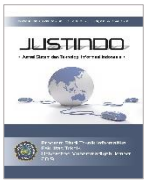
JUSTINDO
Jurnal Sistem dan Teknologi Informasi Indonesia
p-ISSN 2502-5724
e-ISSN 2541-5735

Jurnal Sistem dan Teknologi Informasi Indonesia
JUSTINDO Vol. 8 No. 2, Agustus 2023, hal. 87-98
http://ejurnal.unmuhjember.ac.id/index.php/JUSTINDO/index
https://doi.org/10.32528/justindo.v8i2.320



Deteksi Penipuan Kartu Kredit Menggunakan Algoritma Memetika Dan Pencarian Tersebar

Detect Credit card Fraud Using Memetic Algorithms and Scettered search

Ari Eko Wardoyo

Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Jember
Email: arieko@unmuhjember.ac.id

Diterima: 14 Juli 2023 | Direvisi: 08 Agustus 2023 | Disetujui: 14 Agustus 2023

This work is licensed under a Creative Commons Attribution 4.0 International License.
Copyright (c) 2023 JUSTINDO

ABSTRAK

Kartu kredit merupakan salah satu produk perbankan yang telah diterima oleh masyarakat luas sebagai salah satu media pembayaran yang modern, terutama kemudahan-kemudahan yang ditawarkan kepada pemegang kartu (*cardholder*). Selain kemudahan ada kelemahan yang ada pada sistem perbankan yaitu kejahatan siber, salah satu kejahatan siber adalah *carding* dengan modus membajak data kartu kredit korban dan kemudian menggunakan secara tidak sah untuk berbelanja secara *online*. Sedangkan pola penipuan dengan menggunakan kartu kredit, biasanya ketika seorang penipu mendapatkan kartu maka mereka akan menghabiskan seluruh dana yang tersedia. Sehingga mendeteksi kecurangan kartu kredit dengan limit dana yang besar lebih berharga dibandingkan dengan kartu kredit dengan limit dana yang kecil.
Algoritma-algoritma *heuristik* adalah algoritma yang berbasis populasi. Diantaranya adalah algoritma genetika, memetika, dan pencarian tersebar yang telah sukses diberlakukan untuk masalah-masalah optimalisasi. Penelitian ini diusulkan untuk melakukan deteksi dini terhadap penipuan pada kartu kredit dengan menggabungkan algoritma memetika dan pencarian tersebar dengan tujuan mengurangi kemungkinan pemusatan nilai kebugaran yang prematur sehingga bisa mengatasi permasalahan konvergensi dini. Dataset yang digunakan adalah data transaksi harian kartu kredit sebanyak 1.056.320 transaksi. Data tersebut diuji menggunakan cross validation dengan tiga skenario pengujian. Dan dari hasil pengujian tersebut didapatkan tingkat akurasi sebesar 100%.

Kata kunci: kecurangan kartu kredit, pencarian tersebar, memetika, konvergensi dini, algoritma heuristik.

ABSTRACT

Credit card is a banking product that has been accepted by the wider community as a modern payment medium, especially the conveniences offered to cardholders. Apart from convenience, there are weaknesses in the banking system, namely cybercrime. One of the cybercrimes is carding, by the mode of hijacking the victim's credit card data and then using it illegally to shop online. Meanwhile, the pattern of fraud using a credit card, usually when a fraudster gets a card, they will spend all available funds. So, detecting credit card fraud with a large fund limit is more valuable than a credit card with a small fund limit.
Heuristic algorithms are population-based algorithms. Among them are genetic algorithms, memetics, and distributed search which have been applied successfully to optimization problems. This research proposes an early detection of credit card fraud by combining memetic algorithm and distributed search algorithms with the aim of reducing the possibility of premature fitness value, thus overcome the issue of premature convergence. The dataset used consists of daily credit card transaction data with a total of 1,056,320 transactions. This data is tested using cross-validation with three testing scenarios. From the results of these tests, an accuracy rate of 100% is obtained.

***Keywords**: credit card fraud, scattered search, memetics, early convergence, heuristic algorithm.*

1. Pendahuluan

Kartu Kredit adalah APMK yang dapat digunakan untuk melakukan pembayaran atas kewajiban yang timbul dari suatu kegiatan ekonomi, termasuk transaksi pembelanjaan dan/atau untuk melakukan penarikan tunai, dimana kewajiban pembayaran pemegang kartu dipenuhi terlebih dahulu oleh *acquirer* atau penerbit, dan pemegang kartu berkewajiban untuk melakukan pembayaran pada waktu yang disepakati baik dengan pelunasan secara sekaligus (charge card) ataupun dengan pembayaran secara angsuran (Bank Indonesia, 2021).

Pada kasus penipuan kartu kredit tujuannya adalah melakukan pencurian atau penipuan menggunakan kartu kredit atau mekanisme pembayaran yang sama dalam melakukan transaksi. Tujuannya untuk mendapatkan barang tanpa membayar atau mendapatkan uang dari akun yang tidak sah. Ada dua jenis utama penipuan kartu kredit. Pertama adalah penipuan palsu yang dilakukan oleh sekelompok penjahat terorganisasi. Efek mereka secara total sangat besar dan biasanya mempengaruhi puluhan bahkan ratusan nasabah bank. Kedua adalah penggunaan kartu kredit secara ilegal yang didapat dari kartu kredit yang hilang atau dicuri. Jenis penipuan ini sebagian besar tidak terkait dengan kelompok kriminal dan hanya mempengaruhi satu atau beberapa kartu saja.

Deteksi penipuan kartu kredit biasanya diselesaikan menggunakan *data mining* dengan cara melakukan klasifikasi terhadap transaksi penggunaan kartu kredit. Prosesnya adalah dengan membandingkan transaksi yang terjadi saat ini dengan transaksi-transaksi sebelumnya. Proses yang paling populer mendeteksi dan menentukan penipuan pada kartu kredit ini Adalah dengan menggunakan metode *Decision Tree* (DT), *Random Forest* (RF), *Bayesian Network* (BN), *Naïve Bayes* (NB), *Support Vector Machine* (SVM), dan K* (Leevy, J., Hancock, J., Khoshgoftaar, T. 2023) Metode untuk deteksi penipuan kartu kredit didasarkan pada perilaku pemegang kartu kredit. Kebanyakan nasabah kartu kredit memiliki kebiasaan yang khas dalam transaksi menggunakan kartu dan mereka tidak sering merubah kebiasaan tersebut. Dengan demikian perilaku nasabah bisa didefinisikan dan setiap transaksi yang dilakukan dapat dibandingkan dengan kebiasaan mereka bertransaksi.

Menentukan pola transaksi yang curang maupun yang sah diperlukan proses pelatihan terhadap data yang sudah terbukti sebagai penipuan juga terhadap data yang juga sudah terbukti sebagai transaksi yang sah. Sehingga didapatkan pola kelompok transaksi-transaksi yang sah (K1) dan kelompok transaksi-transaksi yang curang (K2). Dari pola data K1 dan K2 kemudian diambil nilai batas tengahnya (T). Jika kemudian terjadi transaksi maka transaksi tersebut akan dicari nilainya. Misalkan nilainya lebih kecil dari T maka transaksi tersebut termasuk pada kelompok K1 atau transaksinya dianggap sah. Namun jika nilainya lebih besar dari T maka transaksi tersebut termasuk pada kelompok K2 atau transaksi yang dianggap curang, sehingga nanti sistem akan memberikan peringatan kepada petugas bank. Tindakan yang harus dilakukan sepenuhnya tergantung kepada keputusan yang diambil oleh petugas bank. Tindakan yang bisa dilakukan diantarnya pemblokiran kartu kredit, pengiriman pemberitahuan kepada pemilik kartu lewat SMS, atau menelepon langsung pemilik kartu tersebut.

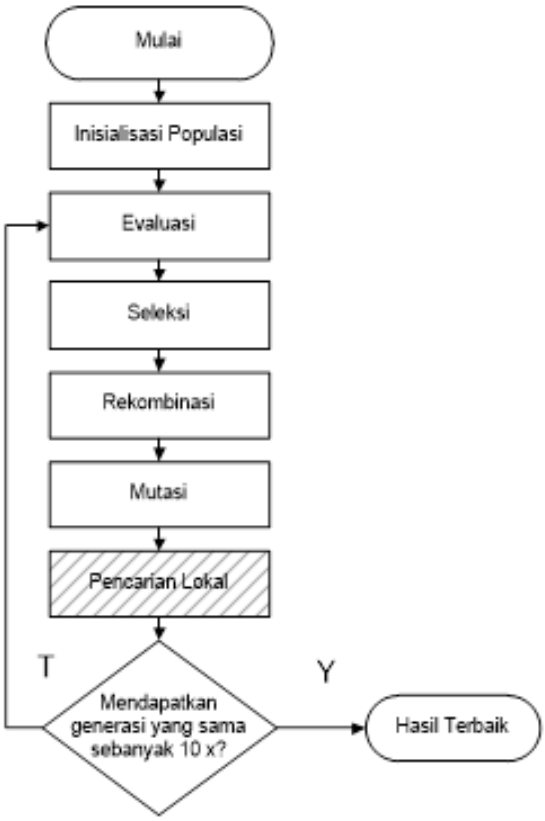
2. Metode Penelitian

2.1. Algoritma memetika dan Pencarian tersebar

Algoritma memetika adalah sebuah pendekatan heuristik untuk masalah optimasi dengan menggabungkan pendekatan optimasi lokal dengan paradigma berdasarkan populasi. Karena algoritma memetika termasuk dalam metode *heuristik* yakni suatu metode yang digunakan ketika ukuran ruang pencarian solusi sulit dikontrol secara eksak dan belum ada algoritma yang dapat mencari solusi optimal secara efektif. Elemen kunci yang dipertimbangkan oleh algoritma memetika adalah operator optimasi lokal dan operator rekombinasi (Ding, et al, 2019).

Algoritma memetika merupakan penggabungan dari algoritma pencarian lokal dengan algoritma genetika. Algoritma memetika memiliki kompleksitas yang lebih tinggi dibandingkan algoritma genetika karena adanya penambahan pencarian lokal (Behmanesh, 2021).

Pencarian tersebar merupakan algoritma evolusioner yang karakteristiknya secara umum sama dengan algoritma genetika. Dalam pencarian tersebar keragaman pada set referensi sangat penting dan selanjutnya waktunya ditentukan sejumlah solusi terbaik yang dipilih dan kemudian digabungkan dengan sejumlah solusi yang paling beragam untuk membentuk himpunan referensi baru. Populasi pencarian tersebar berbeda dengan populasi algoritma genetika, set referensi pencarian tersebar biasanya disimpan lebih kecil karena setiap solusi yang diinginkan dikenakan operator rekombinasi. Skema algoritma memetika dan pencarian tersebar digambarkan seperti pada Gambar 1.



Gambar 1. Algoritma Memetika dan pencarian tersebar.

Langkah – langkah implementasi metode memetika dan pencarian tersebar:

1). Inisialisasi Populasi

Langkah pertama dalam algoritma MESS adalah membentuk sebuah populasi awal yang berisikan sekumpulan individu. Setiap individu dalam algoritma memetika ini direpresentasikan dengan barisan dari nilai-nilai θ_0, θ_1, θ_2, θ_3, θ_4, θ_5, θ_6.

2). Evaluasi

Setelah populasi awal telah terbentuk, langkah selanjutnya adalah mengevaluasi masing-masing individu menggunakan fungsi kebugaran.

3). Seleksi

Dalam metode ini metode yang dipilih adalah metode *Roulette Wheel*, dimana pemilihan individu didasarkan pada suatu permainan *roulette*. Setiap individu akan mendapat bagian dari sebuah roda *roulette* dengan luas masing-masing bagian bergantung kepada nilai kebugaran masing-masing individu.

4). Rekombinasi

Setelah mendapatkan individu-individu yang terpilih menjadi orang tua, maka langkah selanjutnya adalah menghasilkan keturunan dari individu- individu tersebut. Dalam hal ini operator rekombinasi digunakan untuk memenuhi tujuan tersebut.

Dalam setiap operasi rekombinasi, diambil dua individu orang tua yang selanjutnya akan menghasilkan dua individu baru dengan cara memberikan pembobotan kepada orang tua pertama menggunakan nilai acak antara 0 sampai dengan 1.

5). Mutasi

Langkah selanjutnya setelah melakukan rekombinasi adalah melakukan proses mutasi yang berlangsung hanya terhadap individu yang terpilih. Setiap individu memiliki kemungkinan untuk terjadi mutasi, dinamakan dengan probabilitas mutasi. Dalam hal ini, salah satu gen dari individu yang terpilih untuk terjadi mutasi akan diubah dengan sembarang bilangan real yang lain antara 0,01 sampai dengan 9,99. Pemilihan gen dalam suatu individu yang akan diubah dilakukan secara acak.

6). Pencarian Lokal

Setelah mutasi, langkah selanjutnya adalah menerapkan metode pencarian lokal terhadap masing-masing individu dalam populasi tersebut. Metode pencarian lokal yang akan digunakan adalah metode *hill climbing*. Penggunaan teknik *hill climbing* dalam pencarian lokal dikarenakan teknik pencarian ini sangat sederhana namun bisa mengeksploitasi solusi terbaik (Hernando, et al, 2018).

7). Kriteria berhenti

Iterasi akan berhenti ketika dilakukan 10 kali proses perulangan dan tetap menghasilkan populasi dengan nilai kebugaran yang sama.

2.2. Dataset

Jumlah dataset yang digunakan adalah 1000 identitas kartu kredit dengan 1.056.320 transaksi harian. Dataset diperoleh dari PKDD'99 Discovery Challenge, dari alamat situs lisp.vse.cz/pkdd99/Challenge/chall.html. Bentuk datasetnya seperti pada tabel 1.

Tabel 1. Bentuk Dataset

Item	Deskripsi
No_Kartu	Identifikasi no kartu kredit
Tanggal	Tanggal terjadinya transaksi
Jumlah Transaksi	Nominal transaksi dalam sekali transaksi
Total Transaksi	Total transaksi yang dilakukan dalam satu bulan
Jenis Kartu	Jenis Kartu Kredit berdasarkan maksimal total transaksi.

3. Hasil dan Pembahasan

3.1. Proses Inisialisasi Populasi

Pada populasi awal, nilai dari gen-gen setiap individu ditentukan secara acak. Jumlah gen dalam satu individu sebanyak 7 hal ini terkait dengan pola penipuan kartu kredit. Berdasarkan statistik penipu menghabiskan dana pada kartu kredit bisa sampai dengan lima kali. Jika diambil transaksi nasabah dalam satu tahun maka kemungkinan data yang sah adalah tujuh transaksi. Contoh populasi awal ditunjukkan pada tabel 2 berikut

Tabel 2. Contoh Populasi Awal

Ind	**Gen**						
	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6
1	0,32	3,24	0,08	1,23	5,53	9,74	2,25
2	0,01	2,14	3,50	2,43	7,30	5,43	1,50
3	0,20	1,51	6,08	5,53	3,30	2,47	8,51
...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...
1000	3,20	4,20	8,10	3,33	2,53	6,42	7,50

3.2. Proses Evaluasi

Proses evaluasi dilakukan setelah populasi awal terbentuk. Data presentase total transaksi penggunaan kartu kredit ditunjukkan pada tabel 3 berikut:

Tabel 3 Data Persentase Total Transaksi Penggunaan Kartu Kredit

No Kartu	Bulan	Total Transaksi	Batas Kredit	%Total Trans
1005	1	2.500.000	5.000.000	50
1005	2	1.500.000	5.000.000	30
1005	3	2.250.000	5.000.000	45
1005	4	2.500.000	5.000.000	50
1005	5	2.250.000	5.000.000	45
1005	6	2.225.000	5.000.000	44,5
1005	7	2.500.000	5.000.000	50
1005	8	3.750.000	5.000.000	75
1005	9	3.750.000	5.000.000	75
1005	10	4.500.000	5.000.000	90
1005	11	4.500.000	5.000.000	90
1005	12	4.500.000	5.000.000	90

Prediksi akan dilakukan dengan menggunakan data 6 bulan sebelum. Dengan menggunakan model prediksi regresif otomatis akan didapat model prediksi seperti berikut:

$$\hat{X}_7 = \theta_0 + \theta_1 X_1 + \theta_2 X_2 + \theta_3 X_3 + \theta_4 X_4 + \theta_5 X_5 + \theta_6 X_6$$

$$\hat{X}_8 = \theta_0 + \theta_1 X_2 + \theta_2 X_3 + \theta_3 X_4 + \theta_4 X_5 + \theta_5 X_6 + \theta_6 X_7$$

$$\hat{X}_9 = \theta_0 + \theta_1 X_3 + \theta_2 X_4 + \theta_3 X_5 + \theta_4 X_6 + \theta_5 X_7 + \theta_6 X_8$$

$$\hat{X}_{10} = \theta_0 + \theta_1 X_4 + \theta_2 X_5 + \theta_3 X_6 + \theta_4 X_7 + \theta_5 X_8 + \theta_6 X_9$$

$$\hat{X}_{11} = \theta_0 + \theta_1 X_5 + \theta_2 X_6 + \theta_3 X_7 + \theta_4 X_8 + \theta_5 X_9 + \theta_6 X_{10}$$

$$\hat{X}_{12} = \theta_0 + \theta_1 X_6 + \theta_2 X_7 + \theta_3 X_8 + \theta_4 X_9 + \theta_5 X_{10} + \theta_6 X_{11}$$

Dari evaluasi ini, maka setiap individu akan memiliki nilai kebugaran masing-masing sebagai ukuran kualitas dari individu tersebut. Semakin besar nilai kebugaran dari suatu individu, maka semakin baik kualitas dari individu tersebut. Nilai kebugaran dapat dilihat pada tabel 4 berikut

Tabel 4 Nilai Kebugaran

Individu	Nilai Kebugaran
1	0.000901
2	0.000911
3	0.000817
.	.
.	.
.	.
1000	0.000554
Total	0.042205

3.3. Proses Seleksi

Proses yang dilakukan pada tahap ini adalah mencari nilai kebugaran relatif (p_k) dan nilai kebugaran kumulatif (q_k) dari tiap-tiap individu. Nilai kebugaran relatif dan kebugaran komulatif dapat dilihat ada tabel 5 berikut

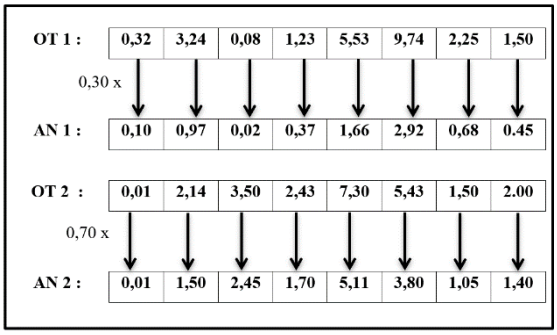
Tabel 5 Nilai Kebugaran Relatif dan Kebugaran Komulatif

Individu	p_x	q_x
1	0.021	0.021
2	0.022	0.043
3	0.019	0.062
.	.	.
.	.	.
.	.	.
1000	0.013	1.000

Proses selanjutnya adalah membangkitkan nilai acak dari 0 sampai dengan 1 sebanyak jumlah populasi. Bilangan acak pertama r1 = 0.019, bisa dilihat bahwa r1 < q1. Dengan demikian maka individu 1 akan terpilih sebagai individu baru yang pertama. Bilangan random yang kedua r2 = 0.030, yang artinya bahwa r2 >= q1 dan r2 < q2. Dengan demikian individu 2 akan terpilih sebagai individu baru yang ke dua.

3.4. Rekombinasi

Dalam setiap operasi rekombinasi, diambil dua individu orang tua yang selanjutnya akan menghasilkan dua individu baru dengan cara memberikan pembobotan kepada orang tua pertama menggunakan nilai acak antara 0 sampai dengan 1. Proses rekomendasi dapat dilihat pada gambar 2 berikut:



Gambar 2 Proses Rekombinasi

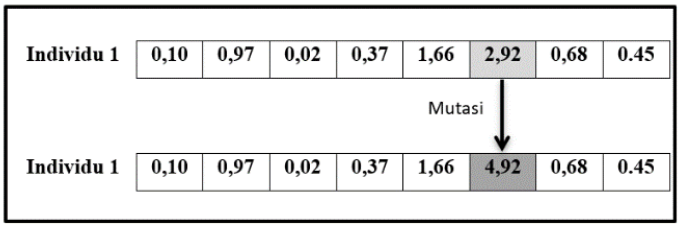
Maka setelah terjadi proses rekombinasi populasi akan mengalami perubahan, populasi dengan tanda * merupakan populasi anak. Populasi hasil dari proses rekombinasi seperti terlihat pada tabel 6.

Tabel 6 Individu Baru Hasil dari Rekombinasi

Ind	Gen							
	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7
1*	0,10	0,97	0,02	0,37	1,66	2,92	0,68	0.45
2*	0,01	1,50	2,45	1,70	5,11	3,80	1,05	1,40
3	0,01	2,14	3,50	2,43	7,30	5,43	1,50	2,00
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
1000	0,20	1,51	6,08	5,53	3,30	2,47	8,51	1,25

3.5. Mutasi

Berikut contoh terjadinya mutasi terhadap individu 1. Dalam individu ini, setelah diacak didapatkan bahwa gen yang akan diubah yaitu gen keenam. Selanjutnya diterapkan mutasi pada individu tersebut dan nilai dari gen keenam digantikan dengan sembarang bilangan real lainnya. Hal ini tentu saja akan mengubah individu 1 menjadi individu yang baru. Proses mutasi dapat dilihat pada gambar 3 berikut:



Gambar 3 Proses Mutasi

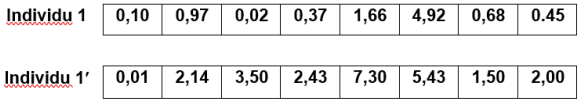
Maka setelah terjadi proses mutasi populasi yang terbentuk akan terlihat seperti pada tabel 7.

Tabel 7 Individu Baru Hasil dari Mutasi

Ind	Gen							
	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7
1	0,10	0,97	0,02	0,37	1,66	4,92	0,68	0.45
2	0,01	1,50	2,45	1,70	5,11	3,80	1,05	1,40
3	0,01	2,14	3,50	2,43	7,30	5,43	1,50	2,00
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.
1000	0,20	1,51	6,08	5,53	3,30	2,47	8,51	1,25

3.6. Pencarian Lokal

Misalkan algoritma pencarian lokal ini diterapkan pada individu 1, maka dari individu 1 tersebut akan dihasilkan individu yang baru yaitu individu 1’ dengan nilai kebugaran yang lebih tinggi, seperti pada gambar 4.



Gambar 4 Proses Pencarian Lokal

Setelah terjadi proses *hill climbing* nilai kebugaran dari individu 1 yang semula 0,002364 ditingkatkan menjadi individu 1’ dengan nilai kebugaran 0,002577. Nilai kebugaran pada individu setelah mutasi dapat dilihat ada tabel 8, sedangkan nilai kebugaran pada individu setelah pencarian lokal dapat dilihat pada tabel 9 beikut

Tabel 8 Nilai Kebugaran pada Individu setelah Mutasi

Individu	Gen								Nilai Kebugaran
	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7	
1	0,10	0,97	0,02	0,37	1,66	4,92	0,68	0.45	0,002364
2	0,01	1,50	2,45	1,70	5,11	3,80	1,05	1,40	0,001302
3	0,01	2,14	3,50	2,43	7,30	5,43	1,50	2,00	0,000911
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.
50	0,20	1,51	6,08	5,53	3,30	2,47	8,51	1,25	0,000817

Tabel 9 Nilai Kebugaran pada Individu setelah Pencarian Lokal

Individu	Gen								Nilai Kebugaran
	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7	
1’	0,30	0,57	0,02	0,27	1,56	4,72	0,70	0,50	0,002577
2’	0,21	1,27	2,03	1,80	5,14	3,65	1,25	1,3	0,001338
3’	0,11	2,34	3,15	2,23	7,32	5,13	1,23	2,21	0,000931
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
.	.	.	.	.	.	.	.	.	.	.
1000’	0,23	1,21	6,18	5,13	3,13	2,52	8,65	1,21	0,000839

Setelah dilakukan teknik pencarian lokal *hill climbing*, maka kita dapatkan populasi baru yang merupakan populasi generasi selanjutnya. Kemudian individu dengan nilai kebugaran terbaik dicatat. Dari populasi pertama individu dengan nilai kebugaran tertinggi adalah individu 1’, maka individu 1’ dijadikan individu terbaik. Kemudian proses dilanjutkan untuk mendapatkan populasi generasi kedua, ketiga, keempat dan seterusnya sampai dengan kriteria berhenti terpenuhi.

3.7. Kriteria berhenti

Iterasi akan berhenti ketika dilakukan 10 kali proses perulangan dan tetap menghasilkan populasi dengan nilai kebugaran yang sama. Misalkan proses perulangan berhenti pada saat populasi mencapai pada generasi ke 100, maka hasil statistik populasi terbaik mulai dari generasi ke 1 sampai dengan generasi ke 100 seperti pada tabel 10.

Tabel 10 Statistik Individu Terbaik pada Tiap Generasi

Generasi	Individu								Kebugaran Terbaik	Rata-Rata Kebugaran
	θ_0	θ_1	θ_2	θ_3	θ_4	θ_5	θ_6	θ_7		
1	0,10	0,97	0,02	0,37	1,66	4,92	0,68	0.45	0,002364	0,000876
2	0,01	1,90	7,45	2,70	5,11	3,80	4,05	1,90	0,009765	0,000997
3	0,71	2,94	3,70	5,43	2,30	7,43	1,30	5,00	0,007376	0,000765
4	0,51	3,50	7,25	4,90	9,11	2,80	4,05	9,40	0,004765	0,000925
5	2,01	4,14	8,50	2,13	7,70	5,93	7,50	1,00	0,005396	0,000543
.	.	.	.	.	.	.	.	.	.	
.	.	.	.	.	.	.	.	.	.	
.	.	.	.	.	.	.	.	.	.	
100	0,01	0,03	0,02	0,05	0,02	0,03	0,08	0,78	0,020296	0,009856

Diketahui transaksi normal bulan ke 12 (X^_12) adalah 49,27% sedangkan transaksi yang terjadi bulan ke 8 sebesar 90% sehingga selisihnya adalah :

$$S = 90 - 49{,}27$$
$$S = 40{,}73.$$

Setelah kemudian diketahui nilai selisihnya (S) maka nilai S tersebut tinggal dibandingkan dengan nilai-nilai dari hasil pelatihan terhadap transaksi yang sudah dikategorikan curang dan transaksi yang sudah dikategorikan sah. Jika ternyata transaksi bulan ke 12 >= dari nilai minimum transaksi curang dari hasil pelatihan dan nilai simpangan (S) >= nilai minimum transaksi curang maka transaksi bulan ke 12 tersebut masuk dalam kategori transaksi curang. Namun jika ternyata transaksi bulan ke 12 < dari nilai minimum transaksi curang dari hasil pelatihan dan nilai simpangan (S) < nilai minimum transaksi curang maka transaksi bulan ke 12 tersebut masuk dalam kategori transaksi sah.

3.8. Pengujian

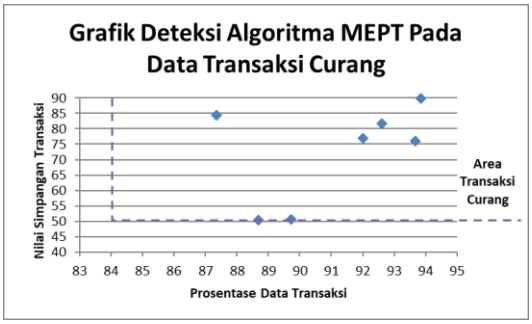
Pengujian dilakukan dengan menggunakan metode *cross validation* Parameter yang digunakan adalah akurasi. Perhitungan akurasi sebagai tolak ukur evaluasi algoritma memetika dan pencarian tersebar diperoleh dengan menggunakan persamaan berikut:
(TP+TN) / (TP+FP+TN+FN)

Pengujian dilakukan dalam tiga skenario:,

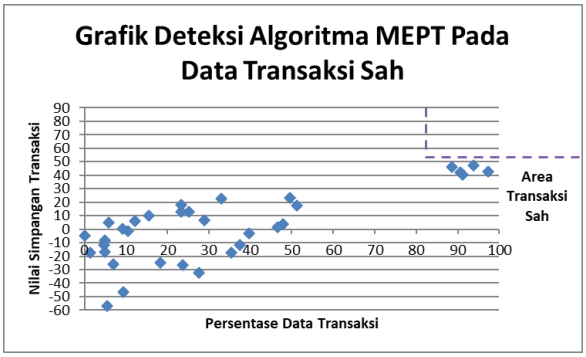
1). Skenario pertama adalah dengan melakukan uji terhadap 20% data dari total data set. Dari 20% data tersebut kemudian dibagi menjadi dua bagian 80 % digunakan sebagai data pelatihan dan 20% digunakan sebagai data testing. Dari 80% data pelatihan 20% adalah data yang dideteksi sebagai transaksi curang sedang 80% sisanya data yang dideteksi sebagai data transaksi sah. Sedangkan dari 20% data testing 20% adalah data yang dideteksi sebagai transaksi curang sedang 80% sisanya data yang dideteksi sebagai data transaksi sah. Kemudian data tersebut dilakukan pengujian terhadap algoritma memetika dan pencarian tersebar untuk mengukur tingkat akurasi dari algoritma tersebut pada tingkat data yang kecil.

Tabel 11 Komposisi Data Uji dan Data Pelatihan Skenario Pertama

Jumlah Data Set	Jumlah Data Uji		Jumlah Data Pelatihan	
	Sah	Curang	Sah	Curang
200	32	8	128	32
Total	**40**		**160**	



Gambar 5 Grafik Deteksi Algoritma MEPT Terhadap Data Transaksi Curang.



Gambar 6 Grafik Deteksi Algoritma MEPT Terhadap Data Transaksi Sah.

Gambar 5 menunjukkan algoritma MEPT tidak mengalami kesalahan deteksi pada data transaksi yang curang. Sedangkan pada gambar 6 algoritma MEPT juga tidak mengalami kesalahan deteksi pada data yang sah.

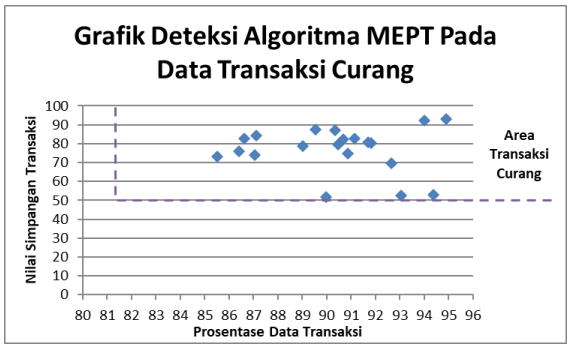
Hasil uji dari skenario satu adalah :
true positive=33, true negative=7, false positive=0, dan false negative=0.
Akurasi MEPT

$$= ((33 + 7) / (33 + 0 + 7 + 0)) \times 100\%$$
$$= (40/40) \times 100\%$$
$$= 100\%$$

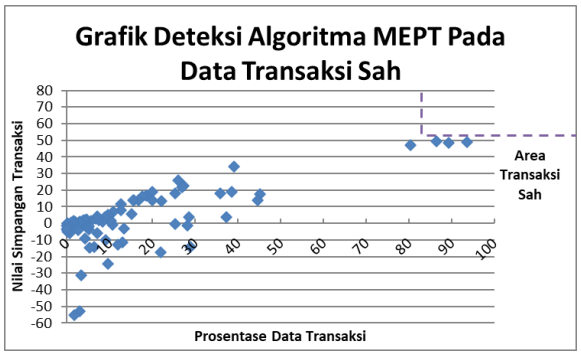
2). Skenario kedua adalah dengan melakukan uji terhadap 50% data dari total data set. Dari 50% data tersebut kemudian dibagi juga menjadi dua bagian 80 % nya digunakan sebagai data pelatihan dan 20% digunakan sebagai data testing. Dari 80% data pelatihan 20% nya adalah data yang dideteksi sebagai transaksi curang sedang 80% sisanya data yang dideteksi sebagai data transaksi sah. Sedangkan dari 20% data testing 20% nya adalah data yang dideteksi sebagai transaksi curang sedang 80% sisanya data yang dideteksi sebagai data transaksi sah. Kemudian data tersebut dilakukan pengujian terhadap algoritma memetika dan pencarian tersebar untuk mengukur tingkat akurasi dari algoritma tersebut pada tingkat data yang sedang.

Tabel 12 Komposisi Data Uji dan Data Pelatihan Skenario Kedua

Jumlah Data Set	Jumlah Data Uji		Jumlah Data Pelatihan	
	Sah	Curang	Sah	Curang
500	80	20	320	80
Total	**100**		**400**	



Gambar 7 Grafik Deteksi Algoritma MEPT Terhadap Data Transaksi Curang.



Gambar 8 Grafik Deteksi Algoritma MEPT Terhadap Data Transaksi Sah.

Gambar 7 menunjukkan algoritma MEPT tidak mengalami kesalahan deteksi pada data transaksi yang curang. Sedangkan pada gambar 8 algoritma MEPT juga tidak mengalami kesalahan deteksi pada data yang sah.

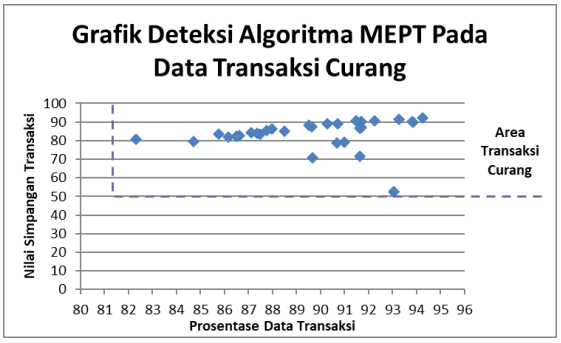
Hasil uji dari skenario satu adalah :
true positive=80, true negative=20, false positive=0, dan false negative=0.
Akurasi MEPT

$$= ((80 + 20) / (80 + 0 + 20 + 0)) * 100\%$$
$$= (100/100) * 100\%$$
$$= 100\%$$

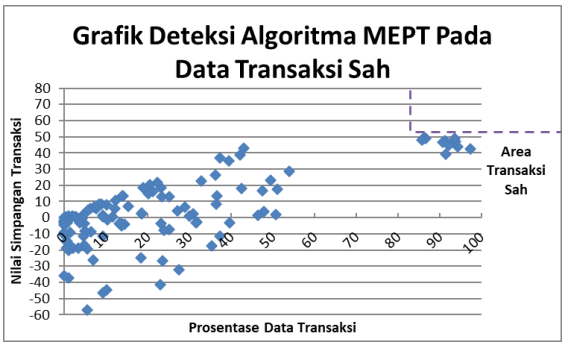
3). Skenario ketiga adalah dengan melakukan uji terhadap 80% data dari total data set. Dari 80% data tersebut kemudian dibagi juga menjadi dua bagian 80 % nya digunakan sebagai data pelatihan dan 20% digunakan sebagai data testing. Dari 80% data pelatihan 20% nya adalah data yang dideteksi sebagai transaksi curang sedang 80% sisanya data yang dideteksi sebagai data transaksi sah. Sedangkan dari 20% data testing 20% nya adalah data yang dideteksi sebagai transaksi curang sedang 80% sisanya data yang dideteksi sebagai data transaksi sah. Kemudian data tersebut dilakukan pengujian terhadap algoritma memetika dan pencarian tersebar untuk mengukur tingkat akurasi dari algoritma tersebut pada tingkat data yang besar.

Tabel 13 Komposisi Data Uji dan Data Pelatihan Skenario Kedua

Jumlah Data Set	Jumlah Data Uji		Jumlah Data Pelatihan	
	Sah	Curang	Sah	Curang
800	128	32	512	128
Total	**160**		**640**	



Gambar 9 Grafik Deteksi Algoritma MEPT Terhadap Data Transaksi Curang.



Gambar 10 Grafik Deteksi Algoritma MEPT Terhadap Data Transaksi Sah.

Gambar 9 menunjukkan algoritma MEPT tidak mengalami kesalahan deteksi pada data transaksi yang curang. Sedangkan pada gambar 10 algoritma MEPT juga tidak mengalami kesalahan deteksi pada data yang sah.

Hasil uji dari skenario satu adalah :
true positive=128, true negative=32, false positive=0, dan false negative=0.
Akurasi MEPT

$$= ((128 + 32) / (128 + 0 + 32 + 0)) * 100\%$$
$$= (160/160) * 100\%$$
$$= 100\%$$

4. Kesimpulan

Tujuan dari serangkaian pengujian ini adalah untuk mengukur tingkat akurasi algoritma Memetika dan Pencarian Tersebar (MEPT) atau Memetic and Scatter Search algorithm pada kasus pendeteksian kecurangan transaksi kartu kredit. Serangkaian pengujian telah dilakukan dan didokumentasikan, yang menghasilkan tingkat akurasi algoritma MEPT. Dari proses pembuktian tersebut diambil kesimpulan bahwa Algoritma MEPT dapat mendeteksi kasus penipuan pada kartu kredit. Tingkat akurasi algoritma MEPT tidak terpengaruh terhadap jumlah data yang diuji. Algoritma MEPT dapat memperbaiki performa algoritma Genetika dan Pencarian tersebar dari tingkat akurasi 87% menjadi 100%.

Daftar Pustaka

Almeida, F., Giménez, D., Espín, J. J., & Pérez, M. P. (2013). Parameterized Schemes of Metaheuristics: Basic Ideas and Applications With Genetic Algorithms, Scatter Search, and GRASP. IEEE Transactions on Systems, Man, and Cybernetics: Systems .

Bank Indonesia, (2021), “Peraturan Bank Indonesia nomor: 14 / 2 /PBI/ 2012 Tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu”,Jakarta.

Behmanesh, E., Pannek, J. (2021). A Comparison between Memetic Algorithm and Genetic Algorithm for an Integrated Logistics Network with Flexible Delivery Path. Operations Research Forum (2021) 2: 47.

Benchaji, I., Douzi, S., & ElOuahidi, B. (2018). Using Genetic Algorithm to Improve Classification of Imbalanced Datasets for Credit Card Fraud Detection. 2018 2nd Cyber Security in Networking Conference (CSNet).

Chunxin, S., Xiaoxia, Z., Hongyang, C., Jiao, Y., Wangpeng, & Weiyu. (2018). A Hybrid Scatter Search Algorithm for QoS Multicast Routing Problem. Chinese Control And Decision Conference (CCDC).

Ding, J., Shen, L., Lü, Z., Xu, L., & Benlic, U. (2019). A Hybrid Memetic Algorithm for the Parallel Machine Scheduling Problem With Job Deteriorating Effects. IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE.

Hernando, L., Mendiburu, A., & Lozano, J. A. (2018). Hill-climbing algorithm: let's go for a walk before finding the optimum. IEEE Congress on Evolutionary Computation (CEC).

Leevy, J., Hancock, J., & Khoshgoftaar, T. (2023). Comparative analysis of binary and one-class classiication techniques for credit card fraud data. Leevy et al. Journal of Big Data 10:118

Mundade, A. A., & Pattewar, T. M. (2015). Comparison study of optimized test suite generation using Genetic and Memetic algorithm. International Conference on Pervasive Computing (ICPC).

Prasad, P. Y., Chowdary, A. S., Bavitha, C., Mounisha, E., & Reethika, C. (2023). A Comparison Study of Fraud Detection in Usage of Credit Cards using Machine Learning. International Conference on Trends in Electronics and Informatics (ICOEI).

Raajha, Y. M., Reshma, K. A., D, R., R., Mekala, R. S., & N. (2023). An Analytical Approach to Fraudulent Credit Card Transaction Detection using Various Machine Learning Algorithms. Second International Conference on Electronics and Renewable Systems (ICEARS).

Rupolo, D., & Mantovani, J. R. (2015). Reconfiguration of Radial Electric Power Distribution System via a Scatter Search Algorithm. IEEE Latin America Transactions.

Singh, A., Singh, A., Aggarwal, A., & Chauhan, A. (2022). Design and Implementation of Different Machine Learning Algorithms for Credit Card Fraud Detection. International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME).

Tomar, P., Shrivastava, S., & Thakar, U. (2021). Ensemble Learning based Credit Card Fraud Detection System. 2021 5th Conference on Information and Communication Technology (CICT).

Zhuang, Z., Fan, S., Xu, H., & Zheng, J. (2016). A memetic algorithm using partial solutions for graph coloring problem. IEEE Congress on Evolutionary Computation (CEC).