2015 Fourth International Conference on Cyber Security, Cyber Warfare, and Digital Forensic

Data Security Using LSB Steganography and Vigenere Chiper in an Android Environment

Chyquitha Danuputri[1], Teddy Mantoro[2], Mardi Hardjianto[1]
[1]Magister of Computer Science Program, Budi Luhur University, Indonesia
[2]FST, USBI-Sampoerna University, Jakarta, Indonesia
[1]chyquitha@gmail.com, [2]teddy.mantoro@sampoernauniversity.ac.id, [1]mardi.hardjianto@budiluhur.ac.id

***Abstract*— LSB steganography and Vigenere chiper methods are integrated in used for data security validation in this study. This approach used Arithmetic Coding method for data compression and data decompression. To maintain the authenticity of the data file, a hash function (SHA 256) technique was added. This paper presents a prototype called Ste-Chy as a proof of concept of the combination of these techniques.This approach helps the user in terms of the exchange of confidential data through an online share in Android-based media. For the confidential authentication purpose, the confidential message is hidden togetherwith the target image. The quality of the original image and stego images in this work produce an image picture in an acceptable level for the user. The bigger the secret of the message, the compression will produce higher compression ratio. With this approach, security process of exchange of confidential message shared through the online share smartphone is considerably secured especially in an android environment.**

Keywords-component; LSB-Insertio;, SHA-25;, Checksum Validation; Hash Function; Cryptography; Steganography.

I. INTRODUCTION

The development of mobile technologies or mobile phones is rapidly increasing. Nowadays, mobile phones have been advanced with a variety of interesting features and has a complex operating system like a computer. Media exchange digital data has been used by a cellphone including Android. Android uses a Linux-based operating system.

Mobile phones have made people able to communicate anywhere anytime. They can talk and as well send messages to one another. When a user sends a message and she/he expected only certain target user allowed to know its contents, for the confidential purpose, an elegant method should be invented to solve this type of problem. This study proposes a solution in the form of a hybrid of cryptography and steganography. This approach is to antisipate before the message is spreading out, as it will threaten the unity and security of the institution or may be bigger organisation such as a country.

As the science and art of security protection of secret messages, crytography can messing up and encode secret messages from a message into secret codes (Chipertext) [1]. As the science and art of hiding secret messages (hiding message), steganography apporach will keep the existing messages which may not detected by human senses [MUN04]. To do this, steganography requires two properties, i.e. the container vessel and confidential data tobe hidden. Digital steganography using digital media as a container vessel, such as images, sounds, text, and video. Hidden secret data can also be images, sounds, text, or video.

Steganography exploits the limitations of human sensory systems such as the eyes and ears. Given this limitation, steganography method is applicable to a variety of digital media. The output of this steganography has a shape similar to the perception of the original form, of course, the perception limited by the ability of the human senses, but not by a computer or other digital processing devices.

This study discusses the approach on how to decode a message and followed by inserting it into a media file so that third parties may not be aware of it. This study proposes a method for processing the secured delivery of messages which contain of confidential data using Vigenere Chiper and Steganography LSB methods. This method uses a compression technique for compressing and decompressing data to be inserted, namely the method of Arithmetic Coding and CheckSum with SHA 256 method.

The prototype were presented in Android environment to deliver messages in mobile android that can hide a secret message into digital images for safekeeping and difficult to read by third parties.

II. RELATED WORK

A. *Vigenere Chiper*

Vigenere chiper is a cryptographic cipher technique which were explained first by Giovan Batista belaso in his book entitled La cifra del. Sig. Giovan Batista belaso (1553). Then the password is enhanced by a French diplomat, Blaise de Vigenere (1586) [2].

Vigenere code includes alphabetic code-compound (polyalphabetic substitution cipher). Techniques to produce chipertext can be done using a substitute numbers and squares vigenere. Vigenere technique using numbers performed by exchanging letters with numbers, similar to the slide code. This method uses a tabula recta vigenere (squares vigenere). Figure 1 presents a sample of Vigenere table. The Vigenere encryption formula:

$$C_i = (P_i+K_i) \bmod 26$$

Vigenere Decryption formula:

$$C_i = (P_i+K_i) - 26$$

978-1-4673-8499-5/15 $31.00 © 2015 IEEE
DOI 10.1109/CyberSec.2015.14