MENDETEKSI DAN MENGHADAPI SKEEPER

SALAH SATU ancaman terhadap hotel berbintang adalah pelaku kejahatan yang menyamar sebagai tamu dan beraktivitas sebagaimana layaknya tamu. Akan tetapi ketika pihak manajemen hotel akan menagih pembayaran atas seluruh *service* yang telah di bebankan, tamu tersebut melarikan diri. Aksi inilah yang dikenal dengan nama *skeeper.*

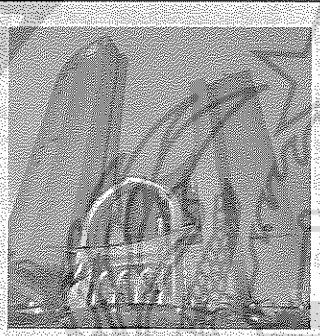
Mendeteksi ciri khas pelaku *skeeper* tidaklah mudah. Ada beberapa petunjuk kecil yang perlu diperhatikan dalam menduga kehadiran pelaku di dalam hotel, yakni:

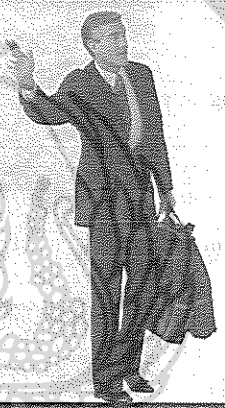
a. Mengenakan perhiasan dan asesoris bagus sehingga tampil dengan *good performance*
b. Berpakaian rapi dan bersikap *high class* seolah sebagai pengusaha ternama
c. Berbicara dengan dialek daerah atau aksen asing yang khas dan meyakinkan

SASARAN PELAKU *SKEEPER*

1 Hotel berbintang di kota-kota besar. Pelaku mengincar hotel berbintang, terutama hotel-hotel yang baru beroperasi di bawah enam bulan karena:

- Hotel baru umumnya menawarkan berbagai paket *discount* dalam program *soft launching.* Ini tentunya menarik perhatian pelaku
- Jaringan antar manajemen hotel berbintang belum terbangun rapi
- Mayoritas karyawan hotel adalah pegawai baru yang belum memahami modus *skeeper*



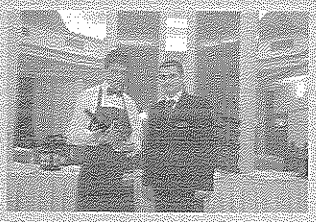


2 Pengusaha. Ada kalanya pelaku mengundang tamu-tamu dalam pertemuan di hotel tempatnya menginap guna melakukan aksi penipuan bisnis. Pelaku memanfaatkan hotel sebagai tempat untuk meningkatkan image dirinya agar korban percaya bahwa pelaku adalah pengusaha besar yang akan melakukan transaksi bisnis

MODUS AWAL PELAKU

1 Menyewa kamar *rate* tinggi untuk tempo waktu yang tidak disebutkan. Umumnya, pada saat melakukan pemesanan, lama waktu menginap disebutkan 2 minggu. Modus lain yang menonjol adalah pelaku memberikan deposit uang muka dalam jumlah besar dengan alasan untuk membiayai pertemuan bisnis yang akan dia adakan di tempatnya menginap

2 Menaruh perhiasan, uang, dan asesoris yang dikenakannya di meja rias kamar hotel sehingga dapat terlihat dengan mudah oleh para petugas yang masuk dan keluar kamar serta tamu hotel sasarannya. Hal ini dilakukan untuk membangun image seolah pelaku adalah seorang pengusaha kaya



3 Mengakrabkan diri dengan petugas-petugas hotel di bagian *room service, F&B,* dan *front office.* Gemar memberikan tips dalam jumlah besar ke petugas-petugas hotel yang dikenalnya

4 Pelaku memahami situasi keamanan hotel dan menghindari sorotan kamera CCTV setiap kali berjalan di dalam ruangan hotel. Hal ini dilakukan agar manajemen tidak memiliki rekaman gambar wajah pelaku.

MODUS TAHAP KEDUA PELAKU

- Pelaku menolak membayar tagihan F&B, sewa kendaraan, dan penggunaan fasilitas hotel lainnya secara tunai. Pelaku meminta seluruh tagihan diakumulasikan ke dalam tagihannya
- Pelaku selalu meminta tambahan layanan hotel dengan cara persuasif ke karyawan hotel
- Pelaku tersinggung bila diberikan informasi bahwa depositnya mendekati batas minimum dengan alasan bahwa dia tengah melakukan transaksi bisnis
- Pelaku mengancam karyawan yang melakukan penagihan dengan alasan mengganggu privasi dan akan melaporkannya ke manajemen dengan menyebut nama pimpinan hotel yang dikenalnya

TINDAKAN PREVENTIF

- Membangun jaringan antar *security manager* hotel-hotel berbintang agar ada pertukaran informasi mengenai identitas dan ciri khas dari pelaku *skeeper*. Pelaku umumnya memiliki dua hingga tiga identitas yang berbeda sama sekali sehingga perlu ada kerja sama untuk menanggulanginya
- Mengawasi aktivitas tamu yang menjalankan modus-modus tersebut
- Meminta pelaku untuk menambah depositnya di hotel sebagai jaminan atau meninggalkan hotel tersebut saat depositnya telah habis

Berdasarkan penjabaran di atas jelas terlihat bahwa pelaku memiliki keahlian dalam *social engineering* guna mengeruk keuntungan besar. Berdasarkan data Asosiasi Security Hotel, para pelaku umumnya membuat sebuah hotel berbintang menderita kerugian hingga 50 juta rupiah akibat aksi mereka. Oleh karenanya, menjaga jaringan security manager antar hotel berbintang merupakan langkah preventif terbaik guna mendeteksi para pelaku sebelum hotel menderita kerugian.(*)

Rubrik "Hotel Security" Merupakan kerjasama antara Asosiasi Security Hotel (ASH) dan Security Journal untuk membantu perbaikan pengetahuan pengamanan perhotelan. ASH merupakan forum tukar-menukar informasi pengamanan antar security manager hotel di Indonesia.

Analisa Ancaman:
Asep Setia Permana
Sekretaris Asosiasi Security Hotel

Sistem Identifikasi Wajah

PADA TAHUN 2001, Kepolisian Tampa memasang sebuah kamera yang mempergunakan teknologi identifikasi wajah pada area kehidupan malam kota Ybor sebagai upaya untuk mengurangi kriminalitas. Sistem tersebut dinilai gagal dan peralatannya dijual sebagai besi tua pada tahun 2003. Penduduk yang terekam gambarnya di area ini terlihat sering memakai topeng dan membuat gerakan yang tidak lazim, sehingga kamera sulit melihat secara jelas untuk mengidentifikasi wajah seseorang. Lapangan udara Logan di Boston juga menjalankan 2 rangkai uji coba terhadap teknologi identifikasi wajah pada pos pemeriksaan keamanan menggunakan tenaga sukarela. Setelah berjalan selama 3 bulan, hasilnya sangat mengecewakan. Menurut Electronic Privacy Information Center, sistem ini hanya memiliki keakuratan 61,4 persen, sehingga para pejabat *airport* menggunakan pilihan pengamanan yang lain.

Manusia selalu mempunyai kemampuan sejak lahir untuk dikenali dan memiliki perbedaan wajah. Pada pertengahan tahun 1960an, para ilmuwan memulai pekerjaan identifikasi wajah manusia menggunakan komputer. Sejak saat itu, perangkat lunak identifikasi wajah telah memulai sebuah perjalanan panjang. Untuk mengaktifkan perangkat lunak ini, harus diketahui bagaimana membedakan bentuk dasar sebuah wajah dengan bagian lain wajah. Perangkat lunak identifikasi wajah ini didasarkan pada kemampuan untuk mengidentifikasi wajah dan membandingkannya dengan berbagai variasi pada wajah tersebut.

Setiap wajah memiliki banyak pembedaan pada bagian yang penting, pada bagian puncak, dan tonjolan yang membedakan wajah manusia. Perangkat lunak ini membedakan bagian penting ini sebagai poin utama. Setiap wajah manusia mempunyai 80 titik poin. Beberapa poin yang diukur perangkat lunak adalah:

- Jarak antar mata
- Lebar hidung
- Kedalaman lekuk mata
- Bentuk tulang pipi
- Panjang garis rahang

Titik poin ini diukur dengan menggunakan kode-kode angka, seperti cetakan di wajah, sehingga menggambarkan wajah pada database komputer.

Pada masa yang lalu, identifikasi wajah memakai gambar 2 dimensi untuk memperbandingkan atau mengidentifikasi gambar 2 dimensi lainnya. Agar lebih efektif dan akurat, gambar yang diperoleh memerlukan wajah yang terlihat langsung pada kamera, dengan variasi yang kecil atau ekspresi wajah dari gambar pada database. Ini tentunya menjadi masalah besar di masa depan. Pada hampir semua instansi, gambar tersebut tidak terdapat pada pengaturan lingkungan. Perubahan kecil di pencahayaan lampu atau orientasi kamera dapat mengurangi efektivitas sistem ini, sehingga tidak dapat memenuhi kriteria wajah yang terdapat di database. Tingkat kegagalannya menjadi sangat tinggi.

Identifikasi Wajah 3 Dimensi

Tren terbaru yang muncul pada *software* identifikasi wajah adalah menggunakan model 3 dimensi, dengan menegaskan pada peningkatan akurasi guna mendapatkan langsung gambar dari kamera 3 dimensi terhadap seluruh bagian wajah manusia. Identifikasi wajah menggunakan 3 dimensi mendapatkan bentuk khusus dari wajah seseorang di mana keras jaringan dan tulang pada bagian yang terlihat nyata seperti cekungan pada mata, hidung dan dagu untuk mengidentifikasi subyek. Semua area sangat unik dan tidak dapat berubah selamanya. Identifikasi wajah dengan 3 dimensi dapat digunakan pada saat gelap dan mempunyai kemampuan untuk mengidentifikasi sebuah subyek dengan menggunakan sudut pandang yang berbeda untuk dan mampu mengidentifikasi sampai sudut 90 derajat (profil pada wajah). Dengan

mempergunakan *software* 3 dimensi, sistem ini terbagi dalam beberapa langkah untuk melakukan identifikasi seseorang yakni:

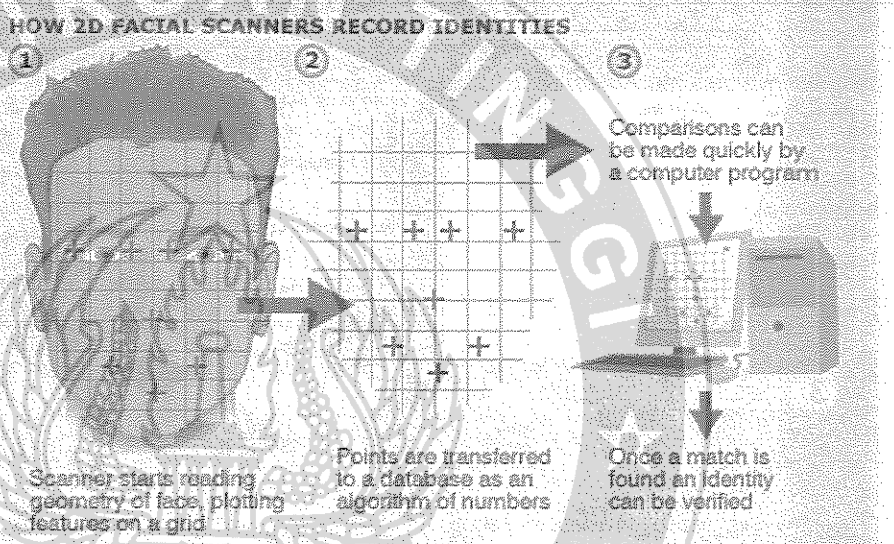
- *Deteksi.* Memperoleh gambar yang dapat memenuhi pengamatan digital dari foto yang sudah ada (2 dimensi) atau menggunakan gambar video untuk memperoleh gambar langsung dari subyek (3 dimensi).
- *Kesejajaran.* Pertama kali mendeteksi wajah, sistem ini akan menentukan bagian kepala, ukuran, dan sikap. Pada keadaan mula-mula, subyek mempunyai potensi untuk dikenali secara 90 derajat, ketika menggunakan 2 dimensi, kepala harus dibelokkan paling tidak 35 derajat dari depan kamera.
- *Penyesuaian.* Sistem akan menentukan tindakan yang diperlukan ketika mendeteksi adanya wajah dengan membelokkan garis wajah sampai ukuran milimeter (atau *microwave*) dan membuat gambar sampingan.
- *Gambaran.* Sistem ini menerjemahkan gambar samping sebagai kode unik. Penyusunan kode ini memberikan setiap gambar tambahan sebuah angka yang mewakili ciri-ciri wajah subyek.
- *Pencocokan.* Apabila gambar 3 dimensi dan database yang menyimpan gambar 3 dimensi disejajarkan, akan menggantikan tanpa mengubah apapun dari gambar. Bagaimanapun, terdapat tantangan dari gambar yang masih menggunakan gambar 2 dimensi. 3 dimensi memberikan sebuah tayangan langsung, menggerakkan subyek yang diperbandingkan secara datar, gambar yang seimbang. Teknologi baru dialamatkan pada tantangan ini. Ketika gambar 3 dimensi digunakan, poin yang berbeda (biasanya tiga) teridentifikasi. Contohnya, bagian luar dari mata, bagian dalam dari mata, dan ujung dari hidung akan diketahui dan diukur. Pertama kali pengukuran pada bagian tersebut, logaritma akan digunakan untuk mengubah menjadi gambar 2 dimensi. Setelah perubahan, *software* akan membandingkan gambar dengan 2 dimensi pada database untuk menemukan kecocokan yang potensial.
- *Pembuktian dan Identifikasi.* Pada proses pembuktian, gambar akan sesuai dengan salah satu gambar yang ada di database (1:1). Sebagai contoh, gambar yang diambil dari sebuah subyek mungkin saja cocok dengan gambar yang terdapat di database Kepolisian untuk membuktikan subyek tersebut adalah siapa yang mengatakan itu siapa. Apabila identifikasi ini berhasil, kemudian gambar ini dibandingkan dengan semua gambar yang terdapat di database untuk menghasilkan penilaian pada semua kecocokan yang potensial (1:N). Pada instansi ini, gambar dapat diperoleh dengan membandingkan dengan database tampak muka untuk mengidentifikasi siapa pemilik gambar tersebut.

Analisa Tekstur Permukaan

Gambar mungkin tidak selalu dapat dibuktikan atau diidentifikasi pada pengenalan wajah sendiri. Beberapa perusahaan membuat produk baru untuk menolong dengan ketelitian. Pengembangan *software* ini menggunakan biometrik kulit, tekstur kulit yang unik, agar menghasilkan kesimpulan yang lebih akurat. Prosesnya disebut dengan Analisa Tekstur Permukaan, bekerja sejalan dengan identifikasi wajah. Sebuah gambar diambil pada bagian kulit, disebut *skin-print*. Potongan tersebut dipisahkan sampai ke kotak-kotak kecil. Menggunakan algoritma untuk mengubah bagian tersebut menjadi simbol matematika, agar dapat diukur. sistem ini akan membedakan garis-garis, pori-pori, dan tekstur kulit yang aktual. Ini dapat mengidentifikasi perbedaan kembar identik, yang tidak mungkin dilakukan dengan *software* identifikasi wajah sendiri. Dengan mengombinasikan identifikasi wajah dengan analisa tekstur kulit, keakuratan identifikasi dapat ditingkatkan sampai 20-25 persen.

Software identifikasi wajah sekarang digunakan dengan 3 tambahan program untuk memastikan atau mengidentifikasikan subyek, garis, analisa ciri-ciri lokal, dan analisa tekstur kulit.

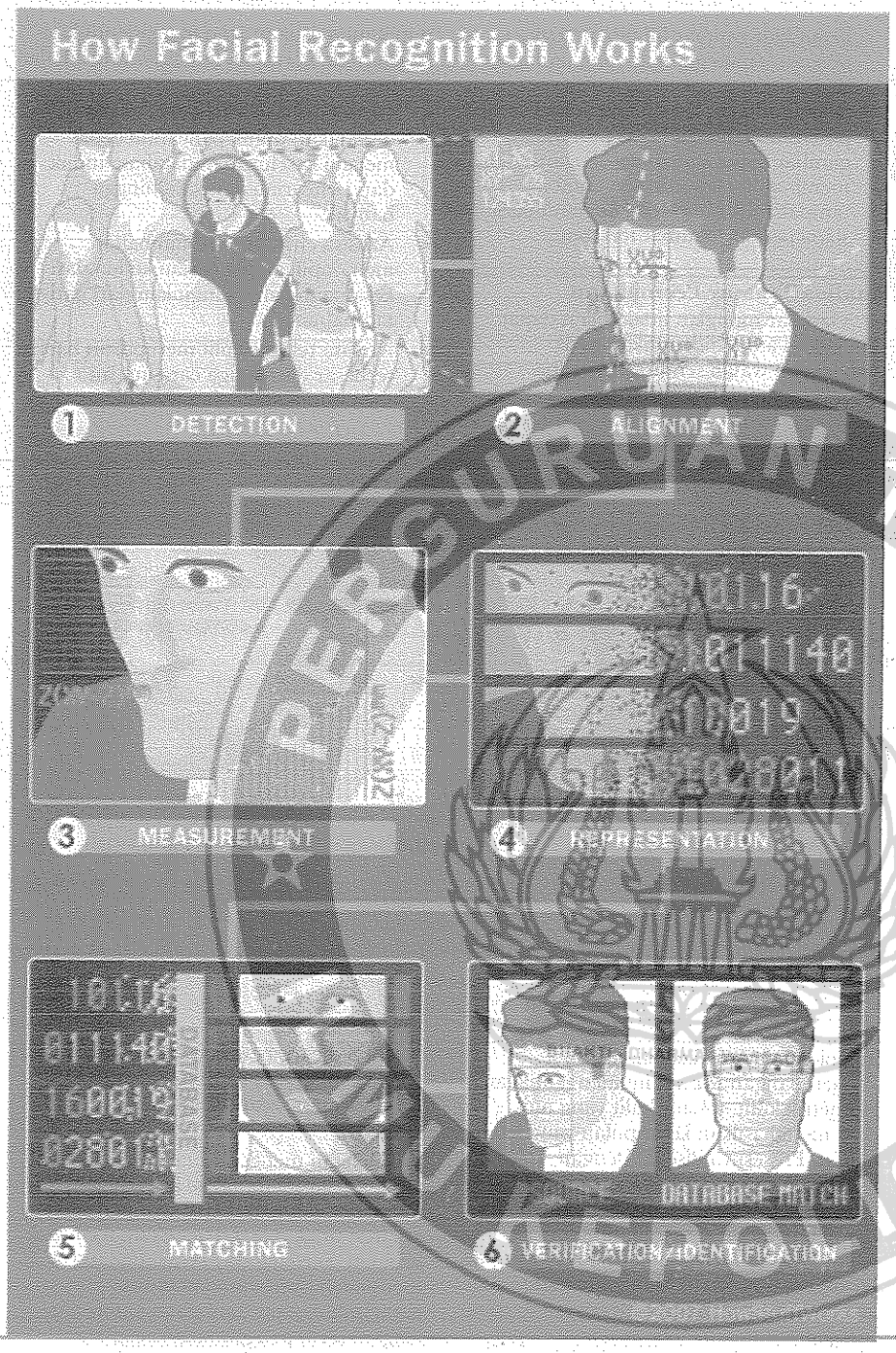
- Garis tambahan sangat kecil dan digunakan untuk pencarian cepat melalui keseluruhan database induk dari pencarian dari satu hingga banyak.
- Analisa ciri-ciri lokal tambahan menampilkan pencarian kedua dari kesamaan yang diinginkan dari garis tambahan.
- Analisa tekstur kulit merupakan bagian terbesar dari ketiga cara ini. Ini menampilkan bagian terakhir setelah LFS dicari, berdasarkan kepada ciri-ciri kulit pada gambar, termasuk informasi secara detail.



Dengan mengombinasikan ketiga hal tadi, *software* mempunyai keuntungan sesuai dengan sistem di mana perubahan ekspresi tidak dapat diacuhkan, termasuk kedipan, kerutan atau senyuman, serta mempunyai kemampuan untuk mengimbangi pertumbuhan kumis dan jenggot serta penggunaan kacamata. Sistem ini dapat digunakan pada keseluruhan ras dan gender.

Bagaimanapun, identifikasi wajah bukanlah sistem yang sempurna. Ada beberapa faktor yang dapat menyulitkan proses identifikasi yaitu:

- Cahaya pantulan dari kacamata atau penggunaan kacamata sinar matahari.
- Rambut panjang yang dapat mengaburkan bentuk pusat wajah.
- Cahaya yang buruk dapat



menyebabkan wajah kelebihan atau kekurangan cahaya.

- Kurangnya resolusi (gambar yang diambil dari jarak terlalu jauh).

Penggunaan di Masa Depan

Pada waktu lalu, pengguna *software* pengenal wajah adalah penegak hukum yang menggunakan sistem ini untuk mengambil gambar secara acak di kerumunan orang. Beberapa perwakilan pemerintah juga menggunakan sistem ini untuk mengurangi kecurangan pemilihan umum. Pemerintah Amerika Serikat telah menggunakan program yang disebut US-VISIT *(United States Visitor and Immigrant Status Indicator Technology)*, kepada para pendatang yang akan memasuki wilayah Amerika Serikat. Ketika pendatang menerima visa, dia akan memasukkan sidik jari dan foto diri. Sidik jari dan foto diri diperiksa kembali apakah mempunyai catatan kriminal atau kemungkinan pelaku teroris. Ketika pendatang asing masuk ke Amerika Serikat melalui gerbang kedatangan, sidik jari dan foto diri yang sama digunakan untuk verifikasi orang yang mempunyai visa dan orang yang memasuki gerbang kedatangan.

Walaupun begitu, banyak situasi yang memungkinkan *software* ini menjadi populer, sebagai sistem yang berbiaya rendah, kegunaannya menjadi lebih luas. Sekarang program ini dapat dikombinasikan dengan kamera dan komputer sehingga dapat digunakan di bank dan bandara. Program ini menyediakan kecepatan pengamanan dalam menyaring penumpang yang informasinya tersedia dan memenuhi penilaian ancaman keamanan. Pada bandara akan terdapat jalur khusus untuk pendaftaran pendatang yang akan melewati atau bergerak dengan cepat, verifikasi orang menggunakan pengidentifikasi wajah mereka. Aplikasi potensial yang lain termasuk ATM dan pengecekan keamanan uang *cash*. *Software* ini dapat dengan cepat memverifikasi wajah pelanggan. Setelah pelanggan menyetujui, mesin ATM atau tempat penarikan uang cash akan mengambil gambar digital pelanggan tersebut. *Software* ini akan menghasilkan cetakan wajah dari foto diri untuk melindungi pelanggan dari pencurian identitas atau penipuan transaksi. Dengan menggunakan *software* pengenalan wajah, tidak diperlukan gambar ID, kartu bank atau nomor identitas personal (PIN) untuk memeriksa identitas pelanggan. Hal ini dapat mencegah kecurangan yang akan terjadi.

Apabila semua contoh tersebut berjalan dengan izin individu, tidak semua sistem akan dipergunakan dengan sepengetahuan anda. Sistem ini mengambil gambar dari semua pengunjung tanpa sepengetahuan dan izin mereka. Kebalikan dari catatan sistem ini apabila pengamanan dilakukan pada sebuah instansi, tidak cukup mengesampingkan perasaan merdeka dan kebebasan. Individu akan merasakan privasi mereka terganggu dengan penggunaan sistem ini dan mereka juga harus memperhitungkan peningkatan risiko pencurian identitas. Ketika perusahaan pembuat pengenal wajah menerima teknologi ini, tingkat kejahatan pencurian identitas dan penipuan pastinya meninggi. (AP/Idr)