Abstrak

Dalam aspek keamanan, suatu perjanjian hanya dapat diketahui oleh pihak satu dan pihak lainnya yang berwenang untuk mengetahui isi dari sebuah dokumen. Digital signature dilakukan dengan cara memakai alat elektronik yang berfungsi sama dengan tanda tangan manual. Secara mudahnya Digital Signature adalah bentuk tiruan tanda tangan konvensional kedalam bentuk digital. Digital Signature merupakan salah satu cara untuk mengamankan dokumen digital agar pesan yang dikirim tidak dapat dilihat oleh pihak yang tidak bersangkutan. Sebuah tanda tangan digital yang valid memberikan alasan bagi penerima untuk mempercayai bahwa pesan yang dikirim benar-benar dibuat oleh pengirim yang diketahui dan tidak dimanipulasi. Pada penelitian ini penulis menggunakan autentikasi biometric *Face Recognition* dan melakukan pengamanan dokumen dengan menggunakan algoritma RSA dan fungsi hash SHA256 yang diharapkan dapat memperbaiki kelemahan data dari sebuah dokumen. Untuk menambah keamanan dari sebuah dokumen dilakukan *Real Time Face Recognition* dengan Menggunakan metode *Eigenface* sebelum sebuah dokumen tersebut ditanda-tangani secara digital dengan menggunakan algoritma RSA(*Rivest Shamir Adleman)*. Setelah autentifikasi biometric Face Reccognition berhasil selanjutnya mengamankan dokumen dengan hash SHA256 dan Algoritma RSA(*Rivest Shamir Adleman)*. Dokumen tersebut dinyatakan sah apabila hasil dari dekripsi dokumen yang sudah dihash dan dienkripsi sama dengan hasil dari hash dokumen. Dari hasil skenario pengujian pada faktor *Authentication, integrity,* dan *Non-repudiation* pada *Digital Signature* menunjukan bahwa sistem dapat memenuhi tiga faktor penting dalam *Digital Signature*

Kata Kunci : ***Digital Signature, Face Recognition, Eigenface, RSA Algorithm, SHA***