Abstract

In the aspect of security, an agreement can only be known by one party and another party authorized to know the contents of a document. Digital signature is done by using an electronic device that functions the same as a manual signature. Simply put, Digital Signature is a form of imitation of conventional signatures into digital form. Digital Signature is one way to secure digital documents so that messages sent cannot be seen by unauthorized parties. A valid digital signature provides reason for the recipient to believe that the message sent was actually created by a known sender and was not manipulated. In this study, the authors use Face Recognition biometric authentication and document security using the RSA algorithm and the SHA256 hash function which is expected to improve data weaknesses from a document. To increase the security of a document, Real Time Face Recognition is carried out using the Eigenface method before a document is digitally signed using the RSA (Rivest Shamir Adleman) algorithm. After successful Face Reccognition biometric authentication, the document is then secured with the SHA256 hash and the RSA (Rivest Shamir Adleman) Algorithm. The document is declared valid if the result of the hashed and encrypted document decryption is the same as the result of the document hash. From the results of the test scenario on the Authentication, Integrity, and Non-Repudiation factors in Digital Signature, it shows that the system can fulfill three important factors in Digital Signature.

Keywords: ***Digital Signature, Face Recognition, Eigenface, RSA Algorithm, SHA***