Chapter 18
A Survey on Digital Image Steganographic Methods

Amritha P. P.
Amrita Vishwa Vidyapeetham, India

Gireesh Kumar T.
Amrita Vishwa Vidyapeetham, India

ABSTRACT

Steganography is the art of hiding information in ways that prevent the detection of hidden message, where as cryptographic techniques try to conceal the contents of a message. In steganography, the object of communication is the hidden message while the cover data is only the means of sending it. The secret information as well as the cover data can be any medium like text, image, audio, video etc. The objective of this chapter is to report various steganographic embedding schemes that can provide provable security with high computing speed and embed secret messages into images without producing noticeable changes.

The embedding schemes utilizes the characteristic of the human vision's sensitivity to color value variations and resistant to all known steganalysis methods. The main requirement of steganography is undetectability, which loosely defines that no algorithm exists that can determine whether a work contains a hidden message.

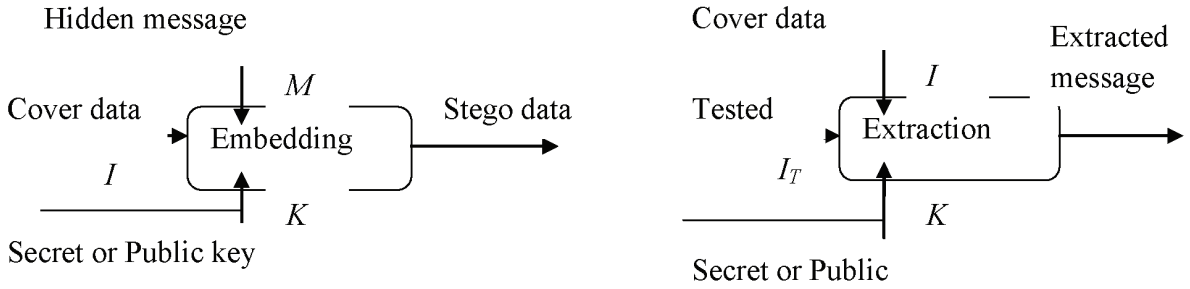
1. GENERIC EMBEDDING AND EXTRACTING SCHEME

Many approaches and techniques are available in the literature for information hiding. Figure 1 shows a generic embedding and extracting scheme. The inputs to the embedding scheme are the hiding message, the cover data and an optional public or secret key *K*. The output is stego data, also called stego object. Inputs to the generic extracting scheme are the tested data, the secret or public key, and the original cover data besides information about steganographic scheme used. The output is the extracted message.

Steganographic techniques can be divided into various categories. The basic and most common

DOI: 10.4018/978-1-60960-123-2.ch018

Figure 1 Generic embedding and extracting scheme



approach in partitioning of hiding techniques is in the spatial domain, frequency domain. Another way for categorization of steganographic methods is based on the condition whether or not they use the original data for extraction of hiding message from tested data. The third method is based on with or without encryption. Three types of steganography can be identified based on their difference in the nature and combination of inputs and outputs (Cox, Miller, Boom, & Fridrich, 2008)

- Pure Steganography
  We call a steganography system pure when it doesn't require prior exchange of some secret information before sending message. The pure steganography can be defined as the quadruple (C, M, D, and E) where:
  C: the set of possible covers.
  M: the set of secret massage with $|C| \geq |M|$.
  E: $C \times M \rightarrow C$ the embedding function.
  D: $C \rightarrow M$ of the extraction function with the property that
  D (E (c, m)) = m for all $m \in M$ and $c \in C$

- Secret key steganography
  We call a steganographic system a shared-secret or shared-key or secret when it requires prior exchange of data like shared keys. Here the sender chooses a cover and embeds the secret message into the cover using a secret key. If the secret key used in the embedding process is known to the receiver, he can reverse the process and extract the secret message. The secret key steganography can be defined as the quintuple (C, M, K, D_K, E_K) where:
  C: the set of possible covers.
  M: the set of secret message.
  K: the set of secret keys.
  E_K: $C \times M \times K \rightarrow C$ with the property that
  D_K ($E_K(c, m, k)$, k) = m for all $m \in M$, $c \in C$ and $k \in K$

- Public key Steganography
  This kind of steganography does not rely on shared key exchange. Instead it is based on the public key cryptography principle in which there are two keys, one being the public key which can be usually obtained from a public database and the other a private key. Usually in this case the public key is used in the embedding process and the private key in the decoding process.

Steganography has to guarantee these requirements

- Undetectability: Embedded information is undetectable if the image with the embedded message is consistent with a model of the source from which images are drawn.