ARMY RESEARCH LABORATORY

Methodology of Spread-Spectrum Image Steganography

by Lisa M. Marvel, Charles G. Boncelet, Jr.,
and Charles T. Retter

ARL-TR-1698 June 1998

The findings in this report are not to be construed as an official Department of the Army position unless so designated by other authorized documents.

Citation of manufacturer's or trade names does not constitute an official endorsement or approval of the use thereof.

Destroy this report when it is no longer needed. Do not return it to the originator.

Army Research Laboratory
Aberdeen Proving Ground, MD 21005-5067

ARL-TR-1698 **June 1998**

Methodology of Spread-Spectrum Image Steganography

Lisa M. Marvel, Charles T. Retter
Information Science and Technology Directorate, ARL

Charles G. Boncelet, Jr.
University of Delaware, Newark, DE

Abstract

This report presents a new method of digital steganography, entitled Spread-Spectrum Image Steganography (SSIS). Steganography, which means "covered writing" in Greek, is the science of communicating in a hidden manner. Following a brief history of this art and a discussion of steganographic communication theory, the new method, SSIS, is introduced. This system hides and recovers messages of substantial length within digital imagery while maintaining the original image size and dynamic range. The hidden messages can be recovered using appropriate keys without any knowledge of the original image. Image processing, error control coding, and spread-spectrum techniques utilized are described, and the performance of the technique is illustrated. A message embedded by this method can be in the form of text, imagery, or any other digital signal. Applications for such data-hiding scheme include in-band captioning, covert communication, image tamperproofing, authentication, embedded control, and revision tracking.

Preface

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.

INTENTIONALLY LEFT BLANK.

Table of Contents

INTENTIONALLY LEFT BLANK.

List of Figures

INTENTIONALLY LEFT BLANK.

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, where 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 as another possible application of digital steganography. This avoids the need for maintaining two separate media, one containing the image itself and one containing the revision data. Authentication and tamperproofing as security measures are yet other functions that could be provided. Digital image steganographic techniques can also provide forward and backward compatibility by embedding information in an image in an imperceptible manner. If a system has the ability to decode the embedded information, new enhanced capabilities could be provided. If a system does not have the capability to decode the information, the image would be displayed without degradation, leaving the viewer unaware that the hidden data exist. An example of forward/backward compatibility is the embedding of closed caption information for the hearing impaired within television signals. The caption information does not interfere with the picture display of older version television but can be readily displayed using a model with the capability to do so. These are but a few of the possible uses of image steganography.

2. Background

Steganography is not a new science, as is evident from several examples from the times of ancient Greece [3]. One is the story of Histiaeus, who wished to inform his allies when to revolt against the enemy. He shaved the head of a trusted servant and then tattooed a message on his head. After allowing time for the hair to grow back, the messenger was then sent through enemy territory to the allies. Upon arrival, the servant reported to the leader to have his head shaven again, thereby revealing the message. There is also the story of the wax tablets; in ancient times the writing medium of the day was a wooden tablet covered with wax. A person etched into the wax, and when he desired to erase the writing, the wax was melted and the tablets reused. In order to convey a message that Greece was about to be invaded, Demeratus concealed his message by writing directly on the wood and then covering it with wax. The seemingly blank tablets were then transported to his collaborators, where the message was literally uncovered.

Modern times have yielded more advanced techniques, such as the use of invisible inks, where certain chemical reactions are necessary to reveal the hidden message. Another method employs routine correspondence where the applying of pin pricks in the vicinity of a particular letter could spell out a secret message. Advances in photography produced microfilm, which was used to transmit messages via carrier pigeon. Further developments in this area improved film and lenses, thus providing the ability to reduce the size of secret messages to that of a printed period. This technique, known as the microdot, was used by the Germans in World War II.

With more communications occurring electronically, there have been advancements in utilizing digital multimedia signals as vehicles for steganographic communication. These signals — which are typically audio, video, or still imagery — are defined as cover signals. Schemes where the original cover signal is needed to reveal the hidden information are known as *cover escrow*. They can be useful in traitor-tracing schemes such as those described in Pfitzmann [4]. In this scenario, copies of the cover signal are disseminated with the assignee's identification embedded within, resulting in a modified cover signal. If illegal copies of the signal are acquired, the source of the copy is established by subtracting the original cover data from the modified signal, thereby exposing the offender's identity. However, 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. Blind strategies are predominant among steganography of the present day.

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.

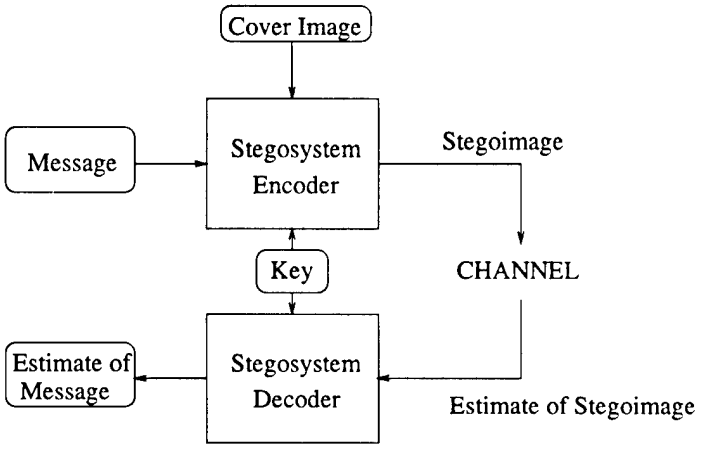


Figure 1. Overview of Steganographic System.

Within the past few years, there has been a surge of research in the area of digital image steganography. A majority of the work in the area has been performed on invisible digital watermarking. The thrust of this work can be attributed to the desire for copyright protection, spurred by the widespread use of imagery on the Internet, and the ease in which perfect reproduction of an image is is obtained. The objective of digital watermarking is to embed a signature within a digital image to signify origin or ownership for the purpose of copyright protection. Once added, a watermark must be resistant to removal and reliably detected even after typical image transformations such as rotation, translation, cropping, and quantization.

Digital steganography, or information-hiding schemes, can be characterized by utilizing the theories of communication [5]. The parameters of information hiding, such as the number of data bits that can be hidden and the invisibility of the message and its resistance to removal, can be related to the characteristics of communication systems: capacity, signal-to-noise ratio (SNR), and jamming margin. The notion of capacity in data hiding indicates the total number of bits hidden and successfully recovered by the stegosystem. The signal-to-noise ratio serves as a measure of invisibility, or detectability. In this context, the message we are trying to conceal, the embedded signal, represents the information-bearing signal and the cover image is viewed as noise. Contrary to typical communication scenarios where a high SNR is desired, a very low SNR corresponds to lower perceptibility, and therefore greater success is achieved when concealing the embedded signal. The measure of jamming resistance can be used to describe a level of resistance to removal or destruction of the embedded signal, intentional or accidental.

It is not possible to simultaneously maximize removal resistance, invisibility, and capacity. Therefore, the acceptable balance of these items must be dictated by the application. For example, an information-hiding scheme may forgo removal resistance in favor of capacity and invisibility, whereas a watermarking scheme, which may not require large capacity or even invisibility, would certainly support increased removal resistance. Finally, steganography used as a method of hidden communication would adopt the utmost invisibility while sacrificing resistance to removal and possibly capacity.

Our method of Spread-Spectrum Image Steganography (SSIS) is a data-hiding/hidden communication steganographic method that uses digital imagery as a cover signal. SSIS provides the ability to hide a significant number of information bits within digital images while avoiding detection by an observer. This objective advocates the maximization of capacity and invisibility. Furthermore, because the original image is not needed to extract the hidden information, SSIS is not a cover escrow scheme. The proposed recipient need only possess a key in order to reveal the hidden message. The very existence of the hidden information is virtually undetectable.

3. Existing Methods

Digital steganography is currently a very active research area, encompassing methods of copyright protection, image authentication, and secure communications. SSIS is a method of

data hiding and hidden communication. Therefore, emphasis is placed upon invisibility and the amount of data successfully hidden. Consequently, we attempt to limit this discussion of existing image steganographic methods to those which have these common goals.

One method of data hiding entails the manipulation of the least significant bit (LSB) plane, from direct replacement of the cover LSBs with message bits to some type of logical or arithmetic combination between the two. Several examples of LSB schemes can be found in van Schnydel, Tirkel, and Osborne [6], Wolfgang and Delp [7], and Machado [8]. LSB manipulation programs have also been written for a variety of image formats and can be found in Milbrandt [9]. LSB methods typically achieve both high capacity and low perceptibility. However, because the fact that the data are hidden in the least significant bit may be known, LSB methods are vulnerable to extraction by unauthorized parties.

There are, of course, many approaches that are cover escrow schemes, where it is necessary to possess the original cover signal in order to retrieve the hidden information. Examples of such schemes can be found in Cox et al. [2], Podilchuk and Zeng [10], and Swanson, Zhu, and Tewfik [11].

Several procedures for data hiding in multimedia can be found in Bender et al. [1]. One of these, entitled Patchwork, alters the statistics of the cover image. First, pairs of image regions are selected using a pseudorandom number generator. Once a pair is selected, the pixel intensities within one region are increased by a constant value while the pixels of the second region are correspondingly decreased by the same value. The modification is typically small and not perceptible, but is not restricted to the LSB. A texture-mapping method that copies areas of random textures from one area of the image to another is also described. Simple autocorrelation of the signal is used to expose the hidden information.

Smith and Comiskey presented several spread-spectrum data-hiding methods in [5]. These techniques utilize the message data to modulate a carrier signal, which is then combined with the cover image in sections of nonoverlapping blocks. The message is extracted via cross correlation between the stegoimage and the regenerated carrier; hence, cover image escrow is not necessary. A thresholding operation is then performed on the resulting cross correlation to determine the binary value of the embedded data bits. Ideally, the modulated carrier signals should be orthogonal to the cover image and to each other for reliable message extraction. Some of the hidden data may be lost if the phase of the modulated carrier is recovered in error.

A data-hiding scheme using the statistical properties of dithered imagery is proposed by Tanaka, Nakamura, and Matsui [12]. With this method, the dot patterns of the ordered dither pixels are controlled by the information bits to be concealed. This system accommodates 2 kilobytes of hidden information for a bilevel 256×256 image, yielding an information-hiding ratio of 1 information bit to 4 cover image bits. An information-hiding ratio of 1:6 is obtained for trilevel images of the same size. The method has high capacity but is restricted to dithered images and is not resistant to errors in the stegoimage.

Davern and Scott presented an approach to image steganography utilizing fractal image compression operations [13]. An information bit is embedded into the stegoimage by transforming one similar block into an approximation for another. The data are decoded

using a visual key that specifies the position of the range and domain regions containing the message. Unfortunately, the amount of data that can be hidden using the method is small and susceptible to bit errors. Additionally, the search for similar blocks in the encoder, and the decoder comparison process, are both computationally expensive operations.

Recent research performed by Swanson, Zhu, and Tewfik [14] has utilized an approach of perceptual masking to exploit characteristics of the human visual system (HVS) for data hiding. Perceptual masking refers to any situation where information in certain regions of an image is occluded by perceptually more prominent information in another part of the scene [15]. This masking is performed in either the spatial or frequency domain using techniques similar to those in Cox et al. [2] and Smith and Comisky [5] without cover image escrow.

4. SSIS

Techniques of spread-spectrum communication, error-control coding, and image processing are combined to accomplish SSIS. 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 the noise inherent to the image acquisition process and, if kept at low levels, is not perceptible to the human eye nor is 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 recover an estimate of the embedded signal that was added to the cover. To accomplish this, image restoration techniques are used. 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. This conglomeration of communication and image processing techniques provides a method of reliable blind-image steganography.

The major processes of the stegosystem encoder are portrayed in Figure 2. Within the system, the message is optionally encrypted with key 1 and then encoded via a low-rate error-correcting code, producing the encoded message, m. The sender enters key 2 into a wideband pseudorandom noise generator, generating a spreading sequence, n. Subsequently, the modulation scheme is used to spread the narrowband spectrum of m with the spreading sequence, thereby composing the embedded signal, s, which is then input into an interleaver and spatial spreader using key 3. This signal is now added with the cover image, f, to produce the stegoimage, g, which is appropriately quantized to preserve the initial dynamic range of the cover image. The stegoimage is then transmitted in some manner to the recipient. At the receiver, the stegoimage is received, and the recipient (who maintains the same keys as the sender) uses the stegosystem decoder (shown in Figure 3) to extract the hidden information. The decoder uses image restoration techniques to produce an estimate of the original cover image, $\hat{f}$, from the received stegoimage, $\hat{g}$. The difference between $\hat{g}$ and $\hat{f}$ is fed into a keyed deinterleaver to construct an estimate of the embedded signal, $\hat{s}$. With key 2, the spreading sequence, n, is regenerated, the encoded message is then demodulated, and an estimate of

the encoded message, $\hat{m}$, is constructed. The estimate of the message is then decoded via the low-rate error-control decoder, optionally decrypted using key 1, and revealed to the recipient.

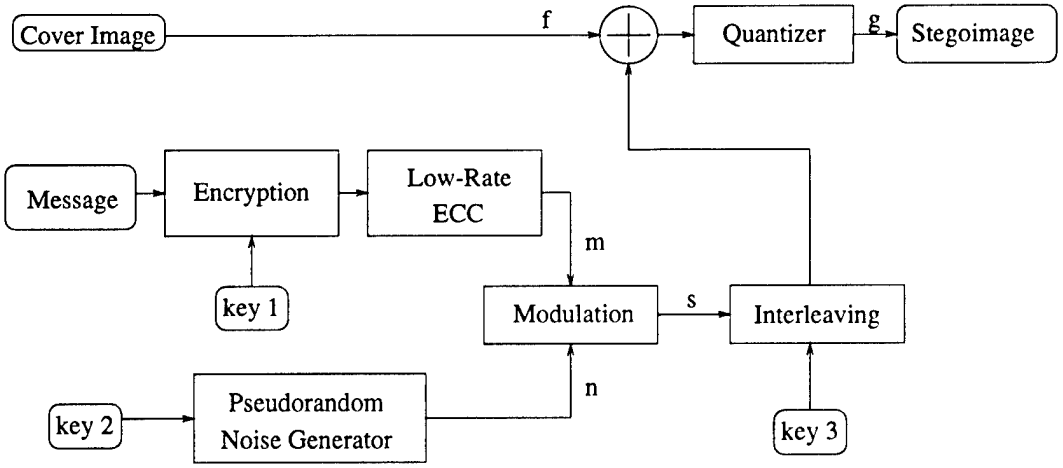


Figure 2. SSIS Encoder.

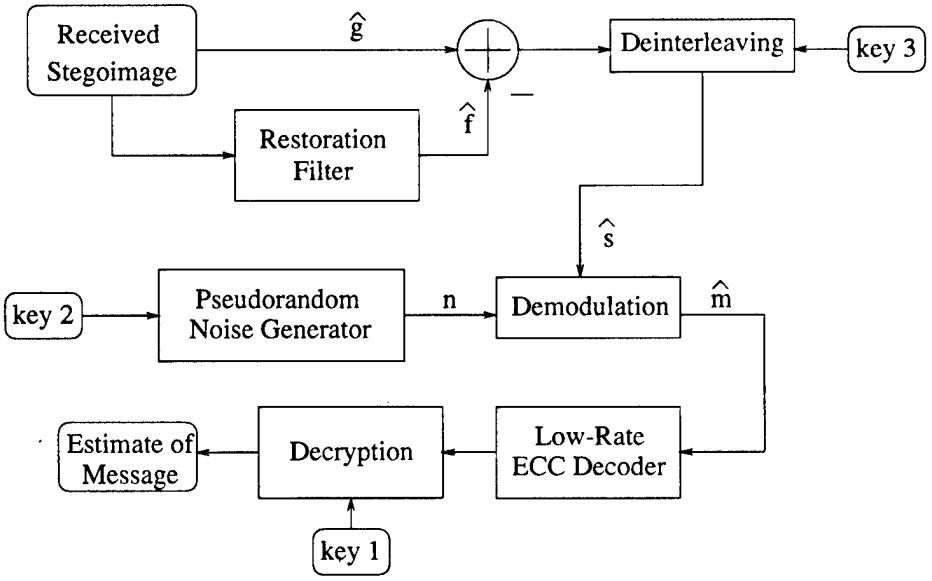


Figure 3. SSIS Decoder.

Wideband thermal noise, which is inherent to imagery captured by photoelectronic systems, can be modeled as additive white Gaussian noise (AWGN) [16]. SSIS uses this inherent noise to hide information within the digital image. In other types of coherent imaging, the noise can be modeled as speckle noise [16], which is produced by coherent radiation from the microwave to visible regions of the spectrum. We postulate that the concepts of SSIS can be extended to imagery with other noise characteristics than those modeled by AWGN. The additional noise that conceals the hidden message is a natural phenomenon of the image and, therefore, if kept at typical levels, is unsuspecting to the casual observer or computer

analysis. Subsequently, even if the methodology of this system is known to eavesdroppers, they will be unable to decipher the hidden information without possession of the appropriate keys.

4.1 Spread Spectrum

Spread-spectrum communication describes the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies. This can be accomplished by modulating the narrowband waveform with a wideband waveform, such as white noise. After spreading, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect. SSIS uses this technique to embed a message, typically a binary signal, within very low power white Gaussian noise. The resulting signal, perceived as noise, is then combined with the cover image to produce the stegoimage. Since the power of the embedded signal is low compared to the power of the cover image, the SNR is also low, thereby indicating low perceptibility and providing low probability of detection by an observer. Subsequently, an observer will be unable to visually distinguish the original image from the stegoimage.

To construct the embedded signal, we incorporate the concept of a stored reference spread-spectrum communications system [17] to provide low probability of detection, either by computer or the HVS. The stored reference principle requires independent generation of identical pseudorandom wideband waveforms at both the transmitter and receiver. This can easily be accomplished by a private or public key [18] and identical pseudorandom waveform generators.

Here we describe a simple sign modulation scheme to provide an example of the spread-spectrum process. This method is similar to the technique used in Hartung and Girod [19]. Assume that the message signal, m, is a bilevel signal consisting of $\{-1, +1\}$ and the spreading sequence, n, is a sequence of real numbers that have a white Gaussian distribution generated by a pseudorandom number generator using a key. The two signals are multiplied (1), thereby spreading the power spectrum of the message signal within the relatively constant spectrum of the noise signal. With this simple system, the sign of each noise value is changed corresponding to the value of the message bit to be embedded and the white Gaussian characteristics of the signal preserved. The decoding process is also elementary. The sequence n is replicated at the receiver, and the sign of this sequence is compared to the sign of the received sequence, $\hat{s}$, to determine the estimated value of the narrowband message signal $\hat{m}$ as shown in equation (2). Although an intruder may be aware of the general strategy of the system, the value of the key needed to generate n is unknown, thereby preventing decoding of the message. In addition, without the appropriate keys, the modulated signal is statistically indistinguishable from white Gaussian noise.

$$s = m * n. \tag{1}$$

$$sign\left(\frac{\hat{s}}{n}\right) = \hat{m}. \tag{2}$$

In order to improve performance, a nonlinear modulation scheme was developed for SSIS to spread the spectrum of the narrowband message signal, m. This technique provides an increase in the Euclidean distance between values modulated by message bits, thereby promoting an improved estimate of the embedded signal. This is accomplished by first generating a random sequence u, which is uniformly distributed between (0,1). A second sequence is generated by applying the nonlinear transformation of equation (3) to u. The spreading sequence is then formed by selecting bits from these two sequences arbitrated by the message bits after the u and u' have been transformed to Gaussian random variable, as shown in (4). Here Φ^{-1} represents the inverse cumulative distribution function for a standard Gaussian random variable. To adjust the power of the embedded signal, a scale factor is applied to s. The signal is then added to the cover image. The result, after quantization, is the stegoimage.

$$u_i' = \begin{cases} u_i + .5 & u_i < .5 \\ u_i - .5 & u_i \geq .5. \end{cases} \tag{3}$$

$$s_i = \begin{cases} \Phi^{-1}(u_i) & m_i = 0 \\ \Phi^{-1}(u_i') & m_i = 1. \end{cases} \tag{4}$$

At the decoder, the stegoimage is obtained and image processing techniques are used to estimate the embedded signal without knowledge of the original cover in order to avoid the need for cover image escrow. By exercising image restoration techniques, an estimate of the embedded signal can be obtained by subtracting a version of the restored image from the stegoimage. Since the pixels of a digital image are highly correlated among neighboring pixels in natural scenes, filtering operations can be used to restore the original image. The problem of embedded signal estimation now becomes an image restoration problem where the objective is to eliminate additive random noise in the received stegoimage. The restored image can be obtained with a variety of image processing filters, such as mean or median filters, or wavelet shrinkage techniques. However, favorable performance was obtained experimentally with adaptive Wiener filtering techniques.

4.2 Image Processing

The adaptive Wiener filter is used by SSIS to reduce the amount of low-level additive random noise in the stegoimage. Wiener filtering preserves the signal while eliminating noise in the degraded image. Due to linear independence between the cover image and the embedded signal, the optimal linear minimum mean square error estimate of the original image is obtained by filtering with an adaptive Wiener filter [20]. The frequency response of the filter is dependent upon the power spectra of the original image and noise as shown in (5), where P_f is the power spectrum of the original image f and P_s is the power spectra of the embedded signal s.

$$H(\omega_1, \omega_2) = \frac{P_f(\omega_1, \omega_2)}{P_f(\omega_1, \omega_2) + P_s(\omega_1, \omega_2)}. \tag{5}$$

The power spectrum of the AWGN, which is constant and independent of ω_1, ω_2, is known at the receiver from the regenerated sequence, n. Although the embedded signal characteristics do not change within the stegoimage, the image characteristics do change from one region to another. For instance, consider an image with smooth background areas and a detailed foreground; the power spectrum will be significantly different in these areas. To compensate for the changing image characteristics, the adaptive Wiener filter is a space-variant filter, whose filter coefficients change as a function of the local image statistics. Adaption to the local image characteristics can be performed on a pixel-by-pixel or block-by-block basis.

The power spectrum of the original image is not known at the receiver and, therefore, must be estimated from the received stegoimage, $\hat{g}$. If we assume that the original image signal $f(n_1, n_2)$ of a small local region of the image is stationary, it can be reasonably modeled as (6), where m_f and σ_f are the local mean and standard deviation of the original image, and w is a zero mean white noise process with unit variance [21, 22].

$$f(n_1, n_2) = m_f + \sigma_f w(n_1, n_2). \tag{6}$$

Therefore, the space-variant local mean and variance are m_f and σ_f^2, respectively. To estimate these parameters from the stegoimage, consider that when the mean of the embedded signal is zero, which is the case with the AWGN embedded signal, m_f is identical to the mean of the local region of the stegoimage, m_g. Additionally, because s is additive, σ_g^2 can be defined as (7), and an estimate of $\hat{\sigma}_f^2$ can be obtained by (8), where $\sigma_{\hat{g}}^2$ is the variance of the local region, of the stegoimage. Within this local region, the transfer function of the space-variant Wiener filter is given by (9) and the restored image, $\hat{f}$, is obtained by (10). This filter is invoked within SSIS using the algorithm developed by Lee [23].

$$\sigma_g^2 = \sigma_f^2 + \sigma_s^2, \tag{7}$$

$$\hat{\sigma}_f^2(n_1, n_2) = \begin{cases} \sigma_{\hat{g}}^2(n_1, n_2) - \sigma_s^2, & if\ \sigma_{\hat{g}}^2(n_1, n_2) > \sigma_s^2 \\ 0, & otherwise. \end{cases} \tag{8}$$

$$H(\omega_1, \omega_2) = \frac{P_f(\omega_1, \omega_2)}{P_f(\omega_1, \omega_2) + P_s(\omega_1, \omega_2)} = \frac{\hat{\sigma}_f^2}{\hat{\sigma}_f^2 + \sigma_s^2}. \tag{9}$$

$$\hat{f}(n_1, n_2) = m_{\hat{g}} + [\hat{g}(n_1, n_2) - m_{\hat{g}}] * \frac{\hat{\sigma}_f^2}{\hat{\sigma}_f^2 + \sigma_s^2} \delta(n_1, n_2). \tag{10}$$

The resultant restored image is scaled according to the relation between $\hat{\sigma}_f^2$, which is estimated from the local region statistics of the stegoimage, and the predetermined σ_s^2. If σ_s^2 is much greater than the contrast of the degraded image, the contrast is assumed to be primarily due to the signal s and is significantly attenuated. Conversely, in the case that the estimated $\hat{\sigma}_f^2$ is greater than σ_s^2, the local contrast is credited to the original image and little processing is done [20].

Once obtained from the image restoration, the restored image is subtracted from the stegoimage to yield an estimate of the embedded signal, $\hat{s}$. This is then compared with an

identical copy of the pseudorandom wideband waveform used at the encoder. The generation of the identical pseudorandom wideband waveforms is accomplished by the possession of a common key, which is used as a seed for duplicate random number generators known only to the sender and receiver. The typical spread-spectrum challenge of synchronization of these waveforms is obviously alleviated in this system because the beginning of the stegoimage is easily identified.

Even though the image restoration yields good performance, the estimate of such a low power signal, which is necessary to provide the degree of invisibility essential for a steganographic system, is rather poor. The probability of error encountered during the estimation process is the embedded signal BER. Therefore, in order to compensate for the suboptimal performance of the signal estimation process, we have incorporated the use of error-control coding.

4.3 Error-Control Coding

The use of error correction by SSIS compensates for the suboptimal estimation of the embedded signal and combats distortion that may be encountered during the transmission process. The despread message signal may have a substantial number of bit errors, indicated by a high embedded signal BER. When a large number of errors are expected to occur in a block of data, a low-rate error-correcting code must be used to correct them. The use of low-rate error-correcting codes within the SSIS system allows the hidden message to be recovered without error when the transmission channel is noiseless, thus compensating for the signal estimation process. When the transmission channel is expected to be noisy, an appropriate low-rate error-correcting code can be selected to provide desired performance. Any error-correcting code that is capable of correcting for the high signal estimation BER can be used within SSIS. For proof of concept, binary expansions of Reed-Solomon codes [24] described here are used by SSIS for error correction.

Error-correcting codes are designated as (n, k) codes with rate k/n, where n indicates the number of output symbols and k the number of input symbols. The simplest low-rate codes are $(n, 1)$ repetition codes, which repeat each information bit n times and decode by voting on the repeated bits. This works well for relatively short block lengths, but as n increases the rate, $1/n$ becomes very low. According to the fundamental theorem of information theory, we should be able to reduce the decoded error rate as low as we want at any fixed rate below channel capacity if we increase the block length and find appropriate codes and decoders.

Reed-Solomon codes are much more flexible than repetition codes. Using an alphabet of size 2^m, a $(2^m - 1, K)$ Reed-Solomon code exists for each K, so the rate can be chosen almost independently of the block length. And the error-correcting capabilities of these codes are optimal in the sense that they can correct as many symbol errors as possible. Any error pattern with fewer than $\frac{(2^m - K)}{2}$ symbol errors can be corrected. Unfortunately, the block length of a Reed-Solomon code is limited by the size of the alphabet.

If we want to use Reed-Solomon codes to correct binary errors, we must map each symbol into m bits. The resulting binary code has a block length of $m(2^m - 1)$ bits and mK

information bits. But if we use a conventional Reed-Solomon decoder, a single bit error will be treated as a symbol error, and most patterns with more than $\frac{(2^m-K)}{2}$ bit errors will not be correctable. This would be far from optimal performance for a binary code.

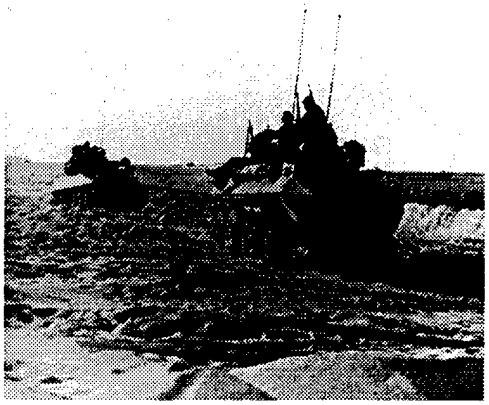
However, we have computed the true minimum distances of many binary expansions of Reed-Solomon codes [24] and found that most of them can correct many more binary errors if a decoder that corrects bits instead of symbols is used. The decoders described in [24] are based on a simple idea of Bossert and Hergert [25]: if we have a large number of low-weight parity checks, then the number of failing parity checks tends to be proportional to the number of errors. Using this idea, we can change whichever bits reduce the number of failing parity checks until no checks fail. This algorithm works very well with binary expansions of low-rate Reed-Solomon codes because they have a large number of low-weight parity checks. With some other improvements described in [24], these decoders can correct far more binary errors than conventional Reed-Solomon decoders for the same codes. For example, the (2040,32) decoder corrects most error patterns with fewer than 763 bit errors, while a conventional Reed-Solomon decoder would be limited to 125 symbol errors, which is typically about 165 bit errors. The rate of this (2040,32) code is similar to that of a (64,1) repetition code, but because it has a much longer block length, its decoded error rate drops much more quickly as the fraction of errors per block is reduced. Even better error correction is possible with these codes if a maximum-likelihood decoder is used. However, this type of coder is practical only with codes that have small block length.

The use of low-rate error-correcting codes within the SSIS system allows the hidden message to be recovered without error when the transmission channel is noiseless, thus compensating for the embedded signal estimation process. When the transmission channel is expected to be noisy, the appropriate low-rate error-correcting code can be selected to provide desired performance.

5. SSIS Performance

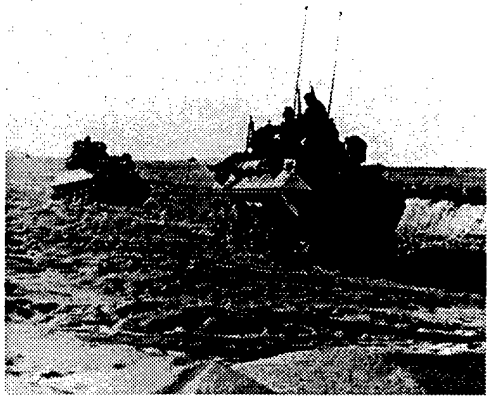
Two images are used to demonstrate the performance of SSIS. The original 512×512 images, containing 262 kilobytes, appear in Figure 4 (entitled LAV-25 and Allison, respectively). To maximize capacity, we presume the hidden message will be compressed. Assuming that the compression method is intolerant of errors, as is the case with Huffman and arithmetic coding, we strive for total error-free recovery of the hidden data.

As an example, we have hidden messages within the images of Figure 4, denoted images with embedded signal, low SNR. The steganographic SNR, the ratio of embedded signal power to cover image power, for these two image is -35 and -31 dB, respectively. For the LAV-25 image, the embedded signal BER is .25, requiring the use of an (889,35) error correcting encoder. This coder can correct a block that is 27% in error. This yields a capacity of 1.2 kilobytes of hidden information. The Allison image with low SNR has an embedded message capacity of 500 bytes, where a (2040,32) code is used to compensate for the BER of .29.



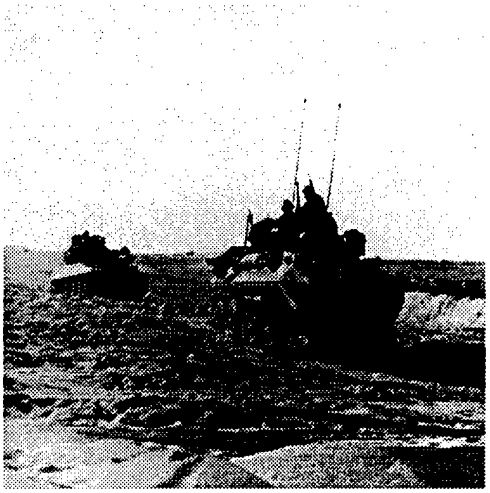
LAV-25 Original Image

Allison Original Image



LAV-25 With Embedded Signal, Low SNR.

Allison With Embedded Signal, Low SNR.



LAV-25 With Embedded Signal, Higher SNR.

Allison With Embedded Signal, Higher SNR.

Figure 4. Example of SSIS Performance.

By increasing the SNR, the performance of embedded signal estimation is improved at the loss of some imperceptiveness. To demonstrate, a higher power AWGN signal is used to embed information into the images of Figure 4, embedded signal with higher SNR, yielding SNR values of -30 and -27 dB, respectively. These images show only slight degradation that is not readily apparent to a human observer. The LAV-25 image of Figure 4 with higher SNR has a capacity of nearly 5 kilobytes using a (155,25) maximum likelihood decoder to compensate for the signal estimation BER of .21. For the Allison image with higher SNR, the (889,35) code is utilized to provide a hiding capacity of 1.2 kilobytes of information.

In order to provide more insight into the presented methodology, a comparison between the original image pixels and the stegoimage pixels is presented in Figure 5. Here a single row of pixels has been extracted from both the original LAV-25 image and the corresponding stegoimage with high SNR. It is evident that slight discrepancies between the two exist. However these discrepancies are slight and undetectable by human observer. Furthermore, without possession of the original image, the embedded signal is undetectable by computer analysis. The text hidden in the images is from an ASCII file containing the Treaty of Paris. This text is attached in the Appendix.

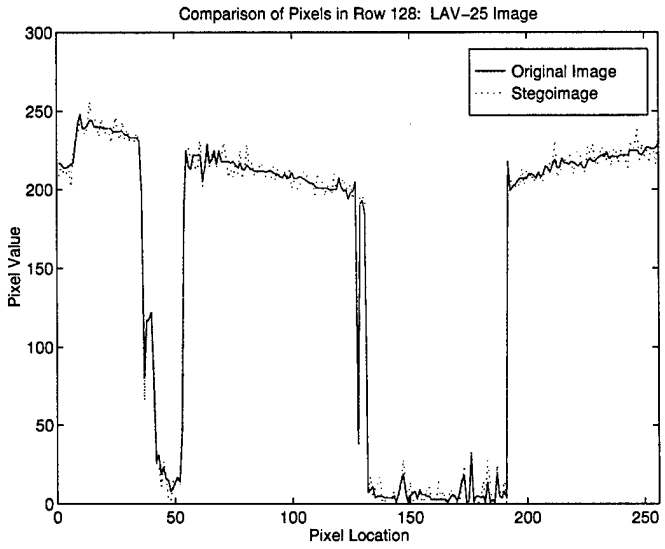


Figure 5. Comparison of Original Image Pixels to Stegoimage Pixels.

6. Conclusions/Future Work

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 or dynamic range of the image. Additionally, the original image is not needed to extract the hidden message. A level of security is provided by the necessity that both sender and receiver possess the same keys. Furthermore, the embedded signal power is insignificant compared to that of the

cover image, providing low probability of detection and leaving an observer unaware that the hidden data exist.

Future work will include improving the embedded signal estimation process in order to lower the signal estimation BER so that higher rate error-correcting codes may be employed, which will increase the capacity of this system.

7. References

[1] Bender, W., D. Gruhl, N. Morimoto, and A. Lu. "Techniques for Data Hiding." *IBM Systems Journal*, vol. 35, nos. 3 and 4, 1996.

[2] Cox, I. J., 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, vol. 3, pp. 243–246, September 1996.

[3] Kahn, D. *The Codebreakers - The Story of Secret Writing*. New York: Scribner, 1967.

[4] Pfitzmann, B. "Trials of Traced Traitors." *Lecture Notes in Computer Science: Information Hiding, First International Workshop*, edited by R. Anderson, vol. 1174, pp. 49–64, Berlin: Springer-Verlag, 1996.

[5] Smith, J. R., and B. O. Comisky. "Modulation and Information Hiding in Images." *Lecture Notes in Computer Science: Information Hiding, First International Workshop*, edited by R. Anderson, vol. 1174, pp. 207–226, Berlin: Springer-Verlag, 1996.

[6] Van Schyndel, R., A. Tirkel, and C. Osborne. "A Digital Wartermark." *Proceedings of the IEEE International Conference on Image Processing*, vol. 2, pp. 86–90, 1994.

[7] Wolfgang, R. B., and E. J. Delp. "A Watermark for Digital Images." *Proceedings of the IEEE International Conference on Image Processing*, Lausanne, Switzerland, vol. 3, pp. 219–222, September 1996.

[8] Machado, R. "Stego." http://www.fqa.com/romana/romanasoft/stego.html, 1997.

[9] Milbrandt, E. "Steganography Info and Archive." http://members/iquest.net/mrmil/stego.html, October 1997.

[10] Podilchuk, C. I., and W. Zeng. "Digital Image Watermarking Using Visual Models." *Human Vision and Electronic Imaging II*, edited by. B. E. Rogowitz and T. N. Pappas, vol. 3016, pp. 100–111, SPIE, February 1997.

[11] Swanson, M. D., B. Zhu, and A. H. Tewfik. "Transparent Robust Image Watermarking." *Proceedings of the IEEE International Conference on Image Processing*, Lausanne, Switzerland, vol. 3, pp. 211–214, September 1996.

[12] Tanaka, K., Y. Nakamura, and K. Matsui. "Embedding Secret Information Into a Dithered Multi-Level Image. *Proceedings of the IEEE Military Communications Conference*, Monterey, CA, pp. 216–220, 1990.

[13] Davern, P., and M. Scott. "Fractal Based Image Steganography." *Lecture Notes in Computer Science: Information Hiding, First International Workshop*, edited by R. Anderson, pp. 279–294, Berlin: Springer-Verlag, 1996.

[14] Swanson, M. D., B. Zhy, and A. H. Tewfik. "Robust Data Hiding for Images." *Proceedings of the IEEE Digital Signal Processing Workshop*, Loen, Norway, pp. 37–40, September 1996.

[15] Cox, I. J., J. Kilian, T. Leighton, and T. Shamoon. "Secure Spread Spectrum, Watermarking for Multimedia." Technical report 95-128, NEC Research Institute, Princeton, NJ, August 1995.

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

[17] Simon, M. K., J. K. Omura, R. A. Scholtz, and B. K. Levitt. *Spread Spectrum Communications, Volume I.* Rockville, MD: Computer Science Press, 1985.

[18] Schneier, B. *Applied Cryptography - Protocols, Algorithms, and Source Code in C.* New York: John Wiley and Sons, Inc., 1996.

[19] Hartung, F., and B. Girod. "Fast Public-Key Watermarking of Compressed Video. *Proceedings of the IEEE International Conference on Image Processing*, Santa Barbara, CA, October 1997.

[20] Lim, J. S. *Two-Dimensional Signal and Image Processing*. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1990.

[21] Trussel, H. J., and B. R. Hunt. "Sectioned Methods in Image Processing." *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 26, pp. 157–164, April 1978.

[22] Kuan, D. T., A. A. Sawchuk, T. C. Strand, and P. Chavel. "Adaptive Noise Smoothing Filters for Images With Signal-Dependent Noise." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 7, pp. 165–177, March 1985.

[23] Lee, J. S.. "Digital Image Enhancement and Noise Filtering by Use of Local Statistics." *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 2, pp. 165–168, March 1980.

[24] Retter, C. T. "Decoding Binary Expansions of Low-Rate Reed-Solomon Codes Far Beyond the BCH Bound." *Proceedings of the 1995 IEEE International Symposium on Information Theory*, Whistler, British Columbia, p. 276, September 1995.

[25] Bossert, M., and F. Hergert. "Hard- and Soft-Decision Decoding Beyond the Half Minimum Distance - An Algorithm for Linear Codes." *IEEE Transactions on Information Theory*, vol. 32, no. 5, pp. 709–714, September 1986.

Appendix:

The Paris Peace Treaty of 1783

INTENTIONALLY LEFT BLANK.

The Paris Peace Treaty of 1783 (Which ended the Revolutionary War)

In the name of the most holy and undivided Trinity.

It having pleased the Divine Providence to dispose the hearts of the most serene and most potent Prince George the Third, by the grace of God, king of Great Britain, France, and Ireland, defender of the faith, duke of Brunswick and Lunebourg, arch-treasurer and prince elector of the Holy Roman Empire etc., and of the United States of America, to forget all past misunderstandings and differences that have unhappily interrupted the good correspondence and friendship which they mutually wish to restore, and to establish such a beneficial and satisfactory intercourse, between the two countries upon the ground of reciprocal advantages and mutual convenience as may promote and secure to both perpetual peace and harmony; and having for this desirable end already laid the foundation of peace and reconciliation by the Provisional Articles signed at Paris on the 30th of November 1782, by the commissioners empowered on each part, which articles were agreed to be inserted in and constitute the Treaty of Peace proposed to be concluded between the Crown of Great Britain and the said United States, but which treaty was not to be concluded until terms of peace should be agreed upon between Great Britain and France and his Britannic Majesty should be ready to conclude such treaty accordingly; and the treaty between Great Britain and France having since been concluded, his Britannic Majesty and the United States of America, in order to carry into full effect the Provisional Articles above mentioned, according to the tenor thereof, have constituted and appointed, that is to say his Britannic Majesty on his part, David Hartley, Esqr., member of the Parliament of Great Britain, and the said United States on their part, John Adams, Esqr., late a commissioner of the United States of America at the court of Versailles, late delegate in Congress from the state of Massachusetts, and chief justice of the said state, and minister plenipotentiary of the said United States to their high mightinesses the States General of the United Netherlands; Benjamin Franklin, Esqr., late delegate in Congress from the state of Pennsylvania, president of the convention of the said state, and minister plenipotentiary from the United States of America at the court of Versailles; John Jay, Esqr., late president of Congress and chief justice of the state of New York, and minister plenipotentiary from the said United States at the court of Madrid; to be plenipotentiaries for the concluding and signing the present definitive treaty; who after having reciprocally communicated their respective full powers have agreed upon and confirmed the following articles.

Article 1: His Britannic Majesty acknowledges the said United States, viz., New Hampshire, Massachusetts Bay, Rhode Island and Providence Plantations, Connecticut, New York, New Jersey, Pennsylvania, Maryland, Virginia, North Carolina, South Carolina and Georgia, to be free sovereign and independent states, that he treats with them as such, and for himself, his heirs, and successors, relinquishes all claims to the government, propriety, and territorial rights of the same and every part thereof.

Article 2: And that all disputes which might arise in future on the subject of the boundaries of the said United States may be prevented, it is hereby agreed and declared, that the following are and shall be their boundaries, viz.; from the northwest angle of Nova Scotia, viz., that angle which is formed by a line drawn due north from the source of St. Croix River to the highlands; along the said highlands which divide those rivers that empty them-

selves into the river St. Lawrence, from those which fall into the Atlantic Ocean, to the northwestern most head of Connecticut River; thence down along the middle of that river to the forty-fifth degree of north latitude; from thence by a line due west on said latitude until it strikes the river Iroquois or Cataraquy; thence along the middle of said river into Lake Ontario; through the middle of said lake until it strikes the communication by water between that lake and Lake Erie; thence along the middle of said communication into Lake Erie, through the middle of said lake until it arrives at the water communication between that lake and Lake Huron; thence along the middle of said water communication into Lake Huron, thence through the middle of said lake to the water communication between that lake and Lake Superior; thence through Lake Superior northward of the Isles Royal and Phelipeaux to the Long Lake; thence through the middle of said Long Lake and the water communication between it and the Lake of the Woods, to the said Lake of the Woods; thence through the said lake to the most northwestern most point thereof, and from thence on a due west course to the river Mississippi; thence by a line to be drawn along the middle of the said river Mississippi until it shall intersect the northernmost part of the thirty-first degree of north latitude, South, by a line to be drawn due east from the determination of the line last mentioned in the latitude of thirty-one degrees of the equator, to the middle of the river Apalachicola or Catahouche; thence along the middle thereof to its junction with the Flint River, thence straight to the head of St. Mary's River; and thence down along the middle of St. Mary's River to the Atlantic Ocean; east, by a line to be drawn along the middle of the river St. Croix, from its mouth in the Bay of Fundy to its source, and from its source directly north to the aforesaid highlands which divide the rivers that fall into the Atlantic Ocean from those which fall into the river St. Lawrence; comprehending all islands within twenty leagues of any part of the shores of the United States, and lying between lines to be drawn due east from the points where the aforesaid boundaries between Nova Scotia on the one part and East Florida on the other shall, respectively, touch the Bay of Fundy and the Atlantic Ocean, excepting such islands as now are or heretofore have been within the limits of the said province of Nova Scotia.

Article 3: It is agreed that the people of the United States shall continue to enjoy unmolested the right to take fish of every kind on the Grand Bank and on all the other banks of Newfoundland, also in the Gulf of St. Lawrence and at all other places in the sea, where the inhabitants of both countries used at any time heretofore to fish. And also that the inhabitants of the United States shall have liberty to take fish of every kind on such part of the coast of Newfoundland as British fishermen shall use, (but not to dry or cure the same on that island) and also on the coasts, bays and creeks of all other of his Britannic Majesty's dominions in America; and that the American fishermen shall have liberty to dry and cure fish in any of the unsettled bays, harbors, and creeks of Nova Scotia, Magdalen Islands, and Labrador, so long as the same shall remain unsettled, but so soon as the same or either of them shall be settled, it shall not be lawful for the said fishermen to dry or cure fish at such settlement without a previous agreement for that purpose with the inhabitants, proprietors, or possessors of the ground.

Article 4: It is agreed that creditors on either side shall meet with no lawful impediment to the recovery of the full value in sterling money of all bona fide debts heretofore contracted.

Article 5: It is agreed that Congress shall earnestly recommend it to the legislatures of the respective states to provide for the restitution of all estates, rights, and properties, which have been confiscated belonging to real British subjects; and also of the estates, rights, and properties of persons resident in districts in the possession on his Majesty's arms and who have not borne arms against the said United States. And that persons of any other description shall have free liberty to go to any part or parts of any of the thirteen United States and therein to remain twelve months unmolested in their endeavors to obtain the restitution of such of their estates, rights, and properties as may have been confiscated; and that Congress shall also earnestly recommend to the several states a reconsideration and revision of all acts or laws regarding the premises, so as to render the said laws or acts perfectly consistent not only with justice and equity but with that spirit of conciliation which on the return of the blessings of peace should universally prevail. And that Congress shall also earnestly recommend to the several states that the estates, rights, and properties, of such last mentioned persons shall be restored to them, they refunding to any persons who may be now in possession the bona fide price (where any has been given) which such persons may have paid on purchasing any of the said lands, rights, or properties since the confiscation.

And it is agreed that all persons who have any interest in confiscated lands, either by debts, marriage settlements, or otherwise, shall meet with no lawful impediment in the prosecution of their just rights.

Article 6: That there shall be no future confiscations made nor any prosecutions commenced against any person or persons for, or by reason of, the part which he or they may have taken in the present war, and that no person shall on that account suffer any future loss or damage, either in his person, liberty, or property; and that those who may be in confinement on such charges at the time of the ratification of the treaty in America shall be immediately set at liberty, and the prosecutions so commenced be discontinued.

Article 7: There shall be a firm and perpetual peace between his Britannic Majesty and the said states, and between the subjects of the one and the citizens of the other, wherefore all hostilities both by sea and land shall from henceforth cease. All prisoners on both sides shall be set at liberty, and his Britannic Majesty shall with all convenient speed, and without causing any destruction, or carrying away any Negroes or other property of the American inhabitants, withdraw all his armies, garrisons, and fleets from the said United States, and from every post, place, and harbor within the same; leaving in all fortifications, the American artillery that may be therein; and shall also order and cause all archives, records, deeds, and papers belonging to any of the said states, or their citizens, which in the course of the war may have fallen into the hands of his officers, to be forthwith restored and delivered to the proper states and persons to whom they belong.

Article 8: The navigation of the river Mississippi, from its source to the ocean, shall forever remain free and open to the subjects of Great Britain and the citizens of the United States.

Article 9: In case it should so happen that any place or territory belonging to Great Britain or to the United States should have been conquered by the arms of either from the

other before the arrival of the said Provisional Articles in America, it is agreed that the same shall be restored without difficulty and without requiring any compensation.

Article 10: The solemn ratifications of the present treaty expedited in good and due form shall be exchanged between the contracting parties in the space of six months or sooner, if possible, to be computed from the day of the signatures of the present treaty. In witness whereof we the undersigned, their ministers plenipotentiary, have in their name and in virtue of our full powers, signed with our hands the present definitive treaty and caused the seals of our arms to be affixed thereto.

Done at Paris, this third day of September in the year of our Lord, one thousand seven hundred and eighty-three.

D. HARTLEY (SEAL) JOHN ADAMS (SEAL) B. FRANKLIN (SEAL) JOHN JAY (SEAL) [Image]

NO. OF COPIES ORGANIZATION

2 DEFENSE TECHNICAL INFORMATION CENTER
DTIC DDA
8725 JOHN J KINGMAN RD
STE 0944
FT BELVOIR VA 22060-6218

1 HQDA
DAMO FDQ
DENNIS SCHMIDT
400 ARMY PENTAGON
WASHINGTON DC 20310-0460

1 DPTY ASSIST SCY FOR R&T
SARD TT F MILTON
RM 3EA79 THE PENTAGON
WASHINGTON DC 20310-0103

1 OSD
OUSD(A&T)/ODDDR&E(R)
J LUPO
THE PENTAGON
WASHINGTON DC 20301-7100

1 CECOM
SP & TRRSTRL COMMCTN DIV
AMSEL RD ST MC M
H SOICHER
FT MONMOUTH NJ 07703-5203

1 PRIN DPTY FOR TCHNLGY HQ
US ARMY MATCOM
AMCDCG T
M FISETTE
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 DPTY CG FOR RDE HQ
US ARMY MATCOM
AMCRD
BG BEAUCHAMP
5001 EISENHOWER AVE
ALEXANDRIA VA 22333-0001

1 INST FOR ADVNCD TCHNLGY
THE UNIV OF TEXAS AT AUSTIN
PO BOX 202797
AUSTIN TX 78720-2797

NO. OF COPIES ORGANIZATION

1 GPS JOINT PROG OFC DIR
COL J CLAY
2435 VELA WAY STE 1613
LOS ANGELES AFB CA 90245-5500

3 DARPA
L STOTTS
J PENNELLA
B KASPAR
3701 N FAIRFAX DR
ARLINGTON VA 22203-1714

1 US MILITARY ACADEMY
MATH SCI CTR OF EXCELLENCE
DEPT OF MATHEMATICAL SCI
MDN A MAJ DON ENGEN
THAYER HALL
WEST POINT NY 10996-1786

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CS AL TP
2800 POWDER MILL RD
ADELPHI MD 20783-1145

1 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CS AL TA
2800 POWDER MILL RD
ADELPHI MD 20783-1145

3 DIRECTOR
US ARMY RESEARCH LAB
AMSRL CI LL
2800 POWDER MILL RD
ADELPHI MD 20783-1145

ABERDEEN PROVING GROUND

4 DIR USARL
AMSRL CI LP (305)

NO. OF COPIES ORGANIZATION

2 DIRECTOR
US ARO
AMXRO EL
DR W SANDER
DR J FREEBERSYSER
PO BOX 12211
RESEARCH TRIANGLE PARK NC
22709-2211

1 COMMANDANT
US MILITARY ACADEMY
WEST POINT NY 10996

1 COMMANDANT
US NAVAL ACADEMY
ANNAPOLIS MD 21404

1 COMMANDANT
US AIR FORCE ACADEMY
COLORADO SPRINGS CO 80840

1 DIRECTOR
NAVAL RESEARCH LABORATORY
WASHINGTON DC
20375-5000

1 ERICSSON INC
ALI KHAYRALLAH
ADVANCED DEV AND RSRCH
7001 DEVELOPMENT DRIVE
RESEARCH TRIANGLE PARK NC
27709

1 UNIV OF DELAWARE
DEPT OF ELECTRICAL ENGR
C BONCELET
NEWARK DE 19716

NO. OF COPIES ORGANIZATION

ABERDEEN PROVING GROUND

21 DIR USARL
AMSRL IS
J GANTT
R SLIFE
P EMMERMAN
AMSRL IS TP
J GOWENS
A COOPER
C RETTER (2 CP)
S CHAMBERLAIN
D TORRIERI
L SADLER
G CIRINCIONE
G HARTWIG
D GWYN
H CATON
M LOPEZ
F BRUNDICK
C SARAFIDIS
L MARVEL (4 CP)

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	June 1998	Final, Feb 97-Feb 98

4. TITLE AND SUBTITLE
Methodology of Spread-Spectrum Image Steganography

5. FUNDING NUMBERS
PN: 611102.H44

6. AUTHOR(S)
Lisa M. Marvel, Charles G. Boncelet, Jr.,* and Charles T. Retter

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
U.S. Army Research Laboratory
ATTN: AMSRL-IS-TA
Aberdeen Proving Ground, MD 21005-5067

8. PERFORMING ORGANIZATION REPORT NUMBER
ARL-TR-1698

9. SPONSORING/MONITORING AGENCY NAMES(S) AND ADDRESS(ES)

10.SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
*Charles C. Boncelet, Jr., is with the Department of Electrical Engineering, University of Delaware, Newark, DE 19716.

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This report presents a new method of digital steganography, entitled Spread-Spectrum Image Steganography (SSIS). Steganography, which means "covered writing" in Greek, is the science of communicating in a hidden manner. Following a brief history of this art and a discussion of steganographic communication theory, the new method, SSIS, is introduced. This system hides and recovers messages of substantial length within digital imagery while maintaining the original image size and dynamic range. The hidden messages can be recovered using appropriate keys without any knowledge of the original image. Image processing, error control coding, and spread-spectrum techniques utilized are described, and the performance of the technique is illustrated. A message embedded by this method can be in the form of text, imagery, or any other digital signal. Applications for such data-hiding scheme include in-band captioning, covert communication, image tamperproofing, authentication, embedded control, and revision tracking.

14. SUBJECT TERMS	15. NUMBER OF PAGES
steganography, information hiding, communications	29
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	SAR

INTENTIONALLY LEFT BLANK.

USER EVALUATION SHEET/CHANGE OF ADDRESS

This Laboratory undertakes a continuing effort to improve the quality of the reports it publishes. Your comments/answers to the items/questions below will aid us in our efforts.

1. ARL Report Number/Author ARL-TR-1698 (Marvel) Date of Report June 1998

2. Date Report Received _____

3. Does this report satisfy a need? (Comment on purpose, related project, or other area of interest for which the report will be used.) _____

4. Specifically, how is the report being used? (Information source, design data, procedure, source of ideas, etc.) _____

5. Has the information in this report led to any quantitative savings as far as man-hours or dollars saved, operating costs avoided, or efficiencies achieved, etc? If so, please elaborate. _____

6. General Comments. What do you think should be changed to improve future reports? (Indicate changes to organization, technical content, format, etc.) _____

CURRENT ADDRESS

_____
Organization

_____
Name E-mail Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

7. If indicating a Change of Address or Address Correction, please provide the Current or Correct address above and the Old or Incorrect address below.

OLD ADDRESS

_____
Organization

_____
Name

_____
Street or P.O. Box No.

_____
City, State, Zip Code

(Remove this sheet, fold as indicated, tape closed, and mail.)

(DO NOT STAPLE)