

ABSTRACT

Chaff point is a part of the essential elements in the Fuzzy Vault Scheme. However, the existing chaff point generation techniques are time consuming as generating more than 200 chaff points. This research offers a new technique that is relatively faster than the existing techniques while generating more than 200 chaff points.

The proposed technique combines chaff point candidate generation procedures and mechanisms for constraining the number of chaff point validations owned by Image Celling Technique with the Square Boundary's chaff point validation processes. The manner of chaff point candidate generation done by Image Celling Technique and how this technique limits the number of chaff point validations not only leverage the generation efficiency and maximize the number of chaff points but also reduce computational time while producing a huge number of chaff points. Meanwhile, the way how Square Boundary Technique validates chaff point has low complexity level, hence it can speed up the validation process.

This research uses three matrices for measuring the performance of the proposed technique, they are computational time, maximum number of chaff points that can be generated, and the efficiency of chaff point generation process. This research's experimental results show the dominance of the proposed technique toward Square Boundary Technique and Image Celling Technique in all measurement matrices previously explained. It means that the proposed technique needs less time while generating a huge number of chaff points, more productive, and has more efficient generation procedure than Square Boundary and Image Celling Technique. However, the proposed technique needs longer computational time than the Square Boundary Technique while generating less than 40 *chaff points*. Moreover, there are about 0.13% of the entire pairs of the pre-vault's members produced by the proposed technique have smaller distance value than the determined minimum distance (δ).

Keywords: chaff point, computational time, efficiency, number of chaff points.

INTISARI

Chaff point adalah salah satu elemen yang cukup penting di dalam Skema *Fuzzy Vault*. Walaupun demikian, teknik pembangkitan *chaff point* yang ada saat ini masih membutuhkan waktu komputasi yang relatif lama pada saat membangkitkan lebih dari 200 *chaff point*. Penelitian ini mengusulkan sebuah teknik baru yang relatif lebih cepat daripada teknik pembangkitan *chaff point* yang ada saat ini ketika membangkitkan lebih dari 200 *chaff point*.

Teknik yang diusulkan menggabungkan prosedur pembangkitan dan mekanisme pembatasan jumlah proses validasi kandidat *chaff point* yang dimiliki oleh Teknik *Image Celling* dengan prosedur validasi kandidat *chaff point* yang dimiliki oleh Teknik *Square Boundary*. Prosedur pembangkitan dan mekanisme pembatasan jumlah proses validasi kandidat *chaff point* dari Teknik *Image Celling* mampu meningkatkan efisiensi pembangkitan *chaff point* sekaligus memaksimalkan jumlah *chaff point* yang dapat dibangkitkan serta mempersingkat waktu komputasi pada saat membangkitkan *chaff point* dengan jumlah yang sangat banyak. Sedangkan prosedur validasi kandidat *chaff point* yang dimiliki oleh Teknik *Square Boundary* memiliki kompleksitas algoritme yang cukup rendah, sehingga dapat mempersingkat waktu komputasi yang dibutuhkan pada saat melakukan validasi kandidat *chaff point*.

Penelitian ini menggunakan tiga matriks untuk mengukur performa dari teknik yang diusulkan, yaitu analisis waktu komputasi, jumlah maksimal *chaff point* yang dapat dibangkitkan dan efisiensi pembangkitan *chaff point*. Hasil eksperimen yang dilakukan pada penelitian ini menunjukkan bahwa teknik yang diusulkan mampu mengungguli Teknik *Square Boundary* dan Teknik *Image Celling* untuk setiap matriks performa yang diujikan. Walaupun demikian, keunggulan performa waktu komputasi dari teknik yang diusulkan hanya dapat terlihat pada saat membangkitkan lebih dari 40 *chaff point*. Selain itu, terdapat sekitar 0.13% dari keseluruhan kombinasi pasangan anggota *pre-vault* yang dihasilkan oleh teknik yang diusulkan memiliki nilai jarak yang lebih kecil daripada jarak minimal yang telah ditentukan (δ).

Kata kunci – *chaff point*, efisiensi, jumlah *chaff point*, waktu komputasi.