Hiding Information in Images *

Lisa M. Marvel and Charles T. Retter
U.S. Army Research Laboratory
Aberdeen Proving Ground, MD 21005
marvel@arl.mil

Charles G. Boncelet, Jr.
University of Delaware
Newark, DE 19716
boncelet@ee.udel.edu

Abstract

In this paper we present a new method of embedding information within digital images, called Spread Spectrum Image Steganography (SSIS). Steganography, which means "covered writing" in Greek, is the science of communicating in a hidden manner. SSIS conceals a message of substantial length within digital imagery while maintaining the original image size and dynamic range. The hidden message can be recovered using the appropriate keys without any knowledge of the original image. Image processing, error control coding, and spread spectrum techniques used to conceal the hidden data are described, and the performance of the technique is illustrated. The message embedded by this method can be in the form of text, imagery, or any other digital signal. Applications for such a data-hiding scheme include in-band captioning, hidden communication, image tamperproofing, authentication, invisible map overlays, embedded control, and revision tracking.

1 Introduction

The prevalence of multimedia data in our electronic world exposes a new avenue for communication using digital steganography. *Steganography*, where the occurrence of communication is concealed, differs from cryptography in which communication is evident but the content of that communication is camouflaged. To be useful a steganographic system must provide a method to *embed data imperceptibly*, allow the data to be *readily extracted*, promote a high information rate or *capacity*, and incorporate a certain amount of *resistance* to removal [1][2].

There are many applications for techniques that embed information within digital images. The dispatch of hidden messages is an obvious function, but today's technology stimulates even more subtle uses. In-band captioning, such as movie subtitles, is one such use where textual information can be embedded within the image. The ability to deposit image creation and revision information within the image provides a form of revision tracking. Authentication and tamper proofing as security measures are yet other functions that could be provided. These are but a few of the possible uses of image steganography.

Schemes where the original cover signal is needed to reveal the hidden information are known as *cover escrow*. In many applications it is not practical to require the possession of the unaltered cover signal in order to extract the hidden information. More pragmatic methods, known as blind or oblivious schemes, allow direct extraction of the embedded data from the modified signal without knowledge of the original cover.

A block diagram of a blind image steganographic system is depicted in Figure 1. A message is embedded in a digital image by the stegosystem encoder which uses a key or password. The resulting stegoimage is transmitted over a channel to the receiver where it is processed by the stegosystem decoder using the same key. During transmission the stegoimage can be monitored by unintended viewers who will notice only the transmittal of the innocuous image without discovering the existence of the hidden message.

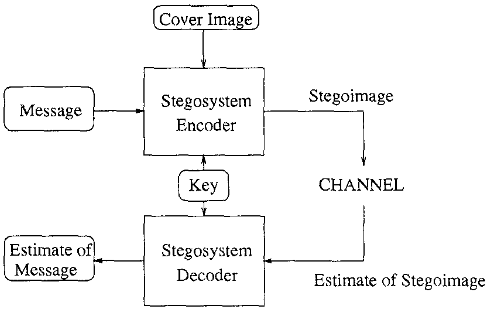

Figure 1: Overview of Steganographic System

2 SSIS

Our method is a data-hiding steganographic method that uses digital imagery as a cover signal. SSIS provides the ability to hide a significant quantity of information bits within digital images while avoiding detection by an observer or computer analysis. Furthermore, by incorporated image processing techniques the original image is not needed to extract the hidden information, thereby resulting in a more pragmatic system. The proposed recipient need only

*Prepared through collaborative participation in the Advanced Telecommunication/Information Distribution Research Program (ATIRP) Consortium sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAL01-96-2-0002.

possess a key in order to reveal the message. The very existence of the hidden information is virtually undetectable by human or computer.

Techniques of spread spectrum communication, error-control coding, and image processing are combined to accomplish SSIS. The SSIS encoder and decoder are shown in Figures 2 and 3. The fundamental concept of SSIS is the embedding of the hidden information within noise, which is then added to the digital image. This noise is typical of that inherent to the image acquisition process [3] and, if kept at low levels, is not perceptible to the human eye nor is it susceptible to detection by computer analysis without access to the original image. In order for SSIS to be a blind steganography scheme, a version of the original image must be acquired from the stegoimage. To accomplish this, image restoration techniques are used. An estimate of the embedded signal that was added to the original cover image is recovered by taking the difference between the restored image and the stegoimage. Finally, because the noise is of low power and the restoration process is not perfect, the estimation of the embedded signal is poor, resulting in a high embedded signal bit error rate (BER). To compensate, a low-rate error-correcting code is incorporated in to the system. This conglomeration of communication and image processing techniques provides a method of reliable blind image steganography.

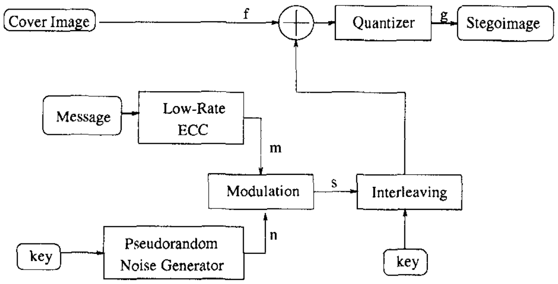

Figure 2: SSIS Encoder

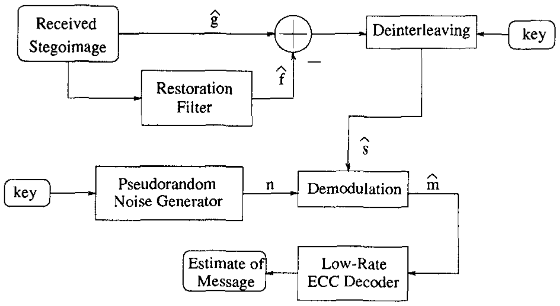

Figure 3: SSIS Decoder

3 Performance

We illustrate the performance of SSIS using the original 512 × 512 image appearing in Figure 4, entitled Sunflower. We strive for total error-free recovery of the hidden data, presuming that the hidden message will be compressed using methods that are intolerant to errors.

As an example we have hidden a message within the image of Figure 5. The steganographic signal-to-noise ratio (SNR), the ratio of embedded signal power to cover image power, for this image is -34 dB. The resulting stegoimage yields a capacity of approximately 5 kilobytes of hidden information.

4 Conclusions

We have presented a novel steganographic methodology that uses error control coding, image processing, and spread spectrum techniques. This process provides a method for concealing a digital signal within a cover image without increasing the size of the image. Additionally, cover image escrow is not needed due the image restoration resulting in a more practical system. A level of security is provided by the necessity that both sender and receiver possess the same public or private keys. Furthermore, the embedded signal power is insignificant compared to that of the cover image. This insignificances provides low probability of detection, and thereby leaves an observer unaware that the hidden data exist.

References

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. Techniques for data hiding. *IBM Systems Journal*, 35(3 & 4), 1996.

[2] I.J. Cox, J. Kilian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for images, audio and video. *Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland*, III:243–246, September 1996.

[3] A.K. Jain. *Fundamentals of Digital Image Processing*. Prentice-Hall, Inc., Englewood Cliffs, NJ, 1989.

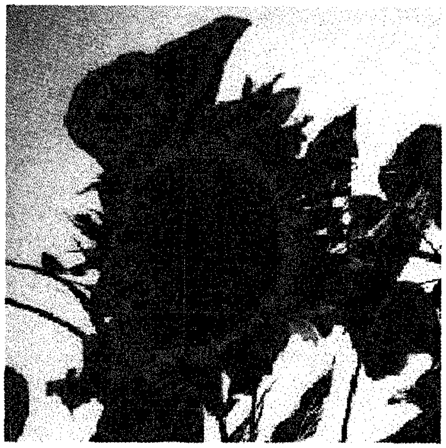

Figure 4: Original Image - Sunflower

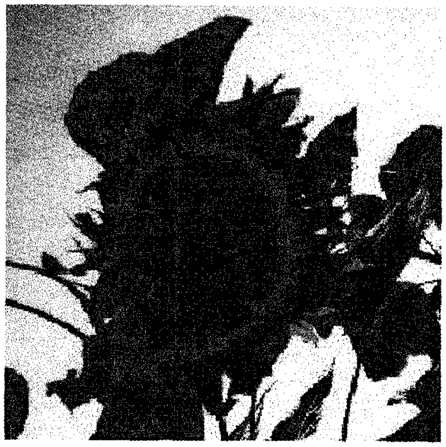

Figure 5: Images With Embedded Signal