RINGKASAN

DETEKSI SPOOF MENGGUNAKAN METODE ANALISIS TEKSTUR WARNA

Triska Arum Sari MK

Sistem keamanan digital telah dirancang sedemikian rupa untuk menghindari kejahatan digital. Namun, masih banyak ancaman bagi pengguna yang dapat terjadi. Salah satunya adalah *face spoofing*, dimana seseorang berpura-pura sebagai orang lain dengan menggunakan metode serangan statik 2D untuk dapat menembus sitsem biometrik secara ilegal. Serangan 2D dapat berupa foto maupun video tayangan ulang yang ditampilkan kembali oleh perangkat dengan spesifikasi terbaik untuk memaksimalkan kemungkinan berhasil. Untuk mengatasi hal tersebut, penelitian deteksi *face spoofing* menggunakan analisis tekstur warna dilakukan.

Penelitian dimulai dengan mempelajari perbedaan reproduksi warna (gamut) antara wajah asli dengan cetak foto hasil tangkapan kamera dari beberapa perangkat dan tampilan video tayangan ulang yang terkumpul dalam dataset *OULU-NPU*. Informasi tekstur warna *luminance* dan *chrominance* dari setiap gambar kategori *real* dan *attack* diekstraksi menggunakan deskriptor *local binary pattern*. Hasil ekstraksi fitur tersebut selanjutnya digunakan oleh algoritma pengklasifikasi untuk melakukan deteksi.

Beberapa algoritma *machine learning* dilatih menggunakan 240 gambar kategori *real* dan 872 gambar kategori *attack*. Algoritma terbaik yang didapat untuk melakukan deteksi *face spoofing* adalah SVM kernel polimonial dan *Multilayer Perceptron* dengan menetapkan 3 *hidden layer* dan *hyperbolic tangen* sebagai fungsi aktifasinya. Manipulasi serangan pada kategori *attack* merupakan kumpulan tangkapan gambar wajah asli yang dicetak menggunakan kertas glossy berukuran A3 dan tangkapan video yang diputar ulang dengan perangkat berbeda.

Kata kunci : *face spoofing detection*, tekstur warna, *local binary pattern*

SUMMARY

SPOOF DETECTION USING COLOR TEXTURE ANALYSIS

Triska Arum Sari MK

Digital security systems have been designed in such a way to avoid digital crimes. However, there are still many threats to users that can occur. One of them is face spoofing, where someone pretends to be someone else by using 2D static attack methods to illegally penetrate biometric systems. A 2D attack can be a photo or video replay that is replayed by the best specs device to maximize the chances of success. To overcome this, research on face spoofing detection using color texture analysis was carried out.

The research began by studying the difference in color reproduction (gamut) between real faces and printed photos captured by cameras from several devices and video replays collected in the OULU-NPU dataset. The luminance and chrominance color texture information from each real and attack category image was extracted using local binary pattern descriptors. The results of the feature extraction are then used by the classification algorithm for detection.

Several machine learning algorithms were trained using 240 real category images and 872 attack category images. The best algorithm found to detect face spoofing is SVM polymonial kernel and Multilayer Perceptron by setting 3 hidden layers and hyperbolic tangent as the activation function. Manipulation of attacks in the attack category is a collection of original facial images printed using glossy A3 size paper and video captures that are played back on different devices.

Keywords: face spoofing detection, color texture, local binary pattern