A new dynamic hash algorithm in digital signature

Abstract:

This paper presents adoption of a new hash algorithm in digital signature. Digital signature presents a technique to endorse the content of the message. This message has not been altered throughout the communication process. Due to this, it increased the receiver confidence that the message was unchanged. If the message is digitally signed, any changes in the message will invalidate the signature. The comparison of digital signature between Rivest, Shamir and Adleman (RSA) algorithms are summarized. The finding reveals that previous algorithms used large file sizes. Finally the new encoding and decoding dynamic hash algorithm is proposed in a digital signature. The proposed algorithm had reduced significantly the file sizes (8 bytes) during the transferring message.