

# APLIKASI MODEL *HIDDEN* MARKOV DISKRET UNTUK MENDETEKSI PENYALAHGUNAAN KARTU KREDIT

UTARI, P.<sup>1)</sup>, B. SETIAWATY<sup>2)</sup>, DAN N. K. K. ARDANA<sup>2)</sup>

<sup>1)</sup>Mahasiswa Program Studi Matematika  
Fakultas Matematika dan Ilmu Pengetahuan Alam  
Institut Pertanian Bogor  
Jl Meranti, Kampus IPB Darmaga, Bogor 16680, Indonesia

<sup>2)</sup>Departemen Matematika  
Fakultas Matematika dan Ilmu Pengetahuan Alam  
Institut Pertanian Bogor  
Jl Meranti, Kampus IPB Darmaga, Bogor 16680, Indonesia

**Abstrak :** Model *Hidden* Markov diskret diaplikasikan pada transaksi suatu kartu kredit untuk mendeteksi penyalahgunaan terhadap penggunaan kartu kredit tersebut. Pendugaan parameter model dilakukan menggunakan Metode *Maximum Likelihood* Rabiner yang terdiri dari: Algoritme *Forward*, Algoritme *Viterbi* dan Algoritme *Baum-Welch*. Dengan menggunakan parameter dugaan proses deteksi kartu kredit dilakukan dengan menghitung peluang observasi untuk setiap transaksi baru. Jika perbandingan selisih dari peluang observasi transaksi baru dengan transaksi sebelumnya lebih besar atau sama dengan nilai ambang batas maka transaksi baru tersebut terdeteksi sebagai penyalahgunaan.

**Kata kunci:** Rantai Markov, *Hidden* Markov model, Metode Rabiner.

## 1. PENDAHULUAN

Model *Hidden* Markov terdiri dari sepasang proses stokastik yaitu proses observasi dan proses yang mempengaruhi terjadinya proses observasi. Proses yang mempengaruhi terjadinya proses observasi diasumsikan membentuk rantai Markov dan tidak diamati. Oleh sebab itu rantai Markov tersembunyi atau *hidden* dibalik proses observasi.

Saat ini penggunaan kartu kredit sudah semakin meningkat. Hal tersebut menyebabkan penyalahgunaan terhadap kartu kredit juga meningkat. Jika rincian transaksi kartu kredit merupakan proses observasi dan penyebab besarnya transaksi tidak diamati secara langsung dan diasumsikan membentuk

suatu rantai Markov, maka pasangan dari proses observasi dan penyebabnya dapat dimodelkan dengan model *Hidden Markov*.

Pada tulisan ini, pendeteksian penyalahgunaan kartu kredit akan dimodelkan menggunakan model *Hidden Markov* diskret yang dikembangkan oleh Srivastaya et. al. (2008).

## 2. MODEL HIDDEN MARKOV DISKRET

**2.1 Karakteristik Model Hidden Markov Diskret:** Model Hidden Markov Diskret terdiri atas pasangan proses stokhastik  $\{(Q_r, O_r)\}$ .  $\{Q_r\}$  merupakan penyebab kejadian yang tidak diamati secara langsung dan membentuk rantai Markov. Sedangkan  $\{O_r\}$  adalah proses observasinya.

Karakteristik model *Hidden Markov* diskret dicirikan oleh parameter berikut.

- 1)  $N$  adalah banyaknya *state* rantai Markov  $\{Q_r\}$  yang tersembunyi dalam model. Ruang *state* yang ditunjukkan yaitu  $S_Q = \{1, 2, \dots, N\}$ .
- 2)  $M$  adalah banyaknya *state* proses observasi  $\{O_r\}$ . Ruang *state* yang ditunjukkan yaitu  $S_O = \{1, 2, \dots, M\}$ .
- 3) Matriks peluang *state* transisi  $A = [a_{ij}]$ , di mana

$$a_{ij} = P(Q_{r+1} = j | Q_r = i), \quad a_{ij} \geq 0, \quad 1 \leq i \leq N, 1 \leq j \leq N,$$

$$\sum_{j=1}^N a_{ij} = 1, \quad 1 \leq i \leq N.$$

- 4) Matriks peluang dari proses observasi  $B = [b_i(j)]$ , dimana
- $$b_i(j) = P(O_r = j | Q_r = i), \quad 1 \leq j \leq M, 1 \leq i \leq N,$$
- $$\sum_{j=1}^M b_i(j) = 1.$$

- 5) Vektor peluang *state* awal  $\pi = [\pi_i]$ , di mana

$$\pi_i = P(Q_1 = i), \quad 1 \leq i \leq N,$$

$$\sum_{i=1}^N \pi_i = 1.$$

Jadi karakteristik model *Hidden Markov* dicirikan oleh parameter  $\lambda = (A, B, \pi)$ .

**2.2 Estimasi Parameter Model Hidden Markov Diskret:** Untuk mengestimasi parameter  $\lambda = (A, B, \pi)$ , digunakan Algoritme Rabiner yang terdiri terdiri atas algoritme *forward-backward*, algoritme Viterbi, dan algoritme Baum-Welch (Rabiner 1989).

**2.2.1 Algoritme Forward-Backward:** Algoritme *forward-backward* digunakan untuk menentukan peluang munculnya barisan observasi  $o_1, o_2, \dots, o_r$  untuk suatu  $\lambda = (A, B, \pi)$  tertentu, yaitu

$$P(O_1 = o_1, O_2 = o_2, \dots, O_R = o_R | \lambda).$$

Pada algoritme ini didefinisikan peubah *forward*, yaitu peluang bersama observasi  $o_1, o_2, \dots, o_r$ ;  $r \leq R$  dan berada pada *state*  $j$  di waktu  $r$ , jika diberikan model  $\lambda$ , yaitu:

$$\alpha_r(j) = P(O_1 = o_1, \dots, O_r = o_r, Q_r = j | \lambda).$$

Prosedur algoritme *forward* adalah sebagai berikut:

1. Diberikan nilai awal untuk  $r = 1$ .

$$\begin{aligned}\alpha_1(j) &= P(O_1 = o_1, Q_1 = j|\lambda) \\ &= P(Q_1 = j|\lambda)P(O_1 = o_1|Q_1 = j, \lambda) \\ &= \pi_j b_j(o_1), \quad j = 1, 2, \dots, N.\end{aligned}$$

2. Dengan cara induksi akan diperoleh

$$\begin{aligned}\alpha_{r+1}(j) &= P(O_1 = o_1, \dots, O_{r+1} = o_{r+1}, Q_{r+1} = j|\lambda) \\ &= [\sum_{i=1}^N \alpha_r(i) a_{ij}] b_j(o_{r+1}), \quad j = 1, 2, \dots, N; 1 \leq r \leq R - 1.\end{aligned}$$

3. Sehingga diperoleh

$$\begin{aligned}P(O_1 = o_1, \dots, O_R = o_R|\lambda) &= \sum_{j=1}^N P(O_1 = o_1, \dots, O_R = o_R, Q_R = j|\lambda) \\ &= \sum_{j=1}^N \alpha_R(j).\end{aligned}$$

Pada algoritme ini juga didefinisikan peubah *backward*,

$$\beta_r(j) = P(O_{r+1} = o_{r+1}, \dots, O_R = o_R|Q_r = j, \lambda).$$

yaitu peluang barisan observasi parsial  $o_{r+1}, o_{r+2}, \dots, o_R$  dan berada pada *state*  $j$  di waktu  $r$ , jika diberikan model  $\lambda$ . Prosedur algoritme *backward* adalah sebagai berikut:

1. Diberikan nilai awal untuk  $r = R$

$$\beta_R(j) = P(O_{R+1} = o_{R+1}|Q_R = j) = 1, \quad j = 1, \dots, N.$$

2. Dengan cara induksi akan diperoleh

$$\begin{aligned}\beta_r(j) &= P(O_{r+1} = o_{r+1}, \dots, O_R = o_R|Q_r = j, \lambda) \\ &= \sum_{i=1}^N b_i(o_{r+1})\beta_{r+1}(i)a_{ji}, \quad j = 1, 2, \dots, N; r = R - 1, R - 2, \dots, 1.\end{aligned}$$

(Bukti lihat Wijayanti 2010)

**2.2.2 Algoritme Viterbi:** Algoritme Viterbi digunakan untuk menentukan pendugaan barisan *state*  $\{Q_r\}$  yang memiliki peluang maksimum yang selanjutnya digunakan untuk menduga barisan observasi  $\{O_r\}$ . Pada masalah ini, akan dipilih barisan *state*  $\{Q_r\}_{r=1}^R$  sehingga  $P(O_1 = o_1, \dots, O_R = o_R, Q_1 = q_1, \dots, Q_R = q_R|\lambda)$  adalah maksimum.

Didefinisikan  $\delta_r(j)$  sebagai berikut:

$$\begin{aligned}\delta_r(j) &= \max_{q_1, q_2, \dots, q_{r-1}} P(O_1 = o_1, \dots, O_r = o_r, Q_1 = q_1, \dots, Q_r = j|\lambda) \\ &= [\max_{i=1, \dots, N} \delta_{r-1}(i) a_{ij}] b_j(o_r).\end{aligned}$$

Barisan yang menghasilkan  $\delta_r(j)$  ditunjukkan oleh

$$\psi_r(j) = \arg \max_{i=1, \dots, N} \delta_{r-1}(i) a_{ij}, \quad j = 1, 2, \dots, N.$$

Prosedur algoritme Viterbi adalah sebagai berikut:

1. Diberikan nilai awal untuk  $r = 1$ .  $\delta_1(j) = \pi_j b_j(o_1), j = 1, 2, \dots, N$

$$\psi_1(j) = \arg \max_{i=1, \dots, N} \delta_0(i) a_{ij} = \emptyset.$$

2. Dengan cara rekursif akan diperoleh

$$\delta_R(j) = [\max_{i=1, \dots, N} \delta_{R-1}(i) a_{ij}] b_j(o_R)$$

$$\psi_R(j) = \arg \max_{i=1, \dots, N} \delta_{R-1}(i) a_{ij}, \text{ untuk } j = 1, \dots, N.$$

3. Sehingga diperoleh

$$j_*(R) = \arg \max_{i=1, \dots, N} \delta_R(i).$$

Kemudian dilakukan penelusuran balik barisan *state* optimal.

$$\text{Untuk } r = R - 1, R - 2, \dots, 1, j_*(r) = \psi_{r+1}(j_*(r + 1)).$$

(Bukti lihat Wijayanti 2010)

**2.2.3 Algoritme Baum-Welch:** Algoritme Baum-Welch digunakan untuk menentukan parameter dugaan model *Hidden Markov*. Pada masalah ini akan dimaksimumkan nilai peluang observasi  $P(O_1 = o_1, \dots, O_r = o_r | \lambda)$  untuk memperoleh nilai parameter model *Hidden Markov*  $\bar{\lambda} = (\bar{A}, \bar{B}, \bar{\pi})$  yang dapat dengan baik mendeskripsikan rangkaian observasi yang terjadi. Prosedur algoritme Baum-Welch adalah sebagai berikut.

- Didefinisikan  $\xi_r(i, j)$  yaitu peluang *state*  $i$  pada waktu  $r$ , dan *state*  $j$  pada waktu  $r + 1$ , jika diberikan model  $\lambda$  dan rangkaian pengamatan.

$$\xi_r(i, j) = \frac{\alpha_r(i) a_{ij} b_j(o_{r+1}) \beta_{r+1}(j)}{\sum_{j=1}^N \alpha_r(j) \beta_r(j)}.$$

- Didefinisikan  $\gamma_r(i)$  yaitu peluang berada di *state*  $i$  pada waktu  $r$ , jika diberikan rangkaian pengamatan  $O = \{o_r; r = 1, \dots, R\}$  dan model  $\lambda$ :

$$\gamma_r(i) = \frac{\alpha_r(i) \beta_r(i)}{\sum_{i=1}^N \alpha_r(i) \beta_r(i)}.$$

- Dengan algoritme *Expectation Maximization* (EM) akan diperoleh  $\bar{\lambda}$  yang memaksimumkan nilai peluang observasi  $P(O_1 = o_1, \dots, O_r = o_r | \lambda)$ . Langkah-langkah algoritme EM sebagai berikut:

1. Diketahui sebuah penduga

$$\lambda_t = (A, B, \pi)$$

2. Hitung nilai fungsi Baum-Welch

$$Q(\lambda, \lambda_t) = E_{\lambda_t} \left( \frac{dP_\lambda}{dP_{\lambda_t}} \middle| O \right)$$

3. Tentukan

$$\begin{aligned} \max_\lambda [Q(\lambda, \lambda_t)] &\Rightarrow P(O_1 = o_1, \dots, O_r = o_r | \lambda_t) \\ &\geq P(O_1 = o_1, \dots, O_r = o_r | \lambda) \end{aligned}$$

$$\lambda_{t+1} = \arg \max_\lambda Q(\lambda, \lambda_t).$$

4. Jika kriteria penghentian dipenuhi, maka keluar. Jika tidak terpenuhi, maka  $\lambda_{t+1} = \lambda_t$ , dan ulangi terus langkah 2.

- Dengan menggunakan metode *Lagrange*, dapat diperoleh formula re-estimasi parameter model *Hidden Markov*, yaitu:

$$\bar{\pi}_i = \gamma_1(i), \quad 1 \leq i \leq N$$

$$\bar{a}_{ij} = \frac{\sum_{r=1}^{R-1} \xi_r(i, j)}{\sum_{r=1}^{R-1} \gamma_r(i)}, \quad 1 \leq i \leq N, 1 \leq j \leq N$$

$$\bar{b}_i(j) = \frac{\sum_{r=1}^R \gamma_r(i)}{\sum_{r=1}^R \gamma_r(i)}, \quad 1 \leq i \leq N, 1 \leq j \leq M$$

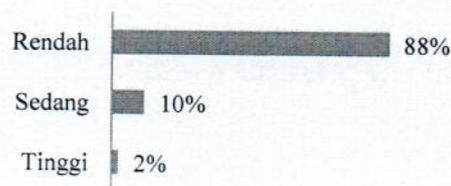
**2.3 Algoritme *K-Means Clustering*:** Algoritme *K-Means clustering* digunakan untuk menentukan kelompok (*cluster*). Pengelompokan dilakukan dengan meminimumkan jumlah kuadrat dari jarak antara setiap data dengan pusat atau rata-rata kelompok yang sudah ditentukan.

### 3. APLIKASI DETEKSI PENYALAHGUNAAN KARTU KREDIT

**3.1 Data Input Transaksi Kartu Kredit:** Dalam tulisan ini, data yang digunakan merupakan data transaksi kartu kredit seseorang yang diperoleh secara pribadi dari tanggal 17 Agustus 2011 sampai dengan 17 Februari 2012. Ada sebanyak 185 data observasi ( $O_r$ ) yang digunakan dalam kasus deteksi penyalahgunaan kartu kredit. Data tersebut dibagi menjadi 2 yaitu data untuk pelatihan sebanyak 150 data yang merupakan data transaksi asli dan data untuk pendeteksian sebanyak 35 data yang merupakan data campuran dari data transaksi asli dan data transaksi penyalahgunaan.

Karena tidak mungkin mendapatkan data dari bank karena kerahasiaan bank, maka penyalahgunaan di sini adalah penggunaan kartu kredit yang dilakukan oleh orang terdekat atau yang sudah dikenal oleh pemegang kartu kredit atas izin pemegang kartu kredit tersebut, sehingga kasusnya sebetulnya legal. Padahal dalam keadaan sesungguhnya, penyalahgunaan penggunaan kartu kredit adalah ilegal karena dilakukan oleh orang lain tanpa izin dari pemilik kartu kredit.

Data tersebut kemudian dikelompokkan menjadi 3 kelompok profil pengeluaran dengan menggunakan algoritme *K-Means clustering*, yaitu rendah = (0, Rp 200.000], sedang = (Rp 200.000, Rp 1.000.000], dan tinggi = (Rp 1.000.000, limit kartu kredit). Dalam komputasi, data input diubah menjadi rendah = 1, sedang = 2, dan tinggi = 3. Data input dapat dilihat pada Lampiran. Persentase jumlah data transaksi untuk setiap profil pengeluaran pemegang kartu dapat dilihat pada Gambar 1.



Gambar 1. Grafik persentase untuk setiap profil pengeluaran.

**3.2 Pemodelan Transaksi Kartu Kredit:** Saat ini kemajuan teknologi sudah jauh meningkat. Hal tersebut dapat terlihat dari penggunaan kartu kredit yang juga meningkat. Dengan meningkatnya penggunaan kartu kredit, maka peluang bagi seseorang untuk melakukan penyalahgunaan kartu kredit juga semakin tinggi. Besar pengeluaran kartu kredit seseorang terjadi karena beberapa penyebab antara lain adanya *discount* pada suatu pusat perbelanjaan sehingga pemegang kartu kredit ingin banyak berbelanja sehingga menyebabkan

pegeluarannya menjadi tinggi. Selain itu suasana hati pemegang kartu kredit juga dapat menyebabkan keinginan untuk banyak berbelanja sehingga pengeluarannya pun menjadi tinggi. Jenis barang pembelian juga bisa menjadi penyebab dari besarnya pengeluaran kartu kredit, misalnya apabila pemegang kartu kredit ingin membelanjakan barang-barang seperti elektronik atau perhiasan, maka pengeluaran kartu kredit akan tinggi juga.

Penyebab kejadian besarnya pengeluaran kartu kredit seseorang diasumsikan bersifat Markov. Artinya meskipun di waktu yang lalu pernah terjadi banyak kejadian yang mempengaruhi besarnya pengeluaran kartu kredit seseorang tetapi penyebab pengeluaran kartu kredit seseorang saat ini cukup dipengaruhi oleh penyebab kejadian kemarin saja.

Jadi karena penyebab kejadian pengeluaran kartu kredit seseorang membentuk suatu rantai Markov dan diasumsikan tidak diamati secara langsung, maka untuk mendeteksi kartu kredit dapat dimodelkan menggunakan model *Hidden Markov*. Proses observasi  $\{O_r, r \in \mathbb{N}\}$  yang digunakan adalah besarnya pengeluaran transaksi kartu kredit seseorang per hari. Banyaknya data adalah 185, sedangkan penyebab kejadian yang tidak diamati secara langsung  $\{Q_r, r \in \mathbb{N}\}$  pada model adalah penyebab terjadinya besar pengeluaran transaksi kartu kredit.

**3.3 Proses Deteksi Kartu Kredit:** Proses pertama merupakan proses pelatihan untuk membangun model *Hidden Markov*. Kemudian proses selanjutnya merupakan proses pendeteksian transaksi kartu kredit. Setelah mendapatkan parameter model *Hidden Markov*, kemudian dilanjutkan dengan proses deteksi penyalahgunaan kartu kredit dengan menghitung peluang dari observasi. Misal  $O_1, O_2, \dots, O_R$  barisan observasi sampai waktu  $R$ , maka peluang observasi menjadi

$$\alpha_1 = P(O_1 = o_1, O_2 = o_2, \dots, O_R = o_R | \lambda).$$

Misal  $O_{R+1}$  merupakan observasi baru dari transaksi yang baru pada waktu  $R + 1$ , maka peluang observasi menjadi

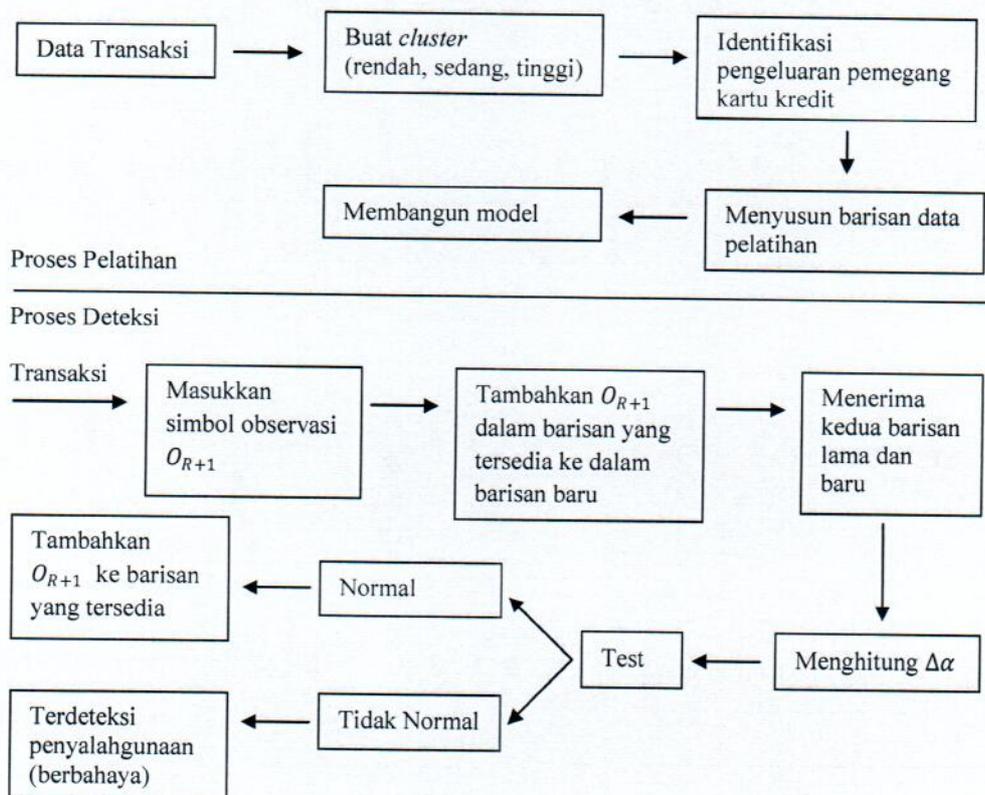
$$\alpha_2 = P(O_2 = o_2, O_3 = o_3, \dots, O_R = o_R, O_{R+1} = o_{R+1} | \lambda).$$

Kemudian didefinisikan  $\Delta\alpha = \alpha_1 - \alpha_2$ .

Jika  $\Delta\alpha > 0$ , berarti barisan baru yang diterima oleh model *Hidden Markov* mempunyai peluang yang rendah, maka itu bisa menjadi suatu penyalahgunaan. Transaksi baru yang ditambahkan diperkirakan sebagai penyalahgunaan jika persentase peluangnya di atas nilai ambang batas, yaitu

$$\Delta\alpha / \alpha_1 \geq \text{nilai ambang batas.}$$

Nilai ambang batas adalah nilai batas deteksi transaksi yang berbahaya (penyalahgunaan) yang dipertimbangkan secara empiris (Srivastava *et al.* 2008). Jika  $O_{R+1}$  berbahaya, maka  $O_{R+1}$  tidak ditambahkan dalam barisan observasi. Jika sebaliknya, maka  $O_{R+1}$  akan ditambahkan dalam barisan secara permanen. Kemudian barisan baru akan digunakan sebagai barisan dasar untuk menentukan validitas transaksi berikutnya. Proses deteksi penyalahgunaan kartu kredit dapat dilihat pada Gambar 2.



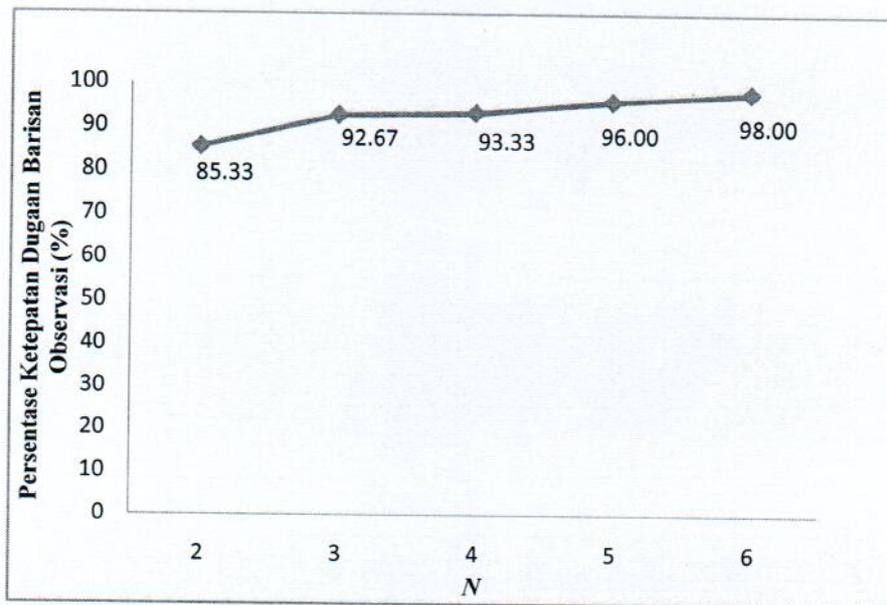
Gambar 2. Proses deteksi penyalahgunaan kartu kredit.

### 3.4 Hasil Komputasi

**3.4.1 Hasil Ketepatan Dugaan Barisan Observasi:** Berikut adalah hasil persentase ketepatan dugaan yang lebih besar dari 60% dengan menggunakan *software Mathematica 7.0*.

Tabel 1. Persentase ketepatan dugaan barisan observasi

N	Frekuensi Persentase Ketepatan di atas 60%	Persentase Ketepatan Dugaan (%)				SeedRandom
		Rendah	Sedang	Tinggi	Barisan Observasi	
2	9	87.41	61.54	100.00	85.33	31653
3	41	95.56	61.54	100.00	92.67	31231
4	65	96.30	61.54	100.00	93.33	7053
5	100	98.52	69.23	100.00	96.00	3157
6	220	97.78	100.00	100.00	98.00	18854



Gambar 3. Grafik ketepatan dugaan barisan observasi

Tabel persentase ketepatan di atas menunjukkan bahwa persentase ketepatan dugaan barisan observasi mencapai lebih dari 80%. Dari tabel tersebut dapat dilihat untuk  $N = 6$ , persentase ketepatan barisan observasi mencapai 98.00%. Ini merupakan ketepatan dugaan yang terbaik untuk hasil yang diperoleh. Parameter-parameter model *Hidden Markov* dapat dilihat pada lampiran.

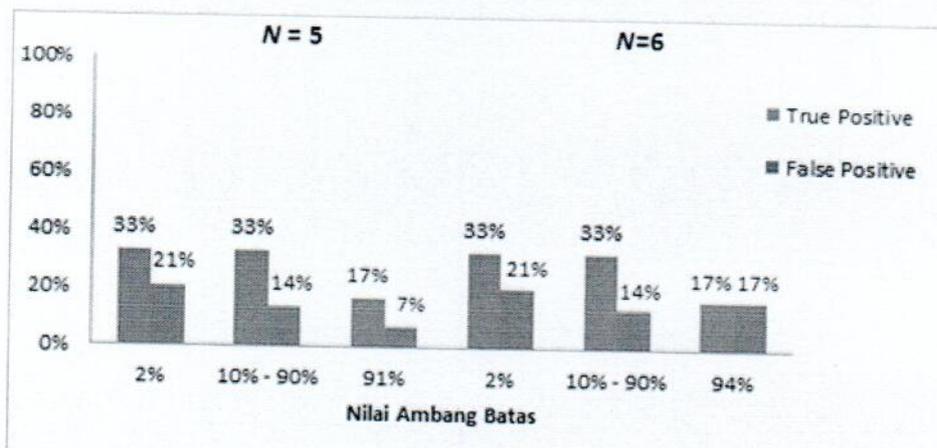
**3.4.2 Hasil Deteksi:** Setelah mendapatkan tiga parameter model *Hidden Markov* dengan nilai  $N$  yang berbeda-beda dan ketepatan dugaan barisan observasi yang mencapai lebih dari 80%, maka selanjutnya akan dilakukan proses deteksi dengan mencari peluang observasi untuk setiap transaksi baru yang merupakan transaksi campuran antara transaksi asli dan transaksi yang disalahgunakan oleh orang lain.

Pertama, nilai  $N$  yang dipilih untuk pendeteksian adalah  $N = 5$  dan  $N = 6$  karena persentase ketepatan dugaan barisan observasi yang diperoleh lebih dari 95% dan merupakan hasil ketepatan barisan observasi yang terbaik. Kemudian menentukan nilai ambang batas yang digunakan untuk pendeteksian. Jadi, jika perbandingan selisih pada peluang observasi lebih dari nilai ambang batas, maka transaksi tersebut diduga sebagai transaksi berbahaya, walaupun itu merupakan transaksi asli. Sehingga transaksi baru tersebut tidak dapat dimasukkan dalam transaksi lama. Pendeteksian ini menggunakan standar metrik *True Positive (TP)*, *False Positive (FP)* dan metrik akurasi untuk mengukur keefektifan sistem.

*True Positive (TP)* merepresentasikan sebagian data transaksi penyalahgunaan yang benar-benar terdeteksi sebagai penyalahgunaan. Sedangkan *False Positive (FP)* merepresentasikan sebagian data transaksi asli diduga sebagai transaksi penyalahgunaan. Akurasi merepresentasikan sebagian total

banyaknya transaksi (transaksi asli dan transaksi penyalahgunaan) yang terdeteksi dengan benar.

Dalam hal ini akurasi didefinisikan sebagai jumlah dari banyaknya transaksi yang terdeteksi asli dan banyaknya transaksi penyalahgunaan yang terdeteksi sebagai penyalahgunaan, dibagi dengan total banyaknya transaksi yang terdeteksi. Hasil deteksi dapat dilihat pada grafik berikut.



Gambar 4. Grafik Nilai *True Positive* dan *False Positive* untuk  $N = 5$  dan  $N = 6$

Dari hasil deteksi di atas dapat dilihat untuk  $N = 5$  dan  $N = 6$  dengan nilai ambang batas dari 10% sampai dengan 90%, nilai TP (*True Positive*) mencapai 33% yang artinya peluang data transaksi penyalahgunaan yang benar-benar terdeteksi sebagai penyalahgunaan sebesar 33%.

Rendahnya nilai *True Positive* (33%) yang diperoleh dapat disebabkan oleh data transaksi yang digunakan merupakan data transaksi penyalahgunaan legal dengan pola data transaksi penyalahgunaan menyerupai pola data transaksi asli, sehingga model *Hidden Markov* sulit membedakan transaksi asli dan transaksi yang disalahgunakan. Nilai akurasi yang diperoleh dari hasil deteksi di atas mencapai 77%.

Tabel 2 Akurasi deteksi untuk  $N = 5$  dan  $N = 6$  dengan nilai ambang batas 10% sampai dengan 90% (banyaknya data yang terdeteksi dan persentasenya)

Data / Deteksi	Asli	Penyalahgunaan	Jumlah data
Asli	25 (86%)	4 (67%)	29
Penyalahgunaan	4 (14%)	2 (33%)	6
Jumlah data	29	6	35

**DAFTAR PUSTAKA**

- [1] **Rabiner LR.** 1989. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. *Proceeding. IEEE*, Vol 77 No.2, pg.257-286.
- [2] **Ross SM.** 1996. *Stochastic Processes*. Ed. ke-2. John Wiley & Sons. New York
- [3] **Srivastava A, Kundu A, Sural S, Majumdar AK.** 2008. Credit Card Fraud Detection Using Hidden Markov Model. *Proceeding. IEEE*, Vol 5 No.1, pg.37-48.
- [4] **Wijayanti H.** 2010. Kajian Model *Hidden Markov* Diskret dengan Algoritme Rabiner dan Aplikasinya pada DNA. [Tesis] IPB.