Penggunaan Visual Cryptography dalam Autentikasi Data Biometrik dan Pengamanan Penyimpanannya

Muhammad Furqan Habibi (13511002)
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung g, Jl. Ganesha 10 Bandung 40132, Indonesia
furqan.habibi1@gmail.com

***Abstrak*—Pada paper ini diajukan sebuah skema penggunaan teknik visual cryptography dalam proses autentikasi data biometric dan pengamanan penyimpanannya. Skema ini bertujuan untuk memberikan keamanan pada penyimpanan data biometric pengguna baik itu di database atau media penyimpanan lain. Penggunaan visual cryptography memiliki keuntungan dalam hal kebutuhan komputasi yang minimal karena pada proses dekripsinya hanya perlu dilakukan penumpukan terhadap share image tanpa komputasi sama sekali.**

Kata kunci*—*Visual Cryptography; Biometric; Keamanan;

I. PENDAHULUAN

Perkembangan teknologi yang terjadi secara terus-menerus telah banyak membawa perubahan pada gaya hidup dan kebiasaan manusia. Dengan datangnya zaman informasi, yang ditandai dengan mudahnya akses terhadap segala informasi dengan cepat, telah membuat kebutuhan untuk mengamankan informasi tersebut menjadi jauh lebih penting. Tanpa adanya teknologi seperti sekarang, berbagai informasi rahasia dapat dengan mudah disimpan, karena akses terhadapnya juga sangat terbatas. Namun dengan kemudahan akses terhadap informasi seperti melalui internet dan jaringan komunikasi lainnya, maka pengamanan informasi menjadi hal yang sangat penting yang harus direncanakan dengan baik.

Dengan kebutuhan pengamanan informasi tersebut, maka para ahli dan praktisi teknologi informasi telah merumuskan berbagai metode untuk pengamanan informasi. Salah satu metode tersebut adalah dengan menerapkan sebuah sistem autentikasi terhadap pengguna untuk menentukan apakah ia berhak mengakses sebuah informasi tertentu atau tidak. Secara definisi, autentikasi berarti sebuah proses menentukan apakah seseorang atau sesuatu adalah benar merupakan seseorang atau sesuatu yang ia klaim merupakan dirinya. Jika kebenaran tersebut dapat dikonfirmasi, maka orang tersebut dapat diberikan hak untuk mengakses suatu informasi tertentu.

Di sepanjang sejarah kemanan informasi, telah banyak sistem autentikasi yang diajukan dan digunakan dalam dunia nyata. Secara umum, terdapat tiga hal yang dapat dijadikan sebagai dasar dalam melakukan autentikasi. Tiga hal tersebut adalah sebagai berikut :

- Sesuatu yang diketahui oleh pengguna
- Sesuatu yang dimiliki oleh pengguna
- Sesuatu yang ada pada pengguna

Ketiga hal di atas umum digunakan sebagai dasar utama sistem autentikasi. Untuk sesuatu yang diketahui pengguna contohnya adalah password, pass phrase, PIN, dll. Untuk sesuatu yang dimiliki pengguna contohnya adalah ID Card, token, handphone, dll. Untuk sesuatu yang ada pada pengguna contohnya adalah data-data biometric seperti wajah, retina, sidik jari, dll.

Di antara ketiga dasar autentikasi di atas, sesuatu yang ada pada pengguna merupakan metode yang dianggap paling aman. Terdapat beberapa alasan mengapa metode ini dianggap merupakan metode yang paling aman di antara metode yang lain. Sebagai contoh misal digunakan sesuatu yang diketahui pengguna seperti password. Password yang singkat memiliki kelemahan dapat ditebak oleh orang lain dengan mudah. Sementara password yang panjang juga memiliki kelemahan yaitu mudah dilupakan oleh pengguna. Sementara pada sesuatu yang ada pada pengguna, tidak ada yang perlu diiingat oleh pengguna sehingga tidak mungkin dilupakan. Juga tidak mungkin ditiru oleh orang lain karena keunikannya yang hanya dimiliki oleh tepat satu pengguna.

Lalu misal digunakan sesuatu yang dimiliki oleh pengguna seperti ID Card. ID Card dapat saja hilang oleh pengguna atau terlupakan tempat penyimpanannya. Sementara sesuatu yang ada pada pengguna tidak akan pernah hilang karena memelekat pada tubuh pengguna.

Namun demikian, sesuatu yang ada pada pengguna tidak juga bebas dari kelemahan. Salah satu kelemahannya adalah penyimpanan datanya pada database atau media penyimpanan lain pada sistem. Jika orang lain dapat mengakses data tersebut, maka ia bisa saja mengubahnya menjadi data lain, atau memalsukannya dengan berbagai teknik yang mulai banyak dilakukan [1].

Mada dari itu, pada paper ini diajukan sebuah skema dalam autentikasi data biometric dengan tujuan meningkatkan keamanan data biometric baik saat autentikasi maupun saat penyimpanan di dalam sistem.

II. DASAR TEORI

A. *Visual Cryptography*

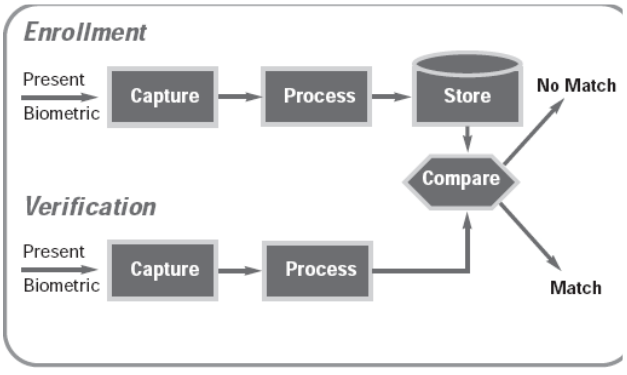
Visual Cryptography adalah salah satu jenis skema pembagian data rahasia di mana sebuah data rahasia yang berbentuk visual (citra, tulisan, dll) dibagi menjadi beberapa bagian (*share*) yang kemudian dapat mengmbalikan data rahasia tersebut dengan menumpuknyua satu sama lain. Visual Cryptography diperkenalkan oleh Moni Naor dan Adi Shamir pada tahun 1994[2].

Pada visual kriptografi, data yang ingin disembunyikan adalah sebuah data citra hitam putih. Kemudian data tersebut disebarkan kepada n buah share yang masing-masing pixelnya diwakili oleh m buah subpixel. Dengan demikian jika m lebih dari 1, maka setiap pixel pada citra asli akan diwakili oleh lebih dari 1 pixel pada citra share, mengakibatkan citra share memiliki dimensi yang lebih besar. Warna putih pada citra-citra ini diasumsikan bersifat transparan sementara warna hitam tidak. Akibatnya ketika ditumpukkan, warna hitam pada lapisan di bawah dapat terlihat jika tertutupi oleh warna putih pada lapisan di atasnya. Dengan demikian, proses dekripsi pada visual cryptography tidak membutuhkan komputasi sama sekali, hanya membutuhkan penumpukan citra share dan melihat langsung dengan indera penglihatan manusia.

Dengan masing-masing share yang dihasilkan, tidak mungkin didapatkan citra asli jika jumlah share yang ditumpuk tidak mencapai suatu nilai batas tertentu. Naor dan Shamir mengajukan skema k dari n [3], di mana citra asli diproses untuk menghasilkan n citra share. Data pada citra asli tidak dapat dikembalikan tanpa menumpuk sedikitnya k buah citra share. Jika k = n, maka dibutuhkan semua citra share untuk mengembalikan citra asli.

Dua parameter utama pada visual cryptography adalah jumlah subpixel untuk masing-masing pixel serta contrast hitam dan putih pada citra hasil dekripsi. Jumlah subpixel harus diusahakan seminimal mungkin, sehingga citra share yang dihasilkan tidak begitu besar. Sementara nilai contrast pada citra hasil dekripsi diusahakan semaksimal mungkin agar terlihat jelas perbedaan antara data dan latar belakang pada citra.

B. *Autentikasi Biometrik*



Di atas adalah diagram sederhana yang menampilkan proses pada sebuah sistem autentikasi biometric. Pada saat pengguna pertama kali berinteraksi dengan sistem, maka pengguna akan melalui proses enrollment. Secara sederhana, enrollment adalah proses di mana data pengguna direkam dan disimpan oleh sistem untuk menjadi data template. Untuk selanjutnya merupakan proses utama dalam sistem autentikasi biometric yaitu verifikasi(autentikasi) penguna yang sedang mengakses. Secara sederhana, proses ini akan mengambil data biometric pengguna pada saat itu dan membandingkannya dengan data yang telah tersimpan di dalam sistem. Jika tingkat kemiripan data biometric sekarang dengan data biometric pada sistem mencapai suatu threshold tertentu, maka pengguna terautentikasi.

Namun pada umumnya, sistem autentikasi biometric tidak bisa langsung membandingkan data biometric sekarang dengan satu data biometric tertentu pada database. Sistem akan melakukan pencocokan dengan seluruh data biometric yang ada dan menentukan data mana yang paling mirip dengan data biometric yang sedang diautentikasi. Proses ini jelas berlangsung lebih lama dibandingkan jika sistem telah mengetahui dengan data yang mana data biometric ini akan dicocokkan.

Untuk itu biasanya pada sistem yang diinginkan bekerja lebih cepat dan lebih aman, maka selain data biometric juga dibutuhkan masukan lain dari pengguna seperti sesuatu yang dimiliki pengguna, seperti ID Card dll. Pada ID Card ini akan tersimpan data lain dari pengguna seperti no ID, nama, dll, sehingga pproses pencocokan data biometric pada sistem dapat terarah dan berlangsung lebih cepat.

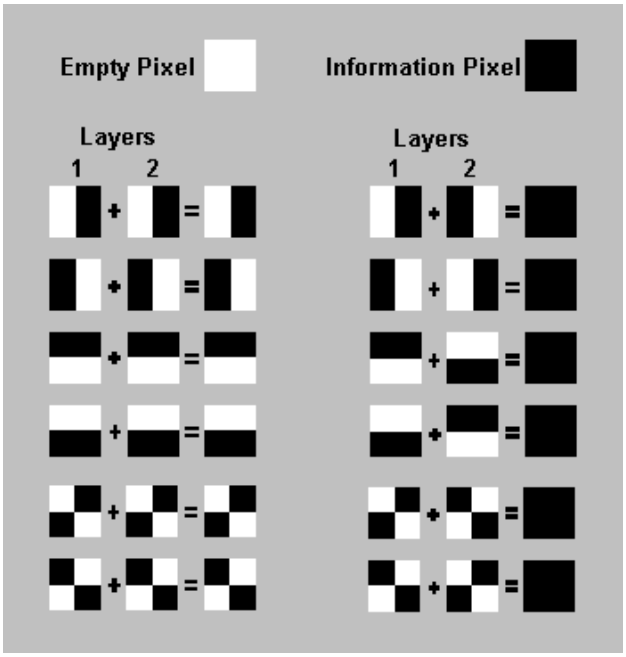
Selain itu dengan skema seperti ini kemanan menjadi lebih baik, karena sesorang harus menyiapkan dua hal untuk melakukan autentikasi yaitu ID Card dan data biometric.

III. RANCANGAN SKEMA AUTENTIKASI DENGAN VISUAL CRYPTOGRAPHY

Proses autentikasi data biometric dengan visual cryptography yang kami ajukan memiliki skema sebagai berikut:

1. Pengguna mendaftarkan sample data biometricnya pada sistem.
2. Pada sample tadi kemudian diterapkan visual cryptography untuk menghasilkan dua buah shared image.
3. Satu shared image disimpan di database, satu lagi diberikan kepada user dalam bentuk ID card atau sejenisnya.
4. Secara opsional, ID card juga dapat mengandung data-data lain yang dibutuhkan seperti masa berlaku, no ID, dll. Sehingga saat autentikasi dilakukan dapat langsung diverifikasi hak akses pengguna.
5. Saat pengguna akan melakukan autentikasi, ia akan memberikan ID cardnya untuk diproses oleh sistem. Dengan menumpuk image pada database dengan image pada ID card, akan dihasilkan image data biometric yang asli. Kemudian sistem akan memindai bagian tubuh pengguna yang bersesuaian untuk menghasilkan data biometric baru. Kedua data biometric tadi kemudian dibandingkan dan diverifikasi. Jika keduanya lolos melalui proses perbandingan, maka dinyatakan pengguna terautentikasi.

Sementara untuk proses visual cryptography yang diterapkan adalah dengan skema 2 dari 2 dengan 4 subpixel untuk masing-masing pixel. Ilustrasi untuk proses pembangkitan citra share adalah sebagai berikut :



Untuk pixel putih, maka subpixel share dipilih dari bagian kiri ilustrasi secara random. Sementara untuk pixel hitam, maka subpixel share dipilih dari bagian kanan ilustrasi secara random.

Citra test yang digunakan diambil dari kompetisi Fingerprint Verification Competition pada tahun 2000 yang diadakan di University of Bologna. Sebelum citra tes diproses dengan visual cryptography, cetiap citra dibinerisasi terlebih dahulu agar hanya terdiri dari piksel putih (transparan) dan hitam.

IV. Eksperimen dan Pembahasan Hasil

Proses eksperimen dijalankan sebagai berikut. Pertama citra sidik jari asli dibandingkan dengan dirinya sendiri dengan perangkat lunak pengenal sidik jari. Kemudian score yang sihasilkan dicatat. Lalu citra hasil visual cryptography dibandingkan juga dengan citra sidik jari asli dan score nya dicatat. Kedua score tadi kemudian dibandingkan. Prosedur ini dilakukan terhadap 10 citra sidik jari test. Lalu dilihat secara keseluruhan perbandingan score citra asli dengan citra hasil visual cryptography. Perangkat lunak yang digunakan dalam pengenalan sidik jari di sini adalah Griaule Fingerprint SDK.

Berikut table hasil perbandingan nilai tersebut :

No	Nama File	Perbandingan Asli	Perbandingan setelah visual cryptography
1	101_1.bmp	316	105
2	101_2.bmp	275	95
3	101_3.bmp	301	121
4	101_4.bmp	293	97
5	101_5.bmp	311	98
6	101_6.bmp	286	106
7	101_7.bmp	271	93
8	101_8.bmp	320	119
9	102_1.bmp	301	115
10	102_2.bmp	295	104

Terlihat bahwa nilai setelah dilakukan visual cryptography menurun cukup jauh. Namun patut dicatat bahwa threshold pada sistem pengenalan sidik jari yang digunakan adalah 60. Artinya semua nilai di atas 60 dikategorikan cocok dan dapat diterima sebagai sidik jari yang sama. Artinya proses visual cryptography yang dilakukan tidak begitu mengubah hasil pencocokan sidik jari yang dilakukan oleh sistem pengenal sidik jari.

V. Kesimpulan dan Saran

Dari eksperimen yang telah dilakukan, dapat dilihat bahwa skema autentikasi biometric dengan menggunakan visual cryptography dapat dilakukan dengan kemampuan rekognisi data yang cukup baik. Artinya solusi autentikasi ini dapat dilakukan di dunia nyata sehingga dapat meningkatkan keamanan data biometric tanpa mengurangi kinerja pengenalan data biometric itu sendiri. Pada akhirnya data biometric yang digunakan dapat disimpan dengan lebih aman, proses autentikasi yang terjadi juga lebih aman, kemampuan rekognisi data biometric tetap baik, dan kinerja sistem secara keseluruhan hampir tidak mengalami perubahan.

Untuk pengembangan selanjutnya, solusi ini dapat diterapkan pada jenis data biometric lainnya seperti wajah, retina, telapak tangan, dan lainnya asalkan dapat direpresentasikan sebagai sebuah citra. Dengan teknik visual cryptography extended yang dapat memroses citra grayscale, maka jenis-jenis data tadi sangat mungkin untuk diproses pada masa yang akan datang.

Acknowledgment

Seiring dengan selesainya penulis dalam menyusun makalah ini, penulis hendak menyampaikan puji dan syukur atas rahmat Allah SWT yang telah memberikan kemudahan bagi penulis selama pengerjaan makalah ini. Selanjutnya penulis juga ingin mengucapkan terima kasih kepada Bapak Rinaldi selaku dosen matakuliah IF4020 Kriptografi, yang telah menyampaikan ilmu yang dapat kami manfaatkan selama pengerjaan makalah ini. Tak lupa kami juga mengucapkan terima kasih kepada seluruh teman-teman yang baik secara langsung ataupun tidak langsung turut andil dalam pengerjaan makalah ini.

Referensi

[1] http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6671991

[2] M. Naor and A. Shamir, “Visual cryptography”,in Eurocrypt’94 Proceeding,LNCS, vol.950, Spring-Verlag, pp.1-12, 1995.

[3] Rinaldi. Bahan KuliahIF3058 Kriptografi: Kriptografi Visual