Chapter 11
Data Hiding in Color Image Using Steganography and Cryptography to Support Message Privacy

Sabyasachi Pramanik
https://orcid.org/0000-0002-9431-8751
Haldia Institute of Technology, India

Ramkrishna Ghosh
Haldia Institute of Technology, India

Digvijay Pandey
https://orcid.org/0000-0003-0353-174X
Department of Technical Education, India & Institution of Engineering and Technology, India

Mangesh M. Ghonge
https://orcid.org/0000-0003-0140-4827
Sandip Institute of Technology and Research Centre, India

ABSTRACT

The immense measure of classified information has been moved on the internet. Information security turns out to be progressively significant for some applications, for instance, private transmission, video observation, military, and clinical applications. Lately, there has been a great deal of enthusiasm for steganography and steganalysis. Steganography is the specialty of covering up and transmitting information through clearly harmless transporters with an end goal to disguise the presence of information. The advanced picture information, for example, BMP, JPEG, and GIF, are generally utilized as a transporter for steganography. Here the mystery message is implanted into a picture (or any media) called spread picture and afterward sent to the beneficiary who extricates the mystery message from the spread message. This picture ought not to be discernible from the spread picture, with the goal that the aggressor can't find any implanted message. The authors have proposed three approaches of steganography that can easily support message privacy.

DOI: 10.4018/978-1-7998-6677-0.ch011

INTRODUCTION

The security of the difference in disguised data can be gotten by two unique ways: encryption (Lorente, A. S. and Berres, S., 2017) what's more, steganography (Pramanik, S. also, Raja, S. S., 2019). A blend of the two procedures can be used to grow the data security. In encryption, the message is changed in such a path thusly that no data can be disclosed if it is gotten by an aggressor. While in steganography, the riddle message is embedded into an image often called spread picture, and subsequently sent to the gatherer who isolates the secret message from the spread message. Exactly when the secret message is embedded into spread picture then it is known as a stego-picture. The deceivability of this image should not to be detectable from the spread picture, with the objective that it almost gets shocking for the attacker to discover any introduced message. Three unique methodologies for concealing information are proposed:

1. Approach based on steganography through LSB Modification for both Sender & Receiver for sending & extracting data respectively.

   Receiver compatible data hiding in color image based on the needed LSB modification

2. Approach based on the symmetric cryptography (Pramanik, S., Bandyopadhyay, S. K., & Ghosh, R., 2020) blending with steganography with concise storage
3. Data Hiding (Kim, P. H et. al., 2019) in Color Image using Steganography blending with Cryptography to support message privacy.

   Motivation:

- Steganography shrouds the presence of records.
- Provides high security (Pramanik, S., Bandyopadhyay, S. K., 2014) for information transmission.
- No one can foresee that the records even exist.

FIRST APPROACH: BASED ON STEGANOGRAPHY THROUGH LSB MODIFICATION

This is an approach based on LSB Modification (Swain, G., 2019) for both Sender and Receiver for sending and extracting data respectively. The content of the information file is converted to equivalent binary value and embedded into cover image and extracted from stego image. Some Tables are shown below that is describing the ASCII (Pramanik, S. et. al., 2019) value of the characters and also the equivalent binary value.

In simple LSB modification, bits from data that has to be hidden are put at the LSB of the cover image. Digitized images are made of pixels in which each pixel can use three bytes i.e. 24 bits. Here, three bytes are the representation of red, green and blue colors respectively. In the LSB method the least significant bit of each byte is set to zero. Now, according to the bits 0 or 1 in data, the LSB is being changed. If data bit is 0, then LSB remains same and if the data bit is 1 then the LSB is changed to 1. For doing this modification, the image becomes a little bit lighter than the original one. Nowadays, more sophisticated approach is used for hiding data. The most widely used technique to hide data is the usage of the LSB.