KEAMANAN DENGAN SISTEM BIOMETRIK

Oleh : Krisnawati

Abstrak

Saat ini teknologi yang umum untuk mengenali seseorang di dunia digital adalah pasangan user ID dan password. Teknologi ini dirasakan memiliki banyak kekurangan sehingga akhir-akhir ini ada kecenderungan untuk menggunakan sistem keamanan lain yang lebih baik. Salah satu keamanan yang dianggap paling akurat adalah sistem biometrik. Perangkat biometrik mengenali orang dari ciri-ciri fisiknya. Misalnya dengan sidik jari, sidik telapak tangan, pengenalan wajah, pengenalan retina, pengenalan suara, dll. Ciri-ciri fisik tesebut bersifat unik satu dengan yang lain.

Kata kunci: keamanan, biometrik.

Pendahuluan

Keamanan di internet merupakan suatu permasalahan besar sejak dunia diperkenalkan dengan trend e-commerce pada tahun 1994, dengan dibukanya situs-situs belanja pertama dan internet banking. Seiring dengan kecepatan informasi yang tersebar karena kemudahan yang ditawarkan oleh internet, informasi mengenai kelemahan sistem jaringan tersebut serta cara memanfaatkannya juga tersebar pula dalam komunitas bawah tanah mereka yang ingin memanfaatkannya.

Namun, dalam perkembangannya kemudian kasus-kasus cybercrime terus berkembang hingga kini. Akibatnya menimbulkan kerugian ratusan juta dollar setiap bulannya. Untuk mengantisipasi kegiatan-kegiatan tersebut maka mulai muncul lahan bidang baru yaitu pengamanan sistem informasi yang berjalan seiring dengan teknologi pengamanannya.

Kita sudah tak asing lagi dengan pasangan user ID dan password untuk identitas di dunia digital. Tapi bisa kita bayangkan jika kita memiliki banyak piranti atau

account Internet yang berbeda-beda, apalagi jika praktek keamanan yang dianjurkan adalah menggunakan password yang berbeda-beda untuk tiap peranti. Belum lagi jika kita mempunyai beberapa kartu ATM yang tentunya juga memerlukan pengamanan berupa PIN. Tentunya ini akan menimbulkan permasalahan karena kita menjadi terbebani dengan keharusan untuk menghafal password pengamanan yang berbeda-beda. Apalagi jika kita sudah mulai merasa bahwa password kita diketahui oleh orang lain tentunya kita akan disibukkan dengan proses updating password yang harus kita lakukan secara berkala.

Salah satu teknologi yang bisa membantu adalah adanya sistem pengamanan dengan smart card yang lebih handal dari pada sekedar password. Walaupun semua orang mengetahui password kita tetapi tanpa smart card tentunya password tersebut tidak akan berarti apa-apa. Namun demikian teknologi ini juga banyak kekurangan. Bagaimanan jika smart card hilang?

Oleh karena itu diperlukan teknologi lain yang lebih aman. Sistem biometrik merupakan sarana yang dikembangkan untuk pengamanan yang lebih baik dari pada teknologi-teknologi sebelumnya. Keamanan dengan sistem biometrik bekerja atas dasar ciri-ciri fisik pelaku (orangnya). Beberapa yang sudah dikembangkan diantaranya adalah dengan sidik jari, telapak tangan, wajah , retina dan suara.

Pengamanan dengan Sidik Jari

Sensor sidik jari sepertinya sudah tidak asing lagi penggunaannya. Dewasa ini banyak hardware yang ada dipasaran menggunakan pengamanan dengan sidik jari. Salah satu yang paling banyak adalah sistem presensi dengan sidik jadi. Bahkan pengamanan biometrik ini sudah merambah pula ke note book. Sebagai contoh IBM ThinkPad T42 menggunakan pengamanan sidik jari pada alas

pergelangan tangan yang didukung sejumlah peranti di dalam notebook yang disebut sebagai Embedded Security Subsystem. Baru-baru ini Hawlet Packard pun menyusul menggunakan teknologi yang sama untuk laptopnya.

Pengamanan dengan Telapak Tangan.

Sistem ini bekerja atas dasar prinsip keunikan pembuluh darah telapak tangan tiap-tiap individu, bahkan pada kembar siam sekalipun. Sistem memiliki sensor yang mampu mengenali pola telapak tangan seseorang selama hemoglobin deoxidized --sel darah merah-- dengan aktif mengaliri pembuluh darah. Dengan kata lain, hanya telapak tangan orang yang masih hidup yang dapat dideteksi.

Salah satu vendor yang sudah memproduksi perangkat ini adalah PT Fujitsu Systems. Baru-baru ini PT Fujitsu Systems Indonesia meluncurkan perangkat otentifikasi pembaca tapak tangan tanpa sentuh. Palm vein, demikian nama teknologi itu, merupakan teknologi keamanan biometrik yang bisa mengidentifikasi seseorang dari pembuluh darah telapak tangan tanpa menyentuh. Teknologi otentifikasi palm vein itu memanfaatkan keunikan dari hemoglobin deoxidized yang ada pada telapak tangan. Perangkat palm vein ini menangkap citra telapak tangan dengan memancarkan sinar sejenis inframerah. Hemoglobin deoxidized di telapak tangan akan menyerap itu. Dengan demikian mengurangi pemantulan dan menyebabkan pembuluh darah tampak seperti pola hitam. Pola pembuluh darah kemudian diverifikasi terhadap pola yang telah didaftarkan untuk mengidentifikasi seseorang. Karena pembuluh darah terletak di dalam tubuh dan mempunyai sangat banyak perbedaan corak. Hal itu menyebabkan pemalsuan identitas menjadi sangat sulit, sehingga memungkinkan tingkat pengamanan yang sangat tinggi.

Pengamanan dengan Pengenalan Wajah

Sistem pengenalan wajah sebagai kunci (password) menggunakan ekspresi seseorang yang tanpa dibuat-buat (dramatic) atau dengan kata lain relaxed face. Para psikolog menggolongkan ekspresi wajah ini, secara universal ke dalam 6 (enam) bentuk yakni: happines, sadness, disgust, anger, surprise dan fear. Dari enam ekspresi wajah ini, dapat dibangun suatu sistem yang dapat memahami dan melakukan komunikasi. Sistem analisis ekspresi wajah tersebut ditekankan pada enam ungkapan secara universal, bedasarkan pada gerakan muka dan aktifitas otot. Sistem pendeteksian wajah yang terdiri dari enam bagian titik dianggap paling dapat dipercaya untuk digunakan. Bagian titik ini terdiri atas : mata, mulut dan alis mata. Akan tetapi jarak antar bagian mata tidaklah cukup diperoleh secara langsung dari bagian titik muka, untuk itu diperlukan suatu bentuk metode pada bagian daerah mata. Bagian yang lain adalah mulut, ini secara global tidaklah cukup untuk menguraikan bentuk mulut. Oleh karena itu untuk mendapatkan bagian ini, diperlukan bagian wajah yang dinormalisir berdasarkan tepian dari pemetaan.

Dari penjelasan diatas, untuk mengenali bagian-bagian titik tersebut dapat digunakan suatu pendekatan vector quantization yang terawasi.

Pengamanan dengan Retina

Salah satu bagian tubuh manusia yang bersifat unik dan bisa dijadikan sebagai media pengamanan adalah iris atau selaput pelangi pada mata manusia. Letak selaput pelangi ini berada antara kornea dan lensa mata. Selaput pelangi ini sendiri akan terlihat oleh mata telanjang dari luar mata dan memiliki pola tertentu.

Dari pola yang dimiliki oleh selaput pelangi ini, ternyata setiap orang mempunyai pola yang unik. Selain unik pola ini juga memiliki kekonsistenan dan kestabilan yang tinggi bertahun-tahun tanpa mengalami perubahan. Dari kondisi ini maka para ahli mata mengusulkan bahwa iris ini dapat dijadikan seperti sidik jari untuk identitas pribadi seseorang.

Iris recognition menggunakan selaput pelangi mata yang dikodekan secara digital dan kemudian dijadikan kunci. Proses otentifikasinya membutuhkan dua tahap yakni : tahap identifikasi dan tahap verifikasi. Proses ini dapat dilakukan secara one-to-many (1:m) atau ane-to-one (1:1).

Proses one-to-many akan melibatkan satu database yang berisi user id dan iris template masing-masing id. Proses capture akan dilanjutkan dengan searching database untuk mencari iris template yang cocok. Sedangkan proses one-to-one akan lebih pada membandingkan dua iris, yaitu hasil scan dan iris template yang sudah disimpan. Dari kedua proses ini sudah tentu proses one-to-one lebih disukai karena prosesnya lebih cepat. Ini disebabkan oleh pembandingan yang dilakukan dalam skala terbatas.

Pengolahan Citra

Dari metode pengamanan yang telah dijelaskan diatas, semua menggunakan konsep pengolahan citra. Citra merupakan dimensi spatial yang berisi informasi warna dan tidak bergantung pada waktu. Citra merupakan sekumpulan titik-titik dari gambar, yang disebut piel (picture elemen). Titik-titik terebut menggambarkan posisi koordinat dan mempunyai intensitas yang dapat dinyatakan dengan bilangan. Intensitas ini menunjukkan warna citra, melalui penjumlahan (misal: Red, Green, Blue/RGB).

Koordinat memberikan informasi warna pixel berdasarkan : Brigthness (ketajaman), warna cahaya (hitam, abu-abu, putih) dari sumber, hue (corak warna) yang ditimbulkan oleh warna (merah, kuning, hijau dll) dan merupakan panjang gelombang dominan dari sumber.

Misalnya citra dengan 8 bit per pixel mempunyai 256 warna dan citra dengan 24 bit mempunyai 32768 warna, jadi tiap pixel dinyatakan dengan:

- bit 0 sampai 7 untuk warna merah
- bit 8 sampai dengan 15 untuk warna hijau.
- Bit 16 sampai dengan 24 untuk warna biru.

Kemungkinan kombinasi warna yang ada adalah = $256^3 + 256^2 + 256^1$ = 16.843.008, dimana nilai 0 menyatakan warna hitam sedangkan nilai 16.843.008 menyatakan warna putih.

Dari penjelasan diatas dapat diketahui bahwa citra dapat diubah dari domain spatial menjadi domain yang lain, dengan tujuan untuk mempermudah pengkodean. Proses perubahan ini dinamakan transformasi.

Transformasi citra dapat menghasilkan energi citra yang terkonsentrasi pada sebagian kecil koefisien transformasi dan kelompok lain yang mengandung sedikit energi. Transformasi ini dapat dilakukan dengan beberapa metode antara lain: Transformasi Cosinus diskret, transformasi wavelet, dan transformasi fourier. Keuntungan penggunaan transformasi adalah hasil dari domain lebih sesuai untuk proses pengkuantisasian.

Daftar Pustaka

Anonim, *Amankah Sistem Kita.* http//:www: students.ukdw.ac.id/~22033120/amankah.html.

Anonim, Perbandingan 3 Metode Iris Scan. http//www: budi.insan.co.id/courses/el7010/2004/agusbr-report.pdf

William Stalling, 2000, *Cryptography and Network Security: Principles and Practice*. Prentice-Hall.

Jani F. Mandala. *PemanfaatanTransformasi Wavelet Citra Wajah Sebagai Sistem Keamanan Kunci Kombinasi.* http//www:budi.insan.co.id/courses/ el695/projects2002-2003/jani-report.pdf

Ying-li Tian and Ruud M Bolle, *Automatic Neurtal Face Detecion Using Location and Shape Features.*