Perbandingan Metode-Metode Pembangkitan Kunci Berdasarkan Fitur Biometrik

Eka Mukti Arifah - 13507100[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]if17100@students.if.itb.ac.id

Abstract* — *Bio-cryptography merupakan teknik yang menggabungkan biometrik dan kriptografi. Dengan teknik ini, diperoleh keunggulan yang dimiliki oleh teknik biometrik dan kriptografi. Teknik ini juga lebih kuat terhadap serangan. Untuk menghasilkan kunci dari fitur biometrik, dapat dilakukan dengan key binding dan key generating. Makalah ini membahas tentang perbandingan metode pembangkitan kunci berdasarkan fitur biometrik dan bagaimana perbedaan metode tersebut dapat mempengaruhi tingkat keamanannya.

***Index Terms* — *bio-cryptography*, fitur biometrik, pembangkitan kunci**

I. PENDAHULUAN

Kunci merupakan sesuatu yang penting dalam kriptografi. Namun untuk menghasilkan kunci yang kuat terkadang digunakan kunci yang panjang dan sulit dihapal. Karena hal tersebut, para peneliti mengusulkan penggunaan fitur biometrik sebagai kunci kriptografi.

Penggunaan biometrik dalam kriptografi ini disebut *bio-cryptography*. Dengan penggabungan biometrik dan kriptografi, *bio-cryptography* mewarisi keunggulan keduanya. *Bio-cryptography* juga lebih kuat dalam menghadapi serangan sistem biometrik.

Fitur biometrik yang dapat digunakan antara lain sidik jari, iris, wajah, dan suara. Ada dua macam teknik untuk menghasilkan kunci dari fitur biometrik, yaitu *key binding* dan *key generating*. *Key binding* menghasilkan kunci dengan cara menggabungkan fitur biometrik dan kunci rahasia. Sedangkan, *key generating* menghasilkan kunci dengan cara membangkitkannya berdasarkan fitur biometrik yang diberikan. Kunci yang dihasilkan dari fitur biometrik ini bersifat kuat dan dapat digunakan berulang-ulang.

Fitur biometrik masing-masing orang memiliki karakteristik yang khas dan bersifat volatil. Pembangkitan kunci berdasarkan fitur biometrik perlu memperhatikan hal-hal tersebut. Saat ini telah banyak metode pembangkitan kunci yang diusulkan, antara lain menggunakan *bio-chaotic function* dan *multimodal biometrics*. Alasan penggunaan fitur tertentu pada metode tersebut tentu memiliki alasan khusus yang dapat dibandingkan satu sama lain. Selain itu, perbedaan metode dan algoritma yang digunakan ini tentu menghasilkan kekuatan kunci yang berbeda-beda.

II. BIO-CRIPTOGRAPHY

Meskipun biometrik memiliki lebih banyak keunggulan dibandingkan dengan teknik lainnya dalam hal keamanan, sistem biometrik rentan terhadap serangan. Serangan terhadap sistem biometrik dapat dibagi menjadi delapan tipe, yaitu:

1. Biometrik palsu, misalnya dengan menggunakan sidik jari yang terbuat dari plastik atau topeng wajah.
2. *Replay attack*, menggunakan sinyal biometrik sebelumnya, misalnya salinan citra sidik jari atau wajah dan sinyal audio yang direkam.
3. Mengganti ekstraktor fitur, misalnya dengan menggunakan pogram *trojan horse* untuk mengontrol proses ekstraksi fitur.
4. Mengubah representasi fitur, penyerang dapat mengganti set fitur asli dengan set fitur berbeda yang disintesis.
5. Mengganti *matcher*, penyerang dapat mengontrol modul pencocokan untuk membangkitkan nilai pencocokan palsu.
6. Mengubah templat yang disimpan, penyerang dapat mengubah templat biometrik terdaftar yang disimpan sehingga sistem dapat melakukan otorisasi terhadap pengguna ilegal secara tidak benar.
7. *Channel attack* di antara basis data dan *matcher*, dengan mengubah templat saat disalurkan melalui jalur transmisi yang menghubungkan basis data dan *matcher*.
8. Mengganti hasil, penyerang dapat mengganti keputusan hasil akhir pencocokan tanpa mempedulikan performansi sistem.

Di antara kedelapan tipe penyerangan tersebut, serangan terhadap templatlah yang menyebabkan kerusakan paling besar dan sulit dilacak. Untuk melindungi templat biometrik, terdapat dua metode utama, yaitu transformasi fitur dan *bio-cryptography*.

Teknik *biometric criptography* atau yang lebih dikenal dengan istilah *bio-cryptography*, melindungi kunci rahasia menggunakan fitur biometrik atau dengan membangkitkan kunci dari fitur biometrik. Dalam sistem seperti itu, beberapa informasi umum disimpan. Baik kunci rahasia maupun templat biometrik disembunyikan dalam informasi umum. Karena bagaimanapun juga, ekstraksi kunci ataupun templat biometrik dari informasi umum merupakan hal yang secara komputasional tidak mungkin untuk dilakukan.

Ada dua sub-kategori dalam teknik *bio-crytpography*, yaitu *key binding* dan *key generating*. *Key binding* menggabungkan kunci rahasia dan templat biometrik untuk menghasilkan informasi umum. Contoh metode *key binding* antara lain *fuzzy commitment* dan *fuzzy vault*. Sedangkan pada *key generating*, informasi umum dibangkitkan hanya dari templat biometrik dan kunci rahasia berasal dari informasi umum dan *query* fitur biometrik.

Contoh penggunaan *bio-cryptography* misalnya pada sistem otentikasi. Sandi lewat, PIN, atau kartu akses mudah hilang atau terlupakan. Selain itu, tidak dapat diketahui apakah orang yang memasukkan sandi lewat atau menggunakan kartu akses adalah orang yang sebenarnya dan bukan peniru. Dengan *bio-cryptography*, sistem otentikasi menjadi lebih kuat. Selain itu, informasi *bio-cryptography* lebih sulit untuk diinterpretasi jika dibandingkan dengan data biometrik biasa yang dapat disalahgunakan oleh penyerang.

III. METODE PEMBANGKITAN KUNCI

Berikut ini adalah beberapa metode pembangkitan kunci yang ada:

1. *Bio-Chaotic Stream Cipher-Based Iris Image Encryption*

Dengan metode ini, kunci rahasia dibangkitkan secara acak dan pada setiap sesi menggunakan kunci yang berbeda. Templat biometrik dienkripsi dengan skema *chaotic cryptography* yang membuatnya lebih sulit untuk didekripsi saat diserang. Langkah-langkah yang dilakukan pada algoritma ini dapat dilihat pada Fig. 1.

Fitur biometrik yang digunakan adalah citra dari iris. Fitur yang telah diekstrak dengan kode L. Rose digunakan sebagai kondisi awal untuk membangkitkan kunci rahasia. Teknik yang digunakan untuk membangkitkan kondisi awal ini adalah *Hamming Distance*, misalnya:

$$Initial\ Condition = 2^n - 1 \quad (1)$$

Kondisi awal ini kemudian diubah menjadi kunci rahasia menggunakan metode LSFR. LSFR dengan panjang n terbatas terdiri dari n tahap [a_{n-1}, a_{n-2}, a_{n-3}, ..., a_0] dengan $a_i \in P_q$ dan sebuah polinomial.

$$B(x) = 1 + c_1 x + c_2 x_2 + .. + c_n x_n \text{ over } P_q \quad (2)$$

Kunci rahasia dan templat iris kemudian di-xor secara paralel untuk membangkitkan kunci biometrik dengan menggunakan persamaan:

$$Biometric\ Key = a_1 \oplus b_1, a_2 \oplus b_2, \ldots, a_n \oplus b_n \quad (3)$$

Kunci biometrik ini kemudian di-xor dengan blok lain pada templat iris yang telah dibagi dalam 128 bit/blok. Agar algoritma bertambah kuat, ditambahkan fungsi *chaotic* untuk kunci biometrik dan mengaplikasikannya ke seluruh citra iris dengan persamaan berikut:

$$x_{n+1} = r x_n (1 - x_n) \quad (4)$$

2. *Multimodal Modalities: Feature Level Fusion of Fingerprint and Iris*

Penggunaan fitur biometrik *multimodal* dapat meningkatkan akurasi. Selain itu, metode ini mempersulit upaya penyerangan terhadap sistem karena untuk melakukan serangan diperlukan lebih dari satu fitur biometrik.

Langkah pertama yang dilakukan pada metode ini adalah ekstraksi *minutiae point* dari sidik jari. Ada dua pendekatan untuk melakukan ekstraksi tersebut. Pada pendekatan pertama, dilakukan *pre-processing* citra sidik jari dengan menggunakan *Histogram Equalization* (HE) dan *Wiener Filtering*.

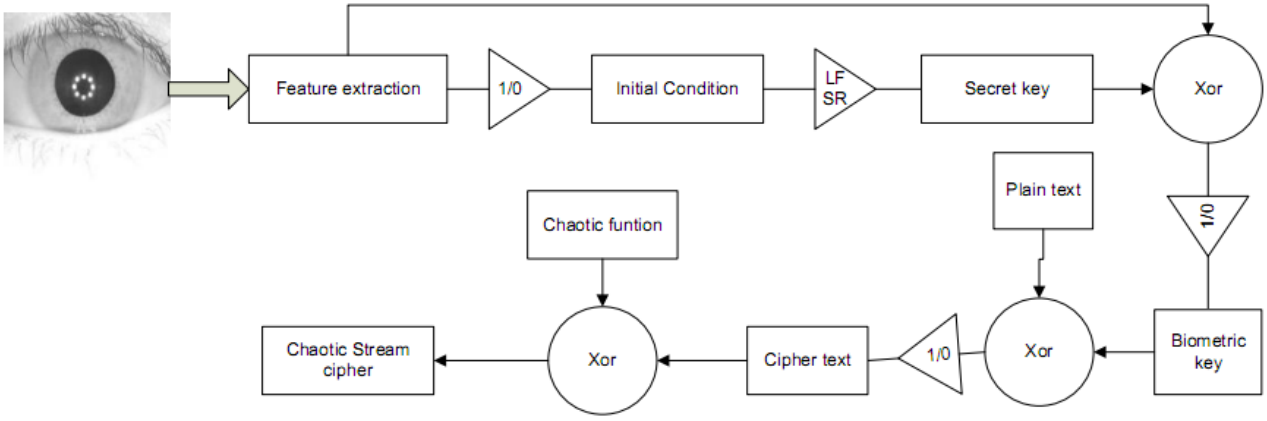

Fig. 1 Blok Diagram Algoritma Bio-Chaotic

Setelah *pre-processing*, kemudian dilakukan segmentasi terhadap citra hasil *pre-processing*. Kemudian, dilakukan estimasi *orientation field*. *Orientation field* sidik jari adalah orientasi lokal dari struktur *ridge-valley*.

Langkah selanjutnya adalah peningkatan citra dengan menggunakan *Gaussian Low-Pass Filter* dan *Gabor Filter*. Setelah itu, citra hasilnya digunakan untuk ekstraksi *minutiae point* dengan menggunakan *binarization* dan *morphological operations*.

Pada pendekatan kedua, ekstraksi *minutiae point* pada sidik jari dilakukan dengan peningkatan citra berdasarkan statistik lokal menggunakan *neighborhood operations*, ekstraksi *region of interest* (ROI), estimasi *orientation field* sidik jari, serta ekstraksi *minutiae point*. Pendekatan kedua ini memberikan solusi yang lebih optimal dibandingkan dengan pendekatan pertama.

Berikutnya adalah ekstraksi fitur dari citra iris. Tahap pertama dalam ekstraksi fitur iris adalah segmentasi. Pada tahap segmentasi ini dilakukan dalam dua tahap, yaitu estimasi dari batasan iris serta pengurangan *noise*.

Estimasi batasan iris dilakukan dengan menggunakan *Canny edge detection* dan *Hough Transform*. Setelah itu dilakukan isolasi bagian lipatan serta bulu mata. Setelah citra iris tanpa *noise* diperoleh, selanjutnya dilakukan normalisasi menggunakan *Daugman's Rubber Sheet Model*.

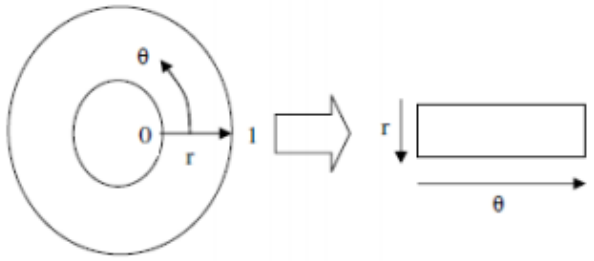

Fig. 2 Daugman's Rubber Sheet Model

Setelah dinormalisasi, kemudian dilakukan ekstraksi tekstur iris. Setelah ekstraksi fitur sidik jari dan iris, langkah selanjutnya adalah menggabungkan hasilnya. Untuk menggabungkan kedua fitur tersebut, pertama-tama keduanya didefinisikan dalam bentuk vektor.

Vektor M_1 berisi setiap nilai koordinat x dari *minutiae point* sidik jari, vektor M_2, berisi nilai koordinat y dari *minutiae point* sidik jari, vektor C_1 berisi bagian bilangan riil dari bilangan kompleks tekstur iris, sedangkan vektor C_2 berisi bilangan imajiner dari bilangan kopleks tersebut.

Kemudian, dilakukan pengacakan pada vektor fitur individual. Untuk vektor M_1, metode pengacakan yang dilakukan adalah sebagai berikut:

i. Pembangkitan vektor R berukuran M_1. Nilai dari vektor ini tergantung nilai *seed*.
ii. Untuk mengacak komponen ke-i dari vektor M_1, dilakukan :
   - Kalikan komponen ke-i pada vektor R dengan nilai integer yang besar.
   - Bagi nilai produk yang diperoleh dengan ukuran vektor M_1 dan ambil sisa hasil pembagiannya
   - Sisa hasil bagi yang disebut j kemudian digunakan untuk penukaran nilai dengan aturan komponen ke i ditukar dengan nilai komponen ke j.
iii. Langkah (ii) diulangi untuk seluruh komponen pada M_1. Vektor hasilnya disebut sebaai P_1.

Pengacakan dilakukan untuk 3 vektor lainnya. Dari proses ini dihasilkan empat buah vektor, yaitu P_1, P_2, P_3, dan P_4. Keempat vektor ini kemudian digabungkan untuk menghasilkan *joined* vektor J_1 dan J_2.

Proses penggabungan untuk P_1 dan P_3 adalah sebagai berikut:

i. Dibuat vektor V_1 yang berisi komponen P_1 secara berulang-ulang.
ii. Untuk setiap komponen P_3,
   - Pemangkatan $P_3^{V_{i(i)}}$, melibatkan dua angka yaitu basis P_3 dan pangkat $v_i(i)$
   - Hasilnya disimpan dalam vektor J_1 saat hasil melibihi level *threshold*.
   - Jika tidak, lakukan pemangkatan $(P_3(i)^{V_{i(i)}})^{V_{i(i+1)}}$ diulangi sampai mencapai nilai *threshold*.

Langkah tersebut diulangi untuk vektor P_2 dan P_4 untuk menghasilkan vektor J_2. Vektor J_1 dan J_2 kemudian dikombinasikan untuk menghasilakan templat biometrik *multimodal* T_B.

Pengkombinasian dilakukan dengan cara:

i. Ambil bilangan prima tertinggi selanjutnya untuk komponen ke-i pada vektor J_1 dan J_2.
ii. Kalikan 2 bilangan prima tersebut
iii. Simpan hasilnya pada komponen ke i vektor T_B.

Langkah tersebut diulangin untuk semua komponen vektor J_1 dan J_2. Dari gabungan fitur sidik jari dan iris T_B inilah kemudian dilakukan pembangkitan kunci kriptografi.

Vektor T_B direpresentasikan sebagai berikut:

$T_B = [t_1\, t_2\, t_3 \ldots t_d]$

Rumus yang digunakan untuk pembangkitan kunci adalah:

$$N = \begin{cases} [t_1 \;\; t_2 \;\; \cdots \;\; t_k] & ;if \;\; |T_B| > k \\ [t_1 \;\; t_2 \;\; \cdots \;\; t_d] << t_i \,;\, d+1 \geq i \geq k & ;if \;\; |T_B| < k \end{cases}$$

$$\text{Where, } t_i = \frac{1}{d}\sum_{j=1}^{d} t_j$$

Finally, the key K_B is generated from the vector N,

$$K_B << \begin{cases} 1 & \text{if} \quad N_i \geq N_{avg} \\ 0 & \text{if} \quad N_i < N_{avg} \end{cases} \quad ; \quad i = 1,2,3\ldots,k$$

$$\text{Where, } N_{avg} = \frac{1}{k}\sum_{i=1}^{k} N_i$$

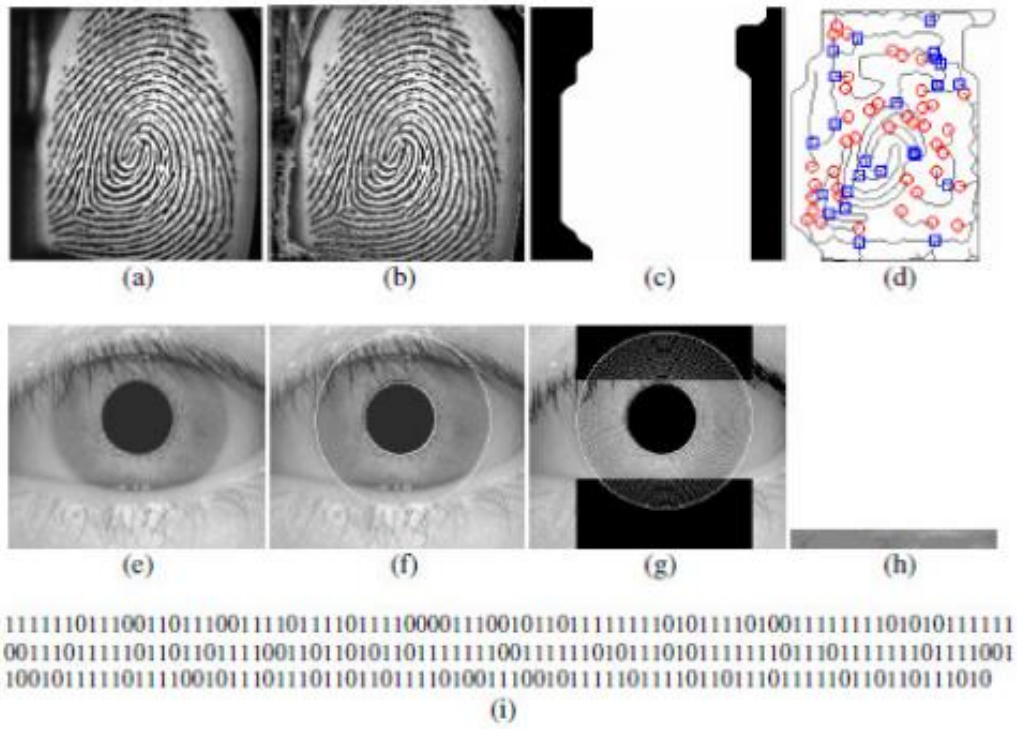

Fig. 3 Proses Ekstraksi Fitur dan Pembangkitan Kunci

Pada Fig. 3 dapat dilihat citra yang terlibat pada algoritma pembangkitan kunci dengan fitur biometrik multimodal gabungan sidik jari dan iris.

(a) masukan citra sidik jari
(b) citra sidik jari yang telah diperjelas
(c) ekstraksi ROI
(d) citra sidik jari dengan minutiae point hasil ekstraksi
(e) ekstraksi tekstur iris mulai dari masukan citra iris
(f) penentuan lokasi dan batasan iris
(g) pendeteksian batas lipatan mata bagian atas dan bawah
(h) citra iris hasil normalisasi
(i) kunci kriptografi 256 bit hasil pembangkitan berdasarkan gabungan fitur ekstraksi sidik jari dan iris.

IV. ANALISIS

Kekuatan dari algoritma pertama, yaitu Bio-Chaotic Algorithm terletak pada kunci biometrik yang dibangkitkan dari hasil xor kunci rahasia dan templat iris.

Sesuai diagram pada Fig.1, dapat dilihat bahwa fitur ekstraksi iris digunakan sebanyak dua kali, yaitu sebagai initial vektor untuk menghasilkan kunci rahasia yang kemudian digunakan lagi untuk menghasilkan kunci kriptografi. Dengan demikian, ekstraksi fitur biometrik iris perlu menggunakan metode yang baik. Dalam algoritma ini, ekstraksi fitur iris menggunakan kode L. Rose.

Skema algoritma ini sederhana, operasi yang dilakukan banyak menggunakan operasi xor saja. Meskipun sederhana, namun hasil enkripsi akan sulit untuk dipecahkan karena cipherteks hasil enkripsi awal masih diproses kembali dengan *chaotic function*.

Dalam pengujiannya, dilakukan pengubahan yang sangat sedikit pada nilai templat iris. Namun, hasil cipherteks dari pengubahan itu bernilai besar. Dari hal tersebut dapat disimpulkan bahwa nilai entropi dari algoritma ini bernilai cukup tinggi.

Pada algoritma kedua, algoritma cukup kompleks. Selain dilakukan ekstraksi fitur sidik jari dan iris, operasi penggabungan hasil ekstraksinya juga kompleks.

Disebutkan bahwa ternyata dari dua jenis pendekatan untuk ekstraksi sidik jari, ternyata pendekatan kedua memberikan hasil yang lebih optimal daripada pendekatan pertama.

Dari hal tersebut dapat diketahui bahwa metode yang digunakan pada ekstraksi fitur biometrik dapat memberikan hasil yang berbeda-beda sehingga pemilihan metode ekstraksi fitur biometrik adalah salah satu hal yang krusial dalam pembangkitan kunci berdasarkan fitur biometrik.

Dengan algoritma tersebut, serangan dengan menggunakan biometrik palsu akan sulit dilakukan karena fitur biometrik yang digunakan pada proses enkripsi adalah gabungan dari beberapa fitur biometrik.

Pada algoritma kedua ini, ada tiga modul utama, yaitu ekstraksi fitur biometrik sidik jari dan iris, modul pembuatan templat fitur biometrik *multimodal* gabungan hasil ekstraksi yang dilakukan sebelumnya, serta modul pembangkitan kunci berdasarkan fitur biometrik *multimodal*.

Ketiga modul tersebut saling mempengaruhi kekuatan kunci yang dihasilkan karena hasil dari satu modul akan diproses lebih lanjut di modul berikutnya. Sehingga jika pada salah satu modul, algoritma atau proses yang dijalankan kurang baik, maka kunci yang dihasilkan pun akan kurang keamanannya.

Fitur biometrik seseorang bersifat volatil dan templat maupun sampel templat fitur yang dihasilkan dapat berbeda-beda dari waktu ke waktu.

Dengan demikian, perancangan algoritma pembangkitan kunci perlu mempertimbangkan hal ini. Apakah perubahan yang sedikit pada fitur biometrik masih dapat menghasilkan plainteks yang sama saat proses dekripsi.

Karena sifat fitur biometrik yang unik dan melekat pada seseorang, jika algoritmanya tidak baik terkadang hal ini juga bisa menjadi kesulitan tersendiri.

Misalnya, plainteks tidak dapat dikembalikan karena algoritma tidak menghasilkan kunci yang sama dengan kunci yang digunakan pada saat proses enkripsi.

Oleh karena itu, perlu pula diusulkan algoritma pembangkitan kunci dimana kunci biometrik tersebut dapat dibatalkan.

Dijelaskan sebelumnya bahwa pembangkitan kunci dengan fitur biometrik ini berfungsi utama untuk melindungi serangan terhadap templat pada sistem biometrik. Namun, seharusnya dipikirkan pula bagaimana kunci yang dihasilkan dari algoritma pembangkitan kunci ini tahan terhadap berbagai jenis serangan lainnya.

Dengan penggunaan fitur biometrik untuk pembangkitan kunci, keuntungan lain yang dapat diperoleh adalah meskipun data dapat disadap oleh penyerang, namun data tersebut tidak dapat diinterpretasi dengan mudah seperti data biometrik tanpa proses enkripsi biasa.

Penggunaan fitur biometrik dalam pembangkitan kunci kriptografi dapat meningkatkan *confusion* dan *diffusion* yang merupakan prinsip penting dalam penyusunan algoritma kriptografi.

Perlu banyak sampel pengujian untuk membuktikan bahwa algoritma yang diusulkan dapat mengakomodasi perubahan-perubahan yang mungkin terjadi pada fitur biometrik, misalnya karena terjadi luka pada jari.

V. KESIMPULAN

1. Operasi yang dilakukan pada *Bio-Chaotic Algorithm* sederhana, namun hasil enkripsinya kuat.
2. *Bio-Chaotic Algorithm* menerapkan prinsip *confusion* dan *diffusion* dengan baik. Dapat dilihat dari perbedaan besar yang dihasilkan dari perubahan yang sedikit pada fitur biometrik.
3. *Bio-Chaotic Algorithm* memiliki nilai entropi (*randomness*) yang tinggi karena penggunaan *chaotic function*.
4. Penggunaan fitur biometrik *multimodal* dapat meningkatkan keamanan, terutama seranganberupa fitur biometrik palsu.
5. Penggunaan fitur biometrik *multimodal* membutuhkan pemrosesan yang kompleks.
6. Perlu dilakukan perbandingan lebih lanjut terhadap metode-metode yang digunakan untuk melakukan ekstraksi fitur biometrik untuk menentukan metode apa yang akan memberikan hasil yang optimal.
7. Kunci yang dihasilkan dari fitur biometrik harus tetap mendukung prinsip *confusion* dan *diffusion* yang merupakan prinsip penting dalam perancangan algoritma kriptografi.
8. Kunci yang dihasilkan dari pembangkitan kunci berdasarkan fitur biometrik ini perlu memiliki nilai entropi (*randomness*) yang tinggi.
9. Kunci yang dihasilkan dari fitur biometrik bersifat unik.
10. Fitur biometrik bersifat volatil dan templat serta contoh templat dapat berubah dari waktu ke waktu sehingga dalam perancangan algoritma perlu memperhatikan hal tersebut.
11. Perlu diusulkan metode *recovery* kunci, misalnya dengan algoritma yang memungkinkan terjadinya pembatalan kunci biometrik.
12. *Bio-cryptography* memiliki gabungan keuntungan dari sistem biometrik dan kriptografi yang meningkatkan keamanan hasil kriptografi sekaligus lebih tahan terhadap serangan.
13. Tidak hanya serangan terhadap templat, algoritma yang terlibat dalm pembangkitan kunci dengan fitur biometrik juga seharusnya dapat didesain untuk lebih tahan pada jenis serangan lain.

REFERENSI

[1] A. Jagadeesan, Thillaikkarasi. T., dan K. Duraiswamy, "Protected Bio-Cryptography Key Invention from Multimodal Modalities: Feature Level Fusion of Fingerprint and Iris", EuroJournals Publishing Inc, 2011.

[2] Abdullah Alghamdi, Hanif Ullah, Maqsood Mahmud, dan Muhammad Khurram Khan, "Bio-Chaotic Stream Cipher-Based Iris Image Encryption", 2009.

[3] K. Xi dan J. Hu, Bio-Cryptography. 2010

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, 23 Maret 2011

Eka Mukti Arifah
13507100