TELKOM UNIVERSITY

Abstract

School of Computing

The Graduate School

Master of Engineering

Modified Headstega Based on Bitwise Operation and Randomization Process

by Hasmawati

Recently, steganography is frequently used for providing covert channel. There are two types of steganography, noisy and noiseless. Noisy steganography approach hides the message by altering the bit of cover. The alteration process produce noise such that it will raise suspicion. In 2010, Desoky introduced Noiseless Steganography or Nostega paradigm. Nostega describes a paradigm for designing steganography system, which does not introduce noise to its cover, nor exploit noise as stego-carrier. One of the Nostega methods is Headstega. Headstega camouflages data only in email header as the cover (e.g., recipient's email addresses) in order to achieve the steganographic goal [1]. Headstega has low embedding capacity and high level of suspicion because the cover is generated based on secret message by using invalid email domains. The modified headstega based on bitwise operation and randomization process exploited bitwise operation and randomization process to conceal message in existing email address and subject. The message was embedded into the cover using a key. The key is agreed upon by the sender and recipient. After embedding the message into the cover, then the sender send the embedded cover and the symbols to the recipient using public channel. Based on the experiment results, the proposed method has better performance in message embedding capacity and also in suspicion level.

Keywords: Steganography, Nostega, Headstega, Key, XOR bitwise operation