FACE PRESENTATION ATTACK DETECTION MENGGUNAKAN METODE LOCAL BINARY PATTERN DAN RESTRICTED BOLTZMANN MACHINES

SKRIPSI

diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Komputer Program Studi Ilmu Komputer

oleh

Nur ‘Aisyah Nadiyah

1705509

PROGRAM STUDI ILMU KOMPUTER

DEPARTEMEN PENDIDIKAN ILMU KOMPUTER

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2021

FACE PRESENTATION ATTACK DETECTION MENGGUNAKAN METODE LOCAL BINARY PATTERN DAN RESTRICTED BOLTZMANN MACHINES

oleh

Nur ‘Aisyah Nadiyah

Sebuah skripsi yang diajukan untuk memenuhi sebagian syarat untuk memperoleh gelar Sarjana Komputer Program Studi Ilmu Komputer

NUR 'AISYAH NADIYAH

FACE PRESENTATION ATTACK DETECTION* MENGGUNAKAN METODE *LOCAL BINARY PATTERN* DAN *RESTRICTED BOLTZMANN MACHINES

disetujui dan disahkan oleh pembimbing:

Pembimbing I,

Lala Septem Riza, M.T., Ph.D.
NIP. 197809262008121001

Pembimbing II,

Dr. Anto Satriyo Nugroho, B.Eng., M.Eng.
NIP. 197010211989111001

Mengetahui,

Ketua Program Studi Ilmu Komputer

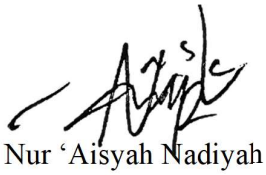
Dr. Rani Megasari, M.T.
NIP. 198705242014042002

PERNYATAAN

Dengan ini penulis menyatakan bahwa skripsi dengan judul "*Face Presentation Attack Detection* Menggunakan Metode *Local Binary Pattern* dan *Restricted Boltzmann Machines*" ini beserta seluruh isinya adalah benar-benar karya penulis sendiri. Penulis tidak melakukan penjiplakan atau pengutipan dengan cara-cara yang tidak sesuai dengan etika ilmu yang berlaku dalam masyarakat keilmuan. Atas pernyataan ini, penulis siap menanggung risiko/sanksi apabila di kemudian hari ditemukan adanya pelanggaran etika keilmuan atau ada klaim dari pihak lain terhadap keaslian karya penulis ini.

Bandung, Juni 2021

Yang membuat pernyataan,



Nur 'Aisyah Nadiyah

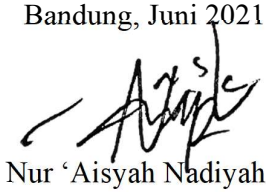
UCAPAN TERIMA KASIH

Pada proses penelitian penulis tentu tidak dapat menyelesaikan tanpa bantuan dan bimbingan dari berbagai pihak baik secara langsung maupun tidak langsung. Oleh karena itu penulis mengucapkan terimakasih yang sebesar-besarnya kepada:

1. Orang tua serta kakak dan adik penulis yang sudah membantu dan memberikan dorongan serta doa kepada penulis.
2. Bapak Lala Septem Riza, M.T., Ph.D. selaku pembimbing I, yang telah meluangkan waktu untuk membimbing penelitian dan penulisan skripsi ini.
3. Bapak Dr. Anto Satriyo Nugroho, B.Eng., M.Eng. selaku pembimbing II, yang telah meluangkan waktu untuk membimbing penelitian dan juga penulisan skripsi ini.
4. Ibu Dr. Rani Megasari, S.Kom., M.T. selaku Ketua Program Studi Ilmu Komputer.
5. Bapak dan Ibu Dosen Prodi Pendidikan Ilmu Komputer dan Ilmu Komputer yang telah memberikan ilmu yang bermanfaat kepada penulis selama masa perkuliahan.
6. Pihak *OULU University*, Finland dan *Northwestern Polytechnical University*, China yang telah menyediakan dan bersedia mengizinkan penggunaan data penelitian.
7. Teman-teman yang telah membantu proses penelitian dan mendukung penulis dalam melakukan penelitian.
8. Seluruh pihak lainnya yang tidak dapat penulis sebutkan satu persatu yang telah membantu dalam proses penelitian.

Semoga segala perbuatan, dukungan, dan doa yang telah diberikan mendapatkan balasan yang berlipat dari Allah SWT. Aamiin.

Bandung, Juni 2021



Nur ‘Aisyah Nadiyah

FACE PRESENTATION ATTACK DETECTION MENGGUNAKAN METODE *LOCAL BINARY PATTERN* DAN *RESTRICTED BOLTZMANN MACHINES*

oleh

Nur 'Aisyah Nadiyah – aisyahnan@upi.edu

1705509

ABSTRAK

Sistem pengenalan wajah saat ini sudah sangat banyak digunakan untuk pengamanan sistem, namun sistem ini merupakan biometrik yang rentan karena paling mudah dimanipulasi. Dari masalah ini, penelitian tentang *face presentation attack detection* dilakukan dengan harapan model yang dibangun dapat digunakan pada sistem pengenalan wajah sebagai alat pendeteksi serangan pemalsuan wajah dengan fokus penelitian pada jenis serangan *photo-attack* dan *video-attack*. Model ini dibangun menggunakan data yang berasal dari *database* OULU-NPU yang diproses *frame* per *frame* sebagai data yang independen. Algoritma *Local Binary Pattern* (LBP) dan *Restricted Boltzmann Machines* (RBM) digunakan sebagai metode ekstraksi fitur dari citra wajah. LBP digunakan untuk mengekstraksi fitur tekstur dari citra wajah, sedangkan RBM digunakan untuk mencari pola hubungan dari citra. Hasil evaluasi model menunjukkan model dengan ekstraksi fitur LBP-RBM berhasil mencapai akurasi sebesar 90% dan model dengan ekstraksi fitur RBM mencapai akurasi sebesar 95%. Sedangkan model terbaik diperoleh saat metode ekstraksi fitur dilakukan dengan mengimplementasikan algoritma LBP dengan tingkat akurasi yang dihasilkan mencapai 98%.

Kata Kunci: *Presentation Attack Detection*, LBP, RBM.

FACE PRESENTATION ATTACK DETECTION USING LOCAL BINARY PATTERN AND RESTRICTED BOLTZMANN MACHINES METHOD

Arranged by

Nur 'Aisyah Nadiyah – aisyahnan@upi.edu

1705509

ABSTRACT

Face recognition systems are currently used widely for system security, but this system is a vulnerable biometric because it is the easiest to manipulate. Based on this problem, research on face presentation attack detection is carried out with the hope that the built model can be used in face recognition systems as a tool for detecting face forgery attacks with research focus on photo-attack and video-attack types. This model is built using data from the OULU-NPU database which is processed frame by frame as independent data. Local Binary Pattern (LBP) and Restricted Boltzmann Machines (RBM) algorithms are used as methods for extracting feature of face images. LBP is used to extract texture features of face images, while RBM is used to find relationship patterns of images. The results of model evaluation show that the model with LBP-RBM feature extraction achieves an accuracy of 90% and the model with RBM feature extraction achieves an accuracy of 95%. The best model is obtained when feature extraction method is carried out by implementing the LBP algorithm with an accuracy rate of 98%.

Keywords: *Presentation Attack Detection*, LBP, RBM.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

LAMPIRAN

DAFTAR PUSTAKA

Aggarwal, C. C. (2018a). *An Introduction to Neural Networks BT - Neural Networks and Deep Learning: A Textbook* (C. C. Aggarwal (ed.); pp. 1–52). Springer International Publishing. https://doi.org/10.1007/978-3-319-94463-0_1

Aggarwal, C. C. (2018b). Neural Networks and Deep Learning: A Textbook. In *Artificial Intelligence*.

Aggarwal, C. C. (2018c). *Teaching Deep Learners to Generalize BT - Neural Networks and Deep Learning: A Textbook* (C. C. Aggarwal (ed.); pp. 169–216). Springer International Publishing. https://doi.org/10.1007/978-3-319-94463-0_4

Atoum, Y., Liu, Y., Jourabloo, A., & Liu, X. (2017). Face anti-spoofing using patch and depth-based CNNs. *2017 IEEE International Joint Conference on Biometrics (IJCB)*, 319–328. https://doi.org/10.1109/BTAS.2017.8272713

Bonetto, R., & Latzko, V. (2020). *Chapter 8 - Machine learning* (F. H. P. Fitzek, F. Granelli, & P. B. T.-C. in C. N. Seeling (eds.); pp. 135–167). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-820488-7.00021-9

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2016). Face Spoofing Detection Using Colour Texture Analysis. *IEEE Transactions on Information Forensics and Security*, *11*(8), 1818–1830. https://doi.org/10.1109/TIFS.2016.2555286

Boulkenafet, Z., Komulainen, J., & Hadid, A. (2015). Face Anti-Spoofing Based on Color Texture Analysis. *2015 IEEE International Conference on Image Processing (ICIP)*, 2636–2640. https://doi.org/10.1109/ICIP.2015.7351280

Boulkenafet, Z., Komulainen, J., Li, L., Feng, X., & Hadid, A. (2017). OULU-NPU: A Mobile Face Presentation Attack Database with Real-World Variations. *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, 612–618. https://doi.org/10.1109/FG.2017.77

Burt, C. (2019). *Web Video, Photos, or Siblings Can Spoof Samsung Galaxy S10*

Facial Recognition. Biometric Update. https://www.biometricupdate.com/201903/web-video-photos-or-siblings-can-spoof-samsung-galaxy-s10-facial-recognition

Cauchy, A.-L. (1847). Methode generale pour la resolution des systemes d'equations simultanees. *C.R. Acad. Sci. Paris*, *25*, 536–538. http://ci.nii.ac.jp/naid/10026863174/en/

Chao, W.-L. (2017). Face Recognition. *GICE*, *1*, 35–39. https://doi.org/https://doi.org/10.1109/ICISC.2018.8399108

Chingovska, I., Anjos, A., & Marcel, S. (2012). On The Effectiveness of Local Binary Patterns in Face Anti-Spoofing. *2012 BIOSIG - Proceedings of the International Conference of Biometrics Special Interest Group (BIOSIG)*, 1–7.

Costa-Pazo, A, Bhattacharjee, S., Vazquez-Fernandez, E., & Marcel, S. (2016). The Replay-Mobile Face Presentation-Attack Database. *2016 International Conference of the Biometrics Special Interest Group (BIOSIG)*, 1–7. https://doi.org/10.1109/BIOSIG.2016.7736936

Costa-Pazo, Artur, Vazquez-Fernandez, E., Alba-Castro, J. L., & González-Jiménez, D. (2019). Challenges of face presentation attack detection in real scenarios. In *Advances in Computer Vision and Pattern Recognition*. Springer International Publishing. https://doi.org/10.1007/978-3-319-92627-8_12

da Silva, I. N., Spatti, D. H., Flauzino, R. A., Liboni, L. H. B., & dos Reis Alves, S. F. (2016). Artificial neural networks: A practical course. In *Artificial Neural Networks: A Practical Course*. https://doi.org/10.1007/978-3-319-43162-8

Erdogmus, N., & Marcel, S. (2013). Spoofing in 2D Face Recognition with 3D Masks and Anti-Spoofing with Kinect. *2013 IEEE Sixth International Conference on Biometrics: Theory, Applications and Systems (BTAS)*, 1–6. https://doi.org/10.1109/BTAS.2013.6712688

Fischer, A., & Igel, C. (2012). An Introduction to Restricted Boltzmann Machines. *CIARP*.

Fletcher, R. (1987). *Practical Methods of Optimization; (2nd Ed.)*. Wiley-Interscience.

Freitas Pereira, T. de, Komulainen, J., Anjos, A., De Martino, J. M., Hadid, A., Pietikäinen, M., & Marcel, S. (2014). Face liveness detection using dynamic texture. *EURASIP Journal on Image and Video Processing*, *2014*(1), 2. https://doi.org/10.1186/1687-5281-2014-2

Galbally, J., & Marcel, S. (2014). Face Anti-spoofing Based on General Image Quality Assessment. *2014 22nd International Conference on Pattern Recognition*, 1173–1178. https://doi.org/10.1109/ICPR.2014.211

Habibi Aghdam, H., & Jahani Heravi, E. (2017). Guide to Convolutional Neural Networks. In *Guide to Convolutional Neural Networks*. https://doi.org/10.1007/978-3-319-57550-6

He, D.-C., & Wang, L. (1991). Texture Features Based on Texture Spectrum. *Pattern Recognition*, *24*(5), 391–399. https://doi.org/https://doi.org/10.1016/0031-3203(91)90052-7

Hernandez-Ortega, J., Fierrez, J., Morales, A., & Galbally, J. (2019). Introduction to face presentation attack detection. In *Advances in Computer Vision and Pattern Recognition*. Springer International Publishing. https://doi.org/10.1007/978-3-319-92627-8_9

Hinton, G. E. (2007). Boltzmann Machine. *Scholarpedia*, *2*, 1668. https://doi.org/doi::10.4249/scholarpedia.1668

Hinton, G. E. (2012). A practical guide to training restricted boltzmann machines. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *7700 LECTU*, 599–619. https://doi.org/10.1007/978-3-642-35289-8_32

Jain, A. K., Ross, A. A., & Nandakumar, K. (2011). *Introduction to Biometrics* (Vol. 53, Issue 9). Springer. https://doi.org/10.1007/978-0-387-77326-1

Jiang, X., Hadid, A., Pang, Y., & Granger, E. (2019). *Deep learning in object detection and recognition* (X. Feng (ed.)). Springer.

https://doi.org/10.1007/978-981-10-5152-4

Landau, L. D., & Lifshitz, E. M. (1980). *Chapter III - The Gibbs Distribution* (L. D. Landau & E. M. Lifshitz (eds.); pp. 79–110). Butterworth-Heinemann. https://doi.org/https://doi.org/10.1016/B978-0-08-057046-4.50010-5

Lecun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE*, *86*(11), 2278–2324. https://doi.org/10.1109/5.726791

LeCun, Y., Haffner, P., Bottou, L., & Bengio, Y. (1999). Object Recognition with Gradient-Based Learning. In *Shape, Contour and Grouping in Computer Vision* (Vol. 1681). Springer. https://doi.org/https://doi.org/10.1007/3-540-46805-6_19

Limonu, N. (2020, May 27). *Cegah Corona, Pemkab Maros Ganti Absen Fingerprint dengan Deteksi Wajah*. SINDONEWS.Com. https://makassar.sindonews.com/read/48886/713/cegah-corona-pemkab-maros-ganti-absen-fingerprint-dengan-deteksi-wajah-1590595554

Liu, S. Q., Yuen, P. C., Li, X., & Zhao, G. (2019). Recent progress on face presentation attack detection of 3D mask attacks. In *Advances in Computer Vision and Pattern Recognition*. Springer International Publishing. https://doi.org/10.1007/978-3-319-92627-8_11

Liu, Y., Jourabloo, A., & Liu, X. (2018). Learning Deep Models for Face Anti-Spoofing: Binary or Auxiliary Supervision. *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 389–398. https://doi.org/10.1109/CVPR.2018.00048

Marcel, S., Nixon, M. S., Fierrez, J., & Evans, N. (2019). *Handbook of Biometric Anti-Spoofing* (S. Singh, R. Vision, C. Donington, & S. B. Kang (eds.); 2nd ed.). Springer. https://doi.org/10.1007/978-3-319-92627-8

Newman, L. H. (2016). *Hackers Trick Facial-Recognition Logins With Photos From Facebook (What Else?)*. Wired. https://www.wired.com/2016/08/hackers-trick-facial-recognition-logins-

photos-facebook-thanks-zuck/

Ojala, T., Pietikäinen, M., & Harwood, D. (1994). Performance Evaluation of Texture Measures with Classification Based on Kullback Discrimination of Distributions. *Proceedings of 12th International Conference on Pattern Recognition*, *1*, 582–585 vol.1. https://doi.org/10.1109/ICPR.1994.576366

Ojala, T., Pietikäinen, M., & Maenpaa, T. (2002). Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *24*(7), 971–987. https://doi.org/10.1109/TPAMI.2002.1017623

Peng, F, Qin, L., & Long, M. (2018). CCoLBP: Chromatic Co-Occurrence of Local Binary Pattern for Face Presentation Attack Detection. *2018 27th International Conference on Computer Communication and Networks (ICCCN)*, 1–9. https://doi.org/10.1109/ICCCN.2018.8487325

Peng, Fei, Qin, L., & Long, M. (2020). Face presentation attack detection based on chromatic co-occurrence of local binary pattern and ensemble learning. *Journal of Visual Communication and Image Representation*, *66*, 102746. https://doi.org/https://doi.org/10.1016/j.jvcir.2019.102746

Phillips, P. J., Grother, P., & Micheals, R. (2011). *Evaluation Methods in Face Recognition BT - Handbook of Face Recognition* (S. Z. Li & A. K. Jain (eds.); pp. 551–574). Springer London. https://doi.org/10.1007/978-0-85729-932-1_21

Pietikäinen, M., Ojala, T., & Xu, Z. (2000). Rotation-Invariant Texture Classification Using Feature Distributions. *Pattern Recognition*, *33*(1), 43–52. https://doi.org/https://doi.org/10.1016/S0031-3203(99)00032-1

Pratomo, Y. (2019). *Pemindai Wajah di Puluhan Ponsel Ini Bisa Dibobol dengan Foto*. Kompas. https://tekno.kompas.com/read/2019/01/10/12140057/pemindai-wajah-di-puluhan-ponsel-ini-bisa-dibobol-dengan-foto

Rosmalia, P. (2020). *Biometrik Wajah Menjelma Kartu Identitas Warga*. Media

Indonesia. https://mediaindonesia.com/teknologi/349795/biometrik-wajah-menjelma-kartu-identitas-warga

Ruder, S. (2016). An overview of gradient descent optimization algorithms. *INSPIRE*, *abs/1609.0*. http://arxiv.org/abs/1609.04747

Rumelhart, D. E., Hinton, G. E., & Williams, R. J. (1986). Learning representations by back-propagating errors. *Nature*, *323*(6088), 533–536. https://doi.org/10.1038/323533a0

Saukani. (2020, August 27). *Masa Pandemi Covid-19, MIN 15 HSU Terapkan Absen Online*. https://kalsel.kemenag.go.id/berita/538686/Masa-Pandemi-Covid-19-MIN-15-HSU-Terapkan-Absen-Online

Smolensky, P. (1986). Information Processing in Dynamical Systems: Foundations of Harmony Theory. In *Parallel Distributed Proceuing: Explorations in the Microstructure of Cognition* (1st ed.). MIT Press/Bradford Books.

Souza, G. B. de, Papa, J. P., & Marana, A. N. (2018). Deep Discriminative Restricted Boltzmann Machine (DDRBM) for Robust Face Spoofing Detection. *Progress in Human Computer Interaction*, *1*(3), 1–8. https://doi.org/10.18063/phci.v1i3.893

Szeliski, R. (2011). Recognition. In D. Gries & F. B. Schneider (Eds.), *Computer Vision* (pp. 575–640). Springer. https://doi.org/10.1007/978-1-84882-935-0_14

Taud, H., & Mas, J. (2010). *Multilayer Perceptron (MLP), in Geomatic Approaches for Modeling Land Change Scenarios*. 451–455. http://www.dtreg.com/mlfn.htm

Wen, D., Han, H., & Jain, A. K. (2015). Face Spoof Detection With Image Distortion Analysis. *IEEE Transactions on Information Forensics and Security*, *10*(4), 746–761. https://doi.org/10.1109/TIFS.2015.2400395

Yang, J., Lei, Z., & Li, S. (2014). Learn Convolutional Neural Network for Face Anti-Spoofing. *CoRR*, *abs/1408.5*. http://arxiv.org/abs/1408.5601