Studi, Analisis, dan Perbandingan Modifikasi Kriptografi Visual *Segment-based* dan *Pixel-based*

Mira Yunarti [1)]

1) Program Studi Teknik Informatika ITB, Bandung 40135, email: if14009@students.if.itb.ac.id

Abstract *– Kriptografi visual adalah kriptografi yang diterapkan terhadap gambar/citra, dan sama sekali tanpa menggunakan komputasi kriptografi seperti yang biasa dilakukan pada teknik-teknik kriptografi lainnya. Pada awal pengembangannya, proses enkripsi kriptografi visual dilakukan dengan membagi citra menjadi sejumlah bagian (share), sedangkan proses dekripsinya cukup dilakukan dengan menumpuk bagian-bagian tersebut. Proses pembagian ini dilakukan berdasarkan pixel dari citra atau gambar. Selama pengembangannya, sudah banyak dilakukan modifikasi terhadap teknik ini. Yang akan dibahas dalam makalah ini adalah salah satu contoh modifikasinya, yaitu kriptografi visual yang segment-based, yang diperkenalkan oleh Bernd Borchert. Pembuatan bagian-bagian pesan sandi dibuat berdasarkan bagian-bagian display yang terlihat oleh indera penglihat manusia. Selanjutnya aka nada analisis dan perbandingan dengan kriptografi visual dasar yaitu yang pixel-based.*

Kata Kunci*: kriptografi, kriptografi visual, pixel-based, segment-based.*

1. PENDAHULUAN

Kriptografi berasal dari bahasa Yunani yang terdiri dari 2 kata, yaitu *kryptos* yang berarti menyembunyikan dan *grafi* yang berarti menulis, dan arti seutuhnya adalah seni dan ilmu untuk menyembunyikan pesan menjadi kode-kode yang tidak dapat dibaca oleh pihak yang tidak berhak. Menurut catatan sejarah, kriptografi sudah ada sejak dahulu kala. Kriptografi sudah digunakan oleh bangsa Mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir.

Aspek-aspek keamanan yang dibutuhkan dalam kriptografi adalah sebagai berikut :

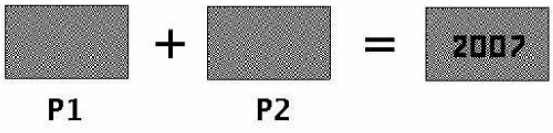
1. *Confidentiality*, yaitu kemampuan untuk menjaga agar isi pesan yang ditransmisikan tidak diketahui oleh pihak-pihak yang tidak berhak untuk mengetahuinya.
2. *Data integrity*, yaitu kemampuan untuk menjamin bahwa pesan masih utuh saat sampai ke penerima, atau dengan kata lain pesan tidak dimanipulasi saat di perjalanan.
3. *Authentication*, yaitu kemampuan untuk mengidentifikasi kebenaran pihak-pihak yang terlibat dalam komunikasi dan kebenaran sumber pesan.
4. *Non-repudiation*, yaitu kemampuan untuk mencegah pihak-pihak yang terlibat dalam komunikasi melakukan penyangkalan terhadap komunikasi yang dilakukan.

Dalam kriptografi, pihak yang saling berkirim pesan akan melakukan dua proses, yaitu proses enkripsi yang dilakukan oleh pengirim pesan dan proses dekripsi yang dilakukan oleh penerima pesan. Proses enkripsi adalah proses penyandian pesan asli (*plainteks*) menjadi pesan rahasia (*ciphertext*). Kemudian cipherteks dikirimkan kepada penerima pesan melalui saluran komunikasi terbuka. Pada saat penerima pesan menerima cipherteks, maka pesan rahasia tersebut diubah lagi menjadi pesan asli melalui proses dekripsi sehingga pesan tadi dapat dibaca kembali oleh penerima pesan.

Hingga saat ini sudah ada banyak variasi algoritma untuk enkripsi dan dekripsi. Salah satunya muncul kriptografi visual untuk file gambar.

Kriptografi visual pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir dalam jurnal *Eurocrypt'94* tahun 1994. Kriptografi jenis ini hanya dapat diterapkan terhadap gambar/citra, dan sama sekali tanpa menggunakan komputasi kriptografi seperti yang biasa dilakukan pada teknik-teknik kriptografi lainnya.

Versi dasarnya merepresentasikan sistem *sharing* rahasia 2-2. Maksudnya adalah dari sebuah gambar hitam putih P dihasilkan dua gambar P1 dan P2. P1 dan P2 dua-duanya adalah acak, yang merupakan distribusi acak dari pixel hitam dan putih, serta tidak menunjukkan informasi apapun. Namun saat P1 dan P2 ditumpuk, maka akan terlihat gambar asli P, dengan kontras hilang sebanyak 50 %. Contoh dari kriptografi visual dapat dilihat pada Gambar - 1.



Gambar - 1 Contoh kriptografi visual

Kriptografi visual mempunyai kekuatan enkripsi – *netime-pad*. Apabila hanya dimiliki P1, maka informasi P tidak dapat diketahui tanpa ada P2. Bahkan komputasi secanggih apapun tetap tidak akan dapat menemukan P bila salah satu *share* tidak ada. Dengan kata lain, sistem enkripsi dengan kriptografi visual *unbreakable.*

Beberapa ekstensi dan modifikasi kriptografi visual telah diperkenalkan. Dari 2-2 ke *m-n (pixel-based)*. Ada juga yang menambahkan fitur steganografi ke kriptografi visual. Variasi lainnya yaitu kriptografi visual untuk gambar berwarna, dimana pixelnya tidak hanya berwarna hitam dan putih. Dan masih banyak variasi lainnya, termasuk kriptografi visual dengan enkripsi berdasarkan segmen (*segment-based)*.

2. KRIPTOGRAFI VISUAL *PIXEL-BASED*

Metode kriptografi visual *pixel-based* yang diajukan Shamir dan Naor, membagi gambar berdasarkan pixel-pixel gambarnya. Misalkan sebuah gambar terdiri dari pixel-pixel berwarna hitam dan putih. Setiap pixel ditampilkan dalam n versi yang telah diubah (disebut *shares*), satu untuk setiap transparensi. Setiap *share* merupakan kumpulan *m* subpixel hitam dan putih yang dicetak berdekatan dengan yang lain sehingga sistem visual manusia dapat melihatnya secara umum sebagai gambaran hitam atau putih.

Struktur yang dihasilkan dapat digambarkan dengan *n* x *m* matriks Boolean $S = [s_{ij}]$ dimana $s_{ij} = 1$ jika dan hanya jika subpixel ke *j* pada transparensi ke *I* berwarna hitam. Bilamana transparensi i_1, i_2, … i_r berpotongan atau bertumpuk dalam satu daerah dimana semestinya sejajar antar subpixelnya, dapat dilihat gabungan *share* yang subpixel hitamnya direpresentasikan oleh Boolean "*or*" pada baris ke i_1, i_2, … i_r dalam S. Level abu-abu pada kombinasi *share* ini sebanding dengan Hamming Weight $H(V)$ dari *m*-vektor V yang "or". Level abu-abu ini diinterpretasi oleh sistem visual *user* sebagai hitam apabila $H(V) \geq d$ dan putih jika $H(V) < d - \alpha m$ untuk sejumlah *threshold* tetap $1 \leq d \leq m$ dan perbedaan relatif $\alpha > 0$. Dengan perhitungan Hamming Weight setiap level abu-abu diinterpretasi sebagai hitam atau putih.

Gambar - 2 Contoh shares *pixel-based*

Warna hitam yang dihasilkan oleh subpixel pada suatu transparensi tidak bisa dinegasikan oleh subpixel pada tranparensi lain. Maka dampaknya akan muncul sejumlah *noise* pada proses enkripsi yang *noise* tersebut tidak dapat dihilangkan saat proses dekripsi.

Proses yang telah dijelaskan di atas berlaku untuk skema linier, dengan perbedaan pentingnya ialah dasar struktur algebraiknya merupakan semi kelompok, bukan kelompok. Secara khusus, efek visual dari subpixel hitam dalam salah satu transparensi tak dapat terlepas warna subpixel di transparensi lain yang ada di atasnya. Aturan monotonisitas ini menunjukkan teknik enkripsi umum yang menambahkan *noise* secara acak ke teks asli selama proses enkripsi, dan mengurangi *noise* yang sama dari cipherteks selama proses dekripsi. Hal inipun menunjukkan model yang lebih natural dimana pixel putih direpresentasikan dengan hanya kumpulan subpixel putih dan pixel hitam direpresentasikan dengan hanya kumpulan subpixel hitam.

Solusi untuk skema *k* dari *m* terdiri dari dua buah matriks Boolean yang berukuran *n* x *m*, C_0 dan C_1. Untuk membagi pixel putih, dipilih salah satu dari matriks C_0, dan untuk membagi pixel hitam dipilih salah satu dari matriks C_1. Matriks yang telah dipilih merupakan representasi dari *m* subpixel yang terletak pada masing-masing *n* transparensi. Solusi benar apabila memenuhi seluruh kondisi berikut :

1. Untuk sembarang matriks *m* pada C_0, hasil operasi "or" dengan *V* pada sembarang baris *k* dari *n* memenuhi $H(V) < d - \alpha m$.
2. Untuk sembarang matriks *m* pada C_1, hasil operasi "or" dengan *V* pada sembarang baris *k* dari *n* memenuhi $H(V) < d - \alpha m$.
3. Untuk sembarang $j < k$ baris yang dipilih, submatriksnya muncul dengan frekuensi yang sama pada C_0 dan C_1.

Terdapat tiga buah parameter yang mempengaruhi kualitas kriptografi visual, yaitu :

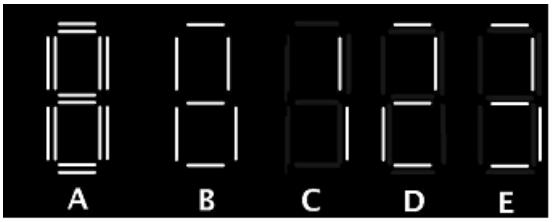
1. *m*, jumlah pixel dalam *share*. Semakin besar nilai *m* maka semakin besar jumlah *noise* yang ditimbulkan. Oleh karena itu nilai *m* diusahakan sekecil mungkin.
2. α, perbedaan relatif antara *share* yang telah digabung dari pixel hitam dan putih. Semakin besar nilai α akan semakin baik.
3. *r,* ukuran C_0 dan C_1. Nilai *r* untuk C_0 dan C_1 tidak harus sama. Nilai *log r* merepresentasikan jumlah bit acak yang diperlukan untuk menciptakan *share* tanpa mengalami penurunan kualitas gambar

3. KRIPTOGRAFI VISUAL *SEGMENT-BASED*

Kriptografi visual dengan teknik ini pada dasarnya menggunakan tampilan *sevent-segmen* yang telah ditemukan pada 1908.Tampilan *sevent-segment* menggunakan tujuh buah bar, yang mana tiga diantaranya horizontal dan empat sisanya vertikal. Dengan menandai subset yang dipilih pada ketujuh segment, akan dapat direpresentasikan digit 0, .., 9, seperti yang terlihat pada Gambar - 3.

Gambar - 3 Tampilan *seven-segment*

Sejumlah tampilan segmen diberikan untuk menampilkan beberapa symbol tertentu, sebagai contoh tampilan *seven-segment* yang dapat menampilkan kumpulan digit 0, …, 9. Prinsip dari kriptograsi visual diaplikasikan ke tampilan segmen, yaitu untuk setiap segmen S yang digambar, baik dalam background hitam atau putih, dua segmen-segmen paralel S1 dan S2 yang dekat satu sama lain namun tidak saling bersilangan. Sebagai contoh adalah bagian A pada Gambar – 4.



Gambar - 4 Prinsip kriptografi visual diaplikasikan ke tampilan segmen

Seperti kriptografi visual yang *pixel-based*, langkah pertama adalah menghasilkan *share* acak. Dalam hal segmen berarti dari setiap pasangan segmen S1 dan S2 salah satu dipilih secara acak. Segmen ini dibiarkan tetap putih, sama dengan transparensi, sedangkan segmen parallel lainnya dihitamkan seperti dasar dari *share*. Pemilihan acak ini dapat dilihat pada bagian B Gambar - 4.

Anggap simbol tertentu akan dimunculkan. Maka subset dari segmen pada tampilan segmen ditandai dengan tujuan untuk menunjukkan simbol tersebut :

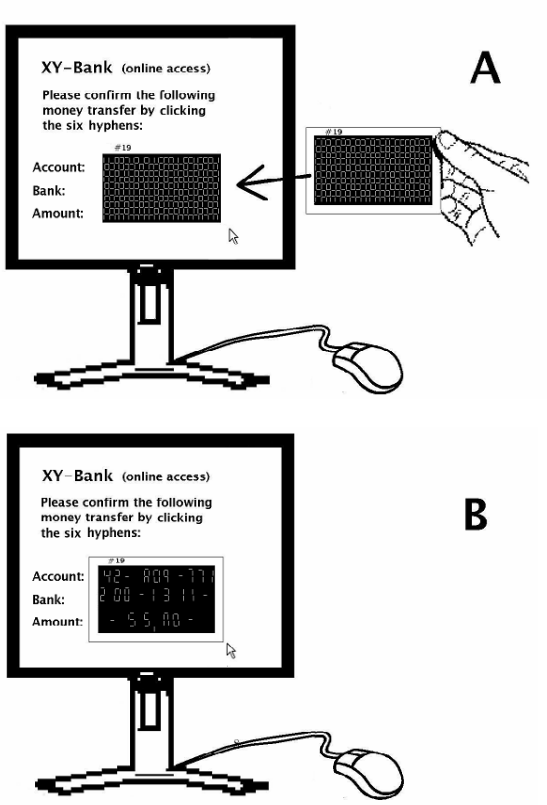
- Jika segmen S termasuk ke subset ini, maka pada *share* kedua seleksi yangs ama antara S1 atau S2 dibuat seperti pada *share* acak yang ditandai, dan segmen paralel lainnya dihitamkan. Langkah ini akan menimbulkan efek dua *shares* yang menumpuk terlihat sebagai segmen putih.
- Sedangkan jika segmen S tidak termasuk ke dalam subset tersebut, maka *share* kedua segmen lain pada kedua segmen paralel S1 atau S2 ditandai, dan segmen terpilih pada segmen acak dihitamkan. Langkah ini menimbulkan efek dalam hal menumpukkan 2 *shares* maka segmen ini tidak menunjukkan area putih.

Secara keseluruhan, segmen-segmen yang termasuk ke dalam subset A menunjukkan area transparensi saat dua *shares* bertumpuk. Setelah penumpukan, simbol akan terlihat. Sebagai contoh pada bagian C Gambar - 4, *share* kedua dipilih untuk menunjukkan digit 1, terihat segmen transparensi. Bagian D dan E Gambar - 4 *share* kedua yang dipilih menunjukkan digit 2 dan 3. Catat bahwa *share* pertama untuk bagian C, D, dan E adalah sama.

4. ANALISIS KRIPTOGRAFI VISUAL *SEGMENT-BASED* DAN PERBANDINGAN DENGAN *PIXEL-BASED*

Kriptografi Visual juga dapat diaplikasikan terhadap kumpulan simbol yang direpresentasikan oleh jenis tampilan segmen lain, sebagai contoh ada sebuah tampilan *fourteen-segment* yang cukup banyak diketahui. Tampilan ini memungkinkan untuk merepresentasikan seluruh huruf dan digit angka.

Kriptografi visual yang *segmen-based* dapat digunakan untuk aplikasi keamanan *online banking*. Teknik ini diterapkan untuk konfirmasi pengiriman uang, yaitu enkripsi nomer tabungan, jumlah pengiriman, dan lain-lain. Lebih lengkapnya dapat dilihat pada Gambar – 5.



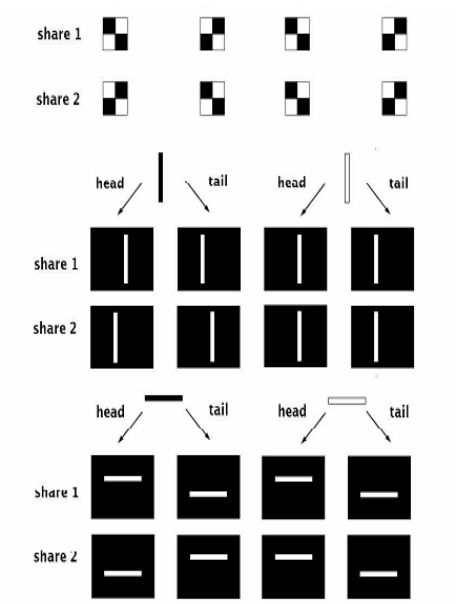
Gambar - 5 Contoh aplikasi pada keamanan *online banking*

Prinsip yang dijelaskan pada bagian sebelumnya dapat dibandingkan dengan *pixel-based*. *Share* pertama adalah diacak, namun tidak menyingkap informasi apapun terutama informasi yang dikodekan dalam pesan. Dengan argumentasi yang sama seperti kriptografi visual *pixel-based*, *share* kedua juga acak. Dapat dibuktikan dengan untuk setiap segmen S kemungkinan untuk memilih S1 adalah ½, independen dengan segmen lainnya.

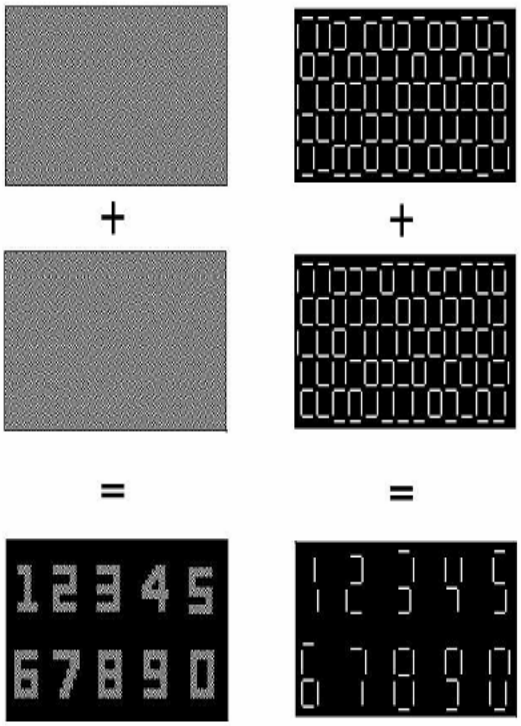
Kelebihan kriptografi visual *segment-based* jika dibandingkan dengan kriptografi *pixel-based* adalah :

1. Kriptografi visual *segment-based* lebih mudah diimplementasikan untuk mengatur dua *shares*, terutama dalam hal *transparency-on-screen*.
2. Simbol-simbol pada kriptografi visual *segment-based* lebih mudah dikenali oleh mata manusia, terutama dalam hal *transparency-on-screen*.
3. Dalam kriptografi visual *segment-based* lebih sedikit bit acak yang dibutuhkan, yang merupakan suatu keuntungan apabila *randomness* yang sebenarnya (bukan hanya *pseudo-randomness*) digunakan dalam sistem enkripsi.
4. Kriptografi visual *segment-based* akan lebih mudah dimengerti dan dipercaya oleh pengguna yang bukan ahli sistem enkripsi, ketimbang kriptografi visual *pixel-based*.

Perbedaan kriptografi visual *segment-based* dan *pixel-based* dalam hal *share* dapat dilihat pada Gambar – 6.



Gambar - 6 Kriptografi Visual *pixel-based vs segment-based*



Gambar - 7 Contoh kriptografi visual *pixel-based* (kiri) dan *segment-based* (kanan)

5. KESIMPULAN

Kriptografi visual diterapkan terhadap gambar/citra, dan sama sekali tanpa menggunakan komputasi kriptografi seperti yang biasa dilakukan pada teknik-teknik kriptografi lainnya. Pada awal pengembangannya, proses enkripsi kriptografi visual dilakukan dengan membagi citra menjadi sejumlah bagian (*share*), sedangkan proses dekripsinya cukup dilakukan dengan menumpuk bagian-bagian tersebut. Proses pembagian ini dilakukan berdasarkan pixel dari citra atau gambar. Kriptografi visual jenis ini dikenal dengan *pixel-based*.

Selama pengembangannya, sudah banyak dilakukan modifikasi terhadap teknik ini. Ada yang menyatukan antara steganografi dengan kriptografi visual. Pengembangan lainnya yaitu teknik enkripsi citra berwarna .

Kriptografi visual yang segment-based, yang diperkenalkan oleh Bernd Borchert. Pembuatan bagian-bagian pesan sandi dibuat berdasarkan bagian-bagian *display* yang terlihat oleh indera penglihat manusia.

Kriptografi visual *segment-based* memiliki beberapa kelebihan dibandingkan dengan *pixel-based*, diantaranya :

1. Lebih mudah diimplementasikan untuk mengatur dua *shares*.
2. Lebih mudah dikenali oleh mata manusia.
3. Lebih sedikit bit acak yang dibutuhkan, yang merupakan suatu keuntungan apabila *randomness* yang sebenarnya (bukan hanya *pseudo-randomness*) digunakan dalam sistem enkripsi.
4. Lebih mudah dimengerti dan dipercaya oleh pengguna yang bukan ahli sistem enkripsi, ketimbang kriptografi visual *pixel-based*.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Diktat Kuliah IF5054 Kriptografi*, Departemen Teknik Informatika Institut Teknologi Bandung, 2006.

[2] M. Naor and A. Shamir, *Visual Cryptography*. Eurocrypt 1994: 1-12.

[3] Borchert, Bernd, *Segment-based Visual Cryptography*. Berlin, 2007.

[4] W.-G. Tzeng and C.-M. Hu, *A New Approach for Visual Cryptography, Designs, Codes, and Cryptography,* Vol. 27, No. 3, pp. 207-227, 2002.

.