ABSTRAK

Dokumen merupakan kumpulan informasi tertulis atau rekaman yang disusun secara sistematis untuk tujuan tertentu. Dokumen digital merupakan dokumen yang dapat dibaca melalui perangkat eletronik tanpa adanya kertas fisik. Dokumen PDF telah menjadi standar dunia sebagai dokumen digital. Maka dari itu, diperlukan suatu metode yang dapat memastikan keamanan pengiriman dan integritas dari sebuah dokumen PDF sehingga tidak menimbulkan masalah yang merugikan bagi pihak pengirim maupun penerima dokumen PDF.

Penelitian ini menggunakan algoritma SHA-256 dan algoritma RSA untuk membuat tanda tangan digital yang dapat mendeteksi perubahan perubahan pada dokumen PDF. Algoritma SHA-256 digunakan untuk mengambil nilai *hash* SHA-256 dari dokumen PDF sementara algoritma RSA digunakan untuk mengenkripsi dan dekripsi nilai *hash* tersebut. Berdasarkan pengujian yang telah dilakukan pada penelitian ini, algoritma *hash* SHA-256 dan algoritma RSA dapat mendeteksi hampir seluruh perbedaan dari dokumen PDF termasuk mendeteksi perbedaan dokumen PDF yang dibuat dari *file* DOCX yang sama tetapi menggunakan *renderer* PDF yang berbeda atau dibuat menggunakan *renderer* PDF yang sama tetapi pada waktu yang berbeda. Meskipun demikian, algoritma *hash* SHA-256 dan algoritma RSA tidak mampu mendeteksi perbedaan dari nama *file* PDF.

Kata kunci: RSA, SHA-256, tanda tangan digital, PDF

ABSTRACT

Document is a collection of written or recorded information that is systematically organized for a specific purpose. Digital documents are documents that can be read through electronic devices without physical paper. PDF documents have become the world standard as digital documents. Therefore, a method is needed that can ensure the security of delivery and integrity of a PDF document so that it does not cause problems that are detrimental to the sender and recipient of the PDF document.

This research uses the SHA-256 algorithm and RSA algorithm to create a digital signature that can detect changes in PDF documents. The SHA-256 algorithm is used to retrieve the SHA-256 hash value of the PDF document while the RSA algorithm is used to encrypt and decrypt the hash value. Based on the tests conducted in this research, the SHA-256 hash algorithm and RSA algorithm can detect almost all differences in PDF documents including detecting differences in PDF documents created from the same DOCX file but using different PDF renderers or created using the same PDF renderer but at different times. However, the SHA-256 hash algorithm and RSA algorithm are not able to detect differences in PDF file names.

Keywords: RSA, SHA-256, digital signature, PDF