

# SISTEM PENGAMANAN MESIN ATM DENGAN MENGGUNAKAN PENGENALAN SIDIK JARI DAN WAJAH *FACE RECOGNITION* UNTUK MEMINIMALISIR *CYBERBANKING CRIME*

Mohamad Arifin  
*Universitas Airlangga*  
mohamad.arifin-2014@fisip.unair.ac.id

## ABSTRACT

Mesin anjungan tunai mandiri (ATM) sangat memudahkan para nasabah perbankan dalam bertransaksi perbankan selama 24 jam tanpa terikat dengan jam operasional kantor bank. Nasabah cukup dengan menggunakan kartu dan memasukkan nomor pin pada mesin, nasabah dapat bertransaksi non tunai dan penarikan uang. Tetapi, kelemahan mesin ATM yang menggunakan kartu sangat rawan peretasan. Biasanya, peretasan data nasabah menggunakan alat skimmer yang terpasang pada slot card mesin. Alat skimmer berfungsi untuk mencuri data nasabah termasuk nomor rekening, jumlah saldo dan nomor PIN yang tersimpan pada pita *electronic magnetic* (berada di bagian belakang kartu). Data nasabah yang terekam dapat digunakan para *hacker* untuk menngandakan kartu nasabah dan mengambil uang nasabah dengan kartu atm duplikat. Tindakan haker tersebut sangat merugikan nasabah. Oleh sebab itu, diperlukan pengamanan mesin ATM yang bersifat biometric atau melekat pada diri manusia yaitu sidik jari dan wajah. Hal tersebut karena bentuk atau pola sidik jari manusia tidak sama antara satu individu dengan lainnya, begitu juga dengan wajah yang memiliki tingkat akurasi yang tinggi. Metode dalam penelitian terbagi dua yaitu pengumpulan data pendukung melalui studi literature tentang topik terkait dan selanjutnya perancangan grafis *prototype* mesin ATM dengan menggunakan pengenalan sidik jari dan wajah. Cara operasional yang dilakukan, nasabah melakukan perekaman sidik jari dan wajah ke kantor bank. Selanjutnya, petugas bank memvalidasi dengan data kependudukan yang memuat informasi *biometrics* nasabah. Jika sudah tervalidasi lalu petugas bank mensinkronisasikan dengan rekening nasabah dan proses selesai. Nasabah dapat bertransaksi pada mesin ATM tanpa menggunakan kartu ATM. Cukup melakukan verifikasi sidik jari dan wajah pada mesin adapun output dari penelitian ini untuk meminimilisir tingkat kejahatan *cyberbanking*.

**Keywords:** Mesin ATM, Sidik Jari, Wajah

*Received 24 February 2021 Accepted 31 January 2022*

## INTRODUCTION

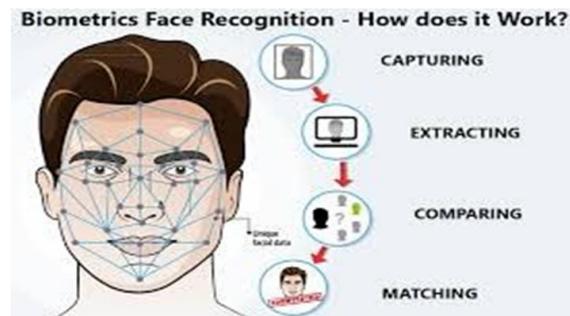
Kejahatan perbankan Indonesia khususnya peretasan kartu ATM (Anjungan Tunai Mandiri) dari tahun ke tahun memiliki tren prevelensi yang cukup tinggi dan diperkuat dengan data persebaran kasus pembobolan ATM dengan modus skimming atau meretas data nasabah melalui alat skimmer yang terpasang pada mesin atm. Jumlah kasus peretasan ATM paling banyak pada bank BCA tahun 2015 dan bank BRI tahun 2016. Pada kasus bank BCA tahun 2015 total korban nasabah adalah 112 rekening [1] sedangkan korban dari kejahatan skimming pada bank BRI tahun 2016 di kantor cabang Mataram provinsi Lombok sebanyak 515 rekening dan mengalami kerugian paling besar sebanyak 2,7 M [2]. Selain itu, juga terjadi kasus skimming pada bank Mandiri pada tahun 2018 yang terjadi di dua tempat sekaligus, yaitu Surabaya dan

Jogja, dengan jumlah korban 141 nasabah. Dari tahun 2011 sampai dengan tahun 2017, kasus skimming terus meningkat. Pada tahun 2015, kasus skimming ATM di Indonesia tercatat sebanyak 1.549 kasus atau 1/3 dari kasus skimming di dunia [3].

Sistem pengamanan berbasis *biometrics* menggunakan sidik jari sangat efektif untuk diterapkan untuk sistem keamanan kendaraan bermotor karena memiliki tingkat akurasi yang sangat tinggi dan tidak mudah dipalsukan karena pola sidik jari tidak memiliki kesamaan atau kemiripan antara individu satu dengan individu lain walaupun kembar identik, dikarenakan pola sidik jari terbentuk saat trimester pertama kehamilan [4]. Selain itu fungsi lain sidik jari dapat diterapkan untuk mesin absensi elektronik menggantikan metode konvensional melalui tanda tangan yang mudah dipalsukan dengan menggunakan sistem absensi menggunakan sidik jari juga memudahkan pihak personalia memantau kedisiplinan dalam hal kehadiran pegawai secara realtime dan memiliki tingkat akurasi sebesar 90 persen yang berguna untuk pertimbangan pemberian *reward* maupun *punishment* bagi pegawai yang bersangkutan [5]. Manfaat lain sidik jari dalam kehidupan dapat dimanfaatkan untuk mendeteksi penyakit kanker payudara dapat dideteksi melalui sidik jari dengan menggunakan analisis pola sudut *ATD phalanx distal* yang ada pada garis tangan manusia. Dengan menunjukkan hasil bahwa sudut *ATD* antara penderita kanker payudara dan non penderita kanker payudara tidak memiliki kecenderungan yang signifikan namun memiliki kecenderungan pola sidik jari yaitu pola *whorl* pada penderita kanker payudara [6].

Selain sidik jari *biometrics* manusia yang dapat diterapkan untuk sistem keamanan dengan memiliki tingkat akurasi yang sangat tinggi yaitu dengan verifikasi wajah atau lebih dikenal dengan istilah *face recognition* yang merupakan sebuah metode analisis wajah berdasarkan karakteristik ukuran kepala, bentuk iris mata, hidung, bibir bentuk rambut yang dipengaruhi unsur *genetics* dan ras karena yang menyebabkan bentuk wajah manusia memiliki karakteristik berbeda antar individu dengan individu yang lain [7] yang telah diterapkan untuk membantu aparat kepolisian dalam mengungkap kasus kriminalitas dengan menggunakan teknologi kamera CCTV *circuit closed television* yang telah diintegrasikan database kependudukan nasional. Dalam sistem kartu penduduk elektronik (E-KTP) telah memuat informasi biologis mulai wajah, kornea mata, dan sidik jari yang memudahkan dalam pengungkapan kasus kriminalitas. Teknologi pengenalan *face recognition* juga diterapkan dalam sistem kunci otomatis *smartphone* karena lebih mengutamakan privasi pengguna akan data data pribadi yang tersimpan pada *smartphone* [8]. Disamping itu sistem keamanan berbasis verifikasi wajah juga dapat diterapkan sistem keamanan ponsel pintar atau *smartphone* berbasis *face recognition* dan untuk keamanan pintu rumah dan kantor untuk mencegah tindakan kriminalitas pencurian dan meminimalisir kunci hilang atau ketinggalan. Dengan menggunakan kamera *webcam* sebagai sensor pendeteksi dan media pengambilan gambar wajah untuk input yang akan diolah menggunakan metode *Grayscale* pada mini PC mendeteksi wajah manusia dan mengambil gambar yang nantinya akan dijadikan sampel untuk pengenalan wajah dan untuk sampel database [9]. Secara umum proses indentifikasi wajah secara umum memiliki *step by step* sebagai berikut:

1. *Capturing* / pengambilan gambar subjek melakukan perekaman wajah menggunakan camera beresolusi tinggi agar mudah untuk dikenali oleh sistem
2. *Extracting* / Pengolahan : wajah yang telah terekam masuk dalam bank data untuk di verifikasi dengan data kependudukan selanjutnya di simpan.
3. *Comparing* / Klasifikasi : proses ini bertujuan untuk memverifikasi apakah adanya kemiripan wajah individu satu dengan individu lain tujuannya untuk
4. *Matching* / Pengenalan : merupakan tahap akhir yaitu proses pengenalan wajah bagi individu yang telah melakukan perekaman akan diterima oleh sistem sebaliknya individu yang belum melakukan perekaman sistem akan ditolak sistem otomatis



Gambar 1. Ilustrasi Proses Identifikasi Menggunakan *Face Recognition*

Metode lain yang akurat untuk pengenalan wajah dengan menggunakan *Histogram Of Oriented Gradient (HOG)* yang dapat melakukan verifikasi wajah. Berdasarkan histogram lokal dari orientasi *gradien* yang diberi bobot dengan *magnitude gradien* [10]. Dari setiap individu yang di jadikan sampel dan hasil pengujian sampel menggunakan metode tersebut menunjukkan tingkat akurasi pengenalan wajah dengan prevelensi keberhasilan tinggi dengan rata-rata akurasi sebesar 80%. Selain metode *Histogram of oriented Gradient* untuk pengenalan wajah ada metode kedua yang serupa yang dikembangkan dengan menggunakan sistem *algoritma* yang lebih berfokus pada estimasi identifikasi ras pada manusia. Dengan cara kerja mengidentifikasi ciri-ciri wajah individu dari berbagai ras yang telah tersimpan sebelumnya dalam database kemudian citra wajah tersebut *diekstrak* menggunakan metode DCT (*Discrete Cosine Transform*) dan diklasifikasikan menggunakan metode *decision tree*. Dari hasil proses tersebut menghasilkan pengelompokan citra wajah berdasarkan klasifikasi ras yang berfungsi sebagai acuan yang akan digunakan untuk memprediksi ras dari individu pada citra wajah masukan sistem output dari sistem ini sangat membantu dalam bidang forensic untuk mengidentifikasi jenazah yang sudah hancur dari korban kecelakaan massal seperti pesawat, kapal,

Fungsi lain pengenalan wajah dapat dimplementasikan sebagai keamanan *folder* yang ada pada komputer atau laptop yang sangat rawan dicuri data data yang bersifat penting dan pribadi oleh orang lain [11]. Terlebih jika komputer kantor yang di gunakan bersama yang memiliki kemungkinan terjadi pembobolan atau peretasan file dan disalahgunakan oleh orang orang tak bertanggung jawab. Hal ini sangat merugikan pemilik asli file tersebut jika data diretas data sangat penting atau *urgent*. Oleh sebab itu perlu di tambahkan fitur keamanan tambahan yaitu biometrik pengenalan wajah dengan alasan karena ciri – ciri fisik wajah manusia memiliki karakteristik yang berbeda – beda yang selalu melekat pada manusia.

## RESEARCH METHODS

Metode yang digunakan dalam penelitian ini dikelompokkan menjadi beberapa komponen antara lain: yang pertama pengumpulan data dengan menggunakan data sekunder yang bersumber dari penelitian terdahulu yang terkait dengan data jumlah kejahatan peretasan data nasabah menjadi korban *debit card fraud crime* pada beberapa bank yang ada di Indonesia. Selanjutnya, dianalisis dengan menggunakan statistik deskriptif pengambilan sampel penelitian ini menggunakan metode *stratified purposive sampling* dengan alasan untuk mengetahui jumlah kerugian yang dialami oleh pihak perbankan yang disebabkan oleh kejahatan *debit fraud crime* yang menggunakan media perantara mesin anjungan tunai mandiri. Kemudian di analisis dengan menggunakan analisis deskriptif dan tahap akhir dilakukan perancangan prototype / rancang bangun *re-design* mesin ATM menggunakan sistem pengenalan sidik jari dan wajah dengan agar memudahkan bagi para pembaca untuk memahami cara kerja sistem operasional mesin ATM dengan menggunakan sidik jari an pengenalan wajah

## FINDINGS AND DISCUSSION

### Jumlah Kasus Peretasan dan kerugian yang dialami perbankan

Tabel 1. Data Kerugian yang Dialami Perbankan akibat Peretasan ATM Periode Tahun 2015–2019

No	Nama Bank	Total Kerugian (IDR)	Lokasi kejadian	Tahun
1	Bank BNI	50.000.000	Bali	2019
2	Bank Central Asia	300.000.000	Jakarta Selatan	2019
3	Bank BRI	145.000.000	Kediri	2018
4	Bank Mandiri	260.000.000	Surabaya	2018
5	Bank Mandiri	260.000.000	Yogyakarta	2018
6	Bank BRI	2.700.000.000.000	Lombok	2016
7	Bank Central Asia	1.250.000.000.000	Jakarta Bandung	2015

Sumber: Admin (2016); Deny (2016); dan Hakim (2016)

Dari data di atas di dapatkan prevelensi kerugian yang *significant* yaitu jumlah kasus paling tinggi pada kisaran tahun 2015-2016 pada bank BRI wilayah Lombok provinsi Nusa Tenggara Barat dengan total kerugian dari peretasan kartu ATM nasabah sebesar IDR 2.700.000.000.000 dan Bank Central Asia wilayah Jakarta dan Bandung sebesar IDR.1.250.000.000.000. Sedangkan prevelensi kasus peretasan ATM nasabah terendah pada tahun 2018-2019 pada peringkat pertama bank BNI wilayah Bali sebesar IDR 50.000.000 kemudian peringkat kedua oleh bank BRI wilayah kediri sebesar IDR 145.000.000 serta peringkat ketiga ada pada mandiri wilayah Yogyakarta dan Surabaya pada tahun 2018 dengan jumlah relatif hampir IDR 260.000.000.

Tabel 2. Data Jumlah Kasus Peretasan kartu ATM Nasabah Berdasarkan Jenis Bank Periode Tahun 2015–2019

No	Nama Bank	Jumlah Kasus	Tahun
1	Bank BCA	115 Rekening Nasabah	2015
2	Bank BRI	515 Rekening Nasabah	2016
3	Bank Mandiri	141 Rekening Nasabah	2018
4	Bank BNI	141 Rekening Nasabah	2019

Sumber: Kompas.com (2019), Supriyatin (2015), dan Yudistira (2018)

Dari pemamparan data di atas pada tahun 2016 merupakan prevelensi kasus peretasan kartu ATM nasabah perbankan yang tertinggi yang ada bank BRI sebagai peringkat pertama dengan jumlah korban sebesar 515 rekening nasabah. Kemudian disusul peringkat kedua bank BCA dengan jumlah 115 rekening nasabah pada tahun 2015. Peringkat ketiga dan keempat ada bank mandiri dan BNI dengan jumlah kasus relatif sama yaitu 141 Rekening nasabah pada tahun 2018 dan 2019.

## Data Pengguna Alat Pembayaran Metode Kartu

Tabel 3. Pengguna APMK

Jenis Kartu	Tahun 2014	Tahun 2015	Tahun 2016	Tahun 2017	Tahun 2018	Tahun 2019
Kartu Kredit	16.043.347	16.863.842	17.406.327	17.244.127	17.275.128	17.487.057
Kartu Debit	7.189.917	7.330.388	8.361.351	8.815.007	8.847.011	8.979.878
Kartu debit + kredit	98.638.287	112.948.818	27.786.999	155.663.442	152.482.094	174.445.472

Sumber: Bank Indonesia (2019a)

Berdasarkan Tabel 3 menunjukkan bahwa secara umum terjadi peningkatan pengguna APMK baik kartu kredit maupun kartu debit. Banyak pengguna yang memiliki kedua kartu yaitu kartu debit dan kartu kredit dibandingkan pengguna yang hanya memiliki salah satu diantara kartu tersebut. Selain itu, bahwa pengguna kartu kredit lebih banyak dibandingkan pengguna kartu debit.

## Keunggulan dan Kelemahan Mesin Atm Sistem Konvensional dan Sistem Pengenalan Sidik Jari dan Wajah

Tabel 4. Perbandingan ATM Konvensional dengan ATM Sidik Jari dan Wajah

No	ATM Konvensional (Kartu)	ATM Sidik Jari dan wajah
1	Tingkat keamanan data nasabah mudah diretas dengan alat skimmer	Keamanan Data Nasabah terjamin tingkat akurasi 99% tidak dapat di salahgunakan
2	Kartu ATM Sering hilang, rusak, Tertelan	Lebih Praktis dalam penggunaan
3	Tidak Semua Mesin ATM Menerima jenis kartu	Mesin ATM semua provider Bank menerima
4	Pengungkapan kasus <i>cyberbanking fraud</i> lebih lambat	Memudahkan aparat kepolisian ungkap kasus perbankan

Selain kelemahan yang di paparkan pada tabel diatas metode konvensional menggunakan kartu atm memiliki kelemahan lain yang ditemukan pada mesin ATM sistem konvensional menggunakan yaitu dapat dilakukan peretasan data nasabah melalui struk ATM. Seringkali nasabah perbankan membuang struk ATM ke tempat sampah di samping mesin tanpa memusnahkan dengan cara menyobek kertas struk hasil penarikan tunai. Padahal di dalam struk ATM tersebut memuat informasi yang sangat penting seperti informasi saldo, tiga digit angka belakang nomor rekening yang dapat di manfaatkan pelaku kejahatan perbankan menguras isi saldo dengan membuat buku rekening palsu dengan cara mencuri data kependudukan melalui data pemilih milik komisi pemilihan umum [12].

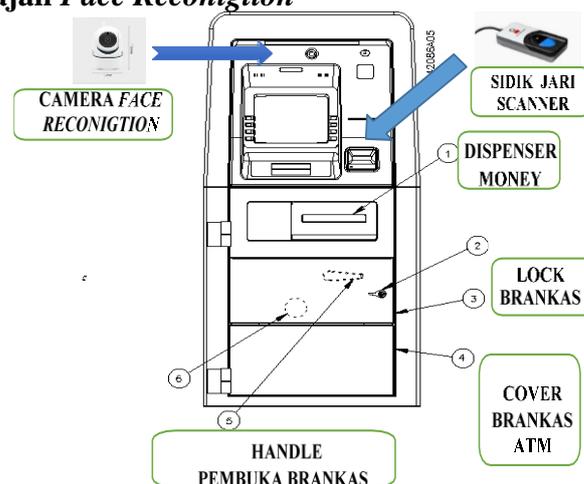
Kelemahan lain yaitu pada kartu ATM yang tersimpan di dalam dompet sangat rawan hilang ataupun *kecopetan*. Proses pengurusan kartu ATM baru memerlukan proses yang tidak mudah yang telah diatur oleh standar operasional prosedur perbankan dalam mekanisme kartu

ATM hilang. Salah satu saratnya adalah surat kehilangan kepolisian, data data kependudukan pendukung dan lain sebagainya. Tidak semua mesin ATM bisa menerima semua kartu ATM yang telah di terbitkan pihak perbankan untuk melakukan transaksi pada mesin. Kalaupun bisa di kenakan biaya tambahan administrasi untuk transaksi kartu ATM yang berbeda. Hal ini sangat merepotkan nasabah dalam bertransaksi karena belum terintegrasinya sistem perbankan [13].

Kelemahan lain yang di timbulkan saat transaksi perbankan menggunakan metode konvensional atau kartu debit dan kredit yaitu sangat rentan peretasan pada saat bertransaksi secara digital melalui situs *e-commerce* [14]. Cara pelaku kejahatan hacker menginput virus *malware* ke dalam situs *e-commerce* dengan tujuan mencuri data nasabah perbankan saat melakukan transaksi pembayaran. Saat memasukkan nomor kartu debit atau kredit dengan cara membaca tiga digit nomor CVV *card verification value* di belakang kartu yang menyimpan data data penting nasabah. Disamping itu, transaksi menggunakan sistem kartu sangat rawan mengalami kerusakan pada pita *magnetic* yang terdapat pada belakang kartu misalnya mengalami goresan, maupun kartu patah dan kemungkinan hilang bersama dompet merupakan beberapa kelemahan bertransaksi menggunakan kartu debit maupun kredit saat ini. Adapun upaya pihak perbankan untuk mengurangi transaksi kartu dengan cara mengalihkan pembayaran menggunakan *mobile banking* dan berkejasama dengan aplikasi fintech untuk pembayaran secara virtual yang lebih aman karena dilengkapi dengan sistem *otentifikasi* transaksi

Kelemahan lain yang di temukan pada mesin ATM sistem konvensional menggunakan kartu dapat dilakukan peretasan data nasabah melalui struk ATM. Seringkali nasabah perbankan membuang struk ATM ke tempat sampah di samping mesin tanpa memusnahkan dengan cara menyobek kertas struk hasil penarikan tunai. Padahal di dalam struk ATM tersebut memuat informasi yang sangat penting seperti informasi saldo, tiga digit angka belakang nomor rekening yang dapat di dimanfaatkan pelaku kejahatan perbankan menguras isi saldo dengan membuat buku rekening palsu dengan cara mencuri data kependudukan melalui data pemilih milik komisi pemilihan umum [15].

### Sistem Operasional Mesin Anjungan Tunai Mandiri dengan Menggunakan Sidik Jari dan Pengenalan Wajah *Face Reconigtion*



Gambar 2. Ilustrasi Prototype Mesin Indetifikasi ATM Sidik jari dan Wajah  
Dari ilustrasi diatas ATM menggunakan pengenalan sidik jari dan wajah memiliki bagian bagian sebagai berikut:

1. *Camera Face recognition*: yang berfungsi mencapture wajah user dan membandingkan dengan database tersimpan pada sistem perbankan yang terkoneksi dengan rekening.

2. Keypad: yang berfungsi untuk memasukan kode personal identification number setelah sistem mengenali wajah dan sidik jari nasabah perbankan
  3. Dispenser uang: yang berfungsi mengeluarkan uang nasabah perbankan jika memilih opsi penarikan tunai
  4. Pemindai sidik jari: yang berfungsi untuk mengenali sidik jari nasabah jika proses pengenalan wajah diterima oleh sistem perbankan
  5. Lock Brankas / Kunci: yang berfungsi untuk mengunci brankas penyimpanan uang.
- Sistem Kerja mesin anjungan tunai mandiri menggunakan sidik jari dan pengenalan wajah di bagi menjadi dua kelompok yang pertama proses perekaman di kantor bank dan yang kedua cara menggunakan mesin ATM setelah selesai melakukan proses perekaman di bank yang akan di jelaskan sebagai berikut:

1. Langkah langkah melakukan perekaman ke kantor bank :
  - a. Nasabah membawa kartu tanda penduduk dan buku rekening tabungan
  - b. Petugas bank menverifikasi data nasabah dan melakukan sinkronisasi kedalam sistem.
  - c. Nasabah dilakukan pengambilan foto menggunakan kamera khusus pendeteksi wajah dan perekaman sidik jari
  - d. Data sidik jari dan wajah yang berhasil terekam di validasi ke sistem E-KTP atau database kependudukan nasional
  - e. Jika proses validasi terdapat kecocokan data, sistem kependudukan nasional mengirimkan notifikasi *approved* ke bank bersangkutan.
  - f. Proses perekaman selesai dan nasabah dapat bertransaksi ke mesin ATM tanpa menggunakan kartu cukup sidik jari dan wajah.
2. Langkah- langkah menggunakan mesin anjungan tunai mandiri :
  - a. Nasabah memasuki bilik ATM dan memilih opsi scan wajah dan sidik jari
  - b. Jika sistem mengenali wajah dan sidik jari mesin meminta memasukan keamanan tambahan yaitu nomor pin. *Personal identification number*
  - c. Setelah proses *completed* sistem memberikan akses ke rekening nasabah
  - d. Nasabah melakukan transaksi di mesin anjungan tunai mandiri
  - e. Jika proses transaksi sudah selesai nasabah menekan tombol *logout* pada mesin. Secara otomatis tampilan berubah ke halaman utama
  - f. Proses transaksi selesai.
3. Fungsi diterapkan mesin anjungan tunai mandiri berbasis pengenalan wajah dan sidik jari :
  - a. Menghindari kartu ATM tertelan dan penyalahgunaan kartu ATM untuk tindak kejahatan penipuan perbankan.
  - b. Memudahkan pelacakan pelaku kejahatan perbankan oleh pihak kepolisian jika terjadi kejahatan cyber karena memuat informasi *biometrics* wajah dan sidik jari
  - c. Memberikan keamanan dan kepraktisan nasabah dalam bertransaksi pada mesin atm.
  - d. Menghindari nasabah mempunyai banyak rekening perbankan dalam satu kartu identitas kependudukan yang berpotensi untuk tindak kejahatan korupsi dengan cara memecah uang kesemua rekening bank.

## CONCLUSION

Pemakainya kartu pada saat bertransaksi menggunakan mesin ATM sangat mempunyai resiko menjadi korban peretasan data nasabah dengan menggunakan alat skimmer. Para hacker mudah dalam membaca data kartu ATM melalui pita magnetic dan chip yang ada di belakang kartu ATM yang berpotensi terkurasnya saldo tabungan. Kekurangan lain kartu ATM mempunyai resiko lain seperti tertelan pada mesin, hilang karena jatuh dan kecopetan, dan rusak karena terendam air dan sebab lain. Kelemahan penggunaan kartu ATM tidak dapat dilakukan untuk bertransaksi di semua mesin ATM merchant atau provider perbankan lain jikalau bisa di kenakan tarif administrasi tertentu saat bertransaksi dengan menggunakan kartu

ATM berbeda.

Sistem pengenalan sidik jari dan wajah atau yang lebih di kenal istilah face reconigition merupakan sistem keamanan dengan akurasi yang tinggi dan tidak dipalsukan. Sidik jari melekat kuat pada ciri biometrik individu yang terbentuk dari trimester pertama kehamilan sampai seumur hidup dengan memiliki karakteristik dan pola yang tetap bisa berubah kecuali adanya trauma atau cedera. Sistem ini telah diterapkan sebelumnya untuk mesin presensi, pengamanan pintu, brankas dan indetifikasi penyakit bawaan dan terbukti significant dalam penerapannya dengan rata rata akurasi mencapai 80-99 %. Oleh sebab itu, sangat relevant untuk pengamanan mesin anjungan tunai mandiri dengan alasan selain memudahkan nasabah atau user dalam bertransaksi di mesin ATM juga melindungi data nasabah dari tindak kejahatan cyberbanking yang sangat merugikan baik dari pihak nasabah maupun pihak institusi perbankan.

## REFERENCES

- [1] D.A. Setiawan, Perkembangan Modus Operandi
- [2] L. Hakim, Kerugian Skimming BRI Rp 2,7 Miliar. <https://radarlombok.co.id/kerugian-skimming-bri-rp-27-miliar.html>, diakses 9 Juni 2019.
- [3] P. Choirina, R.A. Asmara, Deteksi Jenis Kelamin berdasarkan Citra Wajah Jarak Jauh dengan Metode Haar Cascade Classifier, *J. Inform. Polinema*. (2016).
- [4] I.K.S. Widiakumara, I. Putra, Aplikasi Identifikasi Wajah Berbasis Android, *Lontar Komputer*. (2018).
- [5] A.S. Rafika, M. Budiarto, W. Budiarto, Aplikasi Monitoring Sistem Absensi Sidik Jari. (2014) 134–146.
- [6] A. Ightikoma, Variasi Sidik Palmar dan Phalanx Distal pada Penderita Kanker Payudara di Surabaya. (2017).
- [7] M.A. Rahman, I.S. Wasista, M. Kom, L. Belakang, Sistem Pengenalan Wajah Menggunakan Webcam untuk Absensi dengan Metode Template Matching, *Elektronika*. 1–6.
- [8] D.Y. Liliana, M.A. Rahman, Deteksi Wajah Manusia pada Citra Menggunakan Dekomposisi Fourier, *J. Sci. Model. Comput*. (2013) 14.
- [9] G. Ramadhan, E.C. Djamal, T. Darmanto, Klasifikasi Identitas Wajah untuk Otorisasi Menggunakan Deteksi Tepi dan LVQ, *Semin. Nas. Apl. Teknol. Inf*. (2016) 37–41.
- [10] E. Sudarmilah, Pengenalan wajah dengan perbandingan Histogram, *Semin. Nas. Apl. Teknol. Inf*. (2009).
- [11] A. Dewi, B. Hidayat, J. Arif, Identifikasi Ras Manusia Berdasarkan Citra Wajah Berbasis Discrete Wavelet Transform dan Learning Vector Quantization-Neural Networks, *Pros. SENIATI*. (2019).
- [12] W. Firmandani, M. Malik, Kendala Manajemen Risiko Teknologi Informasi pada Kasus Skimming ATM Bank X, *J. ILMU Manaj. DAN BISNIS*. 107–120.
- [13] L.T. Panjaitan, Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik no. 11 Tahun 2008, *J. Telekomun. dan Komput*. 1.
- [14] M.R.H. Rumman, A. Sarker, M.M. Islam, M.I. Hoque, R. Kuri, ATM Shield: Analysis of Multitier Security Issues of ATM in the Context of Bangladesh, *J. Exp. Sci*. (2020) 22–27.
- [15] Y.M. Rihi, A.J. Santoso, I. Wisnubadhra, Menggunakan Verifikasi Sidik Jari Life Fingerprint. (2013) 31–38.