Kriptografi Visual Berbasis Segmentasi

Rio Cahya Dwiyanto 13506041
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
IF16041@students.if.itb.ac.id

Abstract—Salah satu versi dari Visual Kriptografi yang disajikan yang tidak berbasis pixel tapi berdasarkan segmentasi. Hal ini digunakan untuk mengenkripsi pesan yang terdiri dari simbol-simbol yang dapat diwakili oleh suatu segmen layar. Sebagai contoh, angka desimal 0;…; 9 dapat diwakili oleh tampilan tujuh segmen. Tampilan tujuh segmen adalah tampilan yang dapat dilihat pada layar kalkulator berbasis LED Keuntungan dari enkripsi berbasis segmentasi adalah bahwa hal itu mungkin lebih mudah untuk menyesuaikan gambar rahasia dan simbol yang berpotensi lebih mudah untuk mengenali bagi mata manusia, terutama dalam transparansi pada layar skenario.

***Index Terms* — Enkripsi, Kriptografi visual berbasis segmentasi, tampilan tujuh-segmen, Kriptografi visual berbasis pixel.**

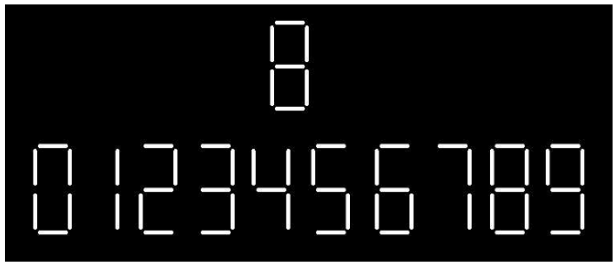
I. PENDAHULUAN

Kriptografi visual diperkenalkan pada tahun 1994 oleh Naor dan Shamir Dalam versi dasar itu dipersekenalkan sistem pembagian rahasia 2 dari 2, yaitu dari sebuah gambar hitam-putih yang diberikan P, dua gambar P1 dan P2 yang dihasilkan. Baik P1 dan P2 adalah acak, yaitu mereka menunjukkan pixel hitam dan putih yang terdistribusi secara acak, yaitu baik P1 dan P2 tidak menunjukkan informasi apapun. Tapi ketika P1 dan P2 saling tindih kemudian mereka menunjukkan gambar P asli.

Sebagai sistem pembagian rahasia yang sempurna 2 dari 2 Visual Kriptografi memiliki kekuatan enkripsi untuk sekali pakai, contoh misalakan P1, informasi asli P tidak dapat diperoleh tanpa mengetahui P2, bahkan dengan komputasi besar tidak akan membantu. Dengan kata lain: sistem enkripsi berdasarkan Visual Kriptografi tidak dapat dipecahkan.

Beberapa perluasan dan modifikasi Visual Kriptografi telah diperkenalkan, pada awalnya gagasan tersebut sudah digeneralisasi dari sistem pembagian rahasia 2 dari 2 untuk menjadi sistem pembagian rahasia m dari n, untuk setiap $m \leq n$. Beberapa modifikasi menyarankan untuk menambahkan fitur steganografi ke Visual Kriptografi, sedangkan saran lain yaitu mencoba untuk beralih dari gambar hitam-putih untuk foto warna.

Pada kali ini akan dijelaskan variasi lain dari Visual Kriptografi, bukannya mengambil piksel sebagai unit terkecil untuk dienkripsi, segmen dari tampilan segmen yang akan dienkripsi. Pada umumnya tampilan segmen yang khas ditunjukkan pada tampilan tujuh-segmen, lihat Gambar 1, digunakan untuk mewakili angka 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (dan mungkin digit heksadesimal A, b, c, d, E, F).

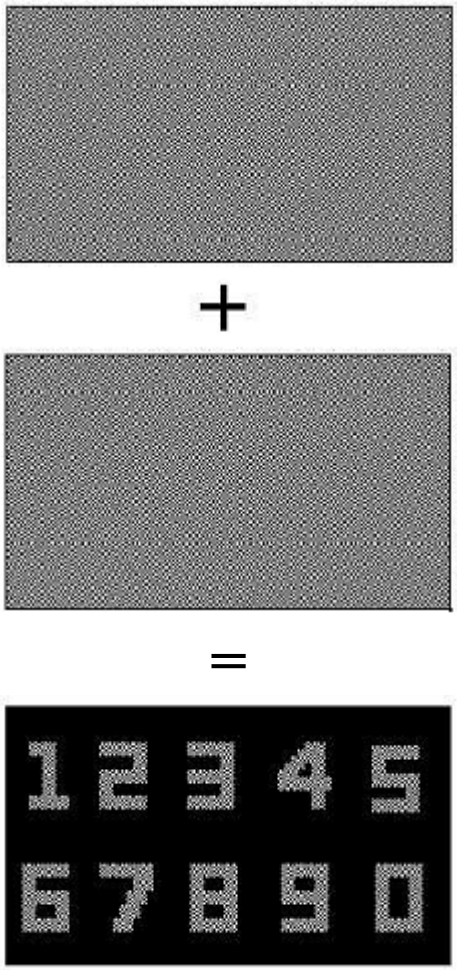


Gambar 1. Tampilan tujuh-segmen.

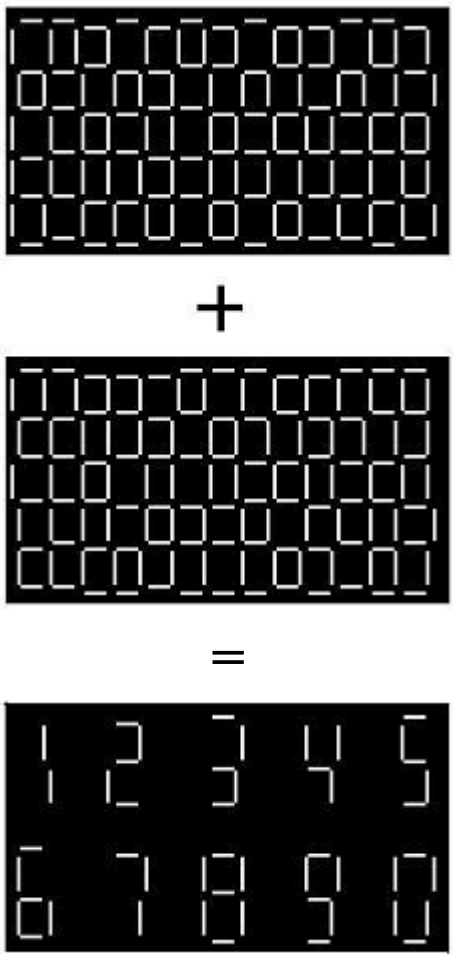
Visual Kriptografi berbasis segmentasi dapat digunakan untuk mengkodekan pesan yang dapat ditampilkan oleh layar segmen. Sebagai contoh, pesan yang hanya terdiri dari nomor dapat dikodekan dengan cara ini melalui Kriptografi Visual berbasis segmentasi menggunakan tampilan tujuh-segmen. Sebuah contoh pesan-pesan demikian informasi yang menggambarkan transfer uang (termasuk nomor rekening, bank nomor dan jumlah uang) selama sesi perbankan online, lihat Gambar 6.

Keunggulan potensi Kriptografi Visual berbasis segmentasi dibandingkan dengan Kriptografi visual berbasis pixel adalah sebagai berikut:

1. Dimungkinkan lebih mudah untuk menyesuaikan dua bagian, terutama dalam skenario transparansi pada layar,
2. Dimungkinkan lebih mudah bagi para mata manusia untuk mengenali simbol, terutama dalam skenario transparansi pada layar,
3. Random bit kurang diperlukan, hal ini mungkin keuntungan jika Random sesungguhnya (bukan pseudorandom) digunakan dalam sistem enkripsi,
4. Dimungkinkan lebih mudah untuk pengguna manusia non-pakar dari sebuah sistem enkripsi untuk memahami dan oleh karena itu mempercayakan Kriptografi Visual berbasis segmentasi daripada Kriptografi Visual berbasis pixel.



Gambar 2. Kriptografi visual berbasis pixel



Gambar 3. Kriptografi visual berbasis segmentasi

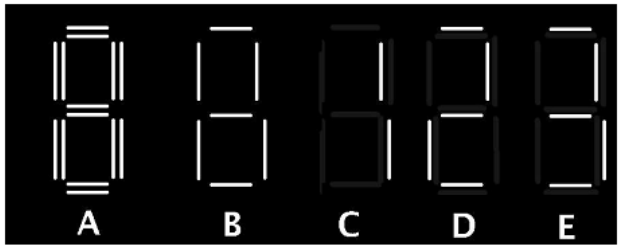
2. KRIPTOGRAFI VISUAL BERBASIS SEGMENTASI

Tampilan tujuh-segmen diciptakan pada tahun 1908. Menggunakan tujuh bar, tiga horisontal dan empat vertikal, disusun seperti angka 8, lihat bagian atas Gambar 1. Dengan menyoroti dipilih himpunan bagian tertentu dari tujuh segmen setiap digit 0 sampai 9 dapat direpresentasikan, lihat bagian bawah Gambar 1.

Beberapa tampilan segmen diberikan mampu menampilkan satu set simbol tertentu, misalnya taampilan tujuh-segmen yang mampu menampilkan set angka 0,..., 9. Prinsip Kriptografi Visual diterapkan pada tampilan segmen: Untuk mengambar segmen S dalam putih di hitam latar belakang dua paralel segmen S1 dan S2 yang dekat satu sama lain tetapi tidak berpotongan. Lihat untuk bagian contoh A Gambar 4 dimana ini diterapkan untuk tampilan tujuh-segmen.

Seperti di Kriptografi Visual berbasis pixel, bagian acak dihasilkan. Ini berarti dalam kasus segmen yang dari setiap pasangan segmen paralel satu S1 dan S2 dipilih secara acak. Segmen ini disimpan pada putih atau transparan, sedangkan segement paralel lain menjadi hitam seperti bagian pada backgorund. Seperti pilihan acak ditunjukkan dalam bagian B dari Gambar 4.

Sekarang bagian kedua diproduksi. Asumsikan bahwa simbol tertentu akan ditampilkan. Pertimbangkan subset dari segmen atas layar segmen yang harus disorot dalam rangka untuk menunjukkan simbol ini.



Gambar 4. Prinsip yang diterapkan pada tampilan tujuh-segmen

Jika segmen S milik subset ini, maka dalam kedua bagian dengan pilihan yang sama S1 atau S2 dibuat seperti dalam bagian acak dan disorot, segmen paralel lainnya adalah berubah hitam. Ini memiliki efek yang dalam kasus tumpang tindih, dua bagian tumpang tindih menunjukkan segmen putih.

Jika di sisi lain S bukan milik subset ini, maka dalam bagian kedua yang lain segmen dari dua segmen paralel S1 atau S2 disorot, dan segmen yang terpilih pada bagian

secara acak (bagian 1) adalah berubah hitam. Ini memiliki efek bahwa dalam kasus melapisi dua bagian segmen ini tidak menunjukkan area putih atau transparan.

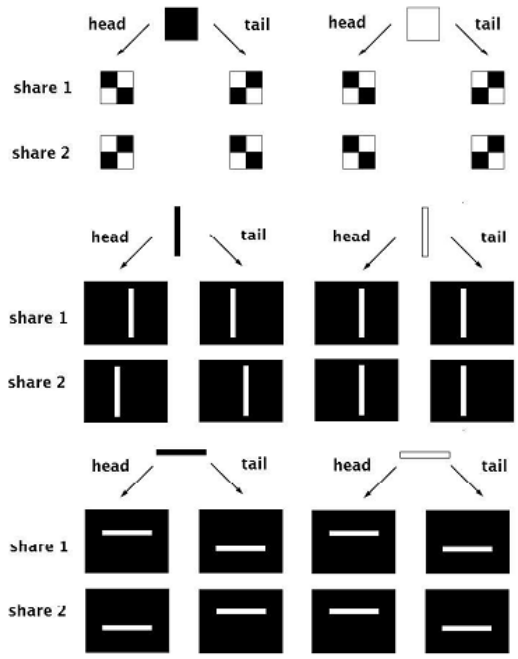
Secara total, segmen yang sama memiliki subset daerah menunjukkan A transparan ketika dua bagian saling tumpang tindih. Oleh karena itu, setelah tumpang tindih, simbol yang akan ditampilkan muncul untuk mata yang melihatnya. Sebagai contoh, dalam Bagian C dari Gambar 4 bagian kedua dipilih dengan cara yang sama segmen-segmen yang dibutuhkan dalam 1 digit pada layar, menunjukkan segmen transparan, dengan kata lain, pemirsa akan melihat 1 digit. Dalam Bagian D dan E dari Gambar 4 bagian kedua dipilih dengan cara itu, bahwa angka 2 dan angka 3 akan ditampilkan untuk melihatnya. Perhatikan bahwa bagian pertama (ditunjukkan dalam Bagian B) selalu sama untuk Bagian C, D, dan juga E.

Prinsipnya dijelaskan di atas juga diperlihatkan pada Gambar 5 di pusat dan di bawah. Dapat membandingkan ini dengan prinsip Kriptografi Visual berbasis pixel yang ditampilkan di dalam gambar.

Tentu saja bagian pertama adalah acak, yaitu tidak pengungkapan informasi, apalagi informasi dari pesan kode. Dengan argumentasi yang sama seperti untuk Kriptografi Visual berbasis pixel menangani untuk bagian kedua yang juga acak: untuk setiap segmen S kemungkinan untuk memilih sarana S1 adalah 1/2, independen dari segmen lain. Jadi itu adalah acak, juga.

Tentu saja, Visual Kriptografi berbasis segmen juga dapat diterapkan untuk set simbol yang representable oleh jenis lain dari tampilan segmen, misalnya ada tampilan empat belas-segment yang terkenal yang mampu mewakili semua huruf dan angka.

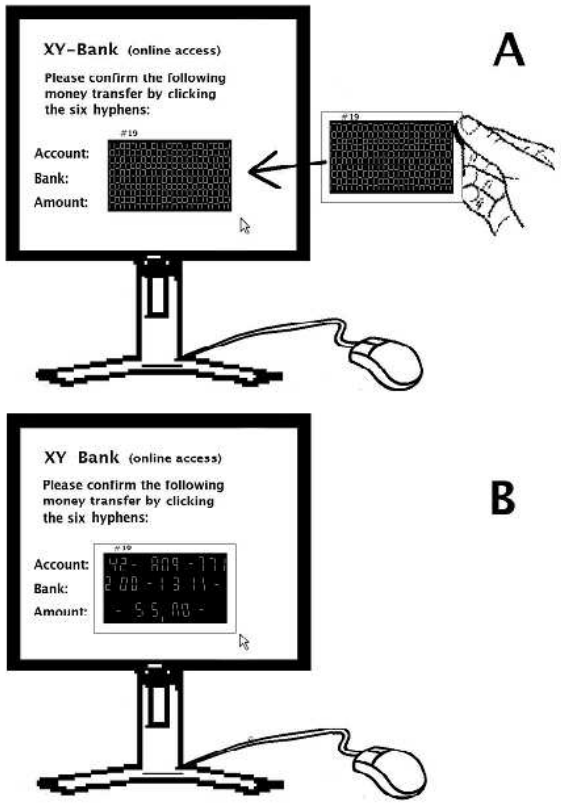
Potensi keuntungan Kriptografi Visual berbasis segmentasi dibandingkan dengan Kriptografi Visual berbasis pixel terdapat pada akhir Pendahuluan.



Gambar 5. Kriptografi visual berbasis pixel (atas) dengan Kriptografi berbasis segmentasi (bawah)

3. APLIKASI UNTUK KEAMANAN ONLINE BANKING

Gambar 6 menunjukkan sebuah aplikasi Visual Kriptografi: itu meningkatkan keamanan online banking. Daripada daftar Transaction Number (TAN atau iTAN's) yang mendapat nasabah bank dari banknya blok sebuah transparansi yang dihasilkan bagian secara acak (1 bagian) akan dicetak. Ketika nasabah bank ingin mengkonfirmasi transfer uang dalam sesi perbankan online server bank meminta konfirmasi kerahasiaan: pelanggan diminta untuk mengklik daerah-daerah tertentu di layar. Para nasabah bank telah menempatkan transparansi dengan nomor yang diminta di atas lembar bagian (2) ditampilkan pada layar. Setelah tumpang tindih bagian dia bisa melihat informasi tentang transfer uang dan juga daerah untuk mengklik. Jika informasi yang ditampilkan tentang transfer uang ok dia akan melakukan klik mouse, dan ini akan dianggap oleh server bank sebagai konfirmasi transfer uang. Enkripsi Ini menghindari serangan orang ketiga. Versi berbasis segmentasi ditunjukkan pada Gambar 6 memiliki empat potensi keuntungan yang terdaftar pada akhir Pendahuluan, dibandingkan dengan versi pixel berbasis. Selain itu, versi berbasis segmentasi dimungkinkan memiliki keuntungan bahwa analisis dan bukti matematis potensi keamanan mungkin lebih mudah daripada dalam kasus versi berbasis pixel asli karena model lebih diskrit.



Gambar 6. Visual TAN (vTAN)

REFERENSI

Moni Naor, Adi Shamir: Visual Cryptography. EUROCRYPT 1994: 1-12.

F.W.Wood: Illuminated Announcement and Display Signal. US Patent 974943, 1908

G. Ateniese, C. Blundo, A. D. Santis, and D. Stinson, "Extended schemes for visual cryptography," Theoretical Computer Science, vol. 250, pp. 143–161, 2001.

A. D. S. G. Ateniese, C. Blundo and D. R. Stinson, "Constructions and bounds for visual cryptography," in 23rd International Colloquium on Automata, Languages and Programming, ser. Lecture Notes in Computer Science, F. M.auf der Heide and B. Monien, Eds., vol. 1099. Berlin: Springer-Verlag, 1996, pp. 416–428.

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, 8 Mei 2011

Rio Cahya Dwiyanto 13506041