koleksi m hitam dan putih sub-pixel yang mewakili pixel pada data asli tertentu.

	Share 1	Share 2	Reconstructed pixel
Version 1			 white pixel
			 black pixel
Version 2			 white pixel
			 black pixel

Gambar 2.1 Kejadian pada 2 potong peta bit pada kriptografi visual.

Pada gambar diatas, pixel putih digambarkan dengan gabungan 4 sub-pixel yang berwarna gabungan, antara hitam dan putih. Sedangkan ketika potongan dalam contoh ini menghasilkan pixel hitam asli dipandang sebagai hitam, Namun, pixel putih mengambil skala “abu-abu”.

Struktur yang diperoleh baik dari representasi pixel putih atau hitam pada gambar 2.1 dapat dijelaskan oleh sebuah matriks boolean $n \times m$ S_p dimana $p \in \{\text{putih, hitam}\}$. Setiap unsur tertentu dari matriks S mengatakan S_{ij} , dianggap menjadi bernilai 1 jika dan hanya jika sub-pixel ke- j dalam transparansi ke- i yang berwarna hitam. Ketika transparansi n benar sejajar, hitam yang dihasilkan sub-pixel adalah nilai **OR** dari kolom untuk masing-masing, baris i_1, i_2, \dots, i_n pada potongan S . Gambar 2.1 pada versi pertama akan menggambarkan i_1 dan i_2 . Oleh karena itu, dengan 2 x 4 matriks Boolean akan diperoleh:

$$S_{white} = \{\{1, 0, 0, 1\}, \{1, 0, 0, 1\}\}$$

dan

$$S_{black} = \{\{1, 0, 0, 1\}, \{0, 1, 1, 0\}\}.$$

Setiap nilai pada elemen matriks menggambarkan potongan-potongan gambar masing-masing secara visual.

Karena m sub-pixel merupakan satu pixel asli dan efek visual keseluruhan dari sebuah sub-pixel hitam di salah satu potongan menyebabkan sub-pixel tertentu ketika digabungkan menjadi hitam, pemeriksaan tingkat “abu-abu” adalah cara penentuan warna asli dari pixel

tertentu. Tingkat “abu-abu” dari gabungan potongan gambar itu setara dengan berat **Hamming** $H(V)$ dari **ORed** m -vektor V . Gabungan sub-pixel diinterpretasikan oleh sistem visual manusia sebagai pixel hitam jika $H(V) \geq d$ dan sebagai pixel putih jika $H(V) < d - am$ untuk beberapa batas nilai, yakni $1 \leq d \leq m$ dan perbedaan relatif $\alpha \geq 0$. Penggunaan batas ambang nilai d dan perbedaan relatif α diperlukan untuk membedakan antarwarna.

Pemecahan k keluar dari Soal Rahasia Sharing n Visual

Naor dan Shamir mengembangkan teknik ini dengan memperluas skema kriptografi visual yang awal dengan memecahkan k dari n potongan rahasia. Sebuah kasus pada kriptografi visual yang diterapkan pada k dari n potongan bisa dimulai dengan menghasilkan n potongan dari gambar rahasia yang asli terlebih dahulu. N potongan dapat didistribusikan melalui beberapa metode untuk n peserta yang berbeda tanpa pengetahuan sebelumnya dari potongan mereka. Untuk melihat gambar asli, k dari n peserta harus berkolaborasi pada potongan mereka. Setiap k dari n peserta bisa mengungkapkan pesan rahasia, tapi lebih sedikit dari k peserta tidak bisa mengungkapkan informasi sama sekali.

Model **threshold** identik dengan yang di atas tetapi juga mencakup dua koleksi matriks Boolean $n \times m$ yaitu S_0 dan S_1 . S_0 bertindak sebagai matriks yang memilih secara acak matriks S untuk mewakili pixel putih sementara tindakan S_1 sebagai matriks yang memilih secara acak matriks S untuk mewakili pixel hitam Matriks yang dipilih sehingga membentuk warna subpixel m di masing-masing dari n transparansi (potongan).

Dalam rangka untuk memastikan bahwa kriptanalisis terbatas kekuasaannya sehingga tidak dapat mendapatkan informasi tentang gambar asli dengan memeriksa lebih sedikit dari k transparansi, kondisi yang harus ada:

1. Untuk setiap S di S_0 , nilai **boolean** **OR** V dari setiap k dari n baris memenuhi $H(V) < d - am$.
2. Untuk setiap S di S_1 , nilai **boolean** **OR** V dari setiap k dari n baris memenuhi $H(V) \geq d$.
3. Untuk setiap himpunan bagian $\{i_1, i_2, \dots, i_q\}$ dari $\{1, 2, \dots, n\}$ dengan $q < k$, kedua koleksi D_t matriks $q \times m$ dimana $t \in \{0, 1\}$ diperoleh dengan membatasi tiap matriks $n \times m$ di S_t ke baris i_1, i_2, \dots, i_q yaitu dibedakan dalam artian bahwa tidak ada cara untuk menentukan D_t yang digunakan untuk menghasilkan pixel putih dan yang digunakan untuk menghasilkan pixel hitam.

Dua hal yang pertama disebut sebagai **kontras** sedangkan kondisi ketiga disebut sebagai **keamanan**.

Tambahan

Alih-alih menggunakan k dari skema pembagian n diatas, Ateniese dkk. mampu membuat subset dari n potongan berkualitas yang akan dapat memulihkan citra visual rahasia. Setiap potongan yang tidak memenuhi

syarat tidak akan memiliki informasi mengenai citra rahasia.

Formulasi matematika yang digunakan untuk enkripsi sama dengan Naor dan Shamir, tetapi dengan definisi dan tata nama yang lebih tepat. Mereka juga menggunakan dua matriks $n \times m$ yang akan digunakan untuk mendistribusikan potongan sesuai dengan pixel putih atau hitam. S_0 dan S_1 disebut matriks dasar untuk skema *threshold* (k, n) pada kriptografi visual dengan skema ekspansi m pixel dan c kontras dengan ketentuan bahwa sifat berikut dipenuhi untuk setiap subset X dari $\{i_1, i_2, \dots, i_p\}$:

- 1) jika $X = \{i_1, i_2, \dots, i_p\}$ dengan $p \geq k$, maka nilai *OR* baris i_1, i_2, \dots, i_p dari S_1 memiliki berat setidaknya tx
- 2) jika $X = \{i_1, i_2, \dots, i_p\}$ dengan $p \geq k$, maka nilai *OR* baris i_1, i_2, \dots, i_p S_0 memiliki berat setidaknya $tx - c$
- 3) jika $X = \{i_1, i_2, \dots, i_p\}$ dengan $p \leq k-1$, maka matriks $p \times m$ dua diperoleh dengan membatasi S_0 dan S_1 ke baris i_1, i_2, \dots, i_p yang identik sampai kolom permutasi.

Tingkat abu-abu dari pixel hitam dan putih masing-masing adalah t_x/m dan $(t_x - c)/m$. Kontras relatif, c/m , juga memainkan peran yang sangat penting dalam menentukan visibilitas gambar. Semakin besar kontras relatif, semakin mudah untuk sistem visual manusia untuk secara jelas memilih garis yang berbeda pada gambar ditumpangtindihkan.

III. APLIKASI KRIPTOGRAFI VISUAL

Kriptografi visual dirancang untuk memungkinkan pengguna untuk dengan mudah mengirimkan gambar dan dokumen, misal penyebaran dengan internet. Proses pengkodean terdiri dari mengambil gambar asli dan membagikan n potongan yang disimpan sebagai file individual. Keamanan melalui kriptografi visual membutuhkan distribusi yang tepat pada pengiriman n potongan. Misalnya, tidak melampirkan seluruh n potongan pada satu pesan surat elektronik, namun lebih baik untuk menyebarkan n potongan dengan mengirimkan beberapa email tersebut kepada penerima yang berbeda. Hal ini akan memaksa sejumlah penerima untuk bekerja sama dalam menghasilkan gambar yang identik dengan gambar asli. Sejak masalah k dari n potongan terselesaikan, intersepsi dari setiap potongan akan menjadi tidak berguna. Secara umum, strategi harus dipikirkan bila menggunakan kriptografi visual yang mengambil keuntungan dari pembagian file individual dan teknik pengiriman yang berbeda. Bila foto adalah *spreadsheet*, karena sedang dikirim sebagai bitmap, penerima tidak dapat dengan mudah mengubah angka di pada file individual.

3.1 Pengaruh “Abu-abu”

Salah satu keterbatasan yang paling jelas dari penggunaan kriptografi visual adalah masalah dari penyatuan berbagai file individual yang mengandung efek “abu-abu” secara keseluruhan karena sisa hitam dari

subpixel yang didapatkan saat pengkodean (proses enkripsi). Ini terjadi karena gambar yang didekode (direkonstruksi) bukan produksi tepat, tapi perluasan dari dokumen asli, dengan ekstra hitam pixel. Pixel hitam dalam dokumen asli tetap ada pixel hitam dalam versi didekode, tetapi pixel putih menjadi “abu-abu”. Hal ini menyebabkan hilangnya *kekонтрасан* pada keseluruhan gambar. Subpixel hitam tambahan tersebut pada gambar menyebabkan gambar menjadi terdistorsi. Masalah ini tidak bisa diterima karena angka yang digunakan dalam dokumen keuangan harus jelas terlihat dan berjumlah banyak.

Untuk mengatasi masalah ini, solusi dibutuhkan untuk melakukan penyaringan menggabungkan *threshold technique* dan mengubah ukuran, untuk mengembalikan citra hasil dekode ke bentuk yang identik dengan aslinya. Untuk menyaring efek “abu-abu”, solusi yang dapat ditawarkan adalah pasca pengolahan penerimaan file individual dapat menyaring pixel “abu-abu” dan menjadikan dokumen tersebut ke bentuk aslinya. Solusi ini juga harus mengevaluasi setiap himpunan m subpixel terhadap batas tertentu; pixel berwarna hitam jika jumlah subpixel hitam di atas ambang dan putih jika di bawah ambang batas.

3.2 Analisis Solusi

Tujuan utama dari aplikasi ini adalah untuk mengambil gambar grafis dan membangkitkan beberapa file individual. Aliran data terdiri dari file grafis yang dikodekan ke dalam beberapa file menggunakan beberapa format file.

Encoding dan Decoding

Opsi encoding digunakan untuk memilih fitur terkait, misalnya 4 dari 6. Artinya proses pembangunan file individual dapat berjumlah 6. Namun, jumlah file individual yang diperlukan untuk menggabungkan (proses tumpang tindih) hanya memerlukan file individual sejumlah 4 buah. Hal ini telah dibahas pada bab sebelumnya.

Solusi ini menggunakan dua matriks *boolean* seperti dijelaskan di bab sebelumnya untuk mengkodekan gambar asli menjadi n file. Setiap matriks *boolean* berisi matriks pengkodean pixel hitam dan putih masing-masing. Matriks *boolean* yang digunakan untuk mengkodekan pixel hitam dan pixel putih, dipilih:

$$B = \{\{0011\ 1100\}, \{0101\ 1010\}, \{0110\ 1001\}, \{1100\ 0011\}, \{1010\ 0101\}, \{1001\ 0110\}\}$$

$$W = \{\{001\ 10011\}, \{0101\ 0101\}, \{0110\ 0110\}, \{1100\ 1100\}, \{1010\ 1010\}, \{1001\ 1001\}\}.$$

Misal, file individual yang diinginkan berjumlah 2. Ketika sebuah matriks tertentu baik dari B atau W dipilih secara acak selama encoding, empat bit pertama dari matriks tersebut digunakan untuk file # 1 dan empat bit kedua digunakan untuk file # 2. Karena pengkodean

memaksa empat bit untuk mewakili satu bit gambar asli di setiap saham, ukuran berbagi file yang dihasilkan akan lebih besar dari file gambar aslinya.

Pilihan decoding melibatkan dua langkah terpisah: *overlay* (proses tumpang tindih) file individual, dan menyaring gambar yang dihasilkan menggunakan didirikan *threshold technique*. Proses *overlay* hanya melakukan operasi AND pada file yang digunakan saat ini.

Setelah proses decoding, yakni penggabungan file individual, proses penyaringan dimulai dengan melihat subpixel yang mewakili pixel asli. Setelah pemeriksaan subpixel, nilai ambang kemudian digunakan untuk menentukan apakah pixel pada gambar hasil dekode akan berwarna hitam atau putih. Hal ini memastikan bahwa setiap pixel dalam gambar yang didekode akan cocok dengan pixel dikodekan dari gambar asli.

3.3 Threshold Technique

Threshold adalah salah satu metode yang banyak digunakan untuk segmentasi gambar. Hal ini berguna dalam membedakan latar depan dari latar belakang. Dengan memilih nilai ambang T yang memadai, gambar tingkat "abu-abu" bisa dikonversi menjadi citra biner. Citra biner harus berisi semua informasi penting tentang posisi dan bentuk obyek tertentu (latar depan). Keuntungan dari memperoleh citra biner terlebih dahulu adalah mengurangi kompleksitas data dan menyederhanakan proses pengakuan dan klasifikasi. Cara yang paling umum untuk mengonversi gambar *gray-level* ke citra biner adalah untuk memilih satu nilai ambang (T). Kemudian, semua nilai tingkat keabuan bawah ini T akan diklasifikasikan sebagai hitam (0), dan mereka T di atas akan menjadi putih (1). Masalah segmentasi menjadi salah satu dalam memilih nilai yang tepat untuk ambang T . Sebuah metode yang sering digunakan untuk memilih T adalah dengan menganalisis histogram dari jenis gambar yang ingin disegmentasi. Kasus yang ideal adalah ketika histogram hanya menyajikan dua mode dominan dan *valley* yang jelas (bimodal). Dalam hal ini nilai T dipilih sebagai lembah titik antara dua mode. Dalam aplikasi nyata histogram lebih kompleks, dengan banyak puncak dan lembah tidak jelas, dan tidak selalu mudah untuk memilih nilai dari T .

Teknik Threshold

Teknik Threshold adalah salah satu teknik penting dalam citra segmentasi. Teknik ini dapat dinyatakan sebagai:

$$T = T [x, y, p(x, y), f(x, y)] \quad (1)$$

Ket:

T : nilai threshold.
 x, y : koordinat titik nilai ambang.
 $p(x, y), f(x, y)$: titik-titik pixel gambar tingkat abu-abu.

Gambar *threshold* $g(x, y)$ dapat didefinisikan:

$$g(x, y) = \begin{cases} 1 & \text{jika } f(x, y) > T \\ 0 & \text{jika } f(x, y) \leq T \end{cases} \quad (2)$$

Makalah ini menerapkan lima teknik ambang:

1. Teknik Rata-rata

Teknik ini menggunakan nilai rata-rata dari pixel sebagai nilai ambang batas dan bekerja dengan baik dalam kasus yang ketat dari gambar yang memiliki sekitar setengah pixel dari objek dan setengah lainnya untuk latar belakang. Kasus dengan teknik jarang terjadi.

2. Teknik P-Tile

Teknik ini menggunakan pengetahuan tentang ukuran area objek yang diinginkan untuk digunakan sebagai *threshold*. Teknik ini adalah salah satu metode yang paling awal berdasarkan histogram tingkat keabuan. Teknik ini mengasumsikan objek dalam foto adalah lebih terang dari latar belakang, dan menempati persentase tetap dari gambar daerah. Persentase tetap ini dari bidang gambar juga dikenal sebagai $P\%$. Nilai ambang didefinisikan sebagai tingkat abu-abu yang sebagian besar sesuai dengan pemetaan setidaknya $P\%$ dari tingkat abu-abu pada objek.

Misalkan n adalah nilai maksimum tingkat abu-abu, $H(i)$ menjadi histogram gambar ($i = 0..n$), dan P adalah perbandingan luas objek. Algoritma P-Tile adalah sebagai berikut:

$$S = \text{sum}(H(i)) \quad (3)$$

$f = s$

For $k=1$ to n

$f = f - H(k-1)$

If $((f/t) < p)$ then stop

$T = k$

Ket:

S : keseluruhan bidang gambar

f : menginisialisasi semua daerah sebagai daerah objek

T : nilai ambang akhir

Metode ini sederhana dan cocok untuk semua ukuran objek. Ini menghasilkan kemampuan *anti-noise* dengan baik, namun jelas tidak berlaku jika perbandingan luas objek tidak diketahui atau bervariasi dari gambar ke gambar.

3. Teknik Histogram Dependent (HDT)

Histogram ini bergantung pada keberhasilan memperkirakan nilai ambang batas yang memisahkan dua kemiripan wilayah dari objek dan latar belakang dari suatu gambar. Hal ini mengharuskan, pembentukan citra menjadi dua kesamaan dan akan menjadi daerah terpisah dan gambar itu memiliki nilai ambang batas yang memisahkan wilayah ini.

HDT cocok untuk gambar dengan kemiripan besar dan akan terpisah daerah di mana semua area objek dan latar belakang yang mirip kecuali daerah antara objek dan latar belakang.

Teknik ini dapat dinyatakan sebagai:

$$C(T) = P_1(T)\sigma_1^2(T) + P_2(T)\sigma_2^2(T)$$

Ket:

- C (T) : variansi dalam kelompok.
- P1 (T) : probabilitas untuk kelompok dengan nilai yang kurang dari T.
- P2 (T) : probabilitas untuk grup dengan nilai lebih besar dari T.
- $\sigma_1(T)$: variansi dari kelompok pixel dengan nilai yang kurang dari atau sama
- T. $\sigma_2(T)$: variansi dari kelompok pixel dengan nilai lebih besar dari T.

4. Teknik EMT

Gambar yang digunakan *threshold* dengan menggunakan **Edge Maximization Technique** (EMT) dapat digunakan bila ada lebih dari satu wilayah yang homogen dalam gambar atau di mana ada perubahan pada pencahayaan antara objek dan yang latar belakang. Dalam hal ini bagian dari objek dapat digabung dengan latar belakang atau bagian dari latar belakang mungkin sebagai obyek. Untuk alasan ini, apapun dari seleksi ambang otomatis menjadi jauh lebih baik dalam gambar dengan homogen besar dan daerah benar-benar terpisah. Teknik segmentasi ini tergantung pada pengetahuan tentang ambang batas tepi maksimum dalam gambar untuk memulai segmentasi pada citra dengan bantuan teknik deteksi tepi operator.

5. Teknik Visual

Teknik ini meningkatkan kemampuan orang untuk secara akurat mencari item tertentu. Teknik ini mirip dengan teknik *P-Tile* bahwa mereka semua menggunakan segmen komponen gambar asli dengan cara baru untuk meningkatkan kinerja pencarian visual tetapi berbeda dari *P-Tile* yaitu tidak aktif ketika kebisingan hadir dalam gambar.

Contoh Penggunaan Threshold



Gambar 3.1 Gambar Asli



Gambar 3.2 Teknik rata-rata



Gambar 3.3 Teknik P-Tile



Gambar 3.4 Teknik EMT



Gambar 3.5 Teknik HDT



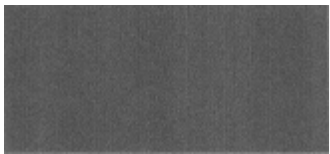
Gambar 3.6 Teknik Visual

3.4 Contoh Pesan Hello World

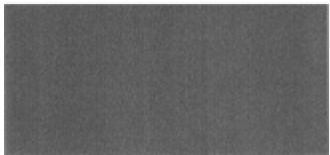
Contoh pesan standar dunia pemrograman Hello World. Pesan asli, berupa bitmap file yang monokrom dengan dimensi 640 x 480 pixel ditunjukkan pada gambar 3.7. Meskipun ini adalah pesan yang relatif sederhana, namun berisi sebuah karakteristik yang dapat menyebabkan masalah ketika gambar visual dikodekan dan diterjemahkan, yaitu : kurangnya garis lurus. Gambar asli akan dikodekan pada 2 file individual, yakni gambar 3.8 dan gambar 3.9.



Gambar 3.7 File Asli



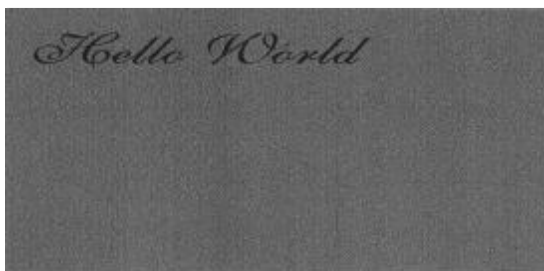
Gambar 3.8 File Individual 1



Gambar 3.9 File Individual 2

Gambar 3.8 dan gambar 3.9 tidak memberikan informasi mengenai pesan asli Hello World sama sekali. Masing-masing dari saham adalah file bitmap monokrom dengan dimensi 1280 x 960 pixel. Peningkatan dimensi terjadi karena perluasan gambar karena pengkodean.

Kemudian, file individual akan saling ditimpa untuk mencari informasi pada pesan asli. Hal ini ditunjukkan pada gambar 3.10. Tidak ada algoritma dekripsi yang digunakan dan pesan yang identik dengan gambar asli sekarang terlihat. Namun, efek “abu-abu” terlihat dan akan sangat tidak dapat diterima dengan *spreadsheet*.



Gambar 3.10 Hasil penimpaan 2 file individual



Gambar 3.11 Hasil penimpaan 2 file individual disertai penyesuaian nilai subpixel dan penyaringan nilai dengan *threshold*

V. KESIMPULAN

Penggunaan kriptografi visual pada pengiriman dokumen melalui internet mempunyai keuntungan, yakni :

1. Algoritma pembagi sangat mudah.
2. Potongan dapat disisipkan *watermark*.
3. Pesan dapat dipecah dan dikirim kepada berbagai penerima.

Penggunaan *threshold* pada dokumen yang digabungkan dari berbagai file dapat dilakukan untuk mengurangi efek “abu-abu”. Penggunaan teknik *threshold* untuk kriptografi visual bernilai relatif terhadap masing-masing gambar karena kesulitan dalam penentuan nilai ambang dan persyaratan dari masing-masing teknik.

REFERENSI

- [1] www.wikipedia.org diakses 4 Mei 2012.
- [2] Salem Saleh Al-amri, N.V. Kalyankar, Khamitkar S.D, *Image Segmentation by Using Thershold Techniques*, 5 Mei 2010.
- [3] Bochert, Bernd, *Segment-based Visual Cryptography*, 2007.
- [4] Malar, Shiny, Kumar, Jeya, *Error Filtering Schemes for Color Images in Visual Cryptography*, 2011.

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, 11 Mei 2012

Ttd,



Dion Jogi Parlinggoman
13509045