

How to Send a Secret Message!

Introduction:

The term Steganography as well cryptography was derived from the Greek language. Cryptography is essentially the art of secret writing and the goal is to maintain the secrecy of the message even if it is visible. Steganography, means covered writing, and is a long-practiced form of hiding information. It should not be seen as a replacement for cryptography but rather as a complement to it.

Cryptography is used to conceal the content of a message, while steganography is used to conceal the existence of a message.

The technology behind effective Steganography is quite complex and involves serious mathematical computations. Computers and technology make this an easy task and make this art of deception a serious threat to the security of information. The strength of a steganographic algorithm depends on its ability to successfully withstand attacks. Companies with important and sensitive information, and relying on the security and integrity of their intellectual property, could be at significant risk.

Steganography under various media:

Steganography includes a vast array of techniques for hiding messages in a variety of media. Among these methods are invisible inks, covert channels, digital signatures, microdots, and spread-spectrum communications. New age technology helps steganography to use various mediums like - text, images, sound, signals, and more.

Steganography in Text:

This process involves using steganography within text, i.e. documents or emails. This process is used to counteract the wide scale piracy or illegal distribution of documents, wherein infringers make identical copies of documents without paying royalties to the original author.

1. Line-Shift coding: In this method, text lines are vertically shifted to encode the document uniquely.
2. Word-Shift coding: In this method, code words are coded into a document by shifting the horizontal locations of words within text lines, while maintaining a natural spacing appearance.
3. Feature coding: In feature coding, certain text features are altered, or not altered, depending on the codeword. For example, one could encode bits into text by extending or shortening the vertical end lines of letters such as p, q, y, etc.

Steganography in Images:

This process involves exploiting the Human Visual System (HVS). Image steganography is being increasingly used due to the development of powerful graphical computers and the increasing softwares over the internet.

1. Image Compression: Image compression helps in reducing the file size by compressing it to a certain extent. Two kinds of image compression are lossless and lossy compression.
2. Image Encoding techniques: This technique involves in hiding the secret information within the image. It can be done in many ways, like encoding every bit of information in the image or encoding only in the noisy areas of the image.

Steganography in Audio:

This form of steganography is very sensitive to handle, as it involves exploiting the Human Auditory System (HAS). We call it sensitive, because the HAS posses a large dynamic range but a small differential range. The following are the methods of this type of steganography -

1. Phase Coding - This process involves substituting the phase of an initial audio segment with a reference phase that represents the data.
2. Low bit encoding - This process is similar to image encoding, wherein binary data is stored in the audio files.
3. Spread Spectrum - In this process, the encoded data is spread across the frequency of the audio data.
4. Echo Data Hiding - Echo data hiding embeds data into a host signal by introducing an echo.

Conclusion:

There are so many components to this form of deception, which are increasingly used either for safeguarding some valuable data or for destroying it. The thing with white collar crimes is that criminals don't necessarily "look" like criminals and they often proceed for years without being caught. This article aims to make people aware of this form of deception and the threat it poses to digital security.

For more information on Steganography, visit us at www.agapeinc.in or www.agapeforensic.com.