Jurnal Ilmiah Ilmu Komputer Vol. 7, No. 2, September 2021 (P) ISSN 2442-451X
Fakultas Ilmu Komputer (O) ISSN 2503-3832
Universitas AL Asyariah Mandar

RANCANG BANGUN APLIKASI PDF SIGNER BERBASIS ANDROID PADA PDAM KABUPATEN TUBAN

Ikhsan Gustya Firmansyah[1], Raden Budiarto Hadiprakoso

[1,2]Kriptografi, Politeknik Siber dan Sandi Negara, Bogor, Indonesia
[1]ikhsan.gustya@student.poltekssn.ac.id, [2]raden.budiarto@poltekssn.ac.id,

ABSTRAK

Perusahaan Air Minum Daerah (PDAM) Kabupaten Tuban selama ini menggunakan prosedur tanda tangan secara manual dengan kertas dan pena sehingga terkadang hal ini dapat menghambat proses persuratan. Hal ini biasa terjadi ketika surat tersebut harus ditandatangani dan dikirim ke pihak atau bagian lain di hari yang sama sementara yang berwenang untuk menandatangani tidak ada di tempat. Terlebih pada situasi pandemi covid-19 seperti yang terjadi saat ini, di mana para pegawai dianjurkan untuk bekerja dari rumah. Berangkat dari masalah tersebut kami mengusulkan rancang bangun aplikasi PDF signer dengan metode pengenalan wajah sebagai proses otentikasi. Metode pengembangan aplikasi yang diusulkan menggunakan metodologi *prototyping*. Aplikasi dibuat berdasarkan arsitektur perangkat Android menggunakan bahasa pemrograman Java. Aplikasi yang dihasilkan memiliki fitur yaitu registrasi pengguna, login pengguna, view dokumen, dan tanda tangan dokumen. Aplikasi dibuat menggunakan basis data SQLcipher untuk menyimpan passphrase pengguna pada direktori root aplikasi yang memudahkan pengguna karena tidak perlu mengisi passphrase setiap akan melakukan tanda tangan.

Kata Kunci— pdf signer. Android, tanda tangan digital, prototipe.

ABSTRACT

The Regional Water Supply Company (PDAM) of Tuban Regency has been using a manual signature procedure with paper and pen so that sometimes this can hinder the correspondence process. This is common when the letter must be signed and sent to another party or department on the same day while the person authorized to sign it is not in place. Especially in the current situation of the COVID-19 pandemic, where employees are encouraged to work from home. Based on this problem, we propose the design of a PDF signer application with a facial recognition method as an authentication process. The proposed application development method uses a prototyping methodology. Applications are made based on the Android device architecture using the Java programming language. The resulting application has features, namely user registration, user login, document view, and document signature. The application is made using the SQLcipher database to store the user's passphrase in the root directory of the application which makes it easier for users because they do not need to fill in the passphrase every time they sign.

Keywords— pdf signer, Android, digital signature, prototyping

(P) ISSN 2442-451X
(O) ISSN 2503-3832

1. PENDAHULUAN

Perusahaan Daerah Air Minum (PDAM) Tirta Lestari Tuban merupakan perusahaan daerah yang bergerak pada bidang pengelolaan air bersih di Kabupaten Tuban. Hampir di semua kecamatan terdapat kantor unit PDAM Tuban. Hal ini bertujuan untuk mempermudah masyarakat dalam memperoleh pelayanan dan mempermudah pegawai di kantor PDAM tuban dalam melayani masyarakat. Oleh karena itu tidak sedikit pula laporan dari masyarakat yang harus diproses oleh bagian pelayanan dan diteruskan oleh bagian persuratan yang ada di kantor PDAM Tuban. Selain itu terdapat juga surat dari bagian lain yang harus ditandatangani oleh bagian yang terkait pada surat tersebut. Sampai saat ini PDAM Kabupaten Tuban masih menggunakan mekanisme tanda tangan secara manual sehingga terkadang hal ini dapat menghambat proses bisnis persuratan di kantor PDAM Kabupaten Tuban ketika surat tersebut harus ditandatangani dan dikirim ke pihak atau bagian lain di hari yang sama sementara yang berwenang untuk menandatangani tidak ada di tempat. Terlebih pada situasi pandemi covid-19 seperti yang terjadi saat ini, di mana para pegawai dianjurkan untuk bekerja dari rumah.

Terdapat beberapa mekanisme tanda tangan elektronik yang dapat digunakan seperti pada Adobe Acrobat. Proses tanda tangan dokumen pada aplikasi ini menggunakan sertifikat berformat p12 atau PKCS#12. Sertifikat p12 membutuhkan *passphrase* untuk digunakan sebagai akses *private key* sertifikat yang dapat menimbulkan kendala seperti lupa *passphrase* yang dimiliki pengguna. Oleh karena itu PDAM Kabupaten Tuban menginginkan adanya aplikasi yang berfungsi sebagai tanda tangan elektronik alternatif yang mudah digunakan.

Sistem otentikasi biometrik merupakan otentikasi menggunakan karakteristik setiap manusia secara fisik [1] maupun kebiasaan yang tak dapat berubah sehingga hal tersebut penting untuk identifikasi dan verifikasi [2]. Berdasarkan penelitian terkait otentikasi biometrik, terdapat banyak keunggulan dibandingkan dengan jenis otentikasi yang lain [2]. Salah satunya adalah otentikasi yang sulit untuk ditiru [3] Dari beberapa otentikasi biometrik yang ada, *face recognition* memiliki tingkat kesulitan yang tinggi untuk ditiru oleh orang lain. Hal ini dikarenakan setiap orang memiliki ciri-ciri fisik yang berbeda-beda. Penggunaan *face recognition* sebagai otentikasi biometrik juga sangat sederhana karena pengguna hanya perlu memindai wajah ke *tools* atau perangkat yang berfungsi untuk memindai wajah pengguna.

Pada penelitian sebelumnya terkait penggunaan digital *signature* menggunakan *face recognition* memiliki tingkat akurasi yang tinggi dan sulit untuk ditiru [4]. Hal ini membuat aplikasi *pdf signer* berbasis android untuk proses tanda tangan elektronik menggunakan *face recognition* sebagai persetujuan dan otentikasi dokumen perlu dibuat untuk memudahkan kantor PDAM Kabupaten Tuban dalam proses bisnis persuratan agar menjadi lebih mudah dan efisien.

2. TINJAUAN PUSTAKA

2.1. Face Recognition

Face recognition biasanya digunakan dalam keamanan sistem dan dapat dibandingkan dengan teknik biometrik yang lain seperti *fingerprint recognition* atau *iris recognition system* [5]. Setiap individu memiliki bentuk wajah yang unik, hal itu dapat menjadi profil biometrik untuk otentikasi yang aman. *Face recognition* biasanya memiliki empat fase atau langkah yang saling terkait. Fase pertama adalah deteksi wajah, yang kedua adalah normalisasi, ketiga adalah ekstraksi fitur, dan langkah terakhir adalah pengenalan wajah [6]. *Face recognition* dapat digunakan untuk mengidentifikasi seseorang melalui foto, video, atau mengidentifikasi secara langsung menggunakan alat atau aplikasi. *Face recognition* menggunakan algoritma komputer untuk mengambil detail wajah seseorang secara spesifik. Detail seperti jarak antara mata atau bentuk dagu dikonversikan menjadi representasi matematika dan dibandingkan dengan data atau wajah lain yang terdapat pada basis data dari *face recognition*.

2.2. Tanda Tangan Elektronik

Tanda tangan elektronik membantu memenuhi tiga aspek keamanan informasi, yaitu otentikasi, integritas, dan mekanisme anti sangkal (*non-repudiation*). Tanda tangan elektronik dapat digunakan pada domain tertutup di mana pengguna menyetujui protokol tanda tangan, memungkinkan identifikasi penandatanganan, membuat hubungan antara penandatanganan dan dokumen, dan mendeteksi setiap perubahan pada dokumen setelah tanda tangan diterapkan [7].

Dalam implementasinya penggunaan tanda tangan elektronik membutuhkan *certification authority (CA)*. CA memiliki wewenang untuk mengeluarkan sertifikat dan membantu pengguna dalam melakukan verifikasi terhadap sertifikat yang telah diterbitkan. Tanggung jawab dari CA ini berupa identifikasi identitas pengguna, memastikan informasi yang ada pada sertifikat benar adanya, serta menandatangani sertifikat yang telah diterbitkan [8]. Berikut adalah fungsi utama dari CA:

1. Membangkitkan kunci
2. Menerbitkan sertifikat digital
3. Verifikasi sertifikat
4. Pencabutan sertifikat

2.3. Penelitian Terkait

Pada makalah [9] membahas penelitian tentang penggunaan digital *signature* menggunakan metode *face recognition* sebagai otentikasinya. Penelitian ini juga memanfaatkan RSA *Encryption* sebagai pengamanan data selama transmisi terhadap jaringan yang tidak aman, kemudian Secure Hash Algorithm (SHA) yang digunakan pada digital *signature*. Penelitian ini berdasarkan perkembangan teknologi otentikasi biometrik yang

(P) ISSN 2442-451X
(O) ISSN 2503-3832

berkembang cukup pesat. Selain itu masalah otentikasi pada digital signature juga membuat penulis makalah ini membuat metode menggunakan *face recognition* sebagai otentikasinya. Pada makalah ini terfokus pada tahap-tahap penggunaan *face recognition* terhadap digital signature. Hasilnya sistem memvalidasi dataset wajah dengan akurasi sebanyak 96%.

Pada *paper* [10] membahas tentang studi komprehensif pada sistem otentikasi biometrik serta tantangan di masa depan. *Paper* ini diawali dengan jenis-jenis biometrik yang terbagi menjadi *Physiological* dan *Behavioral* yang kemudian menjelaskan bagaimana teknik biometrik pada setiap jenis dilakukan. Setelah itu pada *paper* ini dilakukan perbandingan berdasarkan atribut yang meliputi *circumvention, permanence, acceptability, uniqueness, universality, collectability,* dan *measurability. Paper* ini juga membahas bagaimana performa dari sistem biometrik menggunakan berbagai parameter, keuntungan dari penggunaan sistem biometrik, dan aplikasi yang dapat dikembangkan dengan menggunakan sistem biometrik.

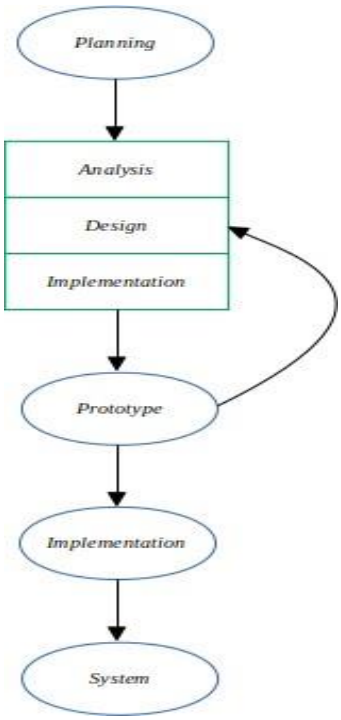
Pada makalah [11] membahas tentang implementasi otentikasi biometrik terhadap keamanan perangkat *mobile*. Pada penelitian ini juga menjelaskan keuntungan otentikasi biometrik dibandingkan dengan metode lain pada perangkat *mobile*. Mekanisme verifikasi otentikasi biometrik pada perangkat *mobile* juga dijelaskan pada makalah ini. Terdapat tantangan pada setiap metode otentikasi biometrik menunjukkan akan adanya teknik yang bervariasi pada masa depan

3. METODE YANG DIUSULKAN

Pada penelitian ini yang menjadi obyek penelitian adalah tanda tangan elektronik menggunakan *face recognition* pada PDAM Kabupaten Tuban di mana direktur dan kepala bagian selaku yang berwenang memberikan otentikasi dan persetujuan berupa tanda tangan pada setiap surat yang ada. Saat ini pada PDAM Kabupaten Tuban masih menggunakan cara manual yaitu dengan menggunakan tanda tangan basah sebagai proses otentikasi. Hal ini membuat proses bisnis pada perusahaan tersebut menjadi kurang efisien dan fleksibel terutama saat kondisi pandemi *COVID-19*. *Face recognition* dipilih karena memiliki tingkat kesulitan yang tinggi untuk ditiru oleh orang lain. Hal ini dikarenakan setiap orang memiliki ciri-ciri fisik yang berbeda-beda.

Desain penelitian yang digunakan adalah studi kasus dengan metode pengembangan perangkat lunak *Software Prototyping*. Metode ini digunakan agar aplikasi benar-benar sesuai dengan kebutuhan pada PDAM Tirta Lestari Kabupaten Tuban.

Gambar 1 menunjukkan tahapan dari metode pengembangan perangkat lunak *prototyping*. Gambar 1 menjelaskan di mana tahap *prototype* adalah hasil dari tahap *analysis, design*, dan *implementation* [12]. Ketika hasil dari *prototype* diberikan kepada pengguna namun belum sesuai dengan kebutuhan pengguna, maka proses akan kembali pada tahap sebelumnya sampai *prototype* sudah sesuai dengan kebutuhan dan menghasilkan sistem yang siap digunakan..



Gambar 1. Tahap-tahap dalam prototyping

Berikut merupakan penjelasan dari tahap-tahap pada *prototyping:*

a. *Planning*

Tahap ini adalah tahap awal dari *prototyping*. Pada tahap ini akan merencanakan spesifikasi apa saja yang diperlukan untuk membangun aplikasi.

b. *Analysis*

Pada tahap ini akan dilakukan pengumpulan data yang kemudian diolah menjadi kebutuhan fungsional dan kebutuhan non-fungsional. Hasil dari tahap ini adalah kebutuhan apa saja yang diperlukan pengguna yang harus ada pada aplikasi.

c. *Design*

Pada tahap ini akan dilakukan perancangan dari aplikasi yang akan dibuat menggunakan *Unified Modelling Language* (UML). Diagram UML yang akan digunakan pada penelitian ini menggunakan Use Case Diagram yang merupakan gambaran atau representasi dari interaksi yang terjadi antara sistem dan lingkungannya, Activity Diagram untuk menjelaskan aktivitas komputer maupun alur aktivitas pada sistem aplikasi, serta Sequence Diagram yang berfungsi untuk menggambarkan objek yang terlibat dalam sistem dan urutan pesan yang dipertukarkan antara objek yang diperlukan untuk menjalankan fungsionalitas sistem.

d. *Implementation*

(P) ISSN 2442-451X
(O) ISSN 2503-3832

Pada tahap ini mulai dibangun aplikasi yang sesuai dengan penelitian dan kebutuhan pengguna berdasarkan analisis serta desain UML yang telah dibuat pada tahap *design*. Pengujian juga dilakukan sehingga aplikasi dapat dianalisis kesesuaiannya dengan kebutuhan pengguna. Pengujian yang akan dilakukan meliputi unit testing, *integration* testing, dan *system testing* oleh pihak internal pada lokasi penelitian.

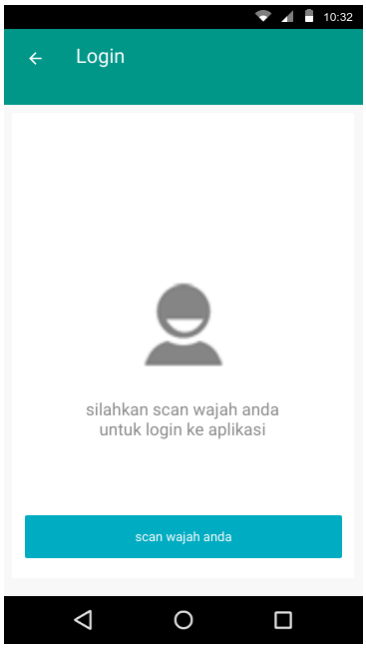
4. HASIL PENELITIAN

Pada tahap ini akan dijelaskan bagaimana aplikasi dijalankan untuk melakukan tanda tangan elektronik melalui perangkat *smartphone*. Aplikasi memiliki fitur yaitu registrasi pengguna, login pengguna, *view* dokumen, dan tanda tangan dokumen. Aplikasi dibuat menggunakan *database* SQLcipher untuk menyimpan *passphrase* pengguna pada direktori *root* aplikasi yang memudahkan pengguna karena tidak perlu mengisi *passphrase* setiap akan melakukan tanda tangan.

1. Proses registrasi

Proses registrasi berguna sebagai pendaftaran akun dan untuk *import* sertifikat elektronik ke direktori yang ada pada sistem dan template *face recognition* pengguna ke dalam *database*. Template *face recognition* ini bertujuan untuk pembatasan akses terhadap aplikasi dari pihak yang tidak memiliki wewenang pada aplikasi, kemudian untuk sertifikat elektronik yang telah di *import* merupakan sertifikat elektronik yang sesuai dengan akun yang digunakan untuk melakukan tanda tangan elektronik.

2. Proses *login*

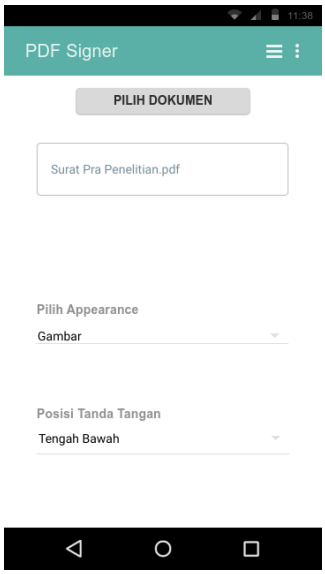


Gambar 2. Login menggunakan face recognition

Proses login menggunakan template *face recognition* pengguna yang tersimpan pada *keystore* yang terdapat pada perangkat android. Proses ini digunakan untuk pembatasan akses bagi pihak yang tidak memiliki wewenang mengakses aplikasi. Tampilan halaman login pengguna diilustrasikan seperti pada gambar 2

3. *View* dokumen

Proses *view* dokumen digunakan untuk menampilkan dokumen yang telah ditandatangani oleh pengguna. Dokumen yang telah ditandatangani disimpan pada direktori yang ditampilkan dalam bentuk *list* dokumen. Adapun tampilan seperti yang digambarkan pada gambar 3.

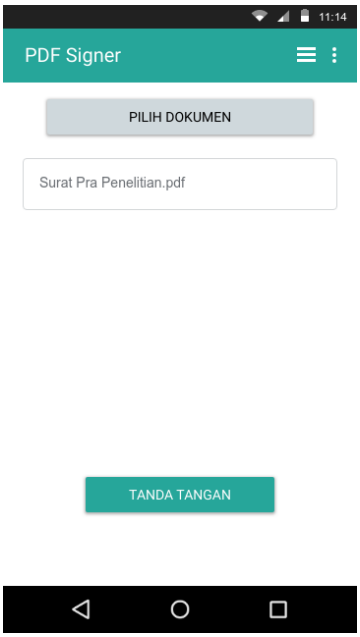


Gambar 3. Tampilan View dokumen

4. Proses tanda tangan dokumen

Pada proses ini, dokumen menggunakan *template face recognition* yang tersimpan pada *keystore*. Autentikasi *face recognition* pada fitur ini digunakan untuk mengakses proses tanda tangan dan mengambil *passphrase* pada *database* SQLcipher.

(P) ISSN 2442-451X
(O) ISSN 2503-3832



Gambar 4. Halaman tanda tangan dokumen

Proses tanda tangan pada implementasi dilakukan secara *selfsign* atau tanpa pemeriksaan terhadap status dari sertifikat yang digunakan untuk tanda tangan elektronik. Tampilan dari halaman tanda tangan dokumen ini digambarkan seperti pada gambar 4.

Tanda tangan dapat dilakukan dengan cara memilih dokumen yang telah ditambahkan ke dalam aplikasi. Setelah pengguna memilih file yang ditandatangani maka pengguna dapat melakukan proses tanda tangan dengan *scanning face recognition*. Tanda tangan akan diproses apabila pengguna melakukan *scanning face recognition* dengan benar dan sesuai. Apabila proses *scanning face recognition* tidak sesuai maka akan muncul notifikasi atau *toast* yang memberitahu bahwa *face recognition* tidak sesuai dan proses tanda tangan dokumen tidak dapat dilanjutkan.

Setelah aplikasi berhasil diimplementasikan, tahap berikut adalah pengujian terhadap penerimaan pengguna. *User acceptance testing* (UAT) adalah pengujian yang dilakukan oleh pengguna berdasarkan hasil dari sistem yang dibuat. Data proses UAT ini dilakukan dengan mengirimkan dan mendemonstrasikan aplikasi kepada Kepala Bagian Kepegawaian dan Direktur PDAM Air Minum Tirta Lestari Kabupaten Tuban. Berdasarkan pengujian yang dilakukan didapatkan hasil sebagai berikut:

Tabe1 Hasil *user acceptance testing*

Kebutuhan	Status	Keterangan
Kontrol akses pada aplikasi menggunakan *face recognition*	Sesuai	Sistem sudah sesuai yaitu menggunakan *face recognition* sebagai kontrol akses
Aplikasi dapat melakukan tanda tangan dokumen	Sesuai	Aplikasi dapat melakukan tanda tangan dokumen dengan sesuai
Fungsi tanda tangan aplikasi menggunakan otentikasi *face recognition*	Sesuai	Aplikasi sudah dapat melakukan tanda tangan dengan otentikasi *face recognition*

5. KESIMPULAN

Berdasarkan dari penelitian yang telah dilaksanakan dapat disimpulkan kesimpulan sebagai berikut. Aplikasi PDF *Signer* dibangun menggunakan bahasa pemrograman Java Android untuk perangkat *smartphone* android. Aplikasi PDF *Signer* dibangun menggunakan otentikasi biometrik *face recognition* saat proses *login* dan tanda tangan dokumen Rangkaian proses tanda tangan pada sistem dilakukan menggunakan otentikasi biometrik. Data yang digunakan adalah data pengguna aplikasi yang telah disimpan pada perangkat android. Proses tanda tangan dan pengambilan *passphrase* dari *database* SQLCipher dapat dilakukan apabila pengguna dapat diotentikasi.

Aplikasi yang dibangun masih dapat dikembangkan dan dapat digunakan sebagai penelitian lanjutan. Saran untuk pengembangan lebih lanjut adalah sebagai berikut. Aplikasi saat ini masih menggunakan *random certification authority*. Hal ini dapat dilakukan pengembangan seperti penggunaan *certificate authority* dari Balai Sertifikasi Elektronik atau menggunakan dari yang terdaftar pada Kementerian Komunikasi dan Informatika.

Daftar Pustaka

[1] Neal, T. J., & Woodward, D. L, "Surveying Biometric Authentication for Mobile Device Security," Journal of Pattern Recognition Research, 2016.

[2] Harakannanavar, S. S., Renukamurthy, P. C., & Raja, K. B., "Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends," International Journal of Advanced Networking and Applications, 2019

[3] D. Wen, "Face Spoof Detection with Image Distortion Analysis," *IEEE Biometrics Compendium*, vol. 10, no. 4, pp. 746 - 761, 2015.

(P) ISSN 2442-451X
(O) ISSN 2503-3832

[4] Ahmed, A., Hasan, T., Abdullatif,, M. & Rahim, M. S. M, "A Digital Signature System Based on Real Time Face Recognition," IEEE 9th International Conference on System Engineering and Technology (ICSET), 2019

[5] B. Setiawan, "Face Anti-spoofing based on Color Texture Analysis," *22nd IEEE International Conference on Image Processing (ICIP)*, Chicago, 2015.

[6] Y. A. Rahman, M. Liu and L. M. Po, "Deep learning for face anti-spoofing: An end-to-end approach," *Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA)*, Hong Kong, 2017.

[7] E. Alexey, "Algorithm for optimization of Viola–Jones object detection framework parameters," *Journal of Physics Conference Series*, no. 1, p. 945, 2018.

[8] Z. Boulkenafet, J. Komulainen and A. Hadid, "Face Anti-Spoofing Based on Color Texture Analysis," *Machine Vision Research*, vol. 1, 2015.

[9] R. Hasan, H. Mahmud and X. Y. Li, "Face Anti-Spoofing Using Texture-Based Techniques and Filtering Methods," *Journal of Physics: Conference Series*, 2019.

[10] I. B. Kusuma, A. Kartika, T. A. Budi, K. N. Ramadhani and F. Sthevanie, "Image Spoofing Detection Using Local Binary Pattern and Local Binary Pattern Variance," *International Journal on Information and Communication Technology (IJoICT)*, vol. 4, no. 2, pp. 11-18, 2018.

[11] K. Larbi, W. Ouarda, H. Drira, B. B. Amor and C. B. Amar, "DeepColorFASD: Face Anti Spoofing Solution Using a Multi Channeled Color Spaces CNN," *International Conference on Systems, Man, and Cybernetics (SMC)*, Miyazaki, 2018.

[12] A. Anjos, J. Komulainen, S. Marcel, A. Hadid and M. Pietik, "Face Anti-spoofing: Visual Approach," Handbook *of Biometric Anti-Spoofing: Trusted Biometrics under Spoofing Attacks*, London, Springer, 2014, pp. 65-82.