ABSTRACT

Fingerprint has a competent level of uniqueness because various features can form a different pattern in each individual. It is a verification requirement in various multiple, such as mobile phones, banking accounts, attendance, etc. This information will then be processed to generate more factual, accurate data. Besides fingerprint recognition can improve security, the scheme turns out to be vulnerable to attacks at the sensor level. Studies have shown that it is possible to trick various fingerprint scanners by using well duplicated synthetic fingers such as gelatin, latex, eco flex, playdoh, wood glue, etc. These materials are humidity-based, and most fingerprint scanners can visualize the preventive measures in maintaining the performance is liveness detection. Liveness detection is proposed to identify this kind of spoof attracts to improve security for the fingerprint recognition system. Liveness detection is a function that determines whether the presented biometric sample originated from a live body. Thus, we deep exploited the handcrafted process to achieve adequate performance. We conjugate the spatial and frequency domain in pixel neighborhood distribution using local binary pattern and phase quantization feature. Meanwhile, in preprocessing, we use image translation to make more variation images. And to encapsulate the noise possibility, we added the wavelet transform as the noise removal. Finally, we map the learning stage using a prominent machine learning way, i.e., support vector machine (SVM). Our experiment is evaluated with accuracy and average error rate. The proposed method has achieved sustainable results in terms of reduction in average error rates 4.2, 2.1, and 5.1 on LivDet 2011, LivDet 2013, and LivDet 2015.

Keywords: Fingerprints; Liveness Detection; Fake; Live; Wavelet; LBP; LPQ;

ABSTRAKSI

Sidik jari memiliki tingkat keunikan yang mumpuni karena berbagai fitur dapat membentuk pola yang berbeda pada setiap individu. Ini adalah persyaratan verifikasi di berbagai kelipatan, seperti ponsel, rekening bank, kehadiran, dll. Informasi ini kemudian akan diproses untuk menghasilkan data yang lebih faktual dan akurat. Selain pengenalan sidik jari dapat meningkatkan keamanan, skema tersebut ternyata rentan terhadap serangan di level sensor. Penelitian telah menunjukkan bahwa adalah mungkin untuk mengelabui berbagai pemindai sidik jari dengan menggunakan jari sintetis yang diduplikasi dengan baik seperti gelatin, lateks, eco flex, playdoh, lem kayu, dll. Bahan-bahan ini berbasis kelembaban, dan sebagian besar pemindai sidik jari dapat memvisualisasikan tindakan pencegahan dalam menjaga kinerja adalah deteksi keaktifan. Deteksi liveness diusulkan untuk mengidentifikasi atraksi spoof semacam ini untuk meningkatkan keamanan sistem pengenalan sidik jari. Deteksi keaktifan adalah fungsi yang menentukan apakah sampel biometrik yang disajikan berasal dari tubuh hidup. Dengan demikian, kami mengeksploitasi proses buatan tangan secara mendalam untuk mencapai kinerja yang memadai. Kami mengkonjugasikan domain spasial dan frekuensi dalam distribusi lingkungan piksel menggunakan pola biner lokal dan fitur kuantisasi fase. Sedangkan pada preprocessing, kita menggunakan image translation untuk membuat gambar yang lebih bervariasi. Dan untuk merangkum kemungkinan noise, kami menambahkan transformasi wavelet sebagai penghilangan noise. Terakhir, kami memetakan tahap pembelajaran menggunakan cara pembelajaran mesin yang menonjol, yaitu, mendukung mesin vektor (SVM). Eksperimen kami dievaluasi dengan akurasi dan tingkat kesalahan rata-rata. Metode yang diusulkan telah mencapai hasil yang berkelanjutan dalam hal pengurangan tingkat kesalahan rata-rata 4.2, 2.1, dan 5.1 pada LivDet 2011, LivDet 2013, dan LivDet 2015.