

BAB 1

PENDAHULUAN

I.1 Latar Belakang

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 (Supriatin, 2015), 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 (Hakim, 2016). 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, dan total kerugian sebesar 260 juta (Yudistira, 2018).

Saat ini sistem pengamanan kartu ATM masih menggunakan PIN (*Personal Identification Number*) yang masih banyak kekurangan, antara lain kurang ada privasi. PIN masih di bagikan dengan orang terdekat dalam satu keluarga inti dan masih diretas dengan menggunakan alat skimmer (pemindai kartu). Masalah ini diperkuat dengan data yang menunjukkan banyaknya kasus skimming yang terjadi. 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 (Prayogo, 2018).

Sebagai upaya pencegahan aksi kriminal *cybercrime* ini pihak kepolisian republik Indonesia telah melakukan pertemuan dengan kepolisian Uni Eropa yang mendiskusikan cara pencegahan terhadap skimming. Uni Eropa telah lama menggunakan cip di kartu ATM di negaranya. Ketika seseorang yang berasal dari Uni Eropa keluar dari negaranya, mereka dapat segera lapor kepada pihak bank. Sehingga pihak bank tersebut dapat melakukan pengamanan, dan hal itu pula yang digunakan di beberapa kartu ATM di Indonesia (Admin, 2016).

Penggunaan kartu ATM selain rawan peretasan oleh oknum tak bertanggung jawab dengan memanfaatkan kurang maksimalnya sistem keamanan data konsumen perbankan juga memiliki kekurangan yaitu tertelannya kartu pada mesin. Jika sistem terjadi kendala teknis yang sangat merugikan nasabah ditambah lagi dengan modus pelaku mengganjal slot kartu pada mesin dengan magnet, besi, dan lidi tujuannya untuk membuat kartu “ *macet* “ atau tertahan di dalam mesin, pelaku skimming menyamar seolah-olah menjadi teknisi dari perbankan untuk mengurus saldo rekening nasabah. Modus lain yang digunakan pelaku kejahatan dengan memasang mini camera pada *keypad* mesin ATM untuk mengetahui nomor PIN (*Personal Identification Number*). Kekurangan lainnya, dengan menggunakan sistem kartu mudah hilang bersama dompet misalnya terjatuh, kecopetan. Selai itu, memerlukan waktu untuk proses pergantian dengan kartu yang baru.

Menurut Meliana dan Hartono (2019), cara peretasan data pengguna atau nasabah yang menggunakan internet banking dan layanan mesin anjungan tunai mandiri dalam bertransaksi, dengan menggunakan teknik *phishing* yang berfungsi menyusup ke dalam jaringan atau system perbankan dengan cara memotong jalur data kemudian mengganti data serta menggunakan untuk menguras saldo tabungan nasabah. Teknik ini juga dapat digunakan untuk peretasan internet banking dengan cara mengirim *malware* yaitu dengan mengirimkan virus komputer pada saat korban akses internet banking sehingga pelaku kejahatan mudah untuk *menguras* isi rekening korban. Adapun cara *preventif* untuk meminimalisir peretasan data nasabah perbankan melalui internet banking yaitu dengan tips secara berkala mengganti nomor pin *personal identification number* pada *account internet banking*, dan menghindari penggunaan *wifi public* untuk meminimalisir peretasan data nasabah perbankan melalui internet banking (Sulisrudatin, 2018) Adapun ciri - ciri nasabah perbankan yang menjadi korban tindak kejahatan *fraud* atau peretasan rekening perbankan pertama yaitu terjadinya permohonan kredit dalam jumlah yang tidak biasa. Kedua, terjadi perubahan pada akun laporan keuangan yang tidak wajar seperti asset yang terlalu besar atau beban yang terlalu kecil ketiga data nasabah yang berubah, tidak konsisten, tampak seperti dimanipulasi. Ketiga, identitas peretas atau pelaku tidak jelas dan ada riwayat atau catatan dari *BI checking* dan tanda tangan nasabah yang tidak konsisten dan nasabah sulit untuk dihubungi. Keempat sistem perbankan yang tidak terpakai sebelumnya dan digunakan kembali untuk alasan tertentu dan kelima, nasabah tidak dapat memberikan jawaban seperti pada data perbankan.

Cara pihak perbankan untuk menghindari tindak kejahatan *fraud* pada nasabah dengan cara sosialisasi agar para nasabah lebih berhati-hati saat menggunakan mesin anjungan tunai mandiri dan mesin EDC (*Elektronik Debit Card*). Upaya tersebut dilakukan agar tidak sembarangan membuang struk transaksi kartu kredit/debit yang telah digunakan, karena dari struk transaksi kartu kredit/debit terdapat data-data yang dapat dilacak untuk digunakan dalam tindak pidana pencurian dana. Selain itu, pengembangan pengetahuan untuk para masyarakat umum terkait dengan jenis-jenis kejahatan perbankan dan modus operandi pelaku kejahatan *skimming* tersebut (Hendarsyah, 2020) untuk meminimalisir atau pencegahan kasus peretasan pada kartu ATM dan kartu kredit. Maka dari itu diperlukan sistem keamanan yang berorientasi *private security sistem* dengan menggunakan sidik jari karena pada prinsipnya pola sidik jari mempunyai karakteristik yang berbeda antar individu walaupun kembar identik sekalipun dan polanya permanen kecuali ada beberapa sebab yang menyebabkan pola tersebut hilang salah satunya luka bakar serius, dan *trauma* (luka) karena kecelakaan yang berpotensi menimbulkan perubahan pola pada sidik jari (Hendarko et al., 2011).

Selain itu fungsi sidik jari memiliki dapat juga diimplementasikan untuk proses penyelidikan kejahatan misalnya kasus: pembunuhan, pencurian dengan cara mengambil sidik jari. Yang tertinggal di barang bukti kemudian di analisis dengan cara membandingkan dengan sistem kependudukan yang telah menggunakan kartu tanda penduduk elektronik untuk memudahkan mencari identitas pelaku kejahatan di samping penyidik dari kepolisian dengan mengumpulkan barang bukti tambahan pendukung untuk melengkapi proses

penyelidikan lebih lanjut dengan tujuan untuk mencari pelaku kejahatan yang di maksud (Yuserlina, 2017).

Selain membantu kepolisian untuk pengungkapan pelaku kejahatan fungsi sidik jari dapat diterapkan berbagai macam keperluan untuk membantu manusia salah satunya dengan cara diterapkan dengan mesin absensi untuk pegawai yang outputnya sebagai indikator untuk menilai kedisiplinan karyawan atau pegawai sekaligus meminimalisir kecurangan *user* misalnya *titip absen* jika di terapkan sistem absensi (Jusuf et al., 2013).

Fungsi sidik jari juga bermanfaat dalam bidang medis yang salah satunya untuk mengetahui kelainan kecacatan mental bawaan atau dikenal dengan istilah *down syndrome*. Cara mengetahui *down syndrome* menggunakan sidik jari yaitu dengan membandingkan pola sulur sidik jari pada individu normal dengan individu yang mengalami kecacatan bawaan *down syndrome*. Penelitian terdahulu menunjukkan hasil bahwa prevelensi tertinggi pola sidik jari pada penderita *down syndrome* adalah *loop ulna* (63,4%), sedangkan pada individu normal adalah *whorl* (37,1%). Selain itu, terdapat perbedaan rerata yang bermakna dari distribusi pola *loop ulna* ($p=0,000$), *whorl* ($p=0,001$) dan *arch* ($p=0,000$), sedangkan untuk *loop radial* ($p=0,691$) tidak menunjukkan perbedaan (Rujito et al., 2010) .

I.2 Rumusan Masalah

1. Apa keunggulan dan kelemahan mesin anjungan tunai mandiri dengan sistem konvensional menggunakan kartu dengan sistem menggunakan pengenalan sidik jari dan pengenalan wajah?

2. Bagaimanakah proses sistem operasional mesin anjungan tunai mandiri menggunakan sistem sidik jari dan pengenalan wajah?

I.3 Tujuan Penelitian

Penelitian bertujuan untuk memberikan inovasi dalam bidang perbankan untuk meminimalisir kejahatan peretasan atau pembobolan kartu ATM nasabah dengan menggunakan sistem indentifikasi sidik jari dalam melakukan transaksi pada mesin anjungan tunai mandiri

I.4 Manfaat Penelitian

1. Untuk meminimalisir tingkat kejahatan *cyber banking* dan melindungi data nasabah yang menggunakan mesin anjungan tunai mandiri untuk bertransaksi perbankan
2. Untuk meminimalisir kejadian kartu ATM nasabah tertelan pada mesin anjungan tunai mandiri
3. Sebagai acuan referensi penelitian selanjutnya yang terkait sistem keamanan menggunakan sidik jari dan pengenalan wajah.

I.5 Tinjauan Pustaka

I.5.1 Sidik Jari

Sidik jari, dalam bahasa inggri disebut *fingerprint* dalam istilah medis disebut *dermatoligfi* yang mempunyai ciri ciri khusus yaitu memiliki garis-garis horizontal dan vertical atau gabungan dan ada juga memiliki jenis memiliki

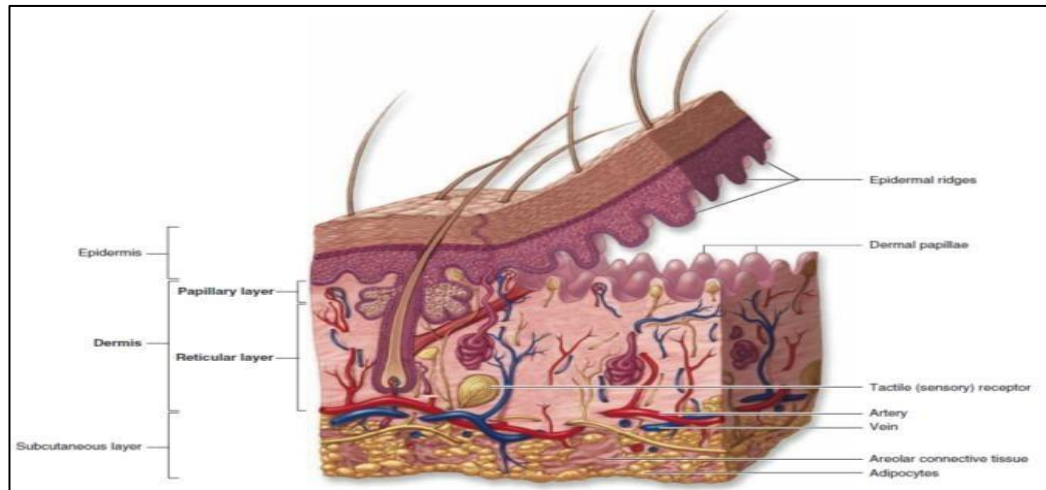
bentuk lengkungan-lengkungan. Karakteristik sidik jari pada manusia memiliki sifat yang permanen yang dapat berubah seumur hidup, kecuali terjadi luka bakar atau luka trauma yang menyebabkan perubahan pola sidik jari (Utomo, 2013). Seiring perkembangan zaman sidik jari di terapkan sebagai alat indentifikasi melalui sistem kartu tanda penduduk elektronik yang berfungsi sebagai database kependudukan dan memudahkan pihak kepolisian melakukan pelacakan pelaku kejahatan dan korban meninggal yang di tak di kenal atau yang di sebut *mr.x* dengan menggunakan sidik jari korban terkoneksi data kependudukan (Santi, 2008). Adapun cara teknik analisis mengidentifikasi pada pola-pola garis sidik jari individu melalui *garis papiler* yang secara genetik permanen melekat pada individu (Fikri, 2010)

Sidik jari dalam bahasa Yunani sering di sebut istilah “*daktilos*” yang artinya jari jemari dan istilah *scopeen* memiliki arti mengamati atau meneliti. Oleh karena itu, istilah *daktiloskopi* bisa didefinisikan sebagai proses mengamati sidik jari khususnya karakteristik pola pola sidik jari yang terdapat pada ujung jari yang berfungsi untuk keperluan pengenalan kembali identifikasi individu. Pola sidik jari manusia tidak pernah berubah dari mulai lahir sampai mati kecuali adanya luka *trauma* berat (Prasasti et. al, 2020).

Champod (2016) menjelaskan bahwa Kulit manusia terdiri dari beberapa lapisan lapisan kulit yang yang terbagi menjadi dua lapisan yaitu yaitu *epidermis* dan *dermis*. Jika di perinci lebih lanjut, lapisan *epidermis* (lapisan luar) memiliki lima lapisan antara lain :

- a. *Stratum germinativum* (lapisan basal),

- b. *Stratum spinosum* (lapisan Spinous),
- c. *Stratum granulosum* (lapisan granular),
- d. *Stratum lucidum*, dan
- e. *Stratum corneum* (lapisan tanduk)



Gambar 1.1 Anatomi Kulit (Mescher, 2016)

Susunan anatomis lapisan epidermis berdasarkan Gambar 1.1 merupakan cikal bakal terbentuknya pola pola sidik jari pada individu di karenakan pada lapisan epidermis terdapat bentukan dasar dari sel *keratinosit*. Lapisan dermis memiliki tingkat ketebalan sebesar 15-40 kali dibandingkan lapisan epidermis sebesar yang terdapat 15-20. Oleh sebab itu lapisan epidermis memiliki peranan menghasilkan lekukan di telapak tangan yang bersifat permanen dan menjadi acuan terbentuknya sel-sel baru. Kecuali bila terdapat kerusakan pada lapisan basal akan membentuk bekas luka yang permanen pada epidermis (Saliyah, 2018).

Proses pembentukan struktur pola sidik jari manusia terbentuk pada trimester pertama kehamilan. Pembentukan struktur pola sidik jari dimulai dengan proses pertumbuhan bantalan pada telapak tangan dan terus berkembang

membentuk lapisan *basal*. Lapisan *Basal* merupakan lapisan utama untuk tumbuhnya lekukan sidik jari dermatoligfi dipermukaan epidermal, dalam istilah medis sering disebut *Primary Dermal Ridge* (Abraham et al., 2013).

Ditinjau dari aspek historis, sidik jari mempunyai tahapan perkembangan berdasarkan hasil penelitian para ahli. Adapun perkembangannya, pada tahun 1684, Dr. Nehemiah Grew (1641-1712) mempresentasikan “*Sidik Jari, Telapak Tangan dan Telapak Kaki Sebuah Pengantar Dermatoglyphics*” kepada Royal Society. Pada tahun 1685, Dr. Bidloo menerbitkan atlas anatomi, *Anatomia Humani Corporis*, dengan ilustrasi yang menunjukkan sosok manusia baik dalam sikap hidup maupun sebagai mayat yang dibedah. Pada tahun 1686, Dr. Marcello Malpighi (1628-1694) mencatat dalam risalahnya, ridges, spiral dan loop pada sidik jari. Pada tahun 1788, JC Mayer adalah orang pertama yang menulis prinsip dasar analisis sidik jari dan berteori bahwa sidik jari itu unik. Pada tahun 1823, Dr. Jan Purkinje mengklasifikasikan garis papiler pada ujung jari menjadi sembilan jenis: lengkung, lengkung tenda, lingkaran ulna, simpul radial, mata merak/majemuk, lingkaran spiral, lingkaran elips, lingkaran melingkar, dan lingkaran ganda/ komposit. Pada tahun 1823, Joannes Evangelista Purkinji menemukan bahwa pola-pola pada ujung jari seseorang dan punggungan serta garis-garis pada cetakan seseorang mulai terbentuk pada sekitar minggu ketiga belas di dalam rahim.

Pada tahun 1832, Dr. Charles Bell (1774-1842) adalah salah satu dokter pertama yang menggabungkan studi ilmiah tentang anatomi saraf dengan praktik klinis. Ia menerbitkan *The Hand: Its Mechanism and Vital*

Endowments sebagai Evincing Design. Pada tahun 1893, Dr. Francis Galton menerbitkan bukunya, "Fingerprints", menetapkan individualitas dan keabadian sidik jari. Buku tersebut memasukkan sistem klasifikasi pertama untuk sidik jari: Arch, Loop dan Whorl. Pada tahun 1897, Harris Hawthorne Wilder adalah orang Amerika pertama yang belajar Dermatoglyphics. Dia menemukan Indeks Garis Utama, mempelajari eminensi hipotenar tenar, zona II, III, IV. Pada tahun 1926, Dr. Harold Cummins & Dr. Charles Midlo menciptakan istilah "Dermatoglyphics". Mereka menunjukkan bahwa tangan mengandung konfigurasi Dermatoglyphics yang signifikan yang akan membantu identifikasi mongolisme pada anak yang baru lahir.

Pada tahun 1936, Dr. Harold Cummins & Dr. Charles Midlo juga meneliti embrio- genesis pola tonjolan kulit dan menetapkan bahwa pola sidik jari benar-benar berkembang di dalam rahim dan sepenuhnya terbentuk pada bulan keempat janin. Pada tahun 1944, Dr Julius Spier Psiko- Analitik Chirologist menerbitkan "Tangan Anak-anak" ia membuat beberapa penemuan penting terutama di bidang perkembangan psiko-seksual dan diagnosis ketidakseimbangan dan masalah di area tangan ini. Tahun 1957, Dr. Walker menggunakan konfigurasi kulit dalam diagnosis mongolisme. Pada tahun 1968, Sarah Holt, yang karyanya berjudul *'The Genetics of Dermal Ridges'* yang diterbitkan pada tahun 1968, merangkum penelitiannya tentang pola dermatoglyphics pada jari dan telapak tangan pada berbagai orang, baik penderita normal maupun bawaan.

Pada tahun 1969, John J. Mulvihill, MD dan David W. Smith, MD menerbitkan *The Genesis of Dermatoglyphics* yang memberikan versi paling

mutakhir tentang bagaimana sidik jari terbentuk. Tahun 1970, Uni Soviet, Bekas Uni Soviet. Menggunakan Dermatoglyphics dalam memilih kontestan untuk Olimpiade. Tahun 1976, Schaumann dan Alter's 'Dermatoglyphics in Medical Disorders' diterbitkan. Investigasi yang signifikan juga telah dilakukan terhadap indikator dermatoglyphics penyakit jantung bawaan, leukemia, kanker, embriopati rubella, penyakit Alzheimer, skizofrenia dll. Penelitian dermatoglyphics diarahkan ke penelitian genetik dan diagnosis cacat kromosom. Pada tahun 1980, Cina melakukan penelitian tentang potensi manusia, kecerdasan dan bakat dalam perspektif dermatoglyphics dan genom manusia.

Pada tahun 1985, Dr. Chen Yi Mou Phd. dari Havard University meneliti Dermatoglyphics berdasarkan teori Multiple Intelligence dari Dr. Howard Gardner. Pertama, terapkan dermatoglyphics ke bidang pendidikan dan fisiologi otak. Tahun 2000, Dr Stowens, Kepala Patologi di rumah sakit St Luke di New York, mengklaim dapat mendiagnosis skizofrenia dan leukemia dengan akurasi hingga 90%. Di Jerman, Dr Alexander Rodewald melaporkan bahwa dia dapat menemukan banyak kelainan bawaan dengan akurasi 90%. Tahun 2004, IBMBS-International Behavioral & Medical Biometrics Society. Lebih dari 7000 laporan dan tesis diterbitkan. Saat ini AS, Jepang, atau China, Taiwan menerapkan dermatoglyphics ke bidang pendidikan, dengan harapan dapat meningkatkan kualitas pengajaran dan meningkatkan efisiensi belajar dengan mengetahui berbagai gaya belajar.

Menurut Saliyah (2018) pola sidik jari di klasifikasikan menjadi beberapa kelompok antara lain :

- 1) Sidik jari laten (*Latent Impression/ Laten Prints*) yaitu sidik jari laten yaitu jenis yang tidak dapat dilihat langsung, harus menggunakan alat bantu atau melalui beberapa cara pengambilan terlebih dahulu agar pola nampak jelas. Jejak sidik jari yang membekas pada suatu permukaan yang tersentuh jari akan mengeluarkan zat sekresi yang dihasilkan oleh keringat. Jejak sidik jari tersebut dibuat lebih jelas terlebih dahulu dengan zat kimia yang bereaksi dengan zat sekresi sehingga akan tampak lebih jelas. Menurut Utomo, (2016) menyatakan bahwa sidik jari latent memiliki usia yang di pengaruhi oleh beberapa faktor yang mempengaruhi antara lain intensitas keringat yang di hasilkan. Semakin banyak banyak keringat semakin lama usia sidik jari kedua faktor di dalam dan luar ruangan sidik jari berasal. Sidik jari *latent* di dalam ruangan memiliki usia jauh lebih lama daripada di luar ruangan. Jenis permukaan benda sidik jari *latent* tertinggal. Di permukaan benda yang dapat menyerap usia sidik jari latent memiliki usia lebih lama daripada benda yang tidak bisa menyerap. Selain itu komposisi pembentuk sidik jari latent terdiri atas keringat dengan komposisi air 98,5% - 99,5 % dan zat padat (garam urea /asam amino 0.5 -1.5%) serta lemak kelenjar (0,5 % - 1,5%)
- 2) Sidik jari paten (*Visible Impression / Patent Prints*) yaitu sidik jari yang dapat langsung dilihat tanpa menggunakan alat bantu, pengambilan sidik jari dengan menggunakan foto.
- 3) Sidik jari plastik (*Plastic Impression / Plastic prints*) yaitu sidik jari yang berbekas pada benda yang lunak seperti sabun, minyak gemuk (oli), lilin, permen coklat. Jejak sidik jari ini bersifat mekanik, misalnya jika tangan

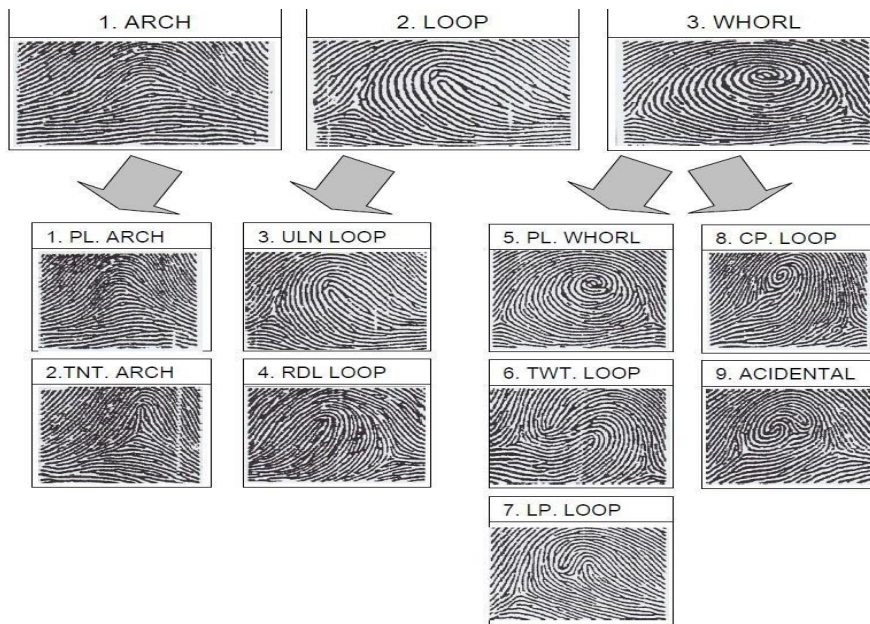
memegang bahan yang sejenis lilin yang lunak, tekanan mekanik jari-jari kita bisa meninggalkan jejak

Setelah mengetahui kategori sidik jari kelompok dan jenisnya selanjutnya mengenali pola pola sidik di karenakan setiap jenis sidik jari memiliki pola yang tidak sama menurut (Mabes polri (departemen pertahanan markas besar kepolisian republik indonesia) 2000) klasifikasi pola sidik jari sebagai berikut :

- 1) *Arch* (busur panah): mempunyai ciri khas tidak ditemukan *delta* dan *core*.
 - a. *Plain Arch* : bentuk pokok lukisan saja, garis-garisnya datang satu sisi lukisan, mengalir ke arah sisi yang lain dengan sedikit menggelombang naik ke tengah seperti busur
 - b. *Tented Arch* : bentuk pokok lukisan sidik jari garis- garisnya datang dari sisi lukisan yg satu ke arah yang lain, membentuk sudut siku- siku di tengah. Satu garis atau lebih berdiri tegak di tengah.
- 2) *Loop*: mempunyai ciri khas mempunyai 1 *delta*, mempunyai *core*, mempunyai hitungan garis minimal satu garis, mempunyai garis melengkung yang cukup.
 - a. *Ulnar Loop (left loop)* : bentuk lukisan sidik jari, satu garis atau lebih datang dari salah satu sisi lukisan itu, melengkung atau menyentuh dan melintasi suatu garis bayangan yang ditarik antara *delta* dan *core* dan berhenti atau cenderung berhenti ke arah sisi semula.
 - b. *Radial Loop (right loop)* : bentuk pokok lukisan loop jika jari kanan posisi *delta* ada di kanan, jika jari kiri delta ada di kiri.
- 3) *Whorl*: mempunyai ciri khas 2 *delta*, bila ditarik suatu garis bayangan dari kedua *delta*, minimal ada satu garis melingkar membentuk suatu bulatan oval,

spiral, berjalan di depan kedua *delta*.

- a. *Plain Whorl* (lingkaran): bentuk pokok lukisan sidik jari yg mempunyai dua buah *delta* di sebelah kanan dan kiri.
- b. *Twinted Loop (double loop / sangkutan kembar)* : bentuk pokok lukisan sidik jari yang terdiri dari dua buah loop dengan besar yang hampir sama, yang terpisah dan masing-masing mempunyai bahu loop sendiri serta mempunyai dua *delta*
- c. *Lateral Pocket Loop (saku sisi)* : bentuk pokok lukisan sidik jari yang terdiri dari dua buah loop yang tidak sama besar terpisah dan masing-masing mempunyai bahu loop sendiri serta mempunyai dua *delta*
- d. *Central Pocket Loop (saku tengah)*: bentuk pokok lukisan sidik jari yang mempunyai dua *delta*, loop yang terdalam mempunyai garis melingkar.
- e. *Accidental* (lukisan istimewa) : bentuk pokok lukisan sidik jari yang mempunyai dua campuran dari bentuk pokok sidik jari dan mempunyai dua *delta* atau lebih.



Gambar 1.2 Macam Macam Pola Lukisan Sidik Jari (Mabes, 2000)

I.5.2 Mesin *Skimmer* (Pemindai Data)

Mesin *skimmer* merupakan alat pemindai kartu ATM yang di letakan pada *slot card* pada mesin anjungan tunai mandiri. Mesin *skimmer* memiliki cara kerja menggandakan informasi data nasabah yang terdapat dalam pita magnetik (*magnetic stripe*) yang ada di bagian belakang pada kartu kredit maupun ATM/debit yang berisi informasi penting misalnya jumlah saldo, informasi pin, dan informasi data pribadi nasabah. Selanjutnya data yang tersimpan pada memori *card reader* alat *skimmer* di transfer data ke kartu credit maupun debit kosongan untuk di gunakan pelaku kejahatan untuk menguras isi saldo rekening korban melalui mesin ATM.



Gambar 1.3 Alat *Skimmer* yang di Gunakan Peretasan Kartu ATM

Selain peretasan dengan menggunakan alat *skimmer* ada beberapa modus lain yang di lakukan pelaku untuk melakukan pembobolan ATM yang pernah terjadi di Indonesia. Modus pertama adalah dengan menggunakan *card rider anti vandal* (tempat memasukkan kartu ATM pada mesin). Cara operasional yang dilakukan dengan menempelkan plastik mika bening di belakangnya dan mengelemnya supaya tidak lepas. Setelah itu, pelaku memasang kembali ke *slot card* pada mesin ATM. Kemudian pelaku melakukan observasi ke calon korban yang masuk ke ruang ATM. Jika melihat korban paknik karena kartu tidak bisa keluar karena terganjal mika. Pelaku berpura pura menyamar sebagai petugas perbankan dengan meminta nomor PIN (*Personal Indetification Number*) dengan alasan membantu korban mengeluarkan kartu padahal telah mengganti kartu ATM palsu (kosong). ATM yang di serahkan ke korban dan kartu asli tetap di dalam ATM seteleh korban meninggalkan ruang ATM baru pelaku mengambil kartu asli milik korban dengan plat besi dan kemudian di cek data pribadi dengan menggunakan mesin skimmer untuk di gandakan (Setiawan, 2019)



Gambar 1.4 Alat *skimmer* yang di gunakan peretasan kartu kredit (Maulana, 2014)

Cara peretasan kartu kredit tidak jauh berbeda dari peretasan kartu ATM. Perbedaannya terletak pada alat yang terpasang di sistem ATM alat skimmer berupa slot yang terpasang pada *card slot ATM* sedangkan pada kartu kredit menggunakan skimmer gesek dengan cara menggesekan kartu kredit nasabah secara diam diam ke mesin skimmer. Sebelum digesekan pada mesin pembayaran resmi yang biasa di sebut EDC (*Electronic Debit Card*) yang disediakan vendor resmi perusahaan penyedia kartu kredit dengan tujuan mengcopy data nasabah kemudian di transfer ke kartu kredit kosong. Selanjutnya kartu kredit di gunakan pelaku untuk bertransaksi dengan user milik korban dan korban baru menyadari setelah tanggal jatuh tempo. Terjadi kenaikan tagihan kartu kredit tanpa merasa transaksi di merchant –merchant yang di lampirkan pada surat tagihan tagihan. Dalam upaya preventif pencegahan yang di lakukan di Indonesia masih sangat minim. Hal ini terbukti dalam setiap transaksi merchant hanya meminta tanda tangan konsumen tanpa di sertai nomor PIN (*Personal Identification Number*) tanpa mengkonfirmasi pemegang kartu pengguna asli atau bukan. Hal ini merupakan peluang bagi pelaku kejahatan *digital banking crime* untuk melakukan

aksinya jika di bandingkan dengan negara negara Eropa dan Amerika dalam perlindungan data nasabah sangat ketat untuk menjamin *security* nasabah dalam bertransaksi. Salah satu upaya pencegahan dengan mencocokkan data kartu kredit dengan identitas yang tertera *resident permit card* atau ktp saat melakukan setiap transaksi dengan demikian tingkat peretasan negara tersebut dapat di minimalisir (Putri, 2017).

Sulisrudatin (2018) mengemukakan dalam artikelnya bahwa kejahatan cyber banking berkaitan dengan perkembangan masyarakat. Semakin maju kehidupan masyarakat, maka kejahatan juga ikut semakin maju serta beraneka ragam modus operasinya khususnya kasus- kasus kejahatan perbankan. Bank Indonesia telah mengidentifikasi dengan mengelompokkan menjadi tiga modus kejahatan perbankan yang paling marak pertama kejahatan perbankan yang berbasis teknologi informasi misalnya peretasan web mobile banking, internet banking, pasar valuta asing. Kejahatan pembobolan data nasabah menggunakan media mesin anjungan tunai mandiri dengan metode *skimming*, *phishing*, dan *malware* yang di gunakan untuk mencuri dana nasabah bank melalui penggandaan kartu ATM. Caranya menggunakan teknologi komputer dan bantuan beberapa software khusus untuk memanipulasi data dengan cara memindahkan data elektronik yang terdapat pada kartu ATM korbannya ke kartu ATM milik pelaku dengan bantuan program komputer.

Untuk memudahkan pemahaman mengenai proses peretasan data nasabah pengguna mesin ATM seperti grafis seperti di tampilkan pada Gambar 1.5.



Gambar 1.5 Grafis Cara kerja peretasan kartu ATM nasabah

Dari ilustrasi di atas dapat dijelaskan bahwa pelaku kejahatan peretasan data nasabah perbankan yang menggunakan mesin anjungan tunai mandiri memiliki langkah langkah sebagai berikut :

1. Pelaku memasang kamera mini yang tak terlihat nasabah di bagian atas keypad mesin ATM dengan tujuan untuk merekam nomor pin (*personal indetification number*) nasabah saat bertransaksi pada mesin
2. Pelaku memasang alat penganda data nasabah atau *skimmer* pada slot card mesin ATM dengan tujuan untuk membaca data data penting nasabah yang tersimpan pada biometrik kartu ATM saat nasabah memasukan kartu ATM ke *slot card* yang kemudian data yang tersimpan di transfer ke kartu ATM kosong yang selanjutnya di gunakan mengurus saldo rekening korban.
3. Pelaku juga memasang *keypad skimmer* diatas keypad asli mesin ATM dengan tujuan mengetahui nomor pin dengan menggunakan *keypad* tiruan

yang ditempel yang berfungsi merekam nomor yang ditekan. Secara tak kasat mata, perangkat ini mungkin sulit dibedakan yang tiruan dengan asli karena bentuknya sangat mirip. Seiring perkembangan zaman teknologi yang di pakai pelaku peretasan semakin canggih dengan menggunakan teknologi *bluetooth* untuk mempermudah. Pelaku tidak perlu lagi segera kembali ke mesin ATM untuk mengambil perangkat dan mengakses data secara manual. Bentuk perangkatnya juga semakin tipis, ringkas, dan sulit dideteksi. Perangkat-perangkat ini ternyata mudah didapatkan para pelaku karena dijual bebas di internet (Republika, 2018).

Menurut Nunuk (2018) dalam penelitiannya yang berjudul “ *Analisa Kasus Cybercrime Bidang Perbankan Berupa Modus Pencurian Data Kartu Kredit* “ menyebutkan bahwa kejahatan *cybercrime* yang di kategorikan berdasarkan jenis aktivitasnya di definisikan sebagai suatu cara yang di lakukan *hacker* meretas sistem keamanan baik situs, *software* dan jaringan yang di kategorikan menjadi beberapa kelompok antara lain:

1. *Carding* : merupakan sebuah proses peretasan nomor dan identitas kartu kredit orang lain, yang datanya dengan mencuri data di internet dengan memanfaatkan keamanan website vendor penyedia kartu kredit untuk di gandakan dan di pergunakan pelaku untuk berbelanja secar *daring* istilah pelaku disebut “*carder*”. Dan sebutan lain yaitu *cyberfroud* atau penipuan di dunia maya.
2. *Hacking* adalah : adalah cara untuk untuk memasuki sistem keamanan website tujuan dengan cara membaca kelemahan yang ada dalam website

dengan tujuan umum untuk mengetahui kode keamanan atau yang di kenal sebuah *password* setelah mengetahui kode pengaman pihak *hacker* atau peretas mengambil dokumen rahasia milik institusi atau lembaga untuk di salahgunakan untuk berbagai hal yang menjadi tujuan khusus metode

3. *Defacing* yaitu sebuah proses mengubah situs website milik orang lain atau lembaga tanpa seizin pihak yang bersangkutan yang tujuannya untuk di perjual belikan ke pihak ketiga secara illegal , untuk kepetingan pribadi
5. *Phising* sebuah kegiatan yang termasuk kategori penipuan online dengan cara membujuk pemakai pengguna internet banking untuk menyebutkan *username* dan *password* dalam modusnya pelaku berpura pura menjadi sebagai pegawai bank yang memberitahukan bahwa akun korban terjadi masalah perlu di perbaiki dengan meminta *password* internet banking yang di miliki korban, setelah mengetahui password dan username sasaran pelaku segera mengganti dengan password baru dan di gunakan berbelanja secara daring dengan pembayaran menggunakan internet banking milik korban.

I.5.3 Kartu ATM / *Debet*

Menurut Bank Indonesia (2013) kartu ATM atau debet di definisikan sebagai alat pembayaran dan penarikan dana dengan menggunakan kartu sekaligus sebagai alat untuk transaksi perbankan melalui mesin anjungan tunai mandiri yang telah di sediakan tujuan di terbitkan. Kartu ATM berfungsi untuk memudahkan nasabah bertransaksi secara mandiri kapan saja tanpa terikat waktu dan jam operasional kantor layanan. Di samping itu, pengguna atau pemakai kartu

ATM juga mendapat beragam manfaat atau keuntungan menggunakan mesin ATM antara lain:

1. Memberikan kemudahan dan kecepatan bertransaksi via ATM untuk penarikan tunai, transfer antar rekening baik sesama maupun antarbank. Serta memudahkan transaksi non tunai lainnya
2. Memberikan kemudahan nasabah pemegang kartu debit untuk melakukan transaksi berbelanja tanpa perlu membawa uang tunai.

Yudianto dan Rivai (2018) menjelaskan dalam proses operasional transaksi menggunakan credit card maupun debit dengan mesin pembyaran EDC (*Electronic Debit Card*) terdapat dua mekanisme yaitu:

1. Menggunakan tanda tangan: dengan cara kartu debit terlebih dahulu di gesekan ke mesin EDC (*eletronic debit card*) pada mesin kasir dan selanjutnya petugas kasir memasukan jumlah total pembayaran pada sistem) Setelah proses verifikasi selesai sistem memotong otomatis saldo nasabah dan mesin EDC akan mengeluarkan bukti transaksi yang akan ditandatangani oleh pemegang kartu setelah melakukan transaksi. Sebagai proses validasi ke sistem
2. Menggunakan PIN: dalam proses transaksi tidak jauh berbeda dengan sistem tangan tangan. Perbedaannya hanya proses otentifikasi untuk menjaga keamanan kartu dari pihak pihak yang tak bertanggungjawab. Cara pertama hanya menggunakan tanda tangan untuk verifikasi transaksi dan proses kedua menggunakan nomor PIN untuk menjamin keamanan transaksi. Hal tersebut karena metode yang pertama sangat rawan di palsukan tanda tangan adapun

cara operasional pertama pihak kasir menggesek kartu debit ke mesin EDC. Input total yang harus di bayarkan ke sistem setelah selesai instruksikan ke konsumen untuk memasukan nomor pin ke mesin EDC jika sesuai mesin dan proses verifikasi selesai, mesin akan mengeluarkan bukti transaksi

I.5.4 Implementasi Pemanfaatan Sidik Jari dalam Kehidupan

Berdasarkan aspek historis sidik jari manusia atau yang lebih di kenal dalam bahasa medis *dermatologi* ditemukan oleh para peneliti yang menyatakan bahwa sidik jari seseorang, memiliki korelasi yang bersifat ilmiah dengan kode genetik dari sel otak dan sebagai indikator untuk mengukur potensi kecerdasan seseorang. Hipotesa tersebut di perkuat oleh penelitian yang di lakukan oleh Govard Bidloo pada tahun 1865, Mayer (1788), John E Purkinje (1823), Noel Jaquin (1958). Beryl Hutchinson tahun 1967 dalam bukunya yang berjudul "*Your Life in Your Hands*", yang menjelaskan tentang pola-pola garis tangan yang di miliki manusia menggambarkan tingkat kecerdasan yang dimiliki suatu individu. Seiring perkembangan zaman konsep tersebut di sempurnakan Beverly C Jaegers (1974), yang menjelaskan bahwa sidik jari dapat mencerminkan karakteristik dan aspek psikologis seseorang. Seiring perkembangan zaman mengacu pada hasil penelitian diatas penerapan sidik jari sudah mulai berkembang telah untuk di terapkan dalam segala aspek seperti sosial, database kependudukan, sistem keamanan, alat indentifikasi kejahatan dikarenakan memiliki pola yang unik yang terdapat pada struktur sidik jari yang tidak memiliki kesamaan antar individu satu sama lain walaupun kembar identik

sekalipun yang terbentuk pada trimester pertama kehamilan. Seiring perkembangan zaman sidik jari dapat di terapkan untuk berbagai macam teknologi terapan memudahkan aktivitas manusia antara lain:

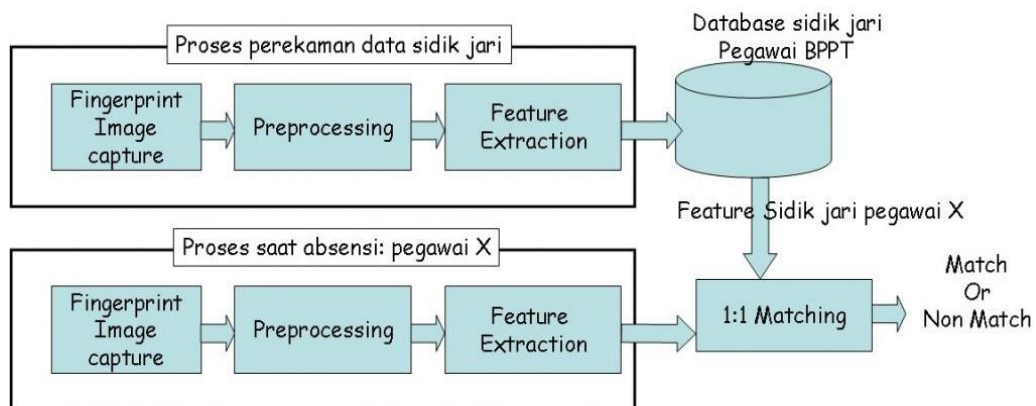
1. Mesin Absensi Sidik Jari (*fingerspot*)

Penggunaan absensi menggunakan sidik jari telah di terapkan dalam institusi baik perusahaan, pemerintahan, pendidikan dan lain sebagainya sebagai cara untuk mengontrol kinerja pegawai atau karyawan melalui mesin presensi berbasis *fingerprints* karena memiliki tingkat akurasi yang tinggi di bandingkan metode konvensional presensi dengan tanda tangan yang mudah di palsukan dan rawan kecurangan di lakukan pegawai dengan menitipkan absen ke rekanya yang masuk kerja, dengan adanya presensi sidik jari memudahkan pihak manajemen dalam mengontrol kehadiran pegawai secara *realtime* adapun cara kerja mesin absensi berbasis fingerprint atau istilah awam di kenal dengan *checklock* sebagai berikut :

- a. Pegawai atau karyawan melakukan perekaman sidik jari pada sistem yang di sediakan
- b. Data sidik jari tersimpan dalam database sistem, selanjutnya sidik jari ini pegawai dikelompokkan menjadi dua bagian yaitu *sentralisasi* dan *desentralisasi* yang membedakan dua kelompok tersebut hanya cara operasional metode sentralisasi
- c. Sidik jari user langsung tersimpan pada mesin absensi yang keuntungan mempercepat proses pencocokan sidik jari saat user melakukan proses *checklock* dan peletakan mesin bisa di tempat yang jauh tanpa terikat

server namun cara ini memiliki kelemahan membutuhkan memori internal yang cukup besar. Metode kedua *desentralisasi* dalam perekaman sidik jari membutuhkan server untuk menampung sidik jari user dan sebelum melakukan proses perekaman di perlukan input data awal meliputi identitas, jabatan pegawai, jenis sidik jari misal : *ulnar, whorl, arch, loop* kelebihan metode ini tidak membutuhkan memori yang cukup besar, memudahkan sistem mengenali sidik jari user karena sudah di kelompokkan sebelumnya namun memiliki kekurangan yaitu peletakan alat *checklock* tidak bisa terlalu jauh dari server.

- d. Tahap terakhir user melakukan uji coba absensi menggunakan mesin absen berbasis sidik jari



Gambar 1.6 Grafis Proses Sistem Kerja Mesin Absensi Sidik Jari (Nusa Komputer, 2018)

2. Kartu Penduduk Elektronik (E-KTP)

Kartu penduduk elektronik merupakan sebuah sistem kependudukan *big data* yang bertujuan untuk mempermudah urusan administrasi warga negara republik indonesia menjadi suatu sistem yang terintegrasi, dari tingkat daerah ke tingkat pusat dengan sistem terintegrasi di dalam chip. Pada kartu tanda

penduduk elektronik termuat informasi biometrik antara lain: identitas diri, sidik jari, iris mata, bentuk hidung tujuannya memuat informasi biometrik sebagai sarana indentifikasi jika terjadi hal hal tak di kenal. Misalnya : mayat tak dikenal atau dikenal istilah *mr-x*, bencana alam maupun bencana karena human error misalnya pesawat jatuh, kapal tenggelam, yang membuat korban sulit terindenfikasi. Dengan data biometrik e-ktp ini bisa dijadikan data *antemortem* atau sebelumnya oleh pihak berwajib seperti indentifikasi sidik jari menggunakan analisa pola sidik jari dengan membandingkan data postmortem setelah kematian sidik jari pada ijazah maupun pada sistem yang tersimpan di database kependudukan. Selain tujuan khusus yang telah di sebutkan diatas fungsi penggunaan E-KTP memiliki tujuan administratif antara lain :

- a. Sebagai identitas diri bersifat nasional dan mencegah identitas ganda dalam kependudukan
- b. Mencegah pemalsuan identitas dan menjamin keakuratan data penduduk untuk dasar perumusan kebijakan publik
- c. Sebagai acuan data utama dalam sistem pemilihan umum
- d. Untuk mempermudah masyarakat dalam mendapat pelayanan publik dan aktivitas sehari hari dan mengakses fasilitas umum seperti transportasi publik, pengurusan surat surat kendaraan, pengajuan kredit.

Selain memiliki beberapa fungsi kegunaan e-ktp yang telah di jelaskan diatas juga memiliki kegunaan lain yaitu untuk sistem pengaman pintu otomatis menggunakan indentifikasi KTP dengan cara menginput terlebih

dahulu nomor induk kependudukan ke sistem selanjutnya data yang sudah di input.

I.5.5 Peran Sidik Jari Sebagai Indetifikasi Kelainan Penyakit

Ightikhoma (2017) menjelaskan bahwa penyakit kanker dapat di deteksi melalui sidik jari dengan menggunakan analisis pola sudut ATD *phalanx distal* yang ada pada garis tangan manusia. Hasil analisis 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. Selain itu, penggunaan sidik jari di samping mengindetifikasi penyakit kanker juga dapat dilakukan untuk mengetahui pola sidik jari anak *down syndrome* atau kebutuhan khusus. Mayoritas yang telah di lakukan pada klan brahmana siwa di provinsi bali yang menghasilkan Frekuensi loop ulnar (LU) sub soroh Brahmana Mas 42,66%, manuaba 36%, Keniten 39%, dan Kemenuh 34,33%. Frekuensi loop radial (LR) sub soroh brahmana Manuaba 42,17%, Keniten 41,83%, Mas 37,83%, dan Kemenuh 29,51%. Frekuensi whorl (W) pada sub soroh brahmana kemenuh, Manuaba, Keniten, dan Mas masing-masing sebesar 35,33%, 22%, 18%, dan 17,83%. Indeks Dankmerijer (ID) diperoleh hasil signifikan antara sub soroh Mas dengan Kemenuh. Indeks Furuhata (IF) didapatkan hasil signifikan antara soroh Kemenuh dengan Mas serta Keniten dan Manuaba. total sulur antara laki-laki dan perempuan keturunan Brahmana Siwa didapatkan hasil tidak berbeda nyata pada taraf 5%, namun terdapat perbedaan total sulur yang signifikan pada sub soroh

Manuaba dengan Mas serta Kemenuh dan Keniten (Bajing Agastya et al., 2017).

Penelitian lain di wilayah provinsi yogyakarta bertempat di sekolah luar biasa bakti kencana dengan menggunakan studi komparasi pola sidik jari anak normal dan anak berkebutuhan khusus down syndrome dengan menggunakan metode independent sample T-Test menunjukkan hasil penelitian sebagian besar sidik jari anak dengan *down syndrome* 22 adalah *whorl* (55%), sedangkan sidik jari anak normal adalah *loop ulna* (53%). Uji Chi Square menunjukkan terdapat perbedaan bermakna ($p < 0,05$) pada distribusi pola whorl pada kedua tangan dan pola whorl tangan kanan antara kedua kelompok subjek penelitian (Ainur et al., 2009).

1.5.6 Pengenalan Wajah (*Face Recognition*)

Pengenalan wajah atau lebih di kenal dengan istilah *face recognition* merupakan sebuah metode analisis wajah berdasarkan karakteristik ukuran kepala, bentuk iris mata, hidung, bibir bentuk rambut yang di pengaruhi unsur *genetics* dan ras karena yang menyebabkan bentuk wajah manusia memiliki karakteristik berbeda antar individu dengan individu yang lain (Rahman et al.,2013). Faktor yang mempengaruhi perbedaan wajah antar individu yaitu faktor ras yang diklasifikasikan menjadi beberapa kelompok antara lain pertama ras *mongoloid* yang memiliki kecenderungan kulit putih, bentuk mata sedikit sipit dan hidung berukuran proposional dengan wilayah persebaran di asia timur china dan japan jenis kedua ras *negroid* dengan ciri khusus kulit hitam persebaran wilayah africa, ras kaukasoid memiliki ciri ciri kulit sawo matang, rambut sedikit lebih ikal,

bentuk hidung berukuran proporsional tidak terlalu panjang dan pendek.

Melalui sistem teknologi yang dinamakan *Discrete Wavelet Transform* (DWT) serta klasifikasi *Learning Vector Quantization* (LVQ) yang digunakan untuk pengolahan citra wajah berdasarkan indentifikasi ras manusia dengan menggunakan 90 citra sampel untuk training yang disimpan pada *database* dan 90 citra uji yang tidak disimpan pada database, membuktikan bahwa metode DWT dan klasifikasi LVQ cocok digunakan dalam mengklasifikasi dan mengidentifikasi 3 kelompok ras manusia dengan memiliki tingkat akurasi sebesar 94,4% dan waktu komputasi sebesar 6,467 per *second*

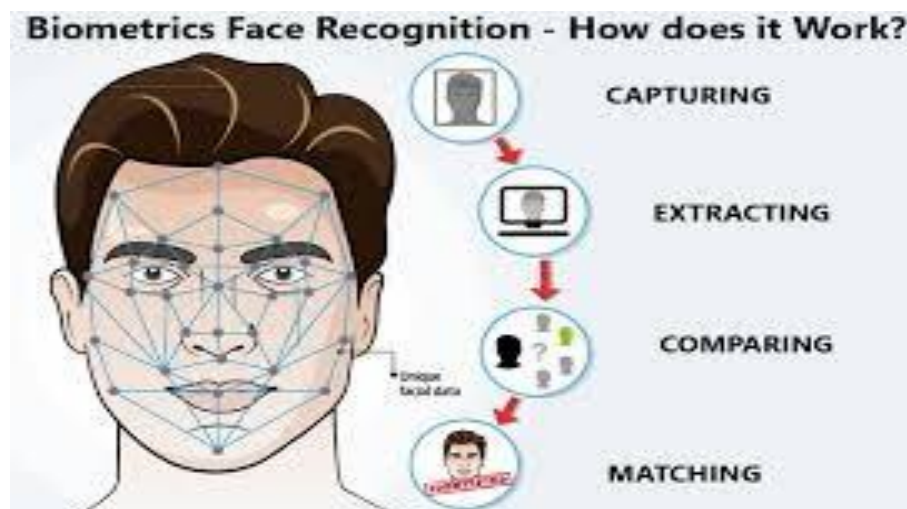
Dewi et al., (2019) Fungsi lain *face reconigition* dapat diimplementasikan untuk membantu aparat kepolisian dalam mengungkap kasus kriminalitas dengan menggunakan teknologi kamera CCTV *circuit closed television* yang telah diintegrasikan database kependudukan nasional. Dalam sistem kartu penduduk elektronik (e-KTP) telah memuat informasi biologis mulai wajah, kornea mata, dan sidik jari yang memudahkan dalam pengungkapan kasus kriminalitas. Teknologi pengenalan *face reconigition* juga diterapkan dalam sistem kunci otomatis *smartphone* karena lebih mengutamakan privasi pengguna akan data data pribadi yang tersimpan pada smarphone. Metode ini menggunakan sistem *Eigenface* yang digunakan untuk mengekstrak informasi yang relevan dari citra wajah saat di lakukan perekaman. Selanjutnya di ubah kedalam satu set kode kemudian kode dari citra wajah yang telah disimpan pada basis data. Kemudian disimpan pada server (MySQL) sebagai bank data wajah dan user bisa menentukan berapa banyak user yang dapat di kenali agar dapat mengakses smartphone dengan

menggunakan metode ini. *Eigenface* memiliki tingkat keberhasilan dari uji coba identifikasi wajah sebesar 68% dan tingkat salah pengenalan sebesar 32%, dari total uji coba sebanyak 25 kali identifikasi (Suprianto, 2013).

Selain dapat untuk sistem keamanan ponsel pintar atau *smartphone face recognition* dapat diterapkan untuk sistem keamanan pintu rumah dan kantor untuk mencegah tindakan kriminalitas pencurian dan meminimalisir kunci hilang atau ketinggalan. Caranya dengan menggunakan kamera *webcam* sebagai sensor pendeteksi dan media pengambilan gambar wajah untuk input yang akan diolah menggunakan metoda *Grayscale* pada mini PC *Raspberry Pi*. Sistem kerja yaitu kamera yang berfungsi sebagai sensor untuk mendeteksi wajah manusia dan mengambil gambar yang nantinya akan dijadikan sampel untuk pengenalan wajah dan untuk sampel database. Selanjutnya, *Raspberry* melakukan proses pengenalan antara sampel wajah yang ada pada database dengan wajah input target. Dari hasil percobaan menunjukkan sistem pengenalan wajah yang dikontrol oleh *raspberry pi* dengan input kamera *webcam* yang dapat mengenali wajah manusia dengan tingkat keberhasilan sebesar 72,5% dan kegagalan sebesar 27,5% dikarenakan berbagai factor diantaranya pencahayaan dan jarak (Ramadhan et al., 2016).

Penerapan lain untuk dunia pendidikan dan perkantoran yaitu dengan menggunakan mesin presensi berbasis pengenalan wajah. Hal ini di maksudkan karena teknologi sebelumnya presensi menggunakan sidik jari masih banyak kekurangan karena sidik jari manusia mudah sekali rusak pola lapisan dermatoligfi karena kecelakaan, luka bakar ataupun penyakit kulit bawaan. Dari segi akurasi metode sidik jari dan pengenalan wajah sama akurat namun sistem

pengenalan wajah memiliki keunggulan kontur wajah manusia cenderung tetap. Hal ini di buktikan dengan hasil percobaan pengenalan wajah membutuhkan waktu kurang dari rata rata kurang 0.25 ms (*menit per second*) jauh lebih cepat dari pengenalan sidik jari. Dengan tingkat akurasi sebesar rata rata 97.67 % (Pratikno, 2013).



Gambar 1.7 Ilustrasi Proses Indetifikasi Menggunakan Face Recognition

Dari ilustrasi di atas dapat di jelaskan bahwa proses indetifikasi 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 tujuanya untuk meminimalisir sistem error saat proses akhir.

4. *Matching* / Pengenalan : merupakan tahap akhir yaitu proses pengenalan wajah bagi individu yang telah melakukan perekaman akan di terima oleh sistem sebaliknya individu yang belum melakukan perekaman sistem akan di tolak sistem otomatis

Menurut Susanti, Fadillah, dan Setiyadi (2019) berpendapat bahwa proses pengenalan wajah (*face recognition*). Dibagi menjadi beberapa metode antara lain :

1. Metode berbasis pengetahuan: aturan didapatkan berdasarkan pengetahuan manusia mengenai fitur terdefinisi dari wajah seseorang manusia. Mayoritas dari aturan-aturan ini membahas tentang hubungan antar fitur.
2. Metode invarian fitur: algoritma dirancang untuk mencari fitur struktural dari wajah yang invariant terhadap masalah umum mengenai pose, halangan, ekspresi, kondisi citra, dan pengrotasian.
3. Metode pencocokan template: dengan suatu set *sample* yang diberikan, sebuah set pola wajah standar yang serupa dapat dihasilkan. Hubungan antara citra sample dan set pola yang telah didefinisikan dapat dihitung dan digunakan untuk menarik kesimpulan.
4. Metode berbasis penampilan: mirip dengan metode pencocokan template. Tujuannya adalah untuk mendapatkan keakuratan yang lebih tinggi dengan variasi yang lebih besar

Menurut Suprianto (2013) sistem pengamanan dengan menggunakan pengenalan biometrik wajah sangat akurat karena memiliki karakteristik yang tidak mudah hilang atau bersifat permanent dan tidak dapat dipalsukan karena ciri

morfotype wajah individu satu dengan lainnya tidak sama. Seperti pengenalan pengenalan *biometrics* lain seperti sidik jari, retina mata, suara yang dapat diimplementasikan dalam berbagai teknologi yang menunjang kehidupan. Salah satu contohnya sistem keamanan pintu ruangan menggunakan verifikasi sidik jari dan wajah secara *real-time* untuk mencegah pencurian dengan menggunakan menggunakan sebuah webcam atau kamera mini yang berfungsi untuk *capture* citra wajah pengguna dan kemudian dibandingkan dengan wajah yang tersimpan di database. Dengan menggunakan sistem yang dinamakan *HaarCascade* untuk proses pengenalan wajah dan metode PCA atau *Eigenface* untuk proses pengenalan wajah. Pengujian dilakukan dengan menggunakan 150 data training dan 150 data menunjukkan tingkat keberhasilan pengenalan secara keseluruhan sebesar 83.33%. Sistem ini dirancang untuk bekerja secara *real-time* dengan harapan mempermudah pengguna dan dapat meminimalisir tindakan kriminal kedepannya dengan memiliki fungsi mengenali wajah mulai bagian depan kepala yang meliputi: dahi dagu, alis, mata, hidung, pipi, mulut, bibir, gigi dan warna kulit kulit jika wajah user dikenali secara otomatis sistem memberikan izin untuk masuk sebaliknya jika tidak mengenali maka sistem akan menolak

Menurut Primanita and Anggraini, (2015) Menjelaskan secara umum pembagian tipe-tipe morfologi wajah manusia dibagi menjadi beberapa kelompok antara lain

1. Bentuk wajah panjang. Ukurannya lebih panjang dari pada lebar wajah. Wajah ini memiliki ukuran yang hampir sama wajah panjang (kadang disebut "persegi panjang") ukurannya lebih panjang dari pada lebar wajah. Wajah ini

memiliki ukuran yang hampir sama pada pipi, dahi, dan rahang.

2. Bentuk wajah persegi kira-kira mempunyai panjang dan lebar yang sama, antara pipi dan panjangnya kira-kira berbeda 2,5 sampai 5 cm. Selain itu, ukuran pipi, dahi, dan rahang wajah persegi hampir sama, sisi wajah atas dan bawah hampir lurus. Rahang wajah persegi pasti mempunyai sudut yang jelas dan tajam pada bagiannya yang terlebar.
3. Bentuk wajah oval adalah bentuk wajah proporsional mirip dengan bentuk telur terbalik. Lebih panjang dari pada lebarnya, dengan dahi lebih lebar dari pada rahang dan dagu yang halus membulat.
4. Bentuk wajah bulat persegi memiliki lebar dan panjangnya. dahi yang relatif kecil dan garis rahang kecil yang melengkung. Bila selisih ukuran pipi dan "panjang" sekitar 2,5 cm, ukuran dahi lebih kecil dari ukuran pipi, dan rahang hampir tidak mempunyai sudut tajam seperti pada wajah persegi, maka Anda mempunyai wajah bulat.

Menurut Sudarmilah (2009) menjelaskan bahwa 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*. 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,

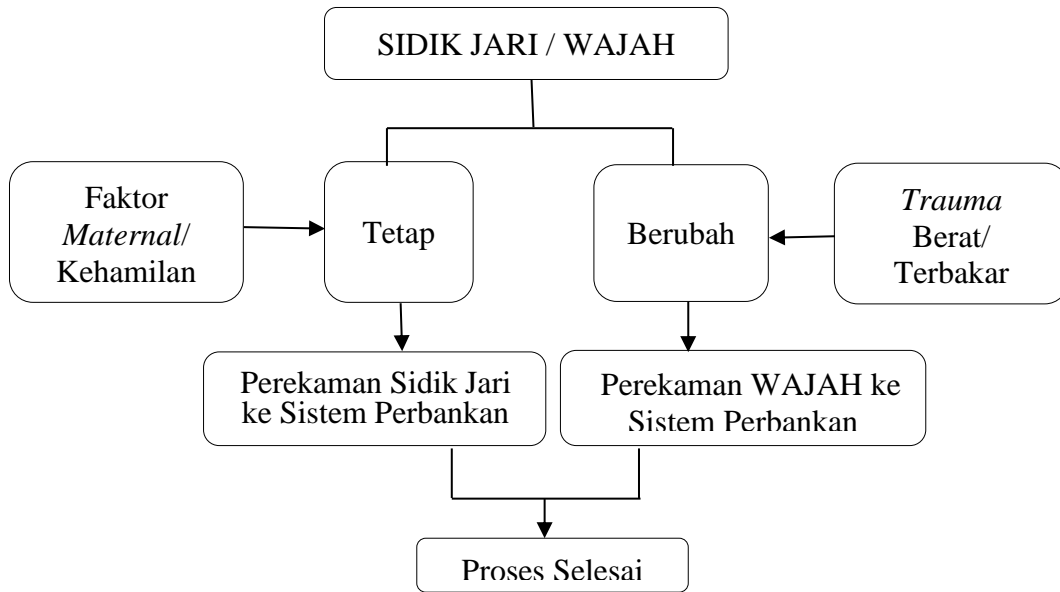
Dewi et al., (2019) Fungsi lain pengenalan wajah dapat dimplementasikan sebagai keamanan *folder* yang ada pada komputer atau laptop yang sangat rawan dicuri data data yang bersifat penting dan pribadi oleh orang lain. Terlebih jika komputer kantor yang di gunakan bersama yang memiliki kemungkinan terjadi 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.

Cara kerja pengenalan wajah dengan menggunakan sebuah kamera atau *webcam* untuk menangkap wajah seseorang yang kemudian akan dibandingkan dengan wajah pemilik *folder* tersebut yang telah di lakukan perekaman

sebelumnya jika sistem mengenali maka *folder* otomatis terbuka jika tidak cocok secara otomatis menolak dan sistem secara langsung *shutdown* atau mati otomatis sistem ini diaplikasikan menggunakan metode *Triangle Face*. Proses identifikasi wajah dilakukan dengan menggunakan fitur – fitur pada wajah seperti jarak antar mata, jarak mata kanan ke hidung, jarak mata kiri ke hidung, jarak mata kanan ke mulut dan jarak mata kiri ke mulut yang akan membentuk segitiga serta ukuran lebar dan tinggi wajah. Dari perancangan sistem ini di dapatkan hasil bahwa sistem pengenalan wajah menggunakan metode *Triangle Face* ini memiliki keakuratan yang baik yaitu 82,6%, sehingga dapat dikatakan sistem ini cukup aman untuk diaplikasikan dalam pengaksesan ruang folder komputer (Arhandi et al., 2018).

I.6 Kerangka Konseptual Penelitian

Penyajian data dilakukan dengan mengklasifikasikan data yang telah di dapat melalui data sekunder dengan melakukan penggolongan berdasarkan beberapa indikator tahun kejadian, total kerugian dan jenis bank. Oleh karena itu, Berikut adalah gambar tentang kerangka konseptual penelitian.



Gambar 1.8 Kerangka konseptual Penelitian

Dari kerangka konsep diatas dapat dijelaskan bahwa sistem kerja mesin anjungan tunai mandiri dibedakan menjadi dua pengenalan yaitu : pertama dengan verifikasi sidik jari dan yang kedua dengan verifikasi wajah alasan menggunakan sidik jari dikarenakan pola pada manusia bersifat tetap karena dipengaruhi faktor genetik yang terbentuk, dari trimester pertama kehamilan yang bersifat seumur hidup kecuali terjadinya luka luka atau trauma pad kulit yang mengakibatkan perubahan pola sidik jari, jika terjadi perubahan struktur sidik jari untuk proses indentifikasi dapat digantikan melalui memindai wajah menggunakan kamera *face recognition* sebagai pengganti sidik jari karena wajah termasuk dalam kategori *human biometrics indentification* yang bersifat personal / privacy yang sulit untuk dipalsukan atau tidak memiliki kesamaan bentuk dari individu satu ke individu lain walaupun kembar indetik sekalipun dengan tingkat akurasi sangat tinggi kurang lebih 90% pengenalan wajah sama halnya dengan indentifikasi sidik jari.

Adapun cara operasional sistem pengamanan mesin anjungan tunai

mandiri dengan menggunakan sidik jari dan wajah, nasabah bank terlebih dahulu melakukan perekaman *biometrics* sidik jari dan wajah nasabah untuk dimasukkan kedalam database perbankan jika salah satu *biometrics* nasabah tidak dapat dikenali oleh sistem karena sebab sebab tertentu misalnya: pola sidik jari berubah disebabkan pengelupasan jaringan kulit karena trauma dan nasabah ada riwayat operasi plastik pada jaringan wajah yang menyebabkan bentuk muka. Maka tahapan perekaman data salah satu dari dua komponen *biometrics* yang bisa dikenali sistem baik pola sidik jari maupun wajah.

I.7 Metode Penelitian

I.7.1 Pendekatan dan Fokus Penelitian

Penelitian ini difokuskan pada kejahatan debit *card fraud crime* dengan menggunakan mesin anjungan tunai mandiri dengan target nasabah perbankan dengan tujuan untuk meretas data yang tersimpan didalam karttu atm dan mengambil saldo rekening korban dengan menggandakan kartu ATM korban. *Output* atau luaran dari penelitian ini untuk meminimalisir *debit card fraud crime* dengan menggunakan mesin ATM berbasis pengenalan sidik jari dan wajah nasabah yang memiliki tingkat akurasi keamanan yang tinggi dan bersifat *personal idetification* yang tidak dapat dipalsukan. Selain itu, dapat memberikan rasa aman nasabah dalam bertransaksi menggunakan mesin ATM.

I.7.2 Metode Penelitian

Metode yang digunakan dalam penelitian ini dikelompokan 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.

1.7.3 Teknik Analisis Data

Penelitian ini dalam menganalisa data menggunakan data sekunder yang berasal dari study literature yang memuat data data statistik jumlah kasus *debit card fraud crime* yang terjadi pada beberapa bank di negara Indonesia baik milik pemerintah maupun swasta. Peneliti menganalisis data dengan menggunakan *analytic descriptive statistic*

1.7.4 Perancangan Layout/ Design Prototype

Di dalam proses ini 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.