

KOMBINASI KUNCI BIOMETRIK CANCELABLE DAN KUNCI KRIPTOGRAFI UNTUK MENGAMANKAN FILE TEKS

Fritz Gamaliel

Sekolah Tinggi Elektro dan Informatika, Institut Teknologi Bandung
Jl. Ganessa No.10, Jawa Barat 40132, Indonesia
fritzgamaliel@gmail.com

Abstrak – Kriptografi membutuhkan kunci. Kunci yang dibangkitkan dari biometrik merepresentasikan orang tetapi biometrik bersifat *irrevocable*. Transformasi *cancelable* membuat biometrik bersifat *revocable*. Penelitian ini menerapkan salah satu metode transformasi *cancelable* pada salah satu metode pembangkit kunci dari biometrik. Persoalan yang muncul dari penerapan tersebut dijawab dengan cara mengkombinasikan kunci pendek yang berhasil dibangkitkan dari template hasil transformasi *cancelable* dengan kunci yang dibangkitkan dari sistem kriptografi sehingga didapatkan panjang kunci yang dibutuhkan oleh algoritma kriptografi yang akan digunakan. Usulan tersebut diimplementasikan ke dalam Matlab 7.11.0 dan PHP 5.4.7. Hasil implementasi diuji dengan menggunakan sampel citra sidik jari yang diambil dari The Third International Fingerprint Verification Competition (FVC2004). Hasil pengujian menunjukkan bahwa individu sama tetapi kunci beda, individu beda tetapi kunci sama, dan transformasi *cancelable* dapat dilaksanakan secara *repeatable*. Dari penelitian yang dilaksanakan disimpulkan bahwa mengkombinasikan kunci pendek yang dibangkitkan dari template *cancelable* dengan kunci dari kriptografi dapat digunakan untuk mendapatkan panjang kunci yang dibutuhkan oleh algoritma kriptografi yang digunakan.

Kata Kunci - Biometrik, Cancelable, Sidik Jari, Kriptografi, Pembangkit Kunci

I. PENDAHULUAN

Komunikasi antara *sender* dan *receiver* bisa berupa verbal atau non-verbal. Semakin banyak komunikasi data, semakin harus memperhatikan aspek keamanannya. Kriptografi, merupakan cara memastikan aspek keamanan data, membutuhkan kunci. Kunci konvensional tidak merepresentasikan orang tetapi kunci yang dibangkitkan dari biometrik merepresentasikan orang. Biometrik bersifat *irrevocable* tetapi biometrik hasil transformasi *cancelable* bersifat *revocable*.

Penelitian Bais dkk. (2012) mengurangi kompleksitas algoritma pembangkitan kunci dari biometrik. Penelitian Solanki (2013) menyediakan yang lebih baik ketika terjadi pengkompromian biometrik dengan cara mengkombinasikan kunci yang dibangkitkan dari biometrik dengan kunci yang dibangkitkan dari kriptografi. Hasil eksperimen yang tertulis pada paper keduanya menunjukkan bahwa Solanki (2013) dan Bais dkk. (2012) menggunakan metode yang sama (*pre-processing*, ekstraksi *minutiae*, dan pembangkitan kunci).

Penelitian Ang dkk. (2005) menerapkan konsep kunci pada transformasi *cancelable* sehingga lebih dari satu template *cancelable* dapat dibangkitkan dari satu template asli (semakin aman).

Kebutuhan atas *many-to-one* harus dipenuhi oleh suatu transformasi *cancelable* untuk menjamin *non-invertibility* pada template hasil transformasinya. Di lain pihak, kebutuhan tersebut mengakibatkan semakin sedikitnya jumlah fitur yang dapat diekstraksi dari template hasil transformasi *cancelable*. Hal tersebut mengakibatkan semakin pendeknya kunci yang dapat dibangkitkan dari template hasil transformasi *cancelable*.

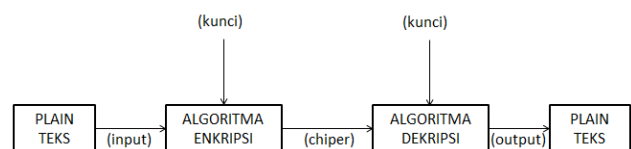
Pada penelitian ini, persoalan yang muncul dijawab dengan cara mengkombinasikan kunci pendek yang berhasil dibangkitkan dengan kunci yang dibangkitkan dari sistem kriptografi sehingga didapatkan panjang kunci yang dibutuhkan oleh algoritma kriptografi yang akan digunakan. Pada penelitian ini, kunci hasil kombinasi digunakan oleh algoritma blowfish untuk mengamankan file teks.

II. DASAR TEORI

II.1 KRIPTOGRAFI

Data yang bersifat rahasia perlu dibuatkan sistem pengamanannya agar tidak diketahui atau diubah oleh pihak yang tidak berhak. Kriptografi merupakan salah satu cara untuk mengamankan suatu data. Perkembangan pada kriptografi diikuti dengan perkembangan upaya pengkompromiannya. Pada prinsipnya, kriptografi memiliki empat komponen utama sebagaimana digambarkan pada Gambar I. Pertama, *plain-text* (pesan yang dapat dibaca). Kedua, *cipher-text* (pesan yang tidak dapat dibaca). Ketiga, *key* (kunci untuk mengenkripsi dan mendekripsi). Keempat, *algorithm* (metode untuk mengenkripsi dan mendekripsi).

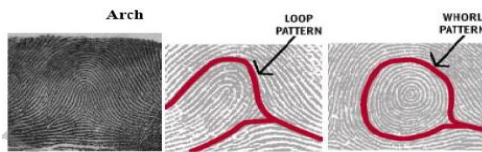
Menurut Mandal (2012), blowfish memiliki keunggulan dalam mengenkripsi dan mendekripsi file teks. Blowfish memiliki 2 bagian, yaitu: ekspansi kunci dan enkripsi / dekripsi. Ekspansi kunci dijalankan sebelum enkripsi / dekripsi.



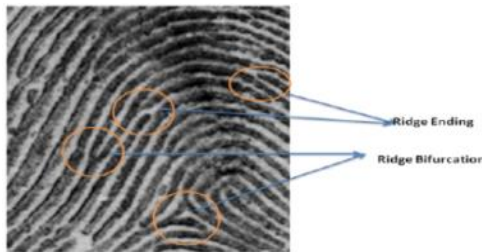
Gambar I. Model sistem kriptografi

II.2 SIDIK JARI

Suatu pola sidik jari dibentuk dari *ridge* dan *valley*. Pada level global, pola tersebut dikategorikan ke dalam tipe: *loop*, *arch* dan *whorl* seperti Gambar II. Pada level lokal, pola tersebut dikategorikan ke dalam tipe: *ridge ending* dan *ridge bifurcation* seperti Gambar III. *Loop* adalah pola sidik jari di mana garis memasuki pokok lukisan dari suatu sisi, melengkung di tengah pokok lukisan, dan kembali ke arah sisi semula. *Arch* adalah pola sidik jari dimana garis datang dari sisi lukisan yang satu mengalir ke sisi lukisan yang lain dengan gelombang naik ditengah. *Whorl* adalah pola sidik jari yang mempunyai dua *delta* dan sedikitnya satu garis melingkar. *Ridge ending* adalah titik dimana *ridge* berakhir, sementara itu *ridge bifurcation* adalah titik di mana *ridge* bercabang.



Gambar II. Fitur sidik jari global



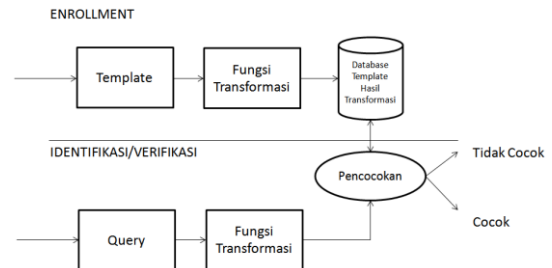
Gambar III. Fitur sidik jari lokal

Tahapan umum pengolahan citra sidik jari adalah: akuisisi, *pre-processing*, ekstraksi *minutiae*, dan *matching*. Akuisisi adalah tahapan menangkap citra sidik jari. *Pre-processing* adalah tahapan memperjelas *ridge* dan *valley*. Tahapan *pre-processing* terdiri atas: segmentasi, normalisasi, filter, binerisasi, dan penipisan. Segmentasi memisahkan *foreground* dari *background*. Normalisasi membuat citra memiliki nilai *mean* dan *variance* yang diinginkan. Filter membersihkan citra dari *noise*. Binerisasi mengkonversi citra abu-abu ke dalam citra biner. *Thinning* mengurangi lebar *ridge* sampai *ridge* memiliki lebar satu pixel. Ekstraksi *minutiae* mengekstraksi *ridge ending* dan *ridge bifurcation*. *Matching* mencocokkan *minutiae* template dengan *minutiae query*.

II.3 TRANSFORMASI CANCELABLE

Konsep transformasi *cancelable* (transformasi yang dapat dibatalkan) dikemukakan pertama kali oleh Ratha dkk. (2001). Ide ini muncul karena ada dua macam kekurangan pada metode pengamanan biometrik yang sudah ada. Pertama, sistem *hash* tidak mengakomodir variasi interaksi subjek terhadap sensor. Kedua, sistem kriptografi tidak mengakomodir serangan-serangan terhadap titik dekripsi. Konsep transformasi *cancelable* menggunakan model seperti Gambar IV. *Enrollment* digunakan untuk menyimpan data

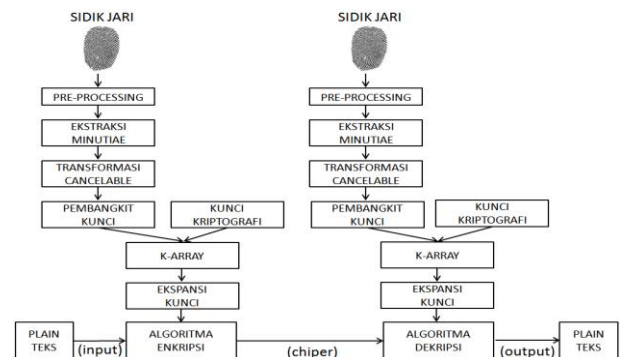
orang sebagai template hasil transformasi. Identifikasi digunakan untuk memkomparasikan data *query* dengan seluruh data template hasil transformasi sampai ditemukan *match*. Verifikasi digunakan untuk memastikan apakah data *query* cocok dengan tepat satu data template hasil transformasi. Baik pada *enrollment* ataupun identifikasi dan verifikasi, unit fungsi transformasi digunakan untuk mengubah data input berdasarkan suatu aturan. Sedangkan unit pencocokan membandingkan data input dengan data template dan menentukan apakah keduanya *match* berdasarkan suatu *threshold*.



Gambar IV. Model sistem cancelable.

III. METODE YANG DIUSULKAN

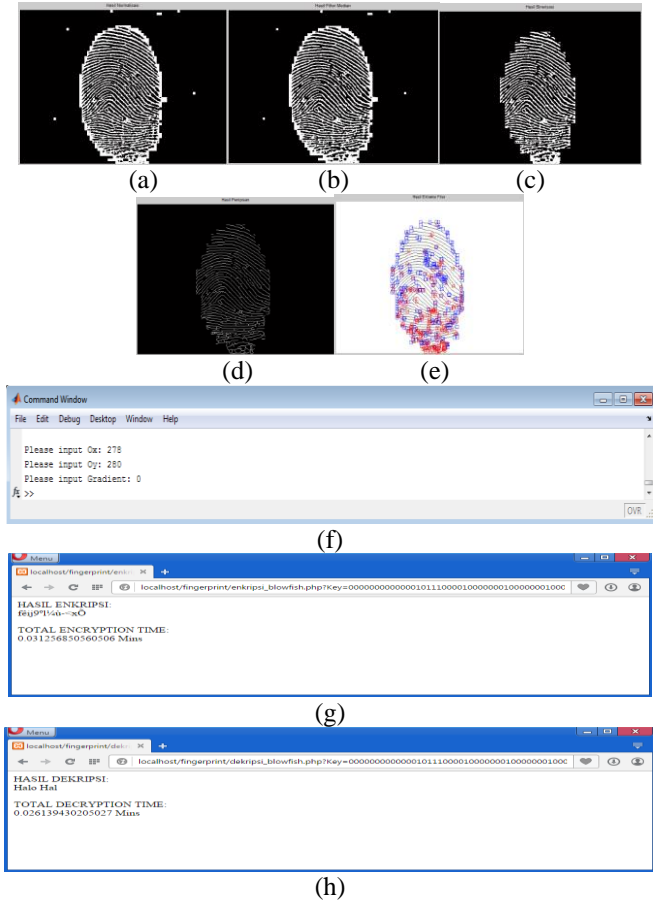
Pada penelitian ini, konsep transformasi *cancelable* diterapkan pada metode pembangkit kunci dari sidik jari *irrevocable*. Secara spesifik, diterapkan metode yang diajukan oleh Ang dkk. (2005) pada metode pembangkit kunci dari sidik jari *irrevocable* yang diajukan oleh Bais dkk. (2012) dan Solanki (2013). Persoalan yang muncul dari penerapan tersebut adalah semakin sedikitnya jumlah fitur yang dapat diekstraksi dari template hasil transformasi *cancelable*. Hal tersebut mengakibatkan semakin pendeknya kunci yang dapat dibangkitkan. Persoalan tersebut dijawab dengan cara mengkombinasikan kunci pendek yang berhasil dibangkitkan dengan kunci yang dibangkitkan dari sistem kriptografi sehingga didapatkan panjang kunci yang dibutuhkan oleh algoritma kriptografi yang akan digunakan. Hasilnya dapat digambarkan seperti pada Gambar V. Pada gambar tersebut, terlihat bahwa sidik jari *query* mesti melalui tahapan *pre-processing*, ekstraksi *minutiae*, transformasi *cancelable*, dan pengkombinasian kunci sebelum dapat digunakan pada tahapan ekspansi kunci dan enkripsi-dekripsi dalam algoritma blowfish.



Gambar V. Metode yang diusulkan

IV. IMPLEMENTASI

Metode yang diusulkan telah diimplementasikan ke dalam Matlab 7.11.0 dan PHP 5.4.7. Hasil akhir tampilan sebagaimana digambarkan pada Gambar VI.








Gambar VI. a) Citra setelah normalisasi b) Citra setelah filter median c) Citra setelah binerisasi d) Citra tipis e) Ekstraksi minutiae f) Parameter transformasi g) Hasil enkripsi h) Hasil dekripsi

V. EKSPERIMEN DAN PEMBAHASAN

Hasil implementasi diuji dengan menggunakan sampel citra sidik jari yang diambil dari The Third International Fingerprint Verification Competition (FVC2004). Di bawah ini adalah salah satu hasil eksperimen yang didapatkan.

Tabel I: Hasil Eksperimen

Citra Sidik Jari	Parameter Transformasi	Kunci Dari Template Hasil Transformasi
	O _x :300 O _y :300 Φ: 0	011110
	O _x :300 O _y :300 Φ: 0	1

	O _x :300 O _y :300 Φ: 0	0111
	O _x :300 O _y :300 Φ: 0	1
	O _x :300 O _y :300 Φ: 0	0

Dari hasil eksperimen didapatkan bahwa adanya kemungkinan individu sama tetapi kunci beda, individu beda tetapi kunci sama, dan transformasi *cancelable* bersifat *repeatable*. Secara spesifik, terdapat kunci yang sama dibangkitkan dari hasil transformasi yang sama terhadap template sidik jari individu yang berbeda. Hal seperti ini menyebabkan aspek keamanan *confidentiality* dan *integrity* menjadi tidak terjamin sepenuhnya. Selain itu, hasil transformasi *cancelable* dapat dibangkitkan secara *repeatable* sehingga kunci hasil transformasi juga dapat dibangkitkan secara *repeatable*. Perlu dicatat bahwa kunci hasil kombinasi belum tentu dapat dibangkitkan secara *repeatable* karena kunci hasil transformasi tersebut harus dikombinasikan terlebih dahulu dengan kunci yang dibangkitkan dari fungsi *random* untuk mendapatkan panjang kunci yang dibutuhkan oleh algoritma kriptografi yang digunakan.

VI. KESIMPULAN DAN SARAN

Langkah-langkah membangkitkan kunci kriptografi dari biometrik hasil transformasi *cancelable* yang diadopsi adalah: Pertama, mengekstraksi *minutiae*. Kedua, *minutiae* yang terekstraksi ditransformasi dengan menggunakan fungsi transformasi *cancelable*. Ketiga, *minutiae* hasil transformasi digunakan untuk membangkitkan kunci. Terakhir, kunci yang berhasil dibangkitkan dikombinasikan dengan kunci kriptografi. Dari penelitian yang dilaksanakan, langkah tersebut dapat digunakan untuk mendapatkan kunci dengan panjang yang dibutuhkan oleh algoritma kriptografi yang digunakan. Oleh karena tidak semua orang memiliki tangan, maka pada penelitian berikutnya akan digunakan biometrik multimodal.

DAFTAR PUSTAKA

- Christina and Irudayaraj, J. (2014) :Optimized Blowfish Encryption Technique, *International Journal of Innovative Research in Computer and Communication Engineering*, **2**,5009-5015.
- Solanki, K. (2013) : A New Approach To Symmetric Key Generation Using Combination Of Biometric Key And Cryptographic Key To Enhance Security Of Data, *International Journal of Engineering Research & Technology*, **2**,1-7.
- Bais, R. and Mehta, K. (2012) :Biometric Parameter Based Cryptographic Key Generation, *International Journal of Engineering and Advanced Technology*, **1**,157-160.

- Ang, R., Naini, R., and McAven, L. (2005) :Cancelable Key-Based Fingerprint Template, *Australasian Conference on Information Security and Privacy*, 242-252.
- Patel, V., Ratha, N., and Chellappa, R. (2015) :Cancelable Biometric: A Review, *IEEE SIGNAL PROCESSING MAGAZINE*, 54-65.
- Mastali, N. (2013) :*Synergizing Fingerprint Biometrics And Cryptography for Improved Authentication*, Tesis Program Magister, University of Technology Sydney
- Thai, R. (2003) :*Fingerprint Image Enhancement and Minutiae Extraction*, Tesis Program Magister, The University of Western Australia
- Jovanovic, N., Kruegel, C., and Krida, E. (2006) : Pixy : A Static Analysis Tool for Detecting Web Application Vulnerabilities, *Proceeding of the 2006 IEEE Symposium on Security and Privacy*.