Progresif: Jurnal Ilmiah Komputer
Jl. Ahmad Yani, K.M. 33,5 - Kampus STMIK Banjarbaru
Loktabat – Banjarbaru (Tlp. 0511 4782881), e-mail: puslit.stmikbjb@gmail.com
e-ISSN: 2685-0877
p-ISSN: 0216-3284

Analisis Perbandingan *Fingerprint* dan *Facelock* pada *Lock Screen Smartphone*

Imantoko[1]*, E.I.H. Ujianto[2]
[1,2]Program Magister Teknologi Informasi, Universitas Teknologi Yogyakarta
[1,2]Jl. Siliwangi (Ringroad Utara), Jombor, Sleman, D.I. Yogyakarta 55285, +62-274-623306
[2]erik.iman@uty.ac.id
**Corresponding Author*: imantoko@student.uty.ac.id,

Abstrak

Informasi yang bersifat krusial dalam *smartphone* seperti data pribadi maupun data perusahaan berupa gambar, cetak biru, suara, serta dokumen penting lainnya perlu dilindungi. Satu dari beberapa pengaman dasar pada smartphone adalah pengunci layar (*lock screen*). *Lock screen* yang populer digunakan diantaranya *fingerprint* dan *facelock*. Serangan sistem pengaman seperti sidik jari palsu (*fingerprint-copy attack*) dan wajah palsu (*face spoof attack*) membahayakan informasi yang terdapat pada smartphone. Artikel dibuat dengan tujuan untuk mengetahui *lock screen* mana yang lebih aman dari sisi kemudahan dalam melakukan serangan oleh pemula, dimana alat dan bahan yang digunakan terbatas yaitu peralatan sehari-hari. Hasil perbandingan menyimpulkan keamanan fingerprint lebih aman dibandingkan *facelock* dikarenakan *fingerprint-copy* attack membutuhkan keahlian khusus dalam praktiknya, sehingga serangan ini sulit dilakukan oleh pemula daripada *face spoof attack*.
Kata kunci: *Fingerprint, Facelock, Smartphone, Lock Screen*

Abstract

Crucial information on smartphones such as personal data and company data in the form of images, blueprints, sounds and other important documents need to be protected. One of the most basic safeguards on a smartphone is the lock screen. Popular lock screens those are used include fingerprint and facelock. Security system attacks such as fake fingerprints (fingerprint-copy attacks) and fake faces (face spoof attacks) leave vulnerable on the information contained on smartphones. The article was made with the aim to find out which lock screen is safer in terms of ease in carrying out attacks by beginners, where the tools and materials used are limited to everyday equipment. The comparison results concluded that fingerprint security is safer than facelock because fingerprint-copy attacks require special expertise in practice, so this attack is more difficult for beginners than face spoof attacks.
Keywords*: Fingerprint, Facelock, Smartphone, Lock Screen*

1. Pendahuluan

Smartphone berguna sebagai sarana penyebaran informasi, layanan transportasi umum, layanan pesan antar makanan, hingga penyimpanan uang digital atau *e-wallet*. Akan tetapi, seiring dengan perkembangannya yang pesat, *smartphone* juga menghadapi ancaman keamanaan yang harus ditanggulangi. Sebagai contoh, *smartphone* mengumpulkan dan menyimpan banyak informasi yang aksesnya harus dikontrol untuk melindungi privasi pengguna maupun kekayaan intelektual dari perusahaan atau institusi milik pemerintah [1]. Informasi yang bersifat krusial seperti data pribadi maupun data perusahaan berupa gambar, cetak biru, suara, serta dokumen penting lainnya perlu dilindungi. Satu dari beberapa pengaman dasar pada *smartphone* adalah pengunci layar (*lock screen*).

Lock screen adalah sistem pengamanan yang diterapkan pada smartphone dan bertujuan untuk mengunci layar utama sehingga tidak dapat difungsikan secara utuh dalam penggunaan fitur-fiturnya, tetapi terdapat beberapa fitur yang masih dapat diakses tanpa harus membuka *lock screen smartphone* [2]. Teknologi *lock screen* muncul dengan berbagai cara penggunaan, mulai dari karakteristik, kemampuan serta kelemahanya. *Lock screen* merupakan

satu dari banyak pengaman data pada *smartphone* bertujuan untuk mencegah agar *smartphone* pengguna tidak digunakan oleh orang yang tidak berhak. *Lock screen* yang populer digunakan diantaranya *fingerprint* dan *facelock* [3]. Berkembangnya *lock screen* tersebut mengundang serangan sistem pengaman seperti sidik jari palsu (*fingerprint-copy attack*) dan wajah palsu (*face spoof attack*) yang bertujuan untuk membuka akses ke *smartphone* pengguna secara paksa atau ilegal. Penggunaan *lock screen* yang semakin banyak menandakan bahwa faktor keamanan merupakan sesuatu yang sangat penting.

2. Tinjauan Pustaka

Hasil percobaan yang dilakukan dalam artikel [4] menunjukkan bahwa pada perangkat seluler kotemporer dengan sensor sidik jari biometrik tertanam dapat digunakan untuk keamanan kunci serta sanksi pembayaran. Tetapi, kemudahannya tersebut mengundang ancaman serangan. Keamanan *fingerprint* dapat ditembus dengan peralatan sederhana serta dilakukan oleh para pemula. Penyerang hanya perlu membuat cetakan sidik jari menggunakan Siligum atau BluTack lalu menambahkan cairan panas pada cetakan. Setelah itu, penyerang melepas hasil cetakan dari cetakan tersebut lalu menggunakannya untuk membuka akses pengguna lain secara illegal.

Artikel [5] mengusulkan teknik untuk menangkap gambar jari dari kamera *smartphone* dan memprosesnya sedemikian rupa sehingga dapat dengan mudah dicocokkan dengan gambar sensor optik. Pendekatan yang diusulkan telah divalidasi pada dataset FVC 2004 DB1 & DB2 dan hasilnya menunjukkan efektivitas metodologi yang diusulkan. Metode ini dapat digunakan untuk penggunaan komersial *real-time*.

Artikel [6] mengidentifikasi kamera digital berdasarkan noise sensor dengan asimetri. Artikel ini fokus pada *fingerprint-copy attack*, di mana penyerang memiliki akses ke gambar JPEG, sementara *defender* dapat memanfaatkan gambar yang tidak terkompresi. Artikel ini mengarah pada gagasan *fragile sensor fingerprints* yang hanya tersedia untuk *defender* tetapi tidak berkerja pada *lossy compression*. Eksperimen dengan tujuh kamera berbeda menunjukkan deteksi serangan yang sangat andal selama tidak ada gambar berkualitas tinggi yang dibagikan kepada publik.

Eksperimen oleh [7] menyatakan bahwa residu minyak yang tersisa pada layar sentuh dapat digunakan untuk melanggar privasi pengguna. Penelitian ini memperkenalkan serangan sidik jari terhadap perangkat yang mendukung sentuhan. Serangan ini dilakukan dengan membersihkan permukaan layar sentuh untuk mengungkap sidik jari, dan menggunakan kamera iPhone untuk memotret sidik jari dengan hati-hati sembari berusaha untuk menghapus gambar virtual telepon dari gambar sidik jari. Eksperimen ekstensif dilakukan pada iPad, iPhone dan ponsel Android dan hasilnya menunjukkan bahwa serangan sidik jari efektif dan efisien dalam menyimpulkan kata sandi dari gambar sidik jari.

Penelitian pada [8] bertujuan untuk mengatasi masalah performa *liveness detection* pada pengenalan wajah yang rendah. Penelitian ini mengusulkan metode baru untuk menemukan *discriminative image patches* yang didefinisikan sebagai daerah yang menonjol, instrumental, dan *class-specific*. Empat pengklasifikasi terkenal yaitu, Support Vector Machine (SVM), Naif-Bayes, Quadratic Discriminant Analysis (QDA), dan Ensemble digunakan untuk membedakan antara wajah asli atau buatan menggunakan skema berbasis voting. Hasil percobaan pada dua basis data yang tersedia untuk umum menunjukkan kinerja komparatif dibandingkan dengan metode yang sudah ada.

Artikel [9] menyarankan pendekatan baru untuk menangkal *face spoof attack* menggunakan Light Field Camera. Dua fitur khusus yang tidak dapat diperoleh dari kamera konvensional diekstrak dengan melihat *raw light field* foto dari sudut pandang yang berbeda. Metode yang diusulkan mencapai setidaknya 94,78% akurasi atau sampai dengan akurasi 99,36% di bawah berbagai jenis serangan *spoofing*.

Perbedaan artikel-artikel diatas dengan artikel yang penulis buat terletak pada fokus penulisannya. Artikel pada kajian pustaka membahas satu jenis *lock screen* secara mendalam sedangkan penulis membandingkan antara dua jenis *lock screen* yaitu *fingerprint* dan *facelock* mengenai kekurangan dan kelebihan dari penggunaanya serta serangan yang mungkin menyerang *lock screen* tersebut berdasarkan pengalaman pribadi penulis. Artikel dibuat dengan tujuan untuk mengetahui *lock screen* mana yang lebih aman dari sisi kemudahan dalam melakukan serangan oleh pemula, dimana alat dan bahan yang digunakan terbatas yaitu peralatan sehari-hari.

3. Metodologi

Penulisan menggunakan pendekatan subjektif atau didasarkan pada penilaian penulis. Data yang digunakan merupakan hasil dari percobaan secara langsung maupun studi literatur penggunaan fitur *lock screen fingerprint* dan *facelock* pada *smartphone*. Serangan yang dicoba penulis yaitu *face spoof attack* pada *facelock* dan *fingerprint-copy attack* pada *fingerprint* menggunakan Samsung Galaxy A20. Penilaianya didasarkan pada pemikiran logis penulis, jurnal, media internet, serta dokumentasi lainnya tentang serangan *lock screen* yang dijadikan sebagai referensi terhadap penulisan artikel ini.

4. Hasil dan Pembahasan

Setiap *lock screen* memiliki cara penggunaan dan tingkat keamanan yang berbeda-beda. Begitu juga serangan yang dapat terjadi pada masing-masing *lock screen*. Pembahasan ini akan menjelaskan bagaimana serangan dapat terjadi pada suatu *lock screen* dalam hal ini *fingertprint* dan *facelock. Fingerprint* rentan terhadap *fingerprint-copy attack pada fingerprint* dan *facelock* rentan terhadap *face spoof attack*. Kedua serangan ini memiliki konsep yang sama yaitu pemalsuan kunci biometrik.

4.1. *Fingerprint*

Fingerprint atau sidik jari merupakan pola hubungan dan lembah pada permukaan ujung jari yang unik untuk setiap individu. Karena kemudahan, individualitas dan efisiensinya, pengenalan sidik jari telah menjadi metode identifikasi pilihan. Identifikasi merupakan proses mengenali sidik jari tertentu dalam basis data. Penggunaan identifikasi sidik jari melibatkan perbandingan antara sidik jari dengan sampel yang disebut sebagai proses verifikasi [10]. Sistem *fingerprint* bekerja dalam dua fase, yaitu, fase pendaftaran, dan fase otentikasi. Fase pendaftaran administrator sistem melakukan pendaftaran individu pada aplikasi biometrik. Pengguna meletakkan jarinya di permukaan sensor di perangkat input. Kualitas sidik jari yang ditangkap oleh sensor tergantung pada keadaan jari, seperti jari basah atau kering, luka pada jari, tekanan yang diterapkan jari, daya tahan sensor dan kondisi lainya. Selanjutnya, fase otentikasi merupakan verifikasi dan identifikasi individu yang diklaim. Verifikasi melibatkan pemeriksaan apakah biometrik yang disajikan adalah milik orang yang diklaim, sedangkan identifikasi yaitu mengungkapkan siapa yang terkait dengan biometrik yang dikirimkan pada saat pengguna meletakkan jarinya di sistem dan mengklaim dirinya sebagai pengguna terdaftar [11]. Smartphone dengan teknologi terbaru memiliki fitur keamanan yang menggunakan sidik jari sebagai objek utamanya [2]. Pendaftaran *fingerprint* pada Samsung Galaxy A20 ditunjukan seperti gambar 1.

Gambar 1. Pendaftaran Sidik Jari

Cara pendaftarannya yaitu dengan menempelkan sidik jari pada sensor di perangkat input dengan berbagai posisi hingga seluruh permukaan sidik jari terekam oleh sensor dan indikator menjadi 100%. Sensor yang digunakan untuk mengambil data sidik jari terlihat pada gambar 2.

Gambar 2. Gambar Sensor Sidik Jari pada Samsung Galaxy A20

Pengembang *smartphone* memilih *fingerprint* untuk dijadikan salah satu pengamanan data karena kelebihanya yang bersifat unik artinya sidik jari setiap orang berbeda-beda antara yang satu dan lainya, pengguna dapat mendaftarkan maksimal tiga sidik jari, serta penggunaanya yang sangat mudah. Kekurangan yang dirasakan oleh penulis yaitu sidik jari tidak dapat digunakan apabila jari dalam keadaan basah, lembab, berminyak, kotor, dan luka. Meskipun begitu, *fingerprint* tidak lepas dari serangan yang mengancam data informasi penggunanya. Serangan yang menyerang sistem keamanan *fingerprint* yaitu *fingerprint-copy attack*. *Fingerprint-copy attack* merupakan serangan dimana penyerang menggunakan duplikasi sidik jari pengguna untuk membuka akses data secara ilegal. Kunci utama sebelum melakukan penyerangan yaitu memiliki sidik jari dari korban [12].

Penulis melakukan percobaan untuk membuktikan serangan yang terjadi pada *fingerprint*. Alat yang digunakan yaitu lem tembak, papan dan gunting. Bahan yang digunakan yaitu isi lem tembak dan lem kaca. Langkah pertama, memanaskan lem tembak dan mengaplikasikanya pada papan. Langkah kedua, tempelkan dan tekan jari pada isian lem tembak yang sudah tidak terlalu panas seperti pada gambar 3.

Gambar 3. Proses pembuatan cetakan sidik jari

Langkah ketiga, angkat jari secara perlahan jika lem tembak mulai mengeras. Pegangkatan jari harus dilakukan dengan hati-hati agar tidak merusak cetakan. Contoh cetakan sidaik jari yang sudah jadi dapat dilihat pada gambar 4.

Gambar 4. Cetakan sidik jari

Langkah keempat, isi cetakan dengan lem kaca seperti pada gambar 5. Pastikan lem kaca tidak bergelembung dan menutupi seluruh cetakan, setelah itu diamkan selama 24 jam sampai cetakan mengeras.

Gambar 5. Cetakan sidik jari yang diisi lem kaca

Langkah terakhir, lepaskan lem kaca dari cetakan dan rapikan dengan gunting. Sidik jari yang sudah jadi dapat digunakan untuk membuka *lock screen smartphone*, seperti yang terlihat pada gambar 6.

Gambar 6. Hasil cetakan sidik jari

Serangan dilakukan sebanyak 20 kali pada *smartphone* Samsung Galaxy A20. Semua percobaan gagal, sehingga menghasilkan presentasi keberhasilan sebesar 0%. Kegagalan ini terjadi karena cetakan yang kurang baik. Cetakan yang kurang baik disebabkan oleh lembah sidik jari yang kurang dalam sehingga sidik jari palsu tidak dapat terdeteksi oleh sensor *fingerprint*. Serangan menggunakan metode ini kurang cocok untuk pemula karena membutuhkan kesabaran dan keterampilan membuat cetakan yang baik. Faktor lain yang mungkin mempengaruhi kegagalan yaitu *liveness detection* dimana sistem dapat mendeteksi kehidupan dari sidik jari yang dibaca oleh sensor. Terlepas dari itu, metode ini kurang cocok diterapkan pada kasus yang sesungguhnya karena sumber sidik jari pada metode ini berasal langsung dari jari korban. Metode yang cocok pada kasus sesungguhnya diusulkan oleh [12], sidik jari korban didapatkan dari benda-benda yang pernah disentuh oleh korban tetapi metode ini sulit dilakukan oleh pemula. Butuh keahlian forensik untuk membuat sidik jari dari benda-benda yang pernah disentuh agar terlihat dengan jelas.

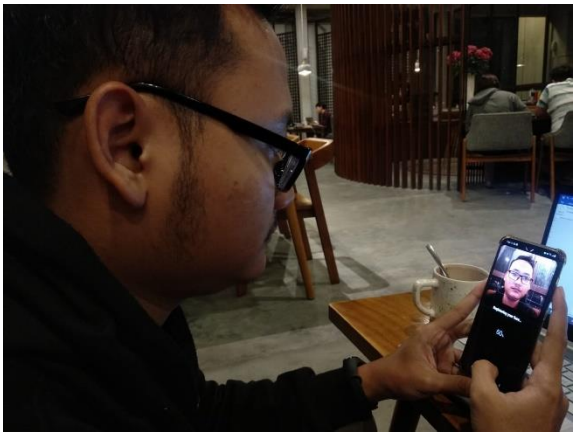
4.2. Facelock

Facelock merupakan fitur penguncian yang terhubung ke wajah pengguna menggunakan kamera bawaan *smartphone*. Wajah pengguna ditangkap dalam batas pengenalan wajah yang akan digunakan untuk sistem penguncian. Ekspresi wajah yang mirip dengan pengaturan wajah harus dikenali untuk membuka kunci [13]. Metode pengenalan wajah menerima masukan berupa citra wajah. Saat pertama kali dijalankan, sistem akan menjalankan deteksi wajah untuk mengisolasi wajah yang akan digunakan sebagai pembuka kunci. Setiap wajah diproses terlebih dahulu dan kemudian direpresentasikan menjadi dimensi rendah (atau *embedding*). Representasi dimensi rendah tersebut selanjutnya diproses untuk klasifikasi [14].

Kelebihan dari penggunaan *facelock* yaitu mudah dalam penggunaanya bahkan *facelock* dapat mendeteksi pengguna yang menggunakan kaca mata. Kelemahan *facelock* yaitu faktor cahaya dan ekspresi wajah misal menutup sebelah mata serta membuka mulut dengan lebar membuat pengguna tidak dikenali. Dirasakan bahwa *facelock* tidak begitu efisien namun, metode ini masih menjadi metode yang praktis untuk otentikasi [2].

Sebuah studi tentang pengenalan wajah menggunakan pencocokan *Commercial Off the Shelf* (COTS) menunjukkan bahwa pencocokan wajah dari versi saat ini rentan terhadap *face spoof attack* [3]. Studi lainnya juga menyatakan bahwa sistem pengenalan wajah yang ada rentan terhadap *face spoof attack*, karena *face liveness detection* belum menjadi modul bawaan. Sistem pengenalan wajah biasa dapat tertipu oleh gambar wajah yang dicetak, pemutaran ulang video, atau topeng mimik [15]. *Face spoof attack* adalah proses di mana penyerang dapat menembus atau menyerang sistem pengenalan wajah dengan menyamar sebagai pengguna terdaftar dan dengan demikian mendapatkan akses dan keuntungan tidak sah [8]. *Face spoof attack* paling mudah dilakukan dengan menggunakan foto pemilik *smartphone*.

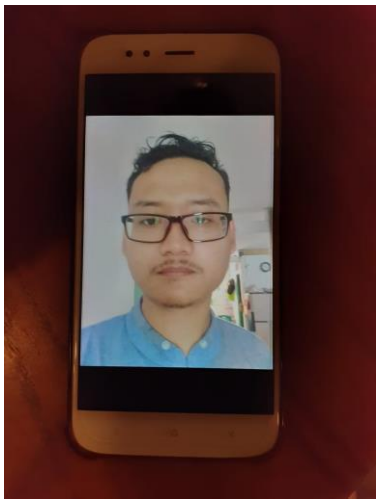
Percobaan dilakukan menggunakan Samsung Galaxy A20 sebagai *smartphone* yang diamankan menggunakan *facelock* dan Xiaomi Mi A1 sebagai *smartphone* yang digunakan untuk melakukan *face spoof attack*. Sebelum melakukan serangan, penulis mendaftarkan wajah sebagai pembuka *lock screen*, seperti pada gambar 7.



Gambar 7. Pendaftaran Wajah untuk *Facelock*

Gambar 7 menunjukkan pendaftaran wajah untuk membuka kunci *lockscreen*. Pendaftaran dilakukan dengan cara menuju menu “Pengaturan”, kemudian masuk ke menu “Lock Screen”, pilih “Screen Lock Type”. Cari menu “Biometrics” dan pilih “Face”. Setelah itu, pengguna akan diminta untuk mengatur posisi wajah di depan kamera. Apabila berhasil maka pendaftaran wajah selesai dan *facelock* bisa digunakan.

Setelah *smartphone* sasaran terpasang *facelock,* proses penyerangan dimulai. Langkah pertama yaitu pencarian foto pengguna yang terdaftar pada *lock screen smartphone* yang akan diserang. Pencarian dapat dilakukan dengan banyak cara, diantaranya media sosial, internet, atau mencari langsung di penyimpanan pribadi pemilik *smartphone* sasaran. Selain pencarian, penyerang juga dapat mengambil foto pemilik *smartphone* secara tersembunyi. Kreativitas penyerang dibutuhkan pada langkah ini.



Gambar 8. Foto Pengguna Terdaftar di *Smartphone* Sasaran

Gambar 8 merupakan foto pengguna terdaftar di *smartphone* sasaran. Foto didapatkan dari penyimpanan pribadi pengguna. Foto tersebut diambil sembilan hari sebelum pendaftaran wajah untuk *facelock*. Langkah terakhir adalah serangan. Pelaksanaan serangan cukup mudah, penyerang hanya perlu memposisikan foto agar *smartphone* sasaran dapat mengotentikasinya. Apabila posisi sesuai *facelock* pun terbuka dalam hitungan detik. Proses penyerangan dengan *face spoof attack* dapat dilihat pada gambar 9.

Gambar 9. Proses *Face Spoof Attack*

Gambar 9 menunjukkan proses *face spoof attack*. Foto yang digunakan untuk melakukan penyerangan adalah foto pada gambar 8. Foto tersebut ditampilkan pada *smartphone* lain, yaitu Xiaomi Mi A1 dengan tingkat kecerahan maksimal. Penyerangan dilakukan saat malam hari dalam ruangan. Serangan dilakukan sebanyak 20 kali pada *smartphone* Samsung Galaxy A20.

Terdapat 16 percobaan yang berhasil dan 4 kali kegagalan, sehingga menghasilkan presentasi keberhasilan sebesar 80%. Metode ini cocok diterapkan pada kasus yang sebenarnya. Selain itu, metode ini dapat dilakukan oleh pemula karena proses serangannya yang sederhana.

4.1. Hasil

Hasil percobaan yang dilakukan menunjukkan bahwa serangan pada *lock screen fingerprint smartphone* Xiaomi Mi A1 telah dilakukan sebanyak 20 kali diantaranya 14 percobaan yang berhasil dan 6 kali gagal dengan presentasi keberhasilan sebesar 70%. Metode ini dapat dilakukan oleh pemula tetapi, metode ini tidak cocok diterapkan pada kasus yang sesungguhnya karena sumber sidik jari berasal langsung dari jari korban. Perlu keahlian forensik untuk membuat sidik jari dari benda-benda yang pernah disentuh agar terlihat dengan jelas.

Face spoof attack yang dilakukan berhasil membuka *lock screen smartphone* sasaran sebanyak 16 kali dari 20 kali percobaan dengan tingkat keberhasilan sebesar 80%. Sebanyak empat kali kegagalan disebabkan posisi *smartphone* sasaran dengan *smartphone* penyerang kurang tepat. Percobaan yang dilakukan membuktikan bahwa *facelock* yang ada pada *smartphone* Samsung Galaxy A20 masih rentan terhadap *face spoof attack.*

Perbandingan *fingerprint-copy attack* dan *face spoof attack* merupakan hasil dari pembahasan ditunjukkan pada tabel 1.

Tabel 1. Perbandingan *fingerprint-copy attack* dan *face spoof attack*

	Face Spoof Attack	***Fingerprint*-copy Attack**
Peralatan	Smartphone	Lem tembak, papan, gunting, isi lem tembak dan lem kaca
Keterampilan	Fotografi, kreativitas	Kreativitas
Kompleksitas	2 Langkah	5 Langkah
Dapat dilakukan oleh pemula	Ya	Tidak
Kasus Sesungguhnya	Cocok	Tidak Cocok

Tabel 1 menunjukan bahwa peralatan yang dibutuhkan untuk melakukan *face spoof attack* hanya *smartphone*, sedangkan *fingerprint-copy attack* membutuhkan banyak peralatan seperti lem tembak, papan, gunting, isi lem tembak dan lem kaca. Kreativitas dibutuhkan dalam *face spoof attack* dan *fingerprint-copy attack*, namun *face spoof attack* membutukan keterampilan lain yaitu fotografi. Berdasarkan kompleksitas langkah yang diperlukan untuk melakukan serangan, *fingerprint-copy attack* lebih kompleks karena membutuhkan 5 langkah dibandingkan dengan *face spoof attack* membutuhkan 2 langkah. *Face spoof attack* dapat dilakukan oleh pemula dan metode yang dipraktikan cocok untuk kasus sesungguhnya sedangkan, *fingerprint-copy attack* sulit untuk dilakukan oleh pemula dan tidak cocok pada kasus sesungguhnya. *Fingerprint-copy attack* yang cocok untuk kasus sesungguhnya membutuhkan keahlian forensik yang mana tidak cocok untuk pemula sehingga dapat disimpulkan bahwa *face spoof attack* lebih mudah dilakukan dibandingkan *fingerprint-copy attack.* Hasilnya *fingerprint lock screen* lebih aman dibandingkan *facelock* berdasarkan perbandingan dari sisi kemudahan dalam melakukan serangan oleh pemula.

5. Kesimpulan

Hasil perbandingan menyimpulkan keamanan *fingerprint* lebih aman dibandingkan *facelock.* Hal ini disebabkan *face spoof attack* lebih mudah dilakukan dari pada *fingerprint-copy attack* mengingat peralatan yang dibutuhkan cukup sederhana. Selain itu, perbandingan kompleksitas untuk melakukan *face spoof attack* lebih sedikit dari *fingerprint-copy attack.* Terlepas dari itu semua, walaupun fingerprint lebih aman dibandingkan facelock, penulis menyadari bahwa tingkat keamanan *facelock* dan *fingerprint* masih tergolong lemah terhadap serangan yang memanfaatkan kunci biometrik buatan seperti *face spoof attack* dan *fingerprint-copy attack* namun, pengguna dapat melihat sisi positif dari kelemahan tersebut yaitu pada *fingerprint-copy attack,* sidik jari palsu dapat dimanfaatkan untuk keadaan darurat misalnya jari

pengguna mengalami kerusakan dan tidak dapat diidentifikasi keunikanya. Begitu juga dengan *facelock* foto pengguna dapat digunakan pada keadaan tertentu seperti wajah pengguna mengalami perubahan dan tidak dapat dikenali.

Penulis menyarankan untuk menggunakan *lock screen* seperti *password, pattern,* atau Personal Identification Number (PIN) disamping penggunan *facelock* atau *fingerprint* agar *smarphone* lebih aman serta penggunaan fitur terbaru *facelock* yaitu *liveness detection*. Namun, fitur tersebut hanya tersedia pada sebagian *smartphone* karena masih tergolong teknologi yang baru. Kedepannya, percobaann selanjutnya dapat menggunakan model *smartphone* yang lebih beragam. Model *smartphone* yang dapat digunakan yaitu *smartphone-smartphone* terbaru yang beredar di pasar. Jenis serangan yang diuji coba juga dibuat lebih bervariasi.

DAFTAR REFERENSI

[1] Alabi, A. A., & Ogundoyin, I. K. A Simple Face-based Mobile Security System Design for Android Phone Protection. *International Journal of Computer Applications*. 2017; *161*(11): 17-23

[2] Yulianto, D. A. Berbagai Macam Pengunci Layar (Lock Screen) Smartphone. in *Prosiding KNPMP III*. 2018; 3: 549-556

[3] Patel, K., Han, H., & Jain, A. K. Secure face unlock: Spoof detection on smartphones. *IEEE transactions on information forensics and security*. 2016; *11*(10): 2268-2283.

[4] Gonzalo, R. B., Corsetti, B., Goicoechea-Telleria, I., Husseis, A., Liu-Jimenez, J., Sanchez-Reillo, R., ... & Azimi, M. (2018, October). Attacking a Smartphone Biometric Fingerprint System: A Novice's Approach. In *2018 International Carnahan Conference on Security Technology (ICCST). IEEE.* 2018: 1-5.

[5] Gupta, S., Anand, S., & Rai, A. (2017). Fingerprint extraction using smartphone camera. *arXiv preprint arXiv:1708.00884*. 2017: 1-11

[6] Quiring, E., & Kirchner, M. Fragile sensor fingerprint camera identification. In *2015 IEEE International Workshop on Information Forensics and Security (WIFS)*. IEEE. November, 2015: 1-6

[7] Zhang, Y., Xia, P., Luo, J., Ling, Z., Liu, B., & Fu, X. Fingerprint attack against touch-enabled devices. In *Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices.* October, 2012: 57-68.

[8] Akhtar, Z., & Foresti, G. L. Face spoof attack recognition using discriminative image patches. *Journal of Electrical and Computer Engineering*. 2016; *2016*: 1-14

[9] Kim, S., Ban, Y., & Lee, S. Face liveness detection using a light field camera. *Sensors*. 2014; *14*(12): 22471-22499.

[10] Macharia, P., Muiruri, P., Kumar, P., Ngari, B., & Wario, R. The feasibility of using an android-based infant fingerprint biometrics system for treatment follow-up. In *2017 IST-Africa Week Conference (IST-Africa)*. IEEE. May, 2017: 1-9

[11] Joshi, M., Mazumdar, B., & Dey, S. Security vulnerabilities against fingerprint biometric system. *arXiv preprint arXiv:1805.07116*. 2018: 1-27

[12] Maro, E. A., & Kovalchuk, M. M. (2018). Bypass Mobile Lock Systems with Gelatin Artificial Fingerprint. *Int. J. Comput. Sci. Eng.*. 2018; 6(6): 32–36

[13] Srilekha, R., & Jayakumar, D. A secure screen lock system for android smart phones using accelerometer sensor. *International Journal of Science Technology & Engineering*. 2015; *10*: 96-100.

[14] Amos, B., Ludwiczuk, B., & Satyanarayanan, M. Openface: A general-purpose face recognition library with mobile applications. *Tech. Rep. C. C. Sch. Comput. Sci.*. 2016; 16(118): 1–18.

[15] Zhang, Z., Yi, D., Lei, Z., & Li, S. Z. Face liveness detection by learning multispectral reflectance distributions. In *Face and Gesture 2011*. IEEE. March, 2011: 436-441.