

Abstrak

Saat ini, teknik autentikasi dengan menggunakan biometrik sidik jari telah banyak digunakan pada berbagai bidang. Hal tersebut dikarenakan teknik autentikasi dengan menggunakan biometrik lebih aman dan nyaman dibandingkan menggunakan kata sandi tradisional. Namun disamping keamanan dan kenyamanan yang ditawarkan oleh autentikasi dengan menggunakan biometrik, terutama template yang disimpan pada media penyimpanan baik secara online maupun offline masih perlu dilindungi. Dalam rangka merealisasikan hal tersebut, sebuah teknik pada biometric cryptosystem diusulkan pada thesis ini, yaitu skema fuzzy vault.

Skema fuzzy vault ini adalah salah satu teknik pada biometric cryptosystem yang mengamankan data atau pesan (misalnya kunci atau pesan rahasia) dengan data sidik jari pengguna. Kemudian beberapa noise (chaff point) juga ditambahkan pada database agar data sidik jari pengguna dapat tersamarkan. Walaupun data sidik jari dalam bentuk minutiae dapat dilindungi dengan skema fuzzy vault dibandingkan sistem autentikasi tradisional, tapi menimbulkan kenyamanan dari pengguna menjadi berkurang. Hal tersebut dikarenakan data yang tersimpan pada database adalah data hasil enkripsi yang berisi gabungan dari pesan rahasia, data sidik jari dan beberapa noise.

Pada penelitian sebelumnya oleh Yadav, dkk, mengusulkan metode distance-

based pada skema fuzzy vault. Metode distance-based ini diusulkan karena tidak diperlukan proses pre-alignment dan rotasi pada gambar sidik jari pada saat registrasi maupun autentikasi. Kemudian dengan metode distance-based juga tidak menghasilkan helper data yang dapat mengakibatkan kebocoran informasi yang dapat dimanfaatkan oleh penyusup. Pada thesis ini, diusulkan metode distance-based dengan beberapa modifikasi, yaitu antara lain teknik minutiae filter, teknik generasi sejumlah chaff point (noise) dan teknik identifikasi kandidat poin. Dari hasil eksperimen dengan menggunakan metode yang diusulkan diperoleh untuk rata-rata kesalahan penolakan terhadap sidik jari pengguna aslinya (false rejection rate/FRR) dan rata-rata kesalahan penerimaan terhadap sidik jari orang lain (false acceptance rate/FAR) pada proses autentikasi mengalami penurunan. Pada metode sebelumnya menghasilkan FRR 13.4375% dan FAR 0.4515% dan pada metode yang diusulkan menghasilkan FRR 8.9475% dan FAR 0.3520%.

Kata kunci: *biometric cryptosystem, fuzzy vault scheme, minutiae filter, chaff point generation, candidate point identification..*