ABSTRACT

BUILDING STEGANOGRAPHY SOFTWARE USING DYNAMIC CELL SPREADING (DCS) METHOD AND DIGITAL SIGNATURE ALGORITHM (DSA) FOR DATA SECURITY

By :

Rezki Nugraha
10107316

Steganography and Digital Signature is part of Cryptography. Steganograph is art or science to hiding message, so the existence of message can not be reliezed. Meanwhile the Digital Signature is an authentication mechanism that allows message maker to add a message code that acts as a signature. From the few research that exist, have not found research that combine steganography and digital signature. Merger of the two techniques are believed to maintain the security of confidential information is better. By combining these two techniques is expected to cover the deficiencies that exist in both techniques. This needs to be proved by this research.

The technique of steganography that used is Dynamic Cell Spreading, where this technique is development from LSB methods. Dynamic Cell Spreading technique using buffer memory for temporary storage during the process of embedding and extraction of the message. To maintain the integrity and authentication of confidential messages use digital signatures using the Digital Signature Algorithm has been standardized. DSA made specifically for authentication and denial issues.

Based on the test results, the combined both technique has several advantages and disadvantages. By adding the benefits are in addition to the hidden secret information, confidential information can be directly authenticated authenticity, so avoid misinformation. The disadvantage is the need for a large enough container media, because a lot of information to be embedded.

Keyword : Steganography, Digital Signature, Dynamic Cell Spreading, Data Security