ANALISIS IMPLEMENTASI CONTRAST LIMITED ADAPTIVE HISTOGRAM EQUALIZATION (CLAHE) UNTUK DETEKSI CITRA SIDIK JARI TIRUAN

Safira Nuraisha[1)], Sri Handayani[2)]

1)Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi Universitas Semarang, Indonesia

2) Teknik Informatika, Fakultas Teknologi Informasi dan Komunikasi, Universitas Semarang, Indonesia

E-mail : safira@usm.ac.id

Abstrak

Autentikasi biometrik dengan sidik jari paling sering digunakan untuk sistem keamanan atau autentikasi sebuah akun. Seiring dengan berkembangnya model sistem keamanan menggunakan autentikasi sidik jari, muncul masalah baru yaitu penggunaan sidik jari Penggunaan sidik jari palsu dapat dilakukan melalui scanner sidik jari yang menerima salinan dari sidik jari asli yang sering disebut dengan artificial fingerprints. Penggunaan sidik jari palsu dapat mengancam keamanan dari sebuah sistem. Permasalahan deteksi sidik jari dan identifikasi bahan yang dapat meniru karakteristik sidik jari diperburuk oleh dua hal, pertama, sensor standar tidak mampu membedakan citra dari sidik jari asli dan sidik jari replika. Kedua, seringkali tidak ada isyarat yang jelas bahwa citra tersebut berasal dari sidik jari replika atau dengan kata lain sidik jari replika yang sangat mirip dengan sidik jari asli sehingga sulit untuk dibedakan. Penelitian ini bertujuan untuk mendeteksi citra sidik jari tiruan dengan tingkat akurasi yang tinggi. Dataset yang digunakan merupakan dataset publik ATVS. Metode yang diusulkan yaitu ekstraksi fitur citra sidik jari dengan kontras GLCM (*Gray Level Co-Occurance Matrix*) dengan metode peningkatan kualitas citra CLAHE (*Contrast Limited Adaptive Histogram Equalization*). Hasil deteksi citra sidik jari menggunakan CLAHE menghasilkan akurasi yang lebih baik dibandingkan tanpa menggunakan CLAHE.

Kata Kunci: deteksi sidik jari tiruan, fake signature, *CLAHE*

Abstract

Biometric authentication with fingerprints is most often used for security systems or authentication of an account. Along with the development of a security system model using fingerprint authentication, a new problem arises, namely the use of fingerprints. The use of fake fingerprints can be done through a fingerprint scanner that accepts a copy of the original fingerprint which is often called artificial fingerprints. The use of fake fingerprints can threaten the security of a system. The problem of fingerprint detection and identification of materials that can mimic fingerprint characteristics is exacerbated by two things. First, the standard sensor is unable to distinguish the image from the original fingerprint and the replica fingerprint. Second, there is often no clear indication that the image comes from a replica fingerprint or in other words a replica fingerprint which is so similar to the original fingerprint that it is difficult to distinguish. This study aims to detect artificial fingerprint images with a high degree of accuracy. The dataset used is the ATVS public dataset. The proposed method is feature extraction of fingerprint images with GLCM contrast (Gray Level Co-Occurance Matrix) with the CLAHE (Contrast Limited Adaptive Histogram Equalization) image quality enhancement method. The results of fingerprint image detection using CLAHE produce better accuracy than without using CLAHE.

Keywords : fake fingerprint detection, fake signature, CLAHE

PENDAHULUAN

Sistem keamanan merupakan sebuah upaya yang dilakukan untuk mengamankan kinerja, fungsi, atau proses. Sistem keamanan berguna untuk menjaga sebuah sistem atau aplikasi agar kerahasiaan dari data yang disimpan didalamnya tidak disalahgunakan, diinterupsi, ataupun dimodifikasi yang pada akhirnya dapat merugikan pengguna sistem. Sistem keamanan yang paling umum digunakan adalah dengan menggunakan kata sandi atau *password*. Autentikasi pengguna dengan menggunakan *password* telah menjadi landasan keamanan sistem selama beberapa dekade. Konsep user id dan *password* merupakan metode yang efisien untuk mempertahankan kerahasiaan antara pengguna dan sistem. Resiko yang terkait dengan autentikasi berbasis kata sandi adalah meningkatnya jumlah pengguna sistem dengan lebih dari satu akun setiap pengguna menyebabkan pengguna harus selalu mengingat *password* dari setap akun yang berbeda[1]. Resiko yang kedua yaitu autentikasi dengan berbasis *password* mudah diretas apabila pengguna menggunakannya dalam jangka waktu yang lama, sehigga dianjurkan untuk mengubah *password* secara berkala. Kedua hal tersebut menunjukkan bahwa penggunaan *password* untuk sistem keamanan menjadi kurang efisien.

Salah satu sistem keamanan yang sudah berkembang pada saat ini adalah autentikasi biometrik. Autentikasi biometrik merupakan suatu metode yang secara otomatis selalu dimiliki dan menjadi ciri khas setiap manusia dengan menganalisa secara statistik dari karakteristik biologis manusia. Biometrik telah menarik perhatian yang signifikan karena biometrik menyederhanakan proses autentikasi dengan menghilangkan kebutuhan akan *password*. Biometriks memecahkan masalah dengan menggunakan berbagai karakteristik yang membedakan setiap individu, seperti : sidik jari, retina mata, wajah, dan suara. Dari beberapa karakteristik yang dimiliki setiap individu, sistem sidik jari yang paling sering digunakan untuk sistem keamanan atau autentikasi sebuah akun[2]. Keamanan menjadi fokus utama dalam aplikasi biometrik, tingkat keakuratan autentikasi dari sidik sangat penting untuk sistem yang memanfaatkan teknologi ini[3]. Sidik jari memiliki karakter yang unik dan dapat dibedakan antar satu individu dengan individu lain, sehingga sidik jari dapat diterima sebagai pengenal yang dapat dibedakan. Pada sidik

jari, terdapat bentuk yang disebut *ridges* dan *valley* yang menjadi pembeda dari setiap sidik jari individu[4].

Seiring dengan berkembangnya model sistem keamanan menggunakan autentikasi sidik jari, muncul masalah baru yaitu penggunaan sidik jari palsu. Scanner sidik jari dapat menerima salinan dari sidik jari asli yang sering disebut dengan artificial fingerprints. Penggunaan sidik jari palsu dapat mengancam keamanan dari sebuah sistem[4]. Permasalahan deteksi sidik jari dan identifikasi bahan yang dapat meniru karakteristik sidik jari diperburuk oleh dua hal, pertama, sensor standar tidak mampu membedakan citra dari sidik jari asli dan sidik jari replika. Kedua, seringkali tidak ada isyarat yang jelas bahwa citra tersebut berasal dari sidik jari replika atau dengan kata lain sidik jari replika yang sangat mirip dengan sidik jari asli sehingga sulit untuk dibedakan[5].

Penelitian mengenai klasifikasi sidik jari asli dan sidik jari palsu dapat membantu memecahkan masalah diatas. Adanya penelitian mengenai deteksi sidik jari palsu dapat membantu menekan kasus pemalsuan sidik jari yang dapat merugikan berbagai pihak, dengan menambahkan fitur untuk memeriksa citra sidik jari yang diinputkan termasuk sidik jari asli atau sidik jari tiruan[6]. Berdasarkan masalah tersebut, peneiti melakukan penelitian untuk mendeteksi suatu citra sidik jari termasuk sidik jari asli atau sidik jari tiruan. Langkah awal yang dilakukan yaitu mengenali karakteristik dari sidik jari asli atau sidik jari tiruan yang berasal dari berbagai bahan seperti silikon, latex, play-doh[2]. Selain mengidentifikasi bahan yang digunakan, sensor dari pengambilan citra sidik jari juga mempengaruhi kualitas dari citra sidik jari[7]. Perbedaan tersebut bisa diidentifikasi berdasarkan tingkat keabuan dari citra sidik jari[8]. Langkah selanjutnya yaitu proses perbaikan kualitas citra, reduksi noise, dan ekstraksi fitur dari citra sidik jari. Klasifikasi dilakukan dari hasil citra yang sudah melalui proses ekstraksi fitur, dan menghasilkan klasifikasi berupa sidik jari asli atau sidik jari tiruan.

Hasil review dari beberapa jurnal, masalah yang ditemui relatif sama yaitu sulitnya mengenali perbedaan karakteristik citra sidik jari asli atau sidik jari tiruan. Masalah tersebut dapat diselesaikan dengan mengkombinasikan beberapa metode preprocessing dan klasifikasi sidik jari. Pendekatan yang mungkin dilakukan berdasarkan masalah yang telah dianalisis dapat diselesaikan dengan mengkombinasikan beberapa metode preprocessing terutama pada fase

feature extraction dan *feature selection* untuk menemukan variabel yang paling tepat dalam membedakan karakteristik dari sidik jari asli atau sidik jari tiruan, serta meningkatkan akurasi pada proses klasifikasi citra sidik jari.

Pendekatan yang dilakukan dengan menggunakan metode CLAHE (*Contrast Limited Adaptive Histogram Equalization*) untuk peningkatan kualitas citra karena berdasarkan penelitian sebelumnya, CLAHE digunakan untuk meningkatkan kontras small tiles dari suatu gambar dan untuk menggabungkan tiles dari setiap ketetanggaan menggunakan interpolasi bilinear yang akan menghilangkan batas-batas yang diinduksi secara artificial [6].

METODE PENELITIAN

Metode penelitian yang digunakan dalam penelitian ini adalah metode penelitian dan pengembangan atau *Reasearch and Development* (R&D). Menurut Sugiono (2017) bahwa metode pengembangan merupakan metode penelitian yang digunakan untuk menghasilkan produk tertentu, dan menguji keefektifan produk tersebut.

Penentuan tahapan penelitian merupakan bagian yang penting dalam sebuah penelitian. Pada gambar 1 tampak tahapan penelitian menggambarkan urutan dari sebuah penelitian, dimulai dari pembacaan data sampai dengan tahapan terakhir yaitu evaluasi.

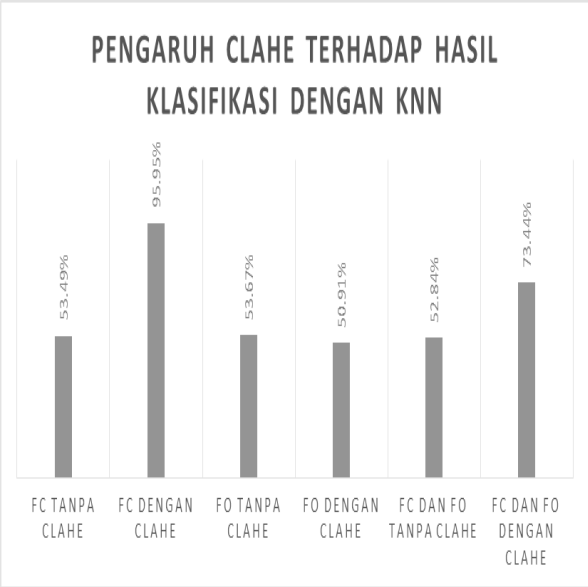
Gambar 1. Tahapan Penelitian

HASIL DAN PEMBAHASAN

Pada bagian analisa hasil penelitian, peneliti melakukan analisa berdasarkan hasil dari beberapa eksperimen yang telah dilakukan. Analisa yang dilakukan yaitu pengaruh metode CLAHE terhadap hasil klasifikasi, yang kedua, menentukan klasifier terbaik dalam kasus pengenalan sidik jari tiruan dengan dataset ATVS yang diambil dengan sensor biometrik dan sensor optik.

Peningkatan kualitas citra dengan CLAHE sangat mempengaruhi hasil klasifikasi

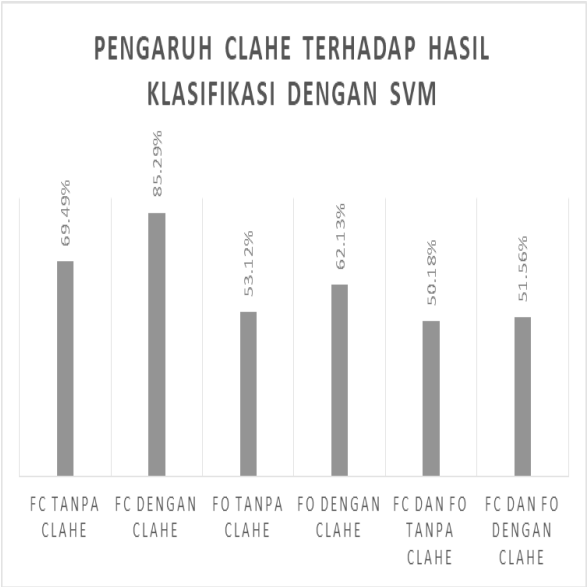
citra sidik jari asli serta tiruan, hal tersebut ditunjukkan pada grafik di gambar 2.



Gambar 2.Hasil Klasifikasi dengan KNN

Grafik gambar 2 diatas menunjukkan pengaruh CLAHE terhadap hasil klasifikasi dengan menggunakan klasifier KNN. Didapatkan hasil, dataset fc yang telah dilakukan peningkatan kualitas citra dengan CLAHE memiliki hasil akurasi terbaik yaitu sebesar 95.95%, dibandingkan dengan dataset fc yang tidak dilakukan CLAHE akurasi yang dihasilkan hanya sebesar 53.49%. Peningkatan hasil akurasi juga ditunjukkan pada dataset gabungan antara fc dan fo, yang sebelum ditambahkan CLAHE akurasinya sebesar 52.84% meningkat menjadi 73.44%.

Sama halnya dengan pengaruh CLAHE terhadap hasil klasifikasi dengan KNN, dengan menggunakan klasifier SVM, akurasi yang dihasilkan mengalami peningkatan, seperti pada grafik di gambar 3 bawah ini:



Gambar 3. Hasil Klasifikasi dengan SVM

Akurasi tertinggi dihasilkan oleh dataset fc dengan penambahan CLAHE yaitu sebesar 85.29%. Dataset fo serta gabungan antara dataset fo dan fc juga mengalami peningkatan setelah penambahan metode CLAHE. Dataset fo, setelah penambahan CLAHE memiliki akurasi sebesar 62.13% sedangkan gabungan antara dataset fo dan fc sebesar 51.56%.

Peningkatan akurasi setelah penambahan CLAHE juga ditunjukkan pada hasil akurasi dengan klasifier NN. Akurasi paling tinggi pada dataset fc dengan penambahan CLAHE yaitu sebesar

97.74%. Seperti yang ditunjukkan pada grafik di gambar 4, semua dataset yang ditambahkan CLAHE mengalami peningkatan akurasi.

Gambar 4. Hasil Klasifikasi dengan NN

Berdasarkan semua eksperimen yang dilakukan untuk melihat pengaruh CLAHE terhadap hasil klasifikasi, hampir seluruh eksperimen menunjukkan bahwa CLAHE dapat meningkatkan akurasi. Dari 9 percobaan yang dilakukan dengan beberapa kombinasi dataset fc dan fo, 8 diantaranya menunjukkan peningkatan hasil akurasi, digambarkan pada grafik gambar 5.

Kesimpulan yang dapat diambil dari eksperimen pertama ini yaitu, metode CLAHE dapat meningkatkan hasil akurasi pada saat klasifikasi.

Gambar 5. Hasil Klasifikasi

SIMPULAN

Dari Penelitian ini maka diperoleh beberapa kesimpulan yang telah menunjukkan bahwa pemalsuan sidik jari dapat dideteksi melalui metode yang telah diusulkan secara baik. Kualitas citra sidik jari yang buruk pada penelitian ini dapat ditingkatkan dengan metode CLAHE (*Contrast Limited Adaptive Histogram Equalization*) dimana sistem deteksi ini dapat dengan mudah digunakan untuk mendeteksi sidik jari asli dan tiruan dan metode CLAHE yang digunakan dalam sistem ini dapat meningkatkan akurasi

dari klasifikasi citra sidik jari asli dan citra sidik jari tiruan.

UCAPAN TERIMAKASIH

Ucapan Terima Kasih dihaturkan untuk :

1. Rektor Universitas Semarang (USM), Andy Kridasusila, S.E.,M.M
2. Dekan Fakultas Teknologi Informasi dan Komunikasi (FTIK) USM, Susanto, S.Kom.,M.Kom
3. Iswoyo, S.Pt., M.P selaku Ketua Lembaga Penelitian dan Pengabdian Kepada Masyarakat (LPPM) USM.

DAFTAR PUSTAKA

[1] A. Conklin, G. Dietrich, D. Walz, N. L. West, and S. Antonio,2004,Password-Based Authentication : A System Perspective, vol. 0, no. C, pp. 1–10.

[2] S. B. N. Ã and S. Agarwal, 2009 Neurocomputing Ridgelet-based fake fingerprint detection, vol. 72, pp. 2491–2506.

[3] A. Chaudhari and P. J. Deore, 2012, Prevention of spoof attacks in fingerprinting using histogram features, pp. 6–8.

[4] I. Conference, N. Security, S. Ap, and T. Coimbatore, 2015, A Comparative Study on the Swarm Intelligence Based Feature Selection Approaches for Fake And Real Fingerprint Classification.

[5] A. Rattani, Z. Akhtar, and G. L. Foresti, 2015, A Preliminary Study on Identifying Fabrication Material from Fake Fingerprint Images, pp. 1–5.

[6] S. S. Kulkarni, 2016, A Fingerprint Spoofing Detection System Using LBP.

[7] A. Rattani, W. J. Scheirer, and A. Ross, 2015, Open Set Fingerprint Spoof Detection Across Novel Fabrication Materials," vol. 10, no. 11, pp. 2447–2460.

[8] K. Abhishek and A. Yogi, 2015, A Minutiae Count Based Method for Fake Fingerprint Detection," Procedia - Procedia Comput. Sci., vol. 58, pp. 447–452.

[9] Q. Huang, S. Chang, C. Liu, B. Niu, M. Tang, and Z. Zhou, 2015, An evaluation of fake fingerprint databases utilizing SVM classification," Pattern Recognit. Lett., vol. 60–61, pp. 1–7.

[10] P. O. R. D, M. Z. E, P. O. J. C, R. A. J. M, G. H. E, F. De Informática, C. Juriquilla, and U. A. De Querétaro, 2014, A Feature Extraction Using SIFT with a Preprocessing by Adding CLAHE Algorithm to Enhance Image Histograms, pp. 20–25.

[11] M. Sepasian, C. Mares, S. M. Azimi, and W. Balachandran, Image Enhancement for Minutiae-Based Fingerprint Identification.