KOMPARASI EKSPERIMENTAL PERFORMA PEMBANGKITAN *CHAFF POINT* TEKNIK *SQUARE BOUNDARY* DAN *IMAGE CELLING*

Bambang Pilu Hartato*[1], Teguh Bharata Adji[2], Agus Bejo[3]
[1]Program Studi Teknologi Informasi, Universitas Amikom Purwokerto, Purwokerto
[2,3]Departemen Teknik Elektro dan Teknologi Informasi, Universitas Gadjah Mada, Yogyakarta
e-mail: *[1]bambang.pilu@amikompurwokerto.ac.id, [2]adji@ugm.ac.id, [3]agusbj@ugm.ac.id

Abstrak

Fuzzy vault adalah sebuah skema bio-enkripsi yang dapat digunakan sebagai pendukung keamanan kriptografi konvensional. Konsep utama dari fuzzy vault adalah menambahkan unsur otentifikasi biometrik pada kriptografi. Fuzzy vault menggunakan fitur-fitur biometrik untuk melakukan enkripsi ataupun dekripsi terhadap kunci rahasia, yang sebelumnya telah diubah menjadi koefisien-koefisien suatu persamaan polinomial. Tingkat kesulitan dalam melakukan rekonstruksi polinomial menentukan tingkat keamanan dari fuzzy vault. Penambahan chaff point (noise) pada vault dapat meningkatkan keamanan dari fuzzy vault. Beberapa penelitian sebelumnya telah membahas teknik-teknik yang dapat digunakan untuk membangkitkan chaff point secara efektif dan efisien. Dua di antarnya adalah teknik square boundary dan image celling. Pada paper ini, kami melakukan komparasi eksperimental terhadap kedua teknik tersebut. Hal ini dilakukan agar kami mendapatkan hasil performa yang lebih objektif dari keduanya. Hasil eksperimen menunjukkan bahwa teknik image celling memiliki kecepatan pembangkitan yang lebih cepat daripada square boundary, namun memiliki tingkat kompleksitas algoritma yang lebih tinggi dari teknik square boundary.

Kata kunci—Chaff point, Fuzzy vault, Image celling, Square boundary

Abstract

Fuzzy vault is a bio-encryption scheme that can be used as a support for conventional cryptographic security. The main concept of the fuzzy vault is to add an element of biometric authentication to cryptography. Fuzzy vault uses biometric features to encrypt or decrypt secret keys, which have previously been converted to the coefficients of a polynomial equation. The level of difficulty in carrying out polynomial reconstruction determines the security level of fuzzy vault. Adding a chaff point (noise) to the vault can increase the security of a fuzzy vault. Several previous studies have discussed techniques that can be used to generate chaff points effectively and efficiently. Two of them are square boundary and image celling. In this paper, we made an experimental comparison of the two techniques. This was done so that we got more objective performance results from both techniques. The experimental results showed that the image celling technique has a faster generation speed than square boundary, but has a higher level of algorithm complexity than the the square boundary technique.

Keywords—Chaff point, Fuzzy vault, Image celling, Square boundary

1. PENDAHULUAN

Fuzzy vault adalah salah satu teknik bio-enkripsi dengan tipe *key-binding* dan *key-release* yang telah diusulkan oleh Juels dan Sudan [1] pada tahun 2002. Tidak seperti pendahulunya, yaitu *fuzzy commitment* [2], teknik ini dirancang untuk dapat menggunakan fitur-fitur biometrik yang

bersifat *fuzzy* dan tidak terurut. Dengan kata lain, *fuzzy vault* lebih *error-tolerant* jika dibandingkan dengan *fuzzy commitment* [3]. Dalam implementasinya, *fingerprint* dianggap sebagai salah satu jenis data biometrik yang paling sesuai dengan skema *fuzzy vault* [4].

Skema *Fuzzy vault* tersusun dari dua fase, yaitu enkripsi (kodifikasi) dan dekripsi (dekodifikasi). Pada fase enkripsi, *fuzzy vault* akan menyembunyikan kunci rahasia atau informasi berharga lainnya dengan mengikatnya pada data biometrik dan menyamarkannya dengan *chaff point*. Sehingga, *chaff point* memiliki peranan yang cukup penting dalam mekanisme *fuzzy vault*. *Chaff point* pada umumnya dibangkitkan secara acak dan dibangkitkan sedemikian rupa sehingga memiliki karakter yang mirip dengan karakter *minutiae* [5] yang asli. Dengan demikian, *minutiae* beserta informasi rahasia yang diikat bersamanya dapat disamarkan dengan baik pada *vault*.

Sedangkan pada fase dekripsi, *fuzzy vault* akan mengekstrak kunci rahasia yang ada pada *vault* dengan menggunakan data biometrik dari subjek yang sama dengan subjek yang melakukan enkripsi. Pada fase ini, *fuzzy vault* akan melakukan proses rekonstruksi polinomial untuk menemukan kunci atau informasi rahasia yang disembunyikan oleh *fuzzy vault*.

Pada paper ini, kami menjabarkan dua teknik pembangkitan *chaff point* pada skema *fuzzy vault* yang telah diusulkan oleh beberapa peneliti sebelumnya, yaitu teknik *square boundary* [4] dan teknik *image celling* [6]. Kami melakukan komparasi eksperimental terhadap kedua metode tersebut untuk mengetahui karakteristik dari keduanya, baik dari sisi kompleksitas maupun waktu komputasi yang digunakan oleh keduanya dalam membangkitkan *chaff point*. Hal yang sama juga dilakukan oleh Dellys et al. pada [3]. Pada penelitian tersebut, Dellys et al. melakukan komparasi yang sama terhadap teknik *online parking* [7] dan teknik *square boundary* [4]. Dari penelitian yang dilakukannya, Dellys et al. menemukan fakta bahwa pertumbuhan waktu komputasi *square boundary* cenderung lebih stabil jika dibandingkan dengan *online parking* untuk setiap pertambahan *chaff point* yang dibutuhkan.

Tujuan dari penelitian ini adalah untuk mengetahui dan menjelaskan karakteristik dari teknik *square boundary* dan *image celling* secara objektif. Performa kedua teknik tersebut akan dianalisis dari sisi efektifitas dan kompleksitas algoritma yang digunakan. Penjelasan mengenai kompleskitas algoritme kami jabarkan pada bagian 2. Bagian 3 menjelaskan proses-proses pembangkitan *chaff point*. Bagian 4 menjelaskan hasil eksperimen yang dilakukan oleh kami. Bagian 5 memberikan kesimpulan atas ulasan yang telah kami jabarkan sekaligus menjeleskan arah penelitian kami selanjutnya.

2. KOMPLEKSITAS ALGORITME

Kompleksitas algoritma menjadi salah satu kriteria perbandingan dalam penelitian ini. Kompleksitas algoritma menunjukkan seberapa rumitnya suatu algoritma atau operasi aritmatika jika dieksekusi oleh mesin atau komputer [4]. Kompleksitas algoritma dilambangkan dengan *big O* (*O*(n^k)), di mana *k* adalah pangkat yang menunjukkan tingkat kompleksitas. Semakin besar nilai *k* maka maka semakin rumit operasi yang dilakukan. Beberapa contoh operasi aritmatika dan kompleksitasnya disajikan pada Tabel 1.

Tabel 1 Tabel Kompleksitas [4]

No.	Operasi	Kompleksitas O(n)
1	Penjumlahan	n
2	Pengurangan	n
3	Perkalian	n^2
4	Pembagian	$4n^2 + 3n$
5	Pangkat dua	n^2
6	Akar pangkat dua	$7n^2 + 3n$
7	Pembangkitan angka acak	1
8	Perbandingan	1

3. PEMBANGKITAN CHAFF POINT

Chaff point adalah data atau titik-titk acak yang dibangkitkan secara *pseudo-random*. *Chaff point* dibangkitkan sedemikian rupa agar memiliki karakter yang sama dengan *minutiae* dari *fingerprint*. Hal tersebut dilakukan agar *chaff point* dapat menyamarkan *minutiae* dengan baik. Setidaknya terdapat tiga syarat utama yang harus diperhatikan dalam melakukan pembangkitan *chaff point* [1]:

1. Sebuah *chaff point* tidak boleh terlalu dekat atau menempati tempat yang sama dengan titik-titik lain yang ada pada *vault*.
2. *Chaff point* tidak boleh berada pada jalur polinomial yang telah diciptakan oleh titik-titk polinomial.
3. Setidaknya dibutuhkan satu *chaff point* untuk menyembunyikan titik-titik polinomial yang ada pada *vault*.

3.1 Jumlah Chaff Point yang Dibangkitkan

Secara teori, semakin banyak *chaff point* yang dibangkitkan maka semakin baik pula tingkat keamanan yang dimiliki oleh *fuzzy vault*. Hal tersebut dikarenakan proses pencarian titik-titik polinomial akan semakin sulit dilakukan bagi yang tidak mengetahui lokasi dari titik-titik polinomial yang sebenarnya. Namun, ada beberapa hal lain yang harus dipertimbangkan dalam menentukan banyaknya *chaff point* yang akan dibangkitkan, yaitu [3]:

1. **Kapasitas penyimpanan**. Semakin banyak *chaff point* yang dibangkitkan maka semakin besar pula ukuran dari *vault*.
2. **Derajat kebebasan (*degree of freedom*) dari *chaff point***. *Chaff point* yang dibangkitkan pada fase-fase akhir cenderung memiliki *degree of freedom* (DoD) yang lebih kecil daripada DoD *chaff point* yang dihasilkan pada fase-fase awal [8]. Sehingga, penyerang akan semakin mudah menemukan titik-titik valid yang ada pada *vault*.
3. **Waktu komputasi yang diperlukan**. Semakin banyak *chaff point* yang harus dibangkitkan maka semakin lama waktu komputasi yang dibutuhkan oleh *fuzzy vault* dalam membangkitkan *chaff point* ataupun dalam melakukan dekripsi.

Mempertimbangkan aspek keamanan, kapasitas penyimpanan, dan waktu komputasi merupakan hal yang cukup penting dalam menentukan jumlah *chaff point* yang akan dibangkitkan. Formula paling praktis untuk menentukan jumlah *chaff point* ditunjukan oleh persamaan (1) [7]:

$$n_{chaff} = 10 \times n_{minutiae} \qquad (1)$$

dengan *n* adalah suatu bilangan bulat yang menujukkan jumlah entitas.

3.2 Metode-metode Pembangkitan Chaff Point

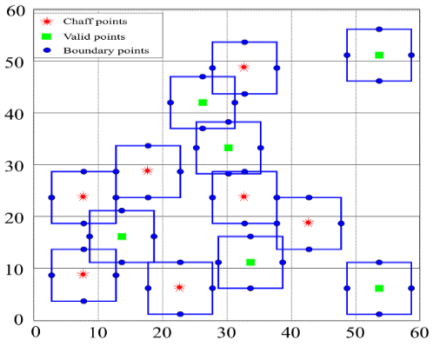
Chaff point pada umumnya digambarkan sebagai sebuah data atau titik yang memiliki dua atribut, yaitu absis dan ordinat. Absis dan ordinat dibangkitkan dengan cara yang berbeda. Berikut kami paparkan beberapa teknik untuk membangkitkan keduanya:

3.2.1 Pembangkitan Absis dari Chaff Point

Absis adalah atribut yang cukup vital dari *chaff point* karena absis merupakan representasi *chaff point* pada *vault domain*. Beberapa teknik pembangkitan absis telah diusulkan oleh beberapa peneliti sebelumnya, namun pada penelitian ini, kami hanya fokus pada teknik *square boundary* dan teknik *image celling* saja.

3.2.1.1 Teknik Square Boundary

Teknik ini dijelaskan lebih detail pada [4]. Ilustrasi singkat dari teknik ini digambarkan pada Gambar 1 Setiap titik, baik itu *mituiae* ataupun *chaff point* yang sudah valid diberikan atribut tambahan yaitu empat titik batas (*boundary points*). Aturan yang paling penting dalam teknik ini adalah tidak ada dua atau lebih titik yang saling tumpang tindih. Tumpang tindih yang dimaksud di sini adalah tidak ada titik (*minutiae*/*chaff point*) yang masuk pada batas wilayah dari titik lainya. Dalam satu kali iterasi pembangkitan, *square boundary* membangkitkan empat kandidat *chaff point* sekaligus. Selain itu *square boundary* tidak menggunakan operasi *Euclidean Distance* dalam prosedurnya. Dalam melakukan evaluasi kandidat, *square boundary* membandingkan keberadaan kandidat terhadap semua titik yang ada pada *pre-vault*.



Gambar 1 Ilustrasi teknik square boundary [4]

3.2.1.2 Teknik Image Celling

Teknik ini dijelaskan lebih detail pada [6]. Ilustrasi singkat dari teknik ini digambarkan pada Gambar 2 *Image* dari *Fingerprint* secara logis dibagai menjadi *cell-cell* yang lebih kecil, sehingga setiap *cell* memiliki maksimal delapan *cell* tetangga terdekat. *Cell-cell* tersebut memiliki ukuran yang sama untuk setiap sisinya. Aturan yang paling penting dalam teknik ini adalah satu *cell* hanya boleh ditempati oleh satu titik saja (*minutiae*/*chaff point*). Dalam satu kali iterasi pembangkitan, *image celling* hanya membangkitkan satu kandidat *chaff point*. Selain itu *image celling* menggunakan operasi *Euclidean Distance* dalam prosedurnya. Dalam melakukan evaluasi kandidat, *image celling* membandingkan keberadaan kandidat hanya terhadap tetangga terdekat dari kandidat tersebut saja.

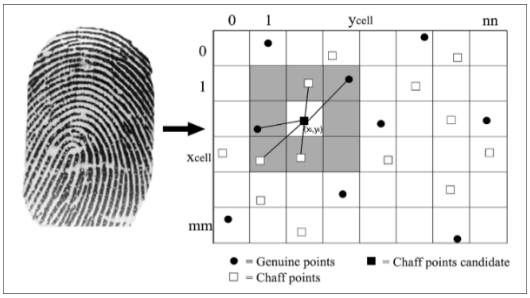
Setelah koordinat-koordinat *chaff point* telah didapatkan, maka akan dilakukan proses konkatenasi koordinat untuk setiap *chaff point*. Sehingga akan didapatkan nilai skalar yang berperan sebagai nilai absis dari setiap *chaff point*.

3.2.2 Pembangkitan Ordinat dari Chaff Point

Pembangkitan ordinat chaff point dapat menggunakan dua teknik, yaitu:

3.2.2.1 Pembangkitan secara acak [1]

Nilai ordinat dibangkitkan secara acak, namun pasangan ($absis_i$, $ordinat_i$) tidak boleh berada pada jalur polinomial, di mana *i* adalah menunjukkan urutan dari *chaff point*.



Gambar 2 Ilustrasi teknik image celling [6]

3.2.2.2 Pembangkitan secara terstruktur [3]

Nilai ordinat dibangkitkan dengan menggunakan suatu persamaan seperti yang ditunjukkan persamaan (2).

$$ordinat_i = P(absis_i) + \alpha \quad (2)$$

dengan *P(x)* adalah fungsi polinomial *fuzzy vault* dan *α* adalah suatu bilangan yang dibangkitkan secara acak dan *i* adalah urutan *chaff point* ke-*i*.

Setelah nilai absis dan ordinat untuk setiap *chaff point* didapatkan, maka pasangan-pasangan absis dan ordinat tersebut dianggap sebagai koordinat dari *chaff point* pada domain *vault*. Koordinat-koordinat tersebut nantinya akan digabungkan dengan titik-titik polinomial *fuzzy vault* untuk membentuk *vault*.

4. EKSPERIMEN

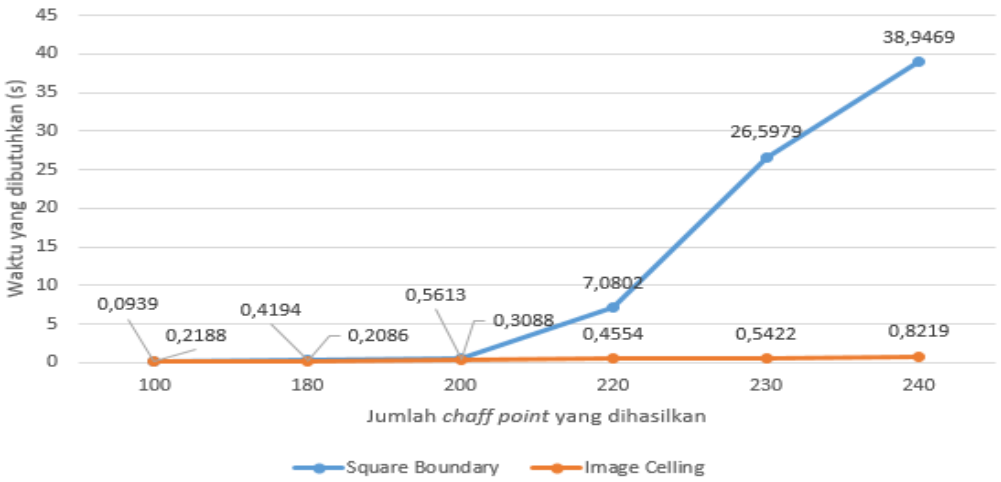
Pada bagian ini kami melakukan komparasi eksperimental terhadap kedua teknik pembangkitan absis *chaff point*, yaitu teknik *square boundary* dan teknik *image celling*. Kami menggunakan beberapa sampel jari yang diambil melalui alat pemindai sidik jari dengan tipe *narrow scanner*. Lalu hasil pemindaian diolah sedemikian rupa hingga sesuai dengan bentuk data yang dibutuhkan. Eksperimen dilakukan dengan menggunakan *software* yang dibangun dengan bahasa C, dan dijalankan pada perangkat komputer dengan spesifikasi prosesor *Intel® Pentium® CPU N3540 (2.2 GHz)* dan memori 2 GB.

4.1 Waktu untuk Membangkitkan Chaff Point

Pada eksperimen pertama, kami fokus untuk membandingkan waktu yang dibutuhkan oleh teknik *square boundary* dan teknik *image celling* untuk membangkitkan *chaff point* dengan jumlah yang ditentukan sebelumnya. Hasil eksperimen kami sajikan pada Tabel 2 dan Gambar 3.

Tabel 2 Tabel Waktu Komputasi

Jumlah Chaff Point	Waktu Komputasi Square Boundary (s)	Waktu Komputasi Image Celling (s)
100	0,2188	0,0939
180	0,4194	0,2086
200	0,5613	0,3088
220	7,0802	0,4554
230	26,5979	0,5422
240	38,9469	0,8219



Gambar 3 Grafik waktu komputasi teknik *square boundary* dan *image celling*

Dari grafik yang ditunjukkan oleh Gambar 3. Kita menyimpulkan bahwa pertumbuhan waktu komputasi teknik *image celling* cenderung linear, sementara perubahan waktu komputasi teknik *square boundary* cenderung berbentuk polinomial.

4.2 Analisis Kecepatan Pembangkitan Chaff Point

Pada eksperimen kedua, kami fokus untuk membandingkan perubahan kecepatan pembangkitan *chaff point* untuk teknik *square boundary* dan teknik *image celling* dalam membangkitkan *chaff point* dengan jumlah yang ditentukan sebelumnya. Untuk melakukan analisis kecepatan pembangkitan, kami mengadopsi persamaan umum dari kecepatan, yaitu:

$$v = \frac{\Delta s}{\Delta t} \quad (3)$$

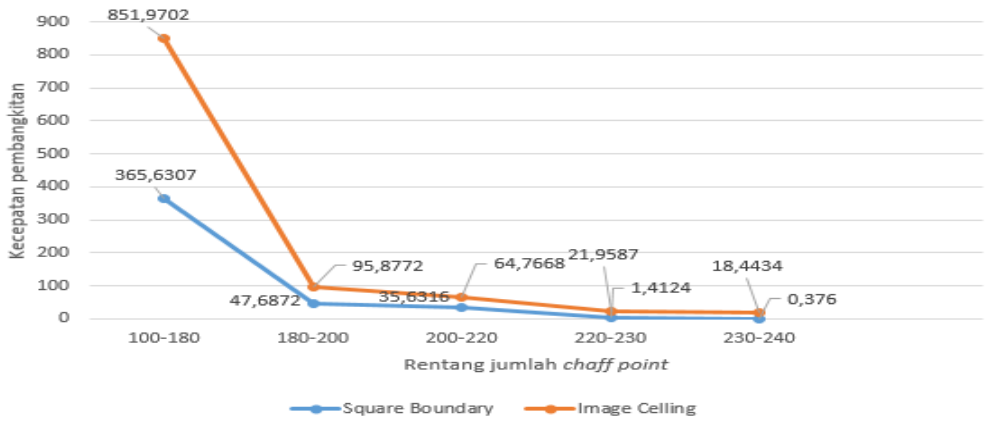
dengan Δs adalah perubahan jarak pada rentang waktu tertentu, sementara Δt adalah perubahan waktu. Kami menyesuaikan beberapa variabel dari persamaan (3) agar dapat digunakan untuk melakukan analisis kecepatan pembangkitan *chaff point* yang kami lakukan, sehingga membentuk persamaan baru seperti yang ditunjukkan pada persamaan (4)

$$v_{generate} = \frac{\Delta n_{chaff}}{\Delta t} \quad (4)$$

dengan Δn_{chaff} adalah perubahan jumlah *chaff point* pada rentang waktu tertentu, sementara Δt adalah perubahan waktu. Hasil eksperimen mengenai kecepatan pembangkitan *chaff point* kami sajikan pada Tabel 3 dan Gambar 4.

Tabel 4 Tabel Kecepatan Pembangkitan *Chaff Point*

Rentang jumlah chaff point	Kecepatan Square Boundary (chaff/s)	Kecepatan Image Celling (chaff/s)
100 – 180	365,6307	851,9702
180 – 200	47,6872	95,8772
200 – 220	35,6316	64,7668
220 – 230	1,4124	21,9587
230 – 240	0,3760	18,4434



Gambar 4 Grafik kecepatan pembangkitan *square boundary* dan *image celling*

Dari grafik yang ditunjukkan oleh Fig 4. Kita dapat menyimpulkan bahwa secara keseluruhan teknik *image celling* lebih cepat daripada teknik *square boundary*.

4.3 Kompleksitas Algoritme

Pada bagian ini kami melakukan anlisis kompleksitas algoritma dari teknik *square boundary* dan teknik *image celling*. Kami melakukan analisis algoritma dengan cara menganalisis *pseudo code* dari dari masing-masing teknik. Dari anaslisis *pseudo code* yang telah dilakukan, ditemukan bahwa teknik *image celling* menggunakan teknik perhitungan jarak *Euclidean* sebagai inti prosedurnya, sementara teknik *square boundary* hanya menggunakan teknik perbandingan, tanpa melibatkan perhitungan jarak *Euclidean*.

Perhitungan jarak *Euclidean* melibatkan operasi penjumlahan, pangkat kuadrat, dan akar kuadrat. Sehingga berdasarkan Table I. diketahui bahwa tingkat kompleksitas perhitungan jarak *Euclidean* mencapai $O(n^2)$, sementara operasi perbandingan hanya memiliki tingkat kompleksitas *O(1)*. Karena kedua teknik diharuskan untuk menghasilkan *n chaff point*, maka tingkat kompleksitas teknik *image celling* mencapai $O(n^3)$, sementara teknik *square boundary* hanya mencapai *O(n)*. Dengan demikian, secara algoritma komputasi teknik *image celling* lebih kompleks daripada teknik *square boundary*.

5. KESIMPULAN DAN ARAH PENELITIAN

Pada paper ini, kami melakukan komparasi eksperimental terhadap teknik *square boundary* dan *image celling*. Hal ini dilakukan agar kami mendapatkan hasil performa yang lebih objektif dari keduanya. Hasil eksperimen menunjukkan bahwa teknik *image celling* memiliki kecepatan pembangkitan yang lebih cepat daripada *square boundary*, namun memiliki tingkat kompleksitas algoritma yang lebih tinggi dari teknik *square boundary*. Hasil dari penelitian ini hanya sebagian dari tahapan-tahapan penelitian kami secara keseluruhan. Untuk penelitian selanjutnya, kami akan mencoba melakukan hibridisasi terhadap kedua teknik tersebut, sehingga akan didapatkan sebuah teknik yang memiliki kecepatan yang cukup baik namun memiliki tingkat kompleksitas algoritma yang cukup rendah.

DAFTAR PUSTAKA

[1] Juels A, Sudan M. 2002. A Fuzzy Vault Scheme. In: IEEE Int. Symp. Inf. Theory. p 408.

[2] Juels A, Wattenberg M. 1999. A Fuzzy Commitment Scheme. In: CCS ’99 Proc. 6th ACM Conf. Comput. Commun. Secur. Singapore, pp 28–36.

[3] Dellys HN, Benadjimi N, Boubakeur MR, Sliman L, Ali F. 2015. Fingerprint Fuzzy Vault Chaff Point Generation by Squares Method. In: 2015 7th Int. Conf. Soft Comput. Pattern Recognit. IEEE, Fukuoka, pp 357–362.

[4] Khalil-hani M, Marsono MN, Bakhteri R. 2013. Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm. *Futur Gener Comput Syst* 29 (3):800–810.

[5] Jain AK, Nandakumar K, Ross A. 2016. 50 years of biometric research: Accomplishments, challenges, and opportunities. *Pattern Recognit Lett* 79:80–105.

[6] Nguyen TH, Wang Y, Ha Y, Li R. 2013. Improved Chaff Point Generation for Vault Scheme in Bio-Cryptosystems. *IET Biometrics* 2(2):48–55.

[7] Clancy TC, Kiyavash N, Lin DJ. 2003. Secure Smartcard based Fingerprint Authentication. In: Proc. 2003 ACM SIGMM Work. Biometrics Methods Appl. ACM, New York, NY, USA, pp 45–52.