Ulasan Ringkas Teknik-Teknik Pembangkitan *Chaff Point* pada Skema Bio-Enkripsi *Fuzzy Vault*

1st Bambang Pilu Hartato, 2nd Muh Nursaddam
Program Studi Teknologi Informasi
Universitas Amikom Purwokerto
Purwokerto, Indonesia
1st bambang.pilu@amikompurwokerto.ac.id, 2nd nursaddam89@gmail.com

Abstrak—Tahap pembangkitan *chaff point* merupakan isu yang cukup penting pada skema bio-enkripsi *Fuzzy Vault.* Prinsip utama dari tahap ini adalah membangkitkan *noise* hingga jumlah tertentu sehingga titik-titik koordinat *minutiae* dapat disamarkan tanpa meningkatkan rasio *false positive* saat melakukan ekstraksi *minutiae* pada fase *decoding*. Akan tetapi, tahapan ini merupakan tahapan yang paling banyak memakan waktu komputasi jika dibandingkan dengan tahapan-tahapan lainnya pada fase *encoding*. Sehingga terdapat beberapa penelitian yang secara spesifik mengusulkan metode-metode yang dapat digunakan untuk membangkitkan *chaff point* secara efektif dan efisien. Beberapa di antaranya adalah *Image Celling, Square Boundary,* dan *Non Random Chaff Point Generator* (NCPG). Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Paper ini membandingkan ketiganya berdasarkan karakteristiknya dengan melihat penjabaran algoritme pada masing-masing paper pengusul metode. Berdasarkan hasil komparasi yang dilakukan, tujuan utama ketiga teknik tersebut adalah meminimalisir waktu komputasi yang dibutuhkan untuk menghasilkan sejumlah *chaff point* sekaligus meningkatkan keamanan *Fuzzy Vault* dari risiko terhadap beberapa jenis serangan. Ketiga teknik tersebut pada prinsipnya menggunakan penghitungan jarak sebagai inti algoritmenya. Namun dari ketiganya, metode *Square Boundary* memiliki kompleksitas paling rendah. Sementara pertumbuhan waktu komputasi yang paling stabil dimiliki oleh metode *Image Celling*. Sedangkan metode yang paling kompleks namun cukup aman dari ketiganya adalah metode NCPG.

Kata kunci—Bio-enkripsi, Biometrik, *Chaff point, Fuzzy vault, Kriptografi, Pembangkitan chaff point.*

I. PENDAHULAN

Setidaknya ada empat aspek yang harus diperhatikan pada konteks keamanan informasi, yaitu *confidentiality*, *integrity*, *availability*, dan *accountability* [1]. Dalam kaitannya dengan masalah keamanan informasi, aspek *confidentiality* merupakan aspek yang memiliki dampak yang cukup signifikan. Hal tersebut dikarenakan *confidentiality* merupakan pondasi utama dari pilar-pilar keamanan informasi. Dengan kata lain, jika sebuah penyerangan telah berhasil melumpuhkan aspek *confidentiality* dari suatu sistem maka penyerang akan dengan mudah menyerang aspek-aspek keamanan yang lainnya. Sehingga, diperlukan metode-metode tersendiri untuk membangun *confidentiality* yang cukup kuat agar dapat mempertahankan keamanan suatu sistem informasi.

Salah satu metode yang dapat digunakan untuk memperkuat *confidentiality* suatu sistem informasi adalah penggunaan kriptografi [2]. Hingga saat ini, kriptografi telah mengalami evolusi dari masa ke masa untuk memperkuat keamanannya. Salah satu bentuk evolusi terbaru dari kriptografi adalah bio-enkripsi, di mana konsep tersebut menggabungkan skema kriptografi dan biometrik.

Penggabungan konsep kriptografi dan biometrik didasari oleh ide untuk meningkatkan keamanan dari kriptografi dengan menambahkan fitur-fitur biometrik. Hal tersebut dikarenakan salah satu kendala terbesar kriptografi adalah kesulitan dalam penyediaan kunci-kunci enkripsi yang benar-benar unik, sedangkan biometrik memiliki fitur-fitur atau data yang bersifat sangat unik [3]. Sehingga, penggabungan keduanya memungkinkan skema kriptografi memiliki kunci-kunci enkripsi yang bersifat sangat unik serta memungkinkan skema kriptografi hanya dapat dilakukan oleh orang-orang yang terotorisasi. Dengan demikian, tingkat keamanan dari suatu skema kriptografi dapat ditingkatkan.

Salah satu teknik bio-enkripsi yang cukup sering dikembangkan karena kehandalan fiturnya adalah skema *Fuzzy Vault* [4]. Teknik ini pertama kali diperkenalkan oleh Juels dan Sudan pada tahun 2002 untuk memperbaharui teknik bio-enkripsi bernama *Fuzzy Commitment* yang diusulkan oleh Juels dan Wattenberg [5]. Skema *Fuzzy Vault* hadir dengan kemampuan yang tidak dimiliki oleh skema *Fuzzy Commitment* sebelumnya, yaitu kemampuan untuk menangani data biometrik yang bersifat *fuzzy* dan tidak terurut. Data biometrik dikategorikan sebagai data yang bersifat *fuzzy* dikarenakan sifatnya yang tidak jelas. Hal tersebut didapatkan dari sebuah fakta bahwa tidak akan ada dua buah sampel

biometrik yang diambil dari suatu individu akan memiliki kesamaan mencapai 100 % [6].

Skema *Fuzzy Vault* merupakan teknik bio-enkripsi dengan tipe *key binding* dan *key release* [7]. Proses enkripsi pada skema *Fuzzy Vault* bekerja dengan melakukan *binding* kunci rahasia ke dalam data biometrik, sementara proses dekripsi bekerja dengan cara melakukan *release* kunci rahasia yang sebelumnya telah ter-*binding* di dalam data biometrik. Inti dari pengamanan yang dilakukan oleh skema *Fuzzy Vault* adalah seberapa tinggi tingkat kesulitan yang dilakukan untuk melakukan *polynomial reconstruction* pada skema *Fuzzy Vault.* Sementara itu, untuk lebih menigkatkan keamanan yang dimilikinya, skema *Fuzzy Vault* menggunakan *chaff point*.

Chaff point dianalogikan sebagai *noise* yang digunakan untuk menyamarkan informasi rahasia yang ada pada *Fuzzy Vault*. Semakin banyak *chaff point* yang digunakan, semakin baik pula tingkat keamanan yang dimiliki oleh skema *Fuzzy Vault* tersebut [8]. Dengan demikian, tahap pembangkitan *chaff point* merupakan tahapan yang cukup penting dalam skema *Fuzzy Vault*. Akan tetapi, tahap pembangkitan *chaff point* menjadi salah satu tahapan yang memiliki tingkat komputasi yang paling tinggi pada skema enkripsi *Fuzzy Vault* [3]. Sehingga, beberapa penelitian mengenai metode pembangkitan *chaff point* telah dilakukan untuk mendapatkan metode yang memiliki tingkat komputasi yang cukup rendah namun tetap mempertahankan keamanan skema *Fuzzy Vault*.

Setidaknya terdapat tiga metode pembangkitan *chaff point* yang baru-baru ini diusulkan oleh beberapa peneliti. Metode-metode tersebut yaitu *Image Celling* [8], *Square Boundary* [3], dan *Nonrandom Chaff Point Generator* [NCPG] [9]. Setiap metode memiliki kelebihan dan kekurangannya masing-masing. Paper ini akan mengulas secara ringkas dan membandingkan ketiganya berdasarkan karakteristiknya dengan melihat penjabaran algoritme pada masing-masing paper pengusul metode.

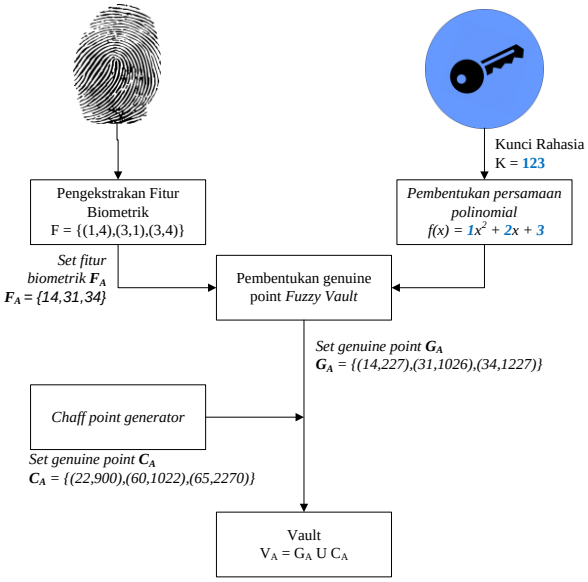
Pada pembahasannya, paper ini akan dibagi menjadi beberapa bagian. Bagian 1 membahas tentang pendahuluan yang melatarbelakangi munculnya konsep *Fuzzy Vault* dan urgensi pembangkitan *chaff point*. Bagian 2 membahas konsep utama dari skema bio-enkripsi *Fuzzy Vault* dan pembangkitan *chaff point*-nya. Bagian 3 membahas ketiga metode pembangkitan *chaff point* yang telah disebutkan sebelumnya. Bagian 4 membahas komparasi dari ketiga metode yang akan disajikan ke dalam sebuah tabel perbandingan, dan kesimpulan disajikan pada bagian 5.

II. SKEMA FUZZY VAULT

A. *Konsep Skema Fuzzy Vault*

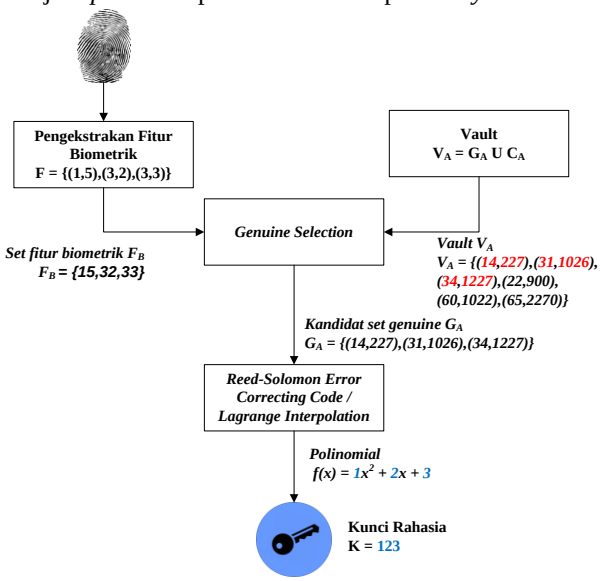
Seperti yang telah dijelaskan sebelumnya, skema *Fuzzy Vault* merupakan teknik bio-enkripsi dengan tipe *key binding* dan *key release*. Pada fase enkripsi, skema *Fuzzy Vault* akan melakukan *binding* kunci rahasia dengan data biometrik, sementara pada fase dekripsi, skema *Fuzzy Vault* akan me-*release* kunci rahasia yang sebelumnya ter-*binding* dengan data biometrik. Data biometrik *fingerprint* dianggap sebagai data biometrik yang paling sesuai dengan skema *Fuzzy Vault* dikarenakan sifatnya yang praktis dan cukup akurat [3].

Gambar 1. menunjukkan mekanisme enkripsi yang dilakukan oleh skema *Fuzzy Vault*. Enkripsi dimulai dengan proses pembentukan persamaan polinomial berderajat *n*, dengan *n* adalah panjang kunci rahasia *k* dikurangi 1. Sebagai contoh, jika panjang kunci rahasia *k* adalah 3 karakter maka derajat polinomial *p* adalah 2 dan setiap karakter yang ada pada kunci rahasia *k* akan menjadi koefisien dari persamaan polinomial *p*. Tahap berikutnya adalah melakukan ekstraksi fitur *fingerprint*. Fitur yang diekstrak adalah koordinat-xy dari *minutiae*. Jumlah minimal dari *minutiae* yang dibutuhkan agar proses enkripsi dapat dilakukan adalah *n*+1. Sebagai contoh, jika polinomial memiliki derajat 2 maka setidaknya dibutuhkan 3 *minutiae*. Setalah koordinat-xy dari setiap *minutiae* didapatkan, maka akan dilakukan penggabungan nilai koordinat-x dari setiap *minutiae* terhadap nilai koordinat-y-nya dan menyimpannya pada himpunan F_A. Setiap elemen dari F_A akan diproyeksikan sebagai nilai dari variabel x ke dalam polinomial *p*. Hasil operasi polinomial dari setiap elemen himpunan F_A akan dipasangkan dengan elemen-elemen dari himpunan tersebut sehingga membentuk pasangan koordinat baru. Pasangan-pasangan koordinat tersebut lalu disimpan pada himpunan G_A. Jika setiap elemen dari himpunan G_A diproyeksikan ke dalam sebuah diagram *Cartesian* maka elemen-elemen tersebut akan membentuk sebuah pola polinomial berderajat *n*. Untuk menyamarkan pola polinomial tersebut, dibangkitkanlah himpunan koordinat acak (*chaff point*) bernama C_A dan menggabungkannya dengan himpunan G_A sehingga membentuk himpunan *Vault* bernama V_A. Himpunan V_A inilah yang menjadi *cipher text* dari sekema enkripsi *Fuzzy Vault*.



Gambar 1. Mekanisme enkripsi skema *Fuzzy Vault* [9]

Gambar 2. menunjukkan mekanisme dekripsi dari skema *Fuzzy Vault*. Dekripsi dimulai dengan proses ekstraksi koordinat-xy dari *fingerprint minutiae*. Seperti pada fase enkripsi, jumlah minimal dari *minutiae* yang dibutuhkan pada proses dekripsi adalah n+1, dengan n adalah derajat polinomial *p*. Setalah koordinat-xy dari setiap *minutiae* didapatkan, maka akan dilakukan penggabungan nilai koordinat-x dari setiap *minutiae* terhadap nilai koordinat-y-nya dan menyimpannya pada himpunan F_B. Setiap elemen dari F_B akan diproyeksikan pada himpunan V_A untuk dilakukan proses *Genuine Selection*. Proses ini adalah sebuah mekanisme pemilihan titik-titik koordinat dari elemen V_A yang memiliki nilai koordinat-x yang sama atau cukup dekat dengan masing-masing elemen dari himpunan F_B. Titik-titik koordinat yang telah terpilih akan disimpan dalam sebuah himpunan G_A. Setelah semua titik koordinat yang terpilih berhasil disimpan pada G_A, maka tahap berikutnya adalah *Polynomial Reconstruction*. Tujuan dari tahapan ini adalah melakukan rekonstruksi atau interpolasi terhadap elemen-elemen yang ada pada G_A untuk membentuk persamaan polinomial berderajat *n*. Dua teknik yang dapat digunakan untuk melakukan interpolasi yaitu *Reed-Solomon Error Correction Code* dan *Lagrange Interpolation*. Setelah tahap interpolasi berhasil dilakukan, maka akan dihasilkan sebuah persamaan polinomial *p'* berderajat n. Setiap koefisian dari polinomial *p'* akan digabungkan dan disusun untuk membentuk kunci rahasia *k*. Kunci rahasia *k* inilah yang menjadi *plain text* pada skema dekripsi *Fuzzy Vault*.



Gambar 2. Mekanisme dekripsi skema *Fuzzy Vault* [9]

B. *Konsep Awal Pembangkitan Chaff Point pada Fuzzy Vault*

Seperti yang telah dijelaskan sebelumnya, *chaff point* dianalogikan sebagai *noise* berupa titik-titik koordinat-xy yang dibangkitkan sedemikian rupa dan digunakan untuk menyamarkan pola polinomial pada *Vault.* Pada saat skema *Fuzzy Vault* pertama kali diperkenalkan pada publik oleh Juels dan Sudan [4], pembangkitan *chaff point* dilakukan secara *pseudo random* tanpa memperhatikan efisiensi dari komputasi yang dilakukan. Pada penelitian [4] hanya terdapat tiga syarat yang harus dipenuhi dalam melakukan pembangkitan *chaff point*:

1) Koordinat-*x* dari *chaff point* tidak boleh sama dengan koordinat-*x* dari setiap *genuine point* yang terdapat pada *Vault.*
2) Koordinat-y dari *chaff point* tidak boleh sama dengan nilai dari *p(x),* dengan *x* adalah koordinat-*x chaff point*. Yang artinya *chaff point* tidak boleh berada pada jalur polinomial.
3) Setidaknya dibutuhkan satu *chaff point* untuk menyamarkan *genuine points* yang terdapat pada *Vault.*

Teknik pembangkitan *chaff point* mulai mengalami evolusi sejak konsep *Euclidean Distance* diterapkan pada proses pembangkitan *chaff point* oleh Clancy et al. [10]. *Euclidean Distance* digunakan untuk melakukan pengukuran jarak optimal antara letak koordinat kandidat *chaff point* dengan koordinat setiap *minutiae* yang digunakan pada *Vault*. Prinsip dari teknik yang dikembangkan oleh Clancy et al. [10] adalah meletakkan *chaff point* pada jarak yang tidak terlalu dekat dengan setiap *minutiae* yang digunakan dalam pembentukan *Vault.* Jika jarak *Euclidean* antara suatu kandidat *chaff point* dengan salah satu *minutiae* ataupun *chaff point* valid lainnya berada di bawah ambang batas jarak yang telah ditentukan (*threshold)* maka kandidat *chaff point* tersebut akan diabaikan. Sebaliknya, jika jarak *Euclidean* antara suatu kandidat *chaff point* dengan semua *minutiae* dan *chaff point* valid sama dengan atau di atas *threshold* maka kandidat *chaff point* tesebut akan dianggap sebagai *chaff point* yang valid. Selain itu, Clancy et al. [10] juga menyatakan bahwa setidaknya dibutuhkan *chaff point* sejumlah 10 kali lipat dari jumlah *minutiae* yang digunakan. Dengan demikian, metode pembangkitan *chaff point* yang diusulkan oleh Clancy et al. [10] diklaim sebagai metode yang cukup efektif dan efisien pada masa tersebut.

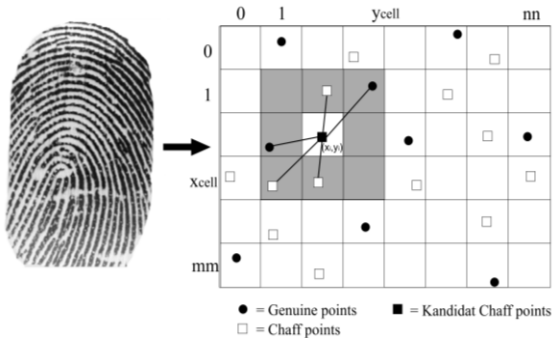
III. METODE BARU PADA PEMBANGKITAN CHAFF POINT

A. *Metode Image Celling*

Metode ini pertama kali diperkenalkan pada tahun 2013 oleh Nguyen et al. [8]. Metode ini terinspirasi dari salah satu kelemahan dari metode yang diusulkan oleh Clancy et al. [10]. Pada metode yang diusulkan oleh Clancy et al. [10] tersebut, *computational time* yang dibutuhkan dalam pembangkitan *chaff point* mengalami pertumbuhan secara eksponensial seiring dengan bertambahnya *chaff point* yang dibutuhkan.

Selain itu, dalam kasus sebuah *Fuzzy Vault* yang menggunakan 20 *minutiae* dan 200 *chaff point* untuk melakukan sebuah mekanisme enkripsi, untuk membangkitkan *chaff point* yang pertama, setidaknya dibutuhkan 20 kali perhitungan jarak *Euclidean*. Untuk membangkitkan *chaff point* yang ke-dua, setidaknya dibutuhkan (20+1) kali perhitungan jarak *Euclidean*. Langkah tersebut akan terus dilakukan hingga *chaff point* ke-200 berhasil ditetapkan sebagai *chaff point* yang valid.

Gambar 3. menunjukkan bagaimana metode *Image Celling* bekerja. Metode tersebut dimulai dengan tahap pengekstrakan titik-titik koordinat *minutiae* dari *fingerprint*. Titik-titik koordinat tersebut ditransformasikan ke dalam sistem koordinat tertentu yang menempatkan titik pusat koordinatnya pada ujung sebelah kiri atas dari sistem koordinat tersebut. Berbeda dengan sistem koordinat *Cartesian*, sistem koordinat yang diusulkan oleh Nguyen et al. [8] tersebut menjadikan garis vertikal sebagai sumbu-*x* dan garis horizontal sebagai sumbu-*y*. Setalah koordinat *minutiae* berhasil ditransformasikan ke dalam sistem koordinat yang baru, sitem koordinat tersebut dibagi menjadi beberapa *cell* persegi dengan ukuran yang sama sedemikian rupa, sehingga setiap *cell* hanya ditempati oleh satu *minutiae* dan setiap *cell* akan memiliki maksimal delapan *cell* tetangga. Tahap berikutnya adalah memilih *cell* secara acak. Jika *cell* yang terpilih sudah terisi maka sistem akan melakukan pememilihan *cell* sekali lagi secara acak. Namun, jika *cell* yang terpilih masih kosong, maka kandidat *chaff point* akan diletakkan pada *cell* tersebut. Setelah kandidat *chaff point* berhasil diletakkan pada *cell* yang kosong, maka tahap berikutnya adalah melakukan pengukuran jarak *Euclidean* antara kandidat *chaff point* dengan titik-titik tetangga terdekatnya. Berbeda dengan metode yang diusulkan oleh Clancy et al. [10], metode *Image Celling* [8] hanya melakukan perhitungan jarak *Euclidean* maksimal sebanyak delapan kali setiap iterasi pembangkitkan *chaff point*. Hal tersebut dikarenakan setiap *cell* maksimal hanya memiliki delapan *cell* tetangga dan setiap *cell* hanya terdapat satu titik. Jika kandidat *chaff point* tidak memiliki titik tetangga atau jarak *Euclidean* kandidat *chaff point* dengan setiap titik tetangganya lebih tinggi atau sama dengan dari *threshold* yang ditentukan maka kandidat *chaff point* diletakkan pada koordinat yang ditempatinya saat itu dan dianggap sebagai *chaff point* yang valid. Namun, jika jarak *Euclidean* antara kandidat *chaff point* dengan salah satu titik tetangganya di bawah *threshold* yang ditentukan, maka proses pembangkitan akan diulang lagi dari tahap pemlilihan *cell.* Langkah-langkah tersebut akan terus dilakukan hingga jumlah *chaff point* yang dibutuhkan dapat terpenuhi.



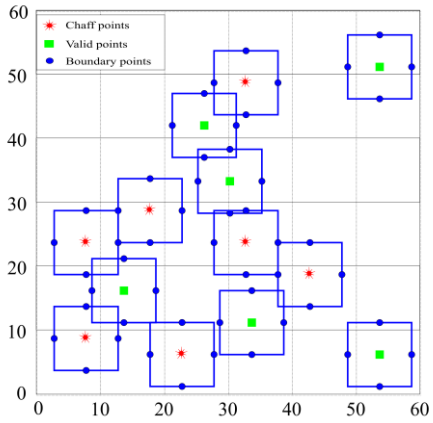
Gambar 3. Ilustrasi metode *Image Celling* [8]

Dari analisa performa yang dilakukan oleh Nguyen et al. [8], *computational time* yang dimiliki oleh metode *Image Celling* mengalami pertumbuhan cenderung linear seiring dengan bertambahnya *chaff point* yang dibutuhkan. Dengan demikian, *Image Celling* memiliki efisiensi *computational time* yang lebih tinggi jika dibandingkan dengan metode yang diusulkan oleh Clancy et al. [10]. Akan tetapi metode *Image Celling* masih memiliki kekurangan pada penggunaan sistem koordinat. Sistem koordinat yang digunakan pada *Image Celling* harus memiliki rasio tertentu agar sistem koordinat tersebut dapat dibagi menjadi *cell-cell* persegi yang berukuran sama. Selain itu, sistem koordinat yang digunakan oleh *Image Celling* mengharuskan titik pusat koordinat diletakkan pada ujung sebelah kiri atas dari sistem koordinat serta menjadikan sumbu vertikal sebagai sumbu-*x* dan sumbu horizontal sebagai sumbu-*y*. Dengan demikian, diperlukan sebuah teknik transformasi koordinat, sehingga koordinat *minutiae* dapat ditransformasikan ke dalam sistem koordinat *Image Celling*. Tentu saja hal tersebut dianggap kurang praktis karena setiap metode tersebut diterapkan pada perangkat yang menggunakan pemindai sidik jari yang berbeda maka diperlukan kalibrasi ulang terhadap metode transformasi yang digunakan.

B. Metode Square Boundary

Metode ini pertama kali diperkenalkan pada tahun 2013 oleh Khalil-Hani et al [3]. Metode ini terinspirasi dari keberhasilan serangan yang dilakukan oleh Chang et al. [11] terhadap metode pembangkitan *chaff point* yang diusulkan oleh Clancy et al. [10]. Serangan ini dilakukan dengan cara menganalisa *Degree of Freedom* (DoF) dari setiap titik yang terdapat pada *Vault*. Dari analisa teresebut, didapatkan sebuah fakta bahwa titik-titik yang dibangkitkan terakhir akan memiliki DoF yang lebih kecil daripada DoF dari titik-titik yang dibangkitkan pertama kali. Dengan fakta tersebut, penyerang akan mengeliminasi titik-titik yang memiliki DoF yang cukup kecil. Berikutnya penyerang akan melakukan *Brute Force* [12] terhadap titik-titik yang tersisa untuk mendapatkan kunci rahasia yang disembunyikan pada *Vault*, dengan asumsi titik-titik yang memiliki DoF cukup besar adalah himpunan *Genuine Point*.

 ISBN: 978-602-60280-1-3



Gambar 4. Ilustrasi metode *Square Boundary* [3]

Selain masalah celah keamanan, Khalil-Hani et al. [3] juga mengkritisi masalah tingkat kompleksitas dari metode yang diusulkan oleh Clancy et al. [10]. Khalil-Hani et al. [3] menemukan bahwa tingkat kompleksitas yang dimiliki oleh metode tersebut mencapai $O(n^3)$ dan mereka beberpendapat bahwa seharusnya tingkat kompleksitas tersebut dapat dikurangi agar skema pembangkitan *chaff point* dapat dijalankan pada perangkat berbasis *System-on-Chip* secara lebih efisien. Untuk melakukannya, Khalil-Hani et al. [3] mengusulkan sebuah metode yang terinspirasi dari teknik *Circle Packing* [13] dan menghilangkan tahap perhitungan jarak *Euclidean* pada mekanismenya.

Gambar 4. menunjukkan bagaimana metode *Square Boundary* bekerja. Setiap titik, baik *genuine point* ataupun *chaff point*, diberi atribut tambahan berupa titik-titik *boundary*. Jika diilustrasikan ke dalam sebuah grafik maka titik-titik *boundary* tersebut akan membentuk batas berupa persegi yang mengelilingi setiap titik yang terdapat pada *Vault* seperti yang ditunjukkan pada Gambar 4. Pada prinsipnya, untuk membangkitkan suatu *chaff point*, metode *Square Boundary* akan memilih koordinat secara acak sebagai koordinat kandidat *chaff point*. Setelah koordinat kandidat telah terpilih, maka sistem akan melakukan pengecekan, apakah kandidat *chaff point* berada di dalam batas titik-titik yang lain atau tidak. Jika kandidat tersebut berada di luar batas titik-titik manapun maka kandidat tersebut dianggap sebagai *chaff point* yang valid dan disimpan beserta atribut titik-titik *boundary*-nya. Namun, jika kandidat tersebut berada di dalam batas setidaknya salah satu titik valid maka kandidat tersebut akan diabaikan dan proses pembangkitan akan diulang sekali lagi dari tahap pemilihan koordinat kandidat *chaff point*. Langkah-langkah tersebut akan terus dilakukan hingga jumlah *chaff point* yang dibutuhkan dapat terpenuhi.

Dari analisa performa yang dilakukan oleh Khalil-Hani et al. [3], *computational time* yang dimiliki oleh metode *Square Boundary* mengalami pertumbuhan yang lebih linear jika dibandingkan dengan metode yang diusulkan oleh Clancy et al. [10]. Selain itu, metode *Square Boundary* memiliki tingkat kompleksitas yang lebih rendah dari metode yang diusulkan oleh Clancy et al. [10], yaitu hanya $O(n^2)$. Metode ini juga diklaim mampu bertahan dari serangan *Statistical Analysis* karena metode ini mampu mendistribusikan DoF secara acak kepada setiap titik yang terdapat pada *Vault*. Akan tetapi, metode ini masih menggunakan metode komparasi yang sama dengan metode yang dilakukan oleh metode Clancy et al. [10]. Sebagai contoh, dalam kasus sebuah *Fuzzy Vault* yang menggunakan 20 *minutiae* dan 200 *chaff point*, untuk membangkitkan *chaff point* yang pertama, setidaknya dibutuhkan 20 kali pengecekan keberadaan kandidat *chaff point*. Untuk membangkitkan *chaff point* yang ke-dua, setidaknya dibutuhkan (20+1) kali pengecekan. Langkah tersebut akan terus dilakukan hingga *chaff point* ke-200 berhasil ditetapkan sebagai *chaff point* yang valid. Sehingga, setidaknya terjadi $200 \times 20 + (1 + 2 + \cdots + 199)$ kali pengecekan, dengan asumsi setiap iterasi pembangkitan *chaff point* pasti menghasilkan satu *chaff point* yang valid. Atau secara umum dapat dimodelkan menjadi persamaan (1)

$$n_{checking} = n_{chaff} \times n_{minutiae} + \sum_{i=1}^{n_{chaff}-1} i \qquad (1)$$

dengan

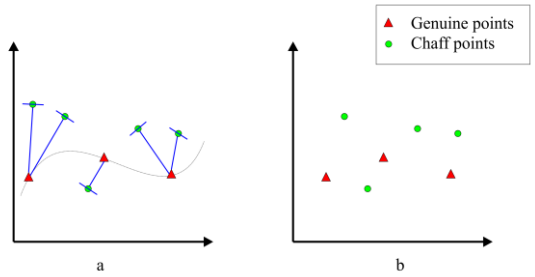
$n_{checking}$: Jumlah pengecekan yang dilakukan
n_{chaff} : Jumlah *chaff point*
$n_{minutiae}$: Jumlah *minutiae*

Dengan demikian, metode tersebut berpotensi untuk mengalami peningkatan *computational time* yang cukup signifikan jika jumlah *chaff point* yang akan dibangkitkan lebih dari 500 titik.

C. *Metode Nonrandom Chaff Point Generator*

Metode *Nonrandom Chaff Point Generator* (NCPG) pertama kali diperkenalkan pada tahun 2016 oleh Nguyen et al [9]. Ide utama dari metode ini adalah membangkitkan *chaff point* dengan pola pembangkitan yang terstruktur tanpa melibatkan proses pembangkitan angka acak. Selain itu, metode ini juga melibatkan proses *hashing* untuk meningkatkan keamanannya.

Metode ini terinspirasi oleh celah keamanan dari *Fuzzy Vault* terhadap serangan *Blend Subtitution* [14]. Serangan tersebut bekerja dengan cara memodifikasi informasi koordinat dari beberapa titik yang terdapat pada *Vault* tanpa mengubah jumlah titik yang terdapat di dalamnya. Sehingga, serangan tersebut dapat meningkatkan *False Rejection Rate* (FRR) terhadap proses otentifikasi yang dilakukan oleh pengguna *Fuzzy Vault* yang asli.



Gambar 5. Ilustrasi metode *Nonrandom Chaff Point Generator* [9]

Gambar 5. menunjukkan ilustrasi pembangkitan *chaff point* dengan metode NCPG. Terlihat bahwa *chaff point* terbentuk dari pola-pola garis yang diciptakan oleh *genuine points*. Terdapat dua perbedaan yang cukup signifikan antara metode NCPG dengan metode-metode pembangkitan yang lainnya [3],[8],[10]. Berikut perbedaan-perbedaan tersebut:

1) Metode pembangkitan *chaff point* pada NCPG menggunakan pola yang diciptakan dari kombinasi titik-titik *genuine point* dan kunci rahasia yang telah dilakukan *hashing*.

2) NCPG melakukan mekanisme pembangkitan *chaff point* tidak hanya pada tahap *enrollment* (enkripsi) melainkan juga pada tahap otentifikasi (dekripsi).

Dari analisa performa yang dilakukan oleh Nguyen et al [9], metode NCPG diklaim mampu menangani serangan *Blend Subtitution* pada skema *Fuzzy Vault*. Hal tersebut dikarenakan NCPG melakukan proses verifikasi terhadap semua titik, baik *chaff point* maupun *genuine point*, yang ada di dalam *Vault* pada fase otentifikasi. Jika terdapat perbedaan yang cukup signifikan pada fase otentifikasi maka *Vault* tersebut terindikasi mengalami serangan *Blend Subtitution* (*integrity attack*), dengan asumsi fitur biometrik yang digunakan pada fase *enrollment* dan fase otentifikasi merupakan fitur biometrik yang sama. Akan tetapi, metode NCPG justru memiliki risiko untuk meningkatkan kemungkinan terjadinya *Collusion Attack* [15] dan serangan *Key Inversion* [9] terhadap skema *Fuzzy Vault* yang bisa saja berujung pada diketahuinya kunci rahasia yang disembunyikan pada *Vault* beserta informasi biometrik yang ada di dalamnya oleh penyerang.

IV. PERBANDINGAN METODE

Pada bagian sebelumnya, konsep, tujuan, kelebihan dan kekurangan serta ilustrasi dari ketiga metode pembangkitan *chaff point* telah dijelaskan secara terpisah. Pada bagian ini, perbandingan dari ketiga metode tersebut dirangkum dan disajikan ke dalam sebuah tabel perbandingan. Sehingga, perbedaan di antara ketiganya dapat ditampilkan dengan cukup jelas. Berikut tabel perbandingan dari ketiga metode pembangkitan *chaff point* yang telah dipaparkan sebelumnya [3],[8],[9]:

TABLE I. TABEL PERBANDINGAN

Metode	Domain/Tujuan	Kelebihan	Kekurangan
Image Celling	• Efisiensi waktu komputasi	• Pertumbuhan waktu komputasi cenderung linear • Maksimal hanya membutuhkan 8 kali pengecekan setiap iterasi pembangkitan 1 *chaff point*	• Membutuhkan sistem koordinat khusus
Square Boundary	• Efisiensi waktu komputasi • Menurunkan tingkat kompleksitas • Meningkatkan keamaan skema *Fuzzy Vault*	• Pertumbuhan waktu komputasi cenderung linear • Tingkat kompleksitas hanya $O(n^2)$ • Mampu mempertahankan *Fuzzy Vault* dari serangan *Statistical Analysis*	• Jumlah pengecekan yang terus bertambah seiring bertambahnya jumlah titik yang terdapat pada *Vault*.
Nonrandom Chaff Point Generator	• Meningkatkan keamaan skema *Fuzzy Vault*	• Mampu mempertahankan *Fuzzy Vault* dari serangan *Blend Subtitution*	• Memiliki risiko terhadap kemungkinan terjadinya *Collusion Attack* dan serangan *Key Inversion*

V. KESIMPULAN

Paper ini membahas beberapa metode pembangkitan *chaff point* yang yang telah diusulkan antara rentang waktu 2013 hingga 2016. Setidaknya terdapat tiga tujuan yang menjadi fokus dari metode-metode tersebut, yaitu efisiensi waktu komputasi yang tinggi, tingkat kompleksitas yang rendah dan tingkat keamanan yang tinggi. Cukup sulit untuk menyelaraskan ketiganya agar tetap seimbang. Hanya metode *Square Boundary* yang mendekati ketiga tujuan tersebut, walaupun tidak semua jenis serangan terhadap *Fuzzy Vault* dapat ditangani oleh metode ini. Setidaknya masih ada dua jenis serangan terhadap *Fuzzy Vault* yang hingga saat ini belum dapat ditangani oleh ketiga metode tersebut, yaitu serangan *Key Inversion* dan *Collusion Attack*. Sehingga, setidaknya masih ada dua tugas yang harus diselesaikan pada penelitian di bidang pembangkitan *chaff point*. Pertama, menemukan metode pembangkitan yang benar-benar mampu menyelaraskan ketiga tujuan yang telah disebutkan sebelumnya. Kedua, menemukan metode pembangkitan yang mampu bertahan setidaknya dari serangan *Key Inversion* dan *Collusion Attack*.

REFERENCES

[1] M. Pastore and E. Dulaney, *Security +*. San Fransisco: SYBEX, 2003.

[2] G. Coulouris, J. Dollimore, and T. Kindberg, *Distributed Systems: Concepts and Design*, vol. 4. 2012.

[3] M. Khalil-hani, M. N. Marsono, and R. Bakhteri, "Biometric encryption based on a fuzzy vault scheme with a fast chaff generation algorithm," *Futur. Gener. Comput. Syst.*, vol. 29, no. 3, pp. 800–810, 2013.

[4] A. Juels and M. Sudan, "A Fuzzy Vault Scheme," in *IEEE International Symposium on Information Theory*, 2002, p. 408.

[5] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme," in *CCS '99 Proceedings of the 6th ACM conference on Computer and communications security*, 1999, pp. 28 – 36.

[6] V. Matyas and Z. Riha, "Security of Biometric Authentication Systems–Extended Version," in *International Conference on Computer Information Systems and Industrial Management Applications, CISIM 2010 (2010)*, 2010, pp. 19–28.

[7] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: Issues and challenges," *Proc. IEEE*, vol. 92, no. 6, pp. 948–959, 2004.

[8] T. H. Nguyen, Y. Wang, Y. Ha, and R. Li, "Improved Chaff Point Generation for Vault Scheme in Bio-Cryptosystems," *IET Biometrics*, vol. 2, no. 2, pp. 48–55, 2013.

[9] M. T. Nguyen, Q. H. Truong, and T. K. Dang, "Enhance fuzzy vault security using nonrandom chaff point generator," *Inf. Process. Lett.*, vol. 116, no. 1, pp. 53–64, 2016.

[10] T. C. Clancy, N. Kiyavash, and D. J. Lin, "Secure Smartcardbased Fingerprint Authentication," in *Proceedings of the 2003 ACM SIGMM Workshop on Biometrics Methods and Applications*, 2003, pp. 45–52.

[11] E.-C. Chang, R. Shen, and F. W. Teo, "Finding the Original Point Set Hidden Among Chaff," in *Proceedings of the 2006 ACM Symposium on Information, Computer and Communications Security*, 2006, pp. 182–188.

[12] P. Mihailescu, "The Fuzzy Vault for fingerprints is Vulnerable to Brute Force Attack," *CoRR*, vol. abs/0708.2, 2007.

[13] C. R. Collins and K. Stephenson, "A circle packing algorithm," *Comput. Geom.*, vol. 25, no. 3, pp. 233–256, 2003.

[14] W. J. Scheirer and T. E. Boult, "Cracking Fuzzy Vaults and Biometric Encryption," in *Biometrics Symposium, 2007*, 2007, pp. 1–6.

[15] H. T. Poona and A. Miria, "A Collusion Attack on the Fuzzy Vault Scheme," *ISC Int'l J. Inf. Secur. Bd*, vol. 1, no. 1, 2009.