Mekanisme “Forgot My Password?” dengan implementasi Kriptografi Visual

Abraham Ranardo Sumarsono - 13507056[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*if17056@students.if.itb.ac.id*

***Abstract*— Kriptografi visual adalah suatu jenis kriptografi yang memungkinkan untuk dapat langsung didekripsi oleh mata manusia tanpa membutuhkan bantuan komputer. Apabila diberikan suatu gambar yang berisi pesan rahasia, kriptografi ini memungkinkan gambar tersebut untuk dienkripsi menjadi beberapa gambar transparan yang tidak merepresentasikan gambar yang berisi pesan rahasia sama sekali. Tentunya dibutuhkan mekanisme dekripsi agar gambar yang berisi pesan rahasia dapat dimunculkan kembali. Kriptografi visual memiliki sebuah mekanisme dekripsi yang unik, yaitu dengan menumpuk semua ataupun hanya beberapa gambar yang dihasilkan dari proses enkripsi sebelumnya.**

Makalah ini memberikan suatu ide baru kepada mekanisme pembangkitan password yang terlupa oleh pengguna. Mekanisme ini didukung oleh implementasi dari kriptografi visual. Pada makalah ini akan dijelaskan bagaimana mekanisme “forgot my password” dengan menggunakan bantuan implementasi dari kriptografi visual, dimana password ataupun keyword yang dapat membangkitkan password yang terlupa dapat dipecah dari sebuah gambar menjadi beberapa gambar dan pengguna memiliki peran menyimpan sebagian gambar yang nantinya akan menjadi kunci di dalam mekanisme pembangkitan password yang terlupa.

***Index Terms*—Forgot My Password, Gambar, Kriptografi Visual, Password.**

I. PENDAHULUAN

Pada saat perkembangan teknologi menjadi salah satu pengaruh yang penting di dalam kehidupan sehari-hari. Salah satu perkembangan teknologi yang paling berpengaruh adalah internet. Dengan adanya internet, masyarakat dapat melakukan kegiatan sehari-harinya seperti berkomunikasi, berbelanja, dan sebagainya di depan komputernya masing-masing. Salah satu kegiatan yang sangat terbantu dengan adanya teknologi internet ini adalah komunikasi.

Dengan memiliki akun email, masyarakat dapat berkomunikasi antar satu dengan lainnya. Komunikasi yang biasanya dilakukan adalah bertukar pesan. Pesan yang dikirimkan pun bermacam-macam, mulai dari pesan yang bersifat tidak rahasia, hingga pesan yang bersifat sangat rahasia. Hal ini membuat keamanan pengaksesan akun email sangat penting. Sehingga digunakan password sebagai sarana otorisasi pengguna akun email.

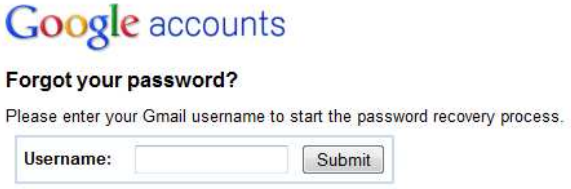
Dengan digunakannya password sebagai sarana otorisasi pengguna akun email, dirancang pula sebuah mekanisme apabila pengguna lupa akan passwordnya, mekanisme “forgot my password”. Mekanisme ini memiliki peran yang sangat penting. Hal ini dikarenakan apabila mekanisme tersebut tidak mangkus, maka tingkat keamanan suatu akun akan menjadi sangat rendah.

II. “FORGOT MY PASSWORD”

“Forgot my password” adalah suatu mekanisme yang dirancang untuk pengguna yang melupakan password yang digunakan untuk memasuki akunnya. Mekanisme ini dapat membangkitkan kunci password yang baru ataupun menunjukkan kunci password yang lama. Mekanisme ini memiliki berbagai proses yang pada umumnya sama untuk setiap penyedia jasa email, seperti Yahoo! Mail dan GMail.

GMail merupakan salah satu penyedia jasa email. GMail pun menyediakan mekanisme “forgot my password” seperti penyedia jasa email lainnya. Mekanisme “forgot my password” yang dimiliki oleh GMail memiliki beberapa tahap. Tahap-tahap tersebut antara lain:

1. Langkah awal adalah dengan memasukkan username yang bersesuaian dengan akun pengguna dimana passwordnya telah hilang (pengguna melupakan passwordnya)

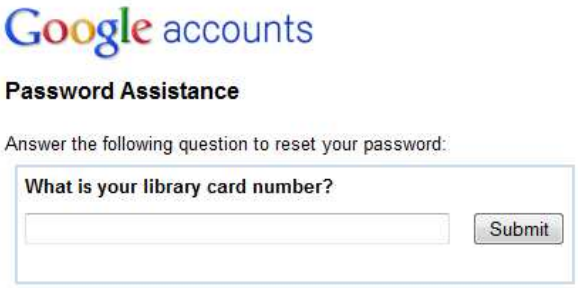


Gambar 1. Tahap awal di GMail

2. Langkah selanjutnya adalah verifikasi apakah pengakses halaman tersebut merupakan manusia asli atau bot komputer yang biasanya digunakan untuk membobol akun. Verifikasi ini biasanya menggunakan CAPTCHA.

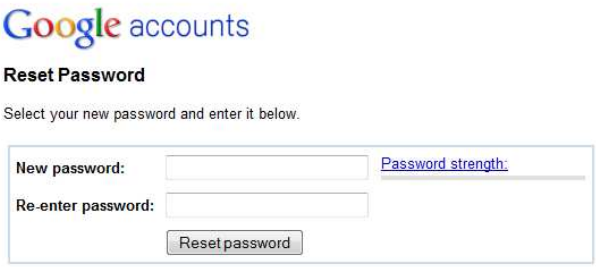
Gambar 2. Mekanisme Verifikasi CAPTCHA

3. Langkah selanjutnya ini merupakan langkah yang dikaitkan dengan informasi awal pada saat pendaftaran akun tersebut. Biasanya pengguna diberikan pertanyaan yang sudah pengguna jawab sendiri pada saat pendaftaran. Jawaban yang dibutuhkan merupakan jawaban unik dari pengguna.



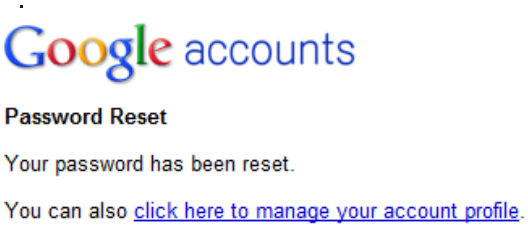
Gambar 3. Pertanyaan Pribadi yang Membutuhkan Jawaban Unik

4. Selanjutnya, merupakan langkah dimana sistem menerima masukan berupa password yang baru dari pengguna untuk menggantikan password yang lama.



Gambar 4. Pengubahan Password Lama

5. Tahap terakhir adalah berupa notifikasi dari GMail tentang keberhasilan dalam mengubah password lama yang dilupakan oleh pengguna menjadi password baru yang dimasukkan pengguna pada tahap sebelumnya.

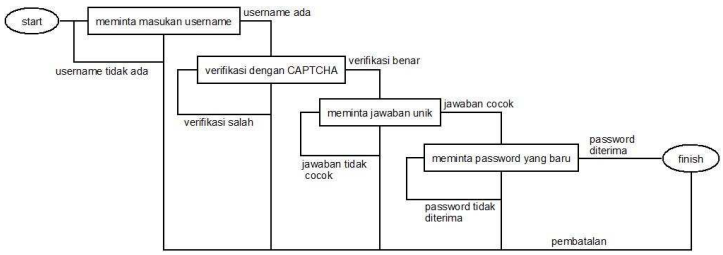


Gambar 5. Notifikasi Keberhasilan GMail

6. Langkah terakhir adalah dengan mengakses akun email dengan password yang baru yang telah dimasukkan pada tahap keempat.

Selain GMail yang dikelola oleh Google, terdapat Yahoo! Mail yang juga memiliki mekanisme “forgot my password” yang tidak berbeda jauh dengan mekanisme yang ada pada GMail. Begitu pula dengan penyedia akun email lainnya seperti Hotmail, Plasa, dan sebagainya.

Secara umum, mekanisme “forgot my password” yang ada membutuhkan username/nama akun, verifikasi CAPTCHA, jawaban unik, dan password yang baru. Mekanisme proses “forgot my password” secara umum dapat digambarkan sesuai dengan diagram berikut:



Gambar 6. Diagram "Forgot My Password"

III. KRIPTOGRAFI VISUAL

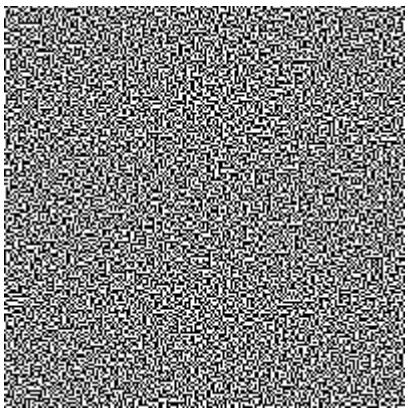
A. Definisi Kriptografi Visual

Kriptografi visual adalah sebuah teknik kriptografi yang mengijinkan informasi visual (gambar, teks, dan sebagainya) untuk dapat dienkripsi sedemikian sehingga proses dekripsinya dapat dilakukan oleh sistem visual manusia, tanpa bantuan komputer.

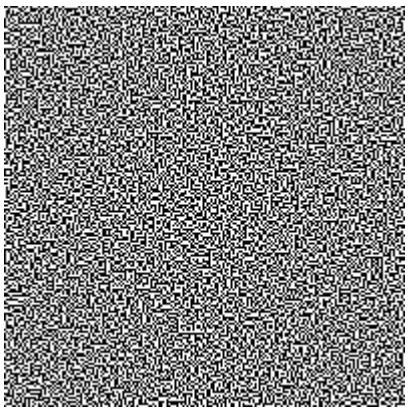
Kriptografi visual ini pertama kali diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994. Mereka mendemonstrasikan sebuah skema *sharing* visual rahasia, dimana sebuah gambar dipecah menjadi n buah gambar sehingga hanya orang yang memiliki semua n buah gambar yang dapat mendekripsi gambar.

Dengan mekanisme kriptografi visual, orang yang meskipun sudah memiliki n-1 buah gambar, tidak akan bisa membangkitkan gambar rahasia tersebut. Setiap bagian gambar dicetak pada sebuah transparansi yang terpisah, dan proses dekripsi dilakukan dengan menumpuk semua transparansi. Ketika semua n buah gambar ditumpuk, gambar asli yang menjadi pesan rahasia akan muncul.

Gambar 7. Gambar Asli



Gambar 8. Share 1

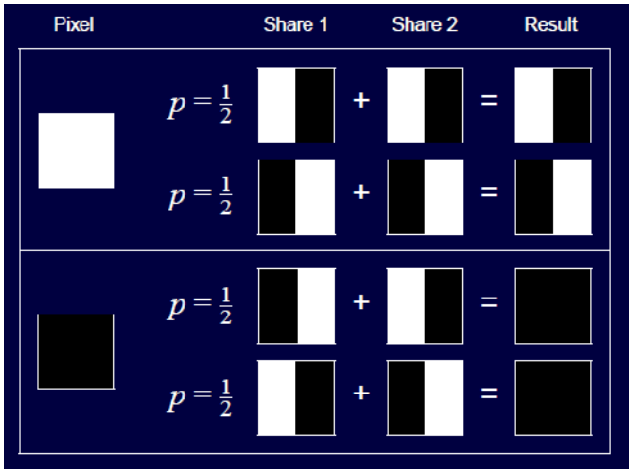


Gambar 9. Share 2

Gambar 10. Share 1 + Share 2

B. Skema Dasar Kriptografi Visual

Skema dasar yang digunakan di kriptografi visual pada awalnya hanya melibatkan 2 buah gambar hasil enkripsi. Sehingga proses enkripsi gambar menjadi sederhana.



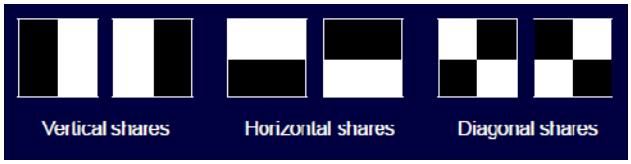
Gambar 11. Skema Dasar Kriptografi Visual

Bagian pixel yang berwarna putih dapat dibagi menjadi dua cara. Cara pertama adalah dengan membagi pixel putih tersebut menjadi dua belahan dengan belahan kanan berwarna hitam dan belahan kiri berwarna putih. Cara

lainnya adalah dengan membaginya menjadi dua belahan terbalik seperti cara sebelumnya. Dengan cara ini, pixel putih tidak akan utuh menjadi pixel putih ketika sudah didekripsi. Namun, hal ini dilakukan agar pesan rahasia tidak dapat terlihat dengan mudah.

Bagian pixel yang berwarna hitam di dalam skema dasar ini dibagi menjadi dua belahan yang masing-masing berlawanan (salah satu memiliki belahan kanan putih dan belahan kiri hitam, dan yang lainnya memiliki belahan kanan hitam dan belahan kiri yang hitam).

Jumlah gambar yang diminta dari hasil enkripsi pun dipertimbangkan untuk lebih dari dua buah gambar untuk menjamin keamanan informasi yang dienkripsi. Oleh karena itu skema dasar tersebut dikembangkan lagi.



Gambar 12. Skema yang sudah Dikembangkan

Pada skema dasar yang sudah dikembangkan tersebut. Satu pixel dibagi menjadi empat buah subpixel. Pixel yang putih dibagi menjadi dua atau lebih tata letak subpixel yang sama. Sedangkan, pixel yang hitam dibagi menjadi dua atau lebih tata letak subpixel yang saling berkomplementer.

Untuk mencapai tingkat keamanan yang optimal, pembangkitan tata letak dilakukan secara acak. Selain itu, untuk setiap tata letak dianjurkan untuk memiliki dua buah subpixel putih dan dua buah subpixel hitam sehingga tingkat keamanan yang dicapai optimal.

C. Algoritma Pembangkit Gambar Enkripsi

Algoritma untuk membangkitkan gambar-gambar hasil enkripsi dari kriptografi visual cukup sederhana. Algoritma tersebut melibatkan matriks 2 dimensi dan fungsi pembangkit acak. Secara umum, pseudocode untuk membangkitkan gambar enkripsi dengan jumlah gambar enkripsi sebanyak dua buah adalah sebagai berikut :

```
ukuran←hitung_ukuran_gambar(gambar)
ukuran←ukuran * 2

matriks_awal[][]←get_pixel(gambar)
matriks_akhir2[][]←inisiasi(ukuran)
matriks_akhir1[][]←random(ukuran)

i←0
while (i < ukuran / 2) do
    j←0
    while (j < ukuran / 2) do
        matriks_akhir2[][] ←
kalkulasi(matriks_awal,
matriks_akhir1, i, j)
        j ← j + 1

    i ← i + 1

gambar[0] ← get_gambar(matriks_akhir1)
gambar[1] ← get_gambar(matriks_akhir2)
```

Pertama-tama dilakukan perhitungan ukuran gambar dan hasil perhitungan akan dikali 2 karena 1 pixel akan memiliki 4 subpixel. Lalu dilakukan proses pemetaan pixel ke matriks dua dimensi. Pemetaan di sini dilakukan menjadi 1 (hitam) dan 0 (putih).

Langkah selanjutnya adalah menginisiasi matriks akhir satu dengan nilai kosong dan matriks akhir satunya lagi dengan fungsi acak. Fungsi acak ini akan membangkitkan dua buah 1 dan dua buah 0 dalam satu tata letak (4 subpixel).

Setelah itu dilakukan iterasi untuk mengisi matriks akhir yang belum terisi. Pengisian matriks didasarkan pada matriks akhir yang lainnya serta posisi pixel pada gambar asli (hitam atau putih)

Setelah kedua matriks akhir terisi penuh, maka dilakukan aksi terakhir. Tahapan terakhir adalah mengkonversi kedua matriks akhir tersebut menjadi dua buah gambar yang mendukung transparansi dengan susunan kombinasi gambar hitam dan transparans.

IV. MEKANISME “FORGOT MY PASSWORD” DENGAN KRIPTOGRAFI VISUAL

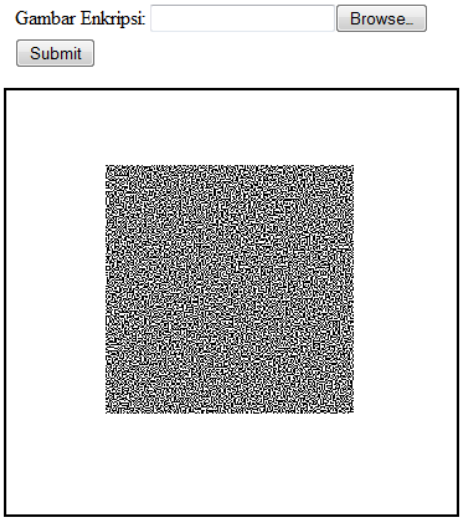
Pada mekanisme “forgot my password” yang biasanya, pengguna diharuskan menghapal jawaban unik. Hal ini sangat rentan, karena pengguna mungkin saja melupakan jawaban unik tersebut. Supaya tidak melupakan jawaban unik tersebut, biasanya pengguna menyimpan jawaban tersebut. Namun, proses menyimpan ini sangat rentan terhadap pembajakan.

Oleh karena itu, penulis mencoba untuk merancang mekanisme baru “forgot my password” dengan menggunakan bantuan implementasi dari kriptografi visual.

Mekanisme baru yang dirancang dibagi menjadi tujuh tahap. Tahap-tahap tersebut antara lain:

1. Memasukkan username yang berkaitan dengan password yang hilang.
2. Melakukan proses verifikasi CAPTCHA seperti proses pada umumnya

3. Langkah selanjutnya adalah mengunggah gambar hasil enkripsi yang diperoleh pada saat pendaftaran akun untuk melihat jawaban unik yang ada
4. Lalu, setelah jawaban unik terlihat pada layar, pengguna memasukkan jawaban unik tersebut untuk mengkonfirmasi



Gambar 13. Screenshoot Uploader

5. Selanjutnya, dilakukan proses pemasukkan password yang baru untuk menggantikan password yang lama

Gambar 14. Screenshoot Ter-upload

6. Setelah password yang baru telah diterima, maka akan ditunjukkan notifikasi kepada pengguna bahwa proses telah selesai
7. Pengguna akan membuka akun dengan memasukkan username dan password yang baru

Tahap-tahapan sebelumnya merupakan tahapan penggunaan implementasi kriptografi visual pada mekanisme “forgot my password”. Sedangkan proses pembuatan kriptografi visual dilakukan pada saat pendaftaran akun email.

Pada proses pendaftaran akun email, terutama pada tahap menentukan pertanyaan unik serta jawaban unik. Sistem akan membuat satu gambar enkripsi yang dihasilkan dari fungsi acak yang menjadi patokan utama untuk membangkitkan gambar yang akan disimpan oleh pengguna.

Jawaban unik akan dimasukkan ke dalam sebuah gambar dan gambar tersebut akan diproses dengan gambar enkripsi hasil fungsi acak tadi. Hasil prosesnya adalah gambar enkripsi yang akan disimpan oleh pengguna.

Salah satu kontribusi yang dilakukan oleh penulis selain merancang mekanisme baru inia adalah dengan membuat prototype pengunggah file gambar hasil enkripsi.

V. ANALISIS

Dengan adanya mekanisme yang tergolong baru ini, maka perlu dilakukan analisis kekuatan dan kelemahan yang ada pada mekanisme tersebut.

Kekuatan utama pada mekanisme yang baru ini adalah pengguna tidak perlu menghapal jawaban unik yang diperlukan di dalam mekanisme “forgot my password”. Seperti cara kerja CAPTCHA, pengguna hanya perlu mengunggah file gambar yang merupakan hasil enkripsi dari gambar jawaban unik. Kemudian dengan tool yang ada pengguna tinggal melihat hasil tumpukan gambar yang ada dan memasukkan jawaban unik yang tertera pada hasil tumpukan.

Kekurangan yang ada pada mekanisme ini adalah keamanan file gambar hasil enkripsi tersebut. Pengguna mungkin saja menghilangkan file gambar tersebut. Bahkan bisa saja file gambar tersebut jatuh ke tangan orang lain dan disalahgunakan. Dengan begitu keamanan mekanisme ini belum dapat dijamin.

Oleh karena itu, disarankan untuk menambahkan unsur biometrik pada mekanisme yang sudah dirancang ini agar tingkat keamanan dapat ditingkatkan. Unsur biometrik dapat ditambahkan di dalam membangkitkan bagian gambar enkripsi default yang akan digunakan untuk menghasilkan gambar enkripsi yang akan disimpan oleh pengguna.

Unsur biometrik ini dapat membuat gambar enkripsi default menjadi unik. Pada saat mekanisme dijalankan, pengguna akan diminta memasukkan unsur biometrik tersebut serta file gambar hasil enkripsi.

VI. KESIMPULAN

Mekanisme “Forgot My Password” yang sudah ada pada saat ini memiliki kelemahan. Kelemahan terletak pada mekanisme pertanyaan unik dimana pengguna dapat dengan mudah melupakan jawaban unik tersebut.

Dengan adanya mekanisme baru ini, pengguna tidak harus khawatir apabila melupakan jawaban unik yang dibutuhkan. Kelebihan yang ditawarkan pada mekanisme ini adalah terenkripsinya jawaban unik yang disimpan sebagai gambar. Namun, kelemahannya adalah mekanisme tersebut rentan terhadap hilangnya file enkripsi yang harusnya disimpan oleh pengguna.

Saran yang dapat diberikan adalah dengan menambahkan sistem biometrik di dalam membuat share utama yang digunakan untuk menggenerasi share yang akan disimpan oleh pengguna. Dengan menggunakan bantuan sistem biometrik, tingkat kemangkusan dari mekanisme “forgot my password” yang baru ini akan menjadi lebih tinggi.

DAFTAR REFERENSI

[1] Munir, Rinaldi, Bahan Kuliah IF3058 Kriptografi. Departemen Teknik Informatika, Institut Teknologi Bandung, 2010.

[2] Naor, Moni, Shamir, Adi, Visual Cryptography, 1998.

[3] Visual Cryptography : http://homes.esat.kuleuven.be/~fvercaut/talks/visual.pdf diakses pada tanggal 15 Mei 2010 pada pukul 20.00 WIB

[4] Visual Cryptography : http://www.cacr.math.uwaterloo.ca/~dstinson/visual.html diakses pada tanggal 15 Mei 2010 pada pukul 20.00 WIB

[5] Mekanisme forgot my password pada Yahoo! Mail : https://edit.yahoo.com/forgotroot?done=http%3A%2F%2Fmail.yahoo.com&src=ym&partner=&intl=us diakses pada tanggal 15 Mei 2010 pada pukul 20.00 WIB

[6] Mekanisme forgot my password pada GMail : https://www.google.com/accounts/ForgotPasswd?service=mail&fpOnly=1 diakses pada tanggal 15 Mei 2010 pada pukul 20.00 WIB

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, 16 Mei 2010

Abraham Ranardo Sumarsono - 13507056