Spread Spectrum Image Steganography

Lisa M. Marvel, *Member, IEEE,* Charles G. Boncelet, Jr., *Member, IEEE,* and Charles T. Retter, *Member, IEEE*

***Abstract*— In this paper, we present 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 discussion of steganographic communication theory and review of existing techniques, the new method, SSIS, is introduced. This system hides and recovers a message of substantial length within digital imagery while maintaining the original image size and dynamic range. The hidden message can be recovered using appropriate keys without any knowledge of the original image. Image restoration, error-control coding, and techniques similar to spread spectrum are described, and the performance of the system is illustrated. A 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, covert communication, image tamperproofing, authentication, embedded control, and revision tracking.**

***Index Terms*—Information hiding, steganography.**

I. 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 *payload*, 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 did not have the capability to decode the information, the image would be displayed without degradation, leaving the viewer unaware that the hidden data exist. These are but a few of the possible uses of image steganography.

Manuscript received February 28, 1998; revised October 23, 1998. This work was performed 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. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Naohisa Ohta.

L. M. Marvel and C. T. Retter are with the U.S. Army Research Laboratory, Aberdeen Proving Ground, MD 21005 USA (e-mail: marvel@arl.mil).

C. G. Boncelet, Jr. is with the Department of Electrical Engineering, University of Delaware, Newark, DE 19716 USA (e-mail: boncelet@ee.udel.edu).

Publisher Item Identifier S 1057-7149(99)05999-0.

II. Background/Existing Methods

Steganography is not a new science. In fact, several examples from the times of ancient Greece are cited in Kahn [3]. Familiar steganography techniques include invisible inks, the use of carrier pigeons, and the microdot. For a more thorough treatment of steganography schemes, the reader is referred to [4].

As more of today's communication occurs electronically, there have been advancements utilizing digital multimedia signals as vehicles for steganographic communication. These signals, which are typically audio, video, or still imagery, are *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 [5]. 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 to extract the hidden information. More pragmatic methods, known as blind 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 generic blind image steganographic system is depicted in Fig. 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.

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

1057–7149/99$10.00 © 1999 IEEE

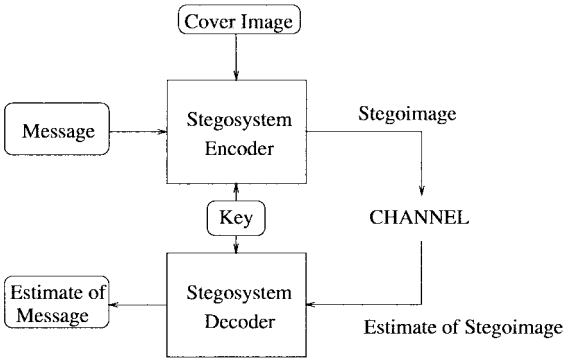


Fig. 1. Overview of steganographic system.

watermarking. This thrust can be attributed to the desire for copyright protection, spurred by the widespread use of imagery on the Internet and the ease in which a perfect reproduction of a digital image 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 utilizing the theories of communication [6]. The parameters of information hiding, such as the number of data bits that can be hidden, 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 maximum number of bits hidden and successfully recovered by the stegosystem. The SNR 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 and capacity while adhering to the low steganographic-SNR constraints. Therefore, the acceptable balance of these items must be dictated by the application. For example, an information-hiding scheme may forego 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. The reader is referred to [7] for more information on the theoretical capacity of the steganographic channel.

Digital steganography is currently a very active research area, encompassing methods of copyright protection, image authentication, and hidden communications. Since our method is one of data hiding for hidden communication, where the emphasis is placed upon invisibility and the amount of payload, we limit our 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 LSB's with message bits to some type of logical or arithmetic combination between the two. Several examples of LSB schemes can be found in [8]–[10]. LSB manipulation programs have also been written for a variety of image formats and can be found in [11]. LSB methods typically achieve both high payload 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 [2], [12], and [13].

Several procedures for data hiding in multimedia can be found in [1]. One of these, called *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 [6]. 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. 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 *et al.* [14]. With this method, the dot patterns of the ordered dither pixels are controlled by the information bits to be concealed. This system accommodates 2 kB of hidden information for a bilevel 256×256 image, yielding a payload of data or information-hiding ratio of one information bit to four cover image bits. An information-hiding ratio of $1:6$ is obtained for trilevel images of the same size. The method has high payload 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 [15]. 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 *et al.* [16] utilizes 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 [17]. This masking is performed in either the spatial or frequency domain using techniques similar to [2] and [6] without cover image escrow.

Our method of *spread spectrum image steganography* (SSIS) is a steganographic communication method that uses digital imagery as a cover signal. It is not to be considered a watermarking method, but rather a data-hiding method that provides the ability to embed a significant amount of information within digital images while avoiding detection by an observer, thereby placing emphasis on the maximization of payload and invisibility. Furthermore, SSIS is a blind scheme where the original image is not needed to extract the hidden information. The proposed recipient need only possess a key to reveal the hidden message; otherwise, the very existence of the hidden information is virtually undetectable.

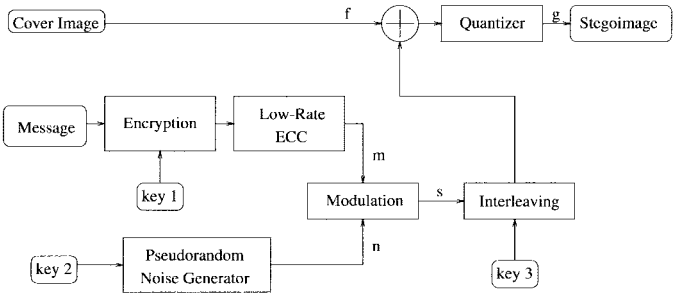


Fig. 2. SSIS encoder.

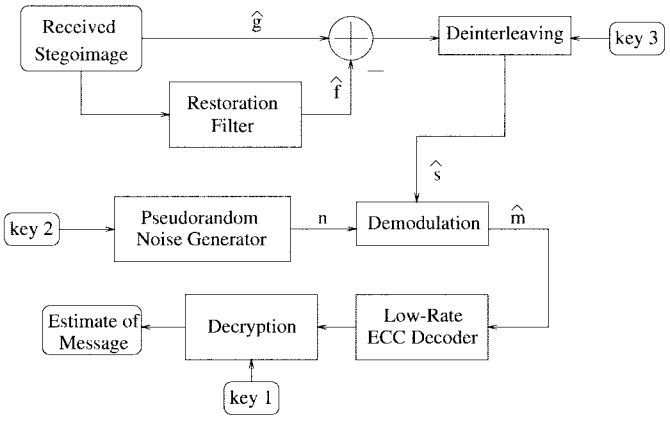


Fig. 3. SSIS decoder.

III. SSIS

Techniques of error-control coding, image restoration, and those similar to spread spectrum communication are combined within the SSIS system. The fundamental concept is the embedding of the hidden information within noise, which is then added to a digital cover 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 or by computer analysis without access to the original image. To successfully decode the message, image restoration techniques and error-control coding are employed. Image restoration is used to obtain an approximate estimate of the original cover image from the stegoimage. This promotes the estimation of the embedded signal that was added to the cover, in addition to allowing SSIS to be a blind steganography scheme. 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 an embedded signal bit error rate (BER) that is rather high. To compensate, the message signal is processed by a low-rate error-correcting code before embedding. 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 Fig. 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, producing a real-valued noise sequence, n. Subsequently, the modulation scheme is used to combine the message with the noise sequence, thereby composing the embedded signal, s, which is then input into an interleaver using key 3. This signal is now added with the cover image f to produce the stegoimage g, which is appropriately quantized and clipped 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 by the recipient, who maintains the same keys as the sender, uses the stegosystem decoder (shown in Fig. 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 noise 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.

The interleaver in this scheme, which reorders the embedded signal before it is added to the cover image, serves a dual function. The first is to prevent a group or *burst* of errors. This allows the errors to occur almost independently within a codeword, thus giving the error-correcting code an equal chance at correcting the errors in all codewords. Second, since the interleaver requires a key to stipulate the interleaving algorithm, this key can serve as another level of security to establish the proper order of the embedded signal before decoding.

Fig. 4. LAV-25.

Fig. 6. Barbara.

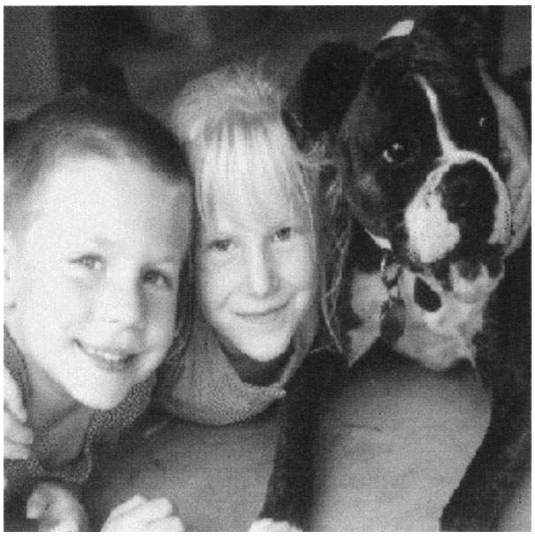


Fig. 5. Allison.

Fig. 7. Ulm.

SSIS uses inherent noise to hide information within the digital image. Since wideband thermal noise, inherent to imagery of natural scenes captured by photoelectronic systems, can be modeled as additive white Gaussian noise (AWGN) [18], this type of noise is used in the SSIS system. In other types of coherent imaging, the noise can be modeled as speckle noise [18], 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.

A. 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 a variation of this technique to embed a message, typically a binary signal, within samples of a low-power white Gaussian noise sequence consisting of real numbers. The resulting signal, which is perceived as noise, is then combined with the cover image to produce the stegoimage. Since the power of the embedded signal is much lower than the power of the cover image, the SNR is low, indicating low perceptibility and low probability of detection by an observer. Subsequently, if embedded signal power is much less than the power of the image, an observer should be unable to visually distinguish the original image from the stegoimage. Additionally, since the message is encoded using a low-rate error-correcting code, the encoding has a similar spreading effect because a few message bits are spread among the many output bits of the error-correcting encoder.

Fig. 8. Eiger.

To construct the embedded signal, we incorporate the concept of a stored reference spread spectrum communications system [19]. 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 [20] and identical pseudorandom number generators. In addition, the pseudorandom number generators can be cryptographically secure.

First, we describe a simple sign modulation scheme to provide an example of our spread spectrum process. This method is similar to the technique used in [21]. 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 normal distribution with zero mean and some variance, N. The two signals are modulated, or multiplied as in (1), resulting in a sequence of real numbers. In this simple example, the sign of each noise sample is changed corresponding to the value of the message bit to be embedded. The white Gaussian characteristics of the signal is 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 embedded sequence, $\hat{s}$, to recover an estimated value of the message signal, $\hat{m}$, as shown in (2).

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

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

Although this very simple system meets the necessary requirements of producing a Gaussian sequence regardless of the message signal values, a major deficiency lies within the detection of this signal in the presence of noise. This noise usually results from poor embedded signal estimation but also can be contributed by the channel during transmission. Since only the variation of the sign of embedded signal samples indicates the message, a majority of the values occur in the vicinity of zero. Moreover, the distance between s when $m = -1$ and s when $m = 1$ is typically small, leading to the problematic detection of m.

TABLE I
SSIS IMAGE RESTORATION FILTER PERFORMANCE

Image Restoration	MSE	Embedded Signal BER
Mean Filter	43.7179	0.1910
Alpha-Trimmed Mean Filter	36.4321	0.1892
Median Filter	23.5004	0.2083
Adaptive Wiener Filter	10.6198	0.2543

Therefore, in order to improve detection performance, a nonlinear modulation scheme was developed for SSIS. This modulation technique provides an increase in the minimum Euclidean distance between the possible modulated values, thereby enabling an improved estimate of the embedded signal. For this modulation technique, a random sequence, u, that is uniformly distributed between (0, 1) is generated. A second sequence is generated by applying the nonlinear transformation of (3) to u, which produces u', another uniform random sequence. The transformation of (3) maximizes the minimum distance between u and u'. The embedded signal value, s_i, is then formed by selecting from u_i or u'_i, arbitrated by the message bit and then transformed to a Gaussian random value, as shown in (4), where Φ^{-1} represents the inverse cumulative distribution function for a standard Gaussian random variable.

$$u'_i = \begin{cases} u_i + 0.5 & 0 \le u_i < 0.5 \\ u_i - 0.5 & 0.5 \le u_i \le 1 \end{cases} \tag{3}$$

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

To adjust the power of the embedded signal, a scale factor is applied to s. The signal is then added to the cover image, which is subsequently quantized and clipped to result in the stegoimage. The scale factor is selected based on human perception and the value to the embedded signal BER. Although an intruder may be aware of the general strategy of the system, the key necessary to generate n is unknown and may thereby prevent decoding of the message. In addition, without the appropriate keys, the modulated signal is statistically indistinguishable from white Gaussian noise.

B. Image Restoration

At the receiver, the embedded signal must be extracted from the received stegoimage in order to be decoded. To do this, image restoration techniques, which filter much of the low-power embedded signal from the stegoimage, are implemented within the system to obtain an estimate of the original cover image. By subsequently subtracting the restored image from the received stegoimage, an estimate of the embedded signal is acquired. Using image restoration with SSIS eliminates the need for the recipient to possess a copy of the cover image.

Since the pixels of a digital image are locally correlated in natural scenes, filtering operations can be used to restore the original image. The challenge of embedded signal estimation can now be viewed as image restoration whose 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.

The performance of several restoration filters was evaluated within the SSIS system. It would seem reasonable that the best-performing filter in this context would be the one which provides the lowest overall mean-squared error (MSE) between the filtered image and the original cover image, thus providing a restored image that was much like the original cover image in a mean-squared sense. However, through experimentation we found that the filter that performed best within SSIS, by providing the lowest BER out of the decoder, was not the same filter that provided the lowest MSE.

To cite a brief example, Table I exhibits the MSE and resulting embedded signal BER $\hat{s}$ (the BER before the error-correcting decoder), for a sampling of the filters tested using the Lena image as a cover with a stegosignal power of 20. As is evident, the filter that produces a restored image with the lowest MSE is the adaptive Wiener filter implemented using Lee's algorithm [22]. However, this filter does not provide the lowest embedded signal BER. Through experimentation, it was determined that the alpha-trimmed mean filter presented in [23] provided lower embedded signal BER. Upon further investigation, it was determined that although the errors between the original image and the Wiener filtered image were small, they were very frequent in number and the errors encountered using the alpha-trimmed mean filter, although much larger in magnitude, were less numerous. Therefore, the alpha-trimmed mean filter provided better overall detection of the estimated embedded signal, $\hat{s}$.

The particular implementation of the alpha-trimmed mean filter used here is an order statistics filter of length N operating on sequence $\{x_j: j = k-M, \cdots, k, \cdots, k+M\}$ for N odd given by

$$y_k = \frac{1}{N-2l} \sum_{i=l}^{N-l} x_{(i)}^k \tag{5}$$

where $x_{(i)}^k$ is formed from the elements of x_j arranged in increasing order:

$$x_{(1)}^k \leq x_{(2)}^k \leq \cdots \leq x_{(N)}^k. \tag{6}$$

The overall parameter selection for our implementation was determined to be the alpha-trimmed filter with $N = 9$ using 3 $\times$ 3 pixel window with $l = 1$. Therefore, this filter estimates the center pixel by "trimming" the minimum and maximum values within the window and subsequently taking the mean of the remaining pixels.

Once obtained from the image restoration, $\hat{s}$ is then compared with an identical copy of the pseudorandom wideband waveform used at the encoder, n. 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. Synchronization of these waveforms is trivial in this system because the beginning of the stegoimage is easily identified.

Fig. 9. LAV-25 Stegoimage.

C. Error-Control Coding

Since the image restoration does not result in a perfect copy of the original cover image and the embedded signal is low power, the estimate of the embedded signal is poor. This results in a demodulated message signal that may have a substantial number of bit errors, indicated by a high embedded signal BER (typically greater than 0.15 BER). Therefore, to allow for the suboptimal performance of the signal estimation process, we have incorporated the use of low-rate error-control codes to correct the large number of bit errors.

Any error-correcting code that is capable of correcting the high signal estimation BER can be used within SSIS. For SSIS proof-of-concept, binary expansions of Reed–Solomon codes with a decoder based on a simple idea of Bossert and Hergert [25] using low-weight parity checks were used for error correction. This has now been extended to convolutional codes [26] using the Viterbi algorithm. The use of error correction by SSIS compensates for the suboptimal estimation of the embedded signal, in addition to combating distortion, which may be encountered during transmission of the stegoimage.

At the encoder, the entire decoding process can be simulated, thus permitting selection of the proper error-correcting code for the chosen cover image and embedded signal strength. This allows the assurance that the hidden message can be recovered, with high probability and error free when the transmission channel is noiseless. When the transmission channel is expected to be noisy, it is possible that an appropriate error-correcting code may be selected to correct for the additional errors caused by the channel. Similarly, the error correction may be able to compensate for the errors generated by the use of low levels of compression applied to the stegoimage.

IV. SSIS Performance

Five images with different characteristics are used to demonstrate the performance of SSIS. The original 256 $\times$ 256 images (containing 64 kB) appear in Figs. 4–8 and are entitled LAV-25, Allison, Barbara, Ulm, and Eiger, respectively. To maximize payload, we presume the hidden message will be

TABLE II
SSIS PERFORMANCE

Image	Stegosignal Power	Steganographic SNR	Embedded Signal BER	ECC Rate	Message BER	Payload (bpp)
LAV-25	30	-22.9595	0.2100	1/6	0	0.1667
Allison	40	-19.0858	0.1986	1/6	0	0.1667
Barbara	40	-17.4665	0.2608	35/889	0	0.0394
Ulm	80	-18.3786	0.1515	1/6	0	0.1667
Eiger	50	-17.2672	0.2637	35/889	0	0.0394

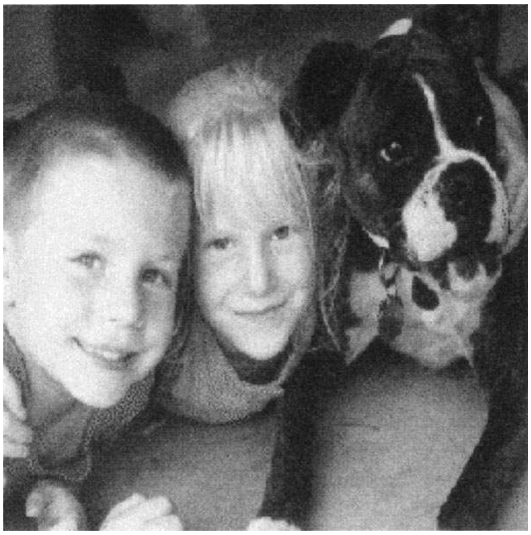


Fig. 10. Allison stegoimage.

Fig. 12. Ulm stegoimage.

Fig. 11. Barbara stegoimage.

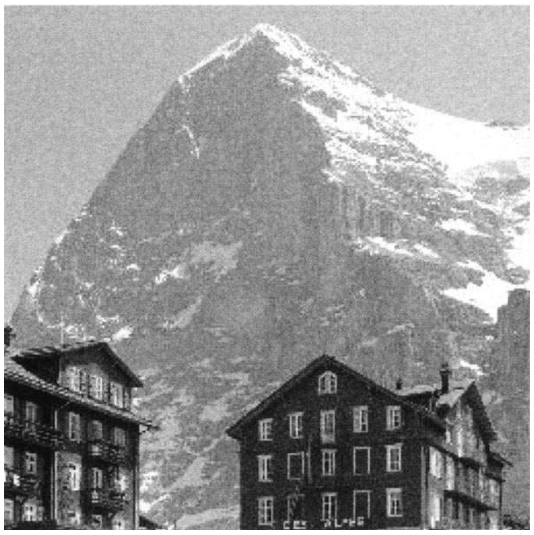


Fig. 13. Eiger stegoimage.

compressed. Furthermore, we assume that this compression method is intolerant of errors, as is the case with Huffman and arithmetic coding. Consequently, we strive for error-free recovery of the hidden data.

A text message was hidden within each of the images. The amplitude of the embedded signal for each image was selected based on visual considerations and embedded signal BER. Table II displays the amplitude or power of the embedded signal, the steganographic SNR (which is the ratio of embedded signal power to cover image power), the embedded signal BER, the rate of the error-correcting code used, the resulting message BER after error correction, and payload in bits per pixel (b/pixel). The stegoimages appear in Figs. 9–13.

The embedded signal estimation performs better for the images that have significant smooth areas such as the Ulm and LAV-25 images. This is reflected in the low embedded signal BER and correspondingly the low steganographic SNR. The embedded signal BER permits the use of the rate 1/6 convolutional code, which has a threshold (the level at which the code can typically correct all errors equal to and less than BER) of 0.22 BER. Conversely, images that have regions of high frequency (such as the Barbara and Eiger images) require

Fig. 14. Ulm stegoimage with added noise.

Fig. 15. Decompressed Ulm stegoimage.

a stronger embedded signal power, thus providing a lower steganographic SNR that yields a higher embedded signal BER and requiring an error-correcting code that can correct more errors. As we mention previously, any error-correcting code that is capable of correcting the embedded signal BER can be used. If higher rate codes can be used, the payload amount will increase, respectively.

The stegoimages can be made resistant to low levels of additive noise by selecting the proper error-correcting code. To demonstrate, we add white Gaussian noise, which is independent of the embedded signal, to the Ulm stegoimage of Fig. 12. When adding noise with a power of ten to the Ulm stegoimage, the embedded signal BER is increased from 0.1515 to 0.1845, which is still within the acceptable BER range for the particular error-control code used. By increasing the added noise to a power of 20, the embedded signal BER is increased to 0.2108—still within the BER range for this code. This noisy stegoimage is shown in Fig. 14. However, when the additive noise power is increased to 30, the embedded signal BER is 0.2311 and the decoded message BER results increase to 0.010 47. Consequently, a stronger error-control code must be used with this much additive noise for error-free message recovery.

Furthermore, the stegoimage can be made resistant to low levels of compression. Using the same stegoimage, we apply JPEG compression with a Q-factor of 95, resulting in a 4.43-b/pixel compressed image. Fig. 15 displays this decompressed JPEG image. After decompression at the decoder, the embedded signal BER is 0.1671, which is within the acceptable BER for this particular error-control code. By decreasing the Q-factor to 90, which results in a 3.30-b/pixel compressed image, the embedded signal BER is increased to 0.2057—remaining within the acceptable threshold for the error-correcting code. When the Q-factor is decreased to 85, yielding a 2.64-b/pixel compressed image, the resulting embedded signal BER is 0.2583, slightly above the BER threshold for the code. The compressed stegoimage in the present scenario produces a message BER of 0.0686. Furthermore, when the Q-factor is decreased once more to 80, providing a 2.21-b/pixel compressed image, the embedded signal BER becomes 0.3001, which is beyond the capabilities of this error-control code. In this case, the (2040, 32) binary expansion of the Reed–Solomon code could be used. The threshold of this code is a BER of approximately 0.35.

As an aside, it should be noted that the sender of the stegoimage selects the format in which the stegoimage is transferred to the recipient. Therefore, if a compressed image were necessary, so as not to arouse suspicion from unintended parties, the compression parameters could be chosen in such a way that the embedded signal remains recoverable.

V. Conclusion and 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, and a level of security is provided by the necessity that both sender and receiver possess the same keys. An eavesdropper will be unable to decipher the hidden information without possession of the appropriate keys even though the system methodology may be known. 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.

The performance of this system has been illustrated by embedding text messages within five images to produce stegoimages. When these stegoimages are decoded, the text messages are completely recoverable. In addition, the system's ability to cope with added noise and compression of the stegoimage has been exhibited.

Future work should 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 payload of this system. Additionally, more complex error-correction could be implemented and it may be advantageous to have the embedded signal be adaptive.

Finally, the method presented here could be extended to color imagery and audio signals.

ACKNOWLEDGMENT

The authors would like to take this opportunity to thank the anonymous reviewers for their efforts and insightful suggestions.

REFERENCES

[1] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, 1996.
[2] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for images, audio and video," in *Proc. IEEE Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, vol. 111, pp. 243–246.
[3] D. Kahn, *The Codebreakers—The Story of Secret Writing.* New York: Scribner, 1967.
[4] F. Johnson and S. Jajodia, "Exploring steganography: Seeing the unseen," *IEEE Computer Mag.*, pp. 26–34, Feb. 1998.
[5] B. Pfitzmann, "Trials of traced traitors," in *Information Hiding, First International Workshop, Lecture Notes in Computer Science*, R. Anderson, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1, pp. 49–64.
[6] J. R. Smith and B. O. Comisky, "Modulation and information hiding in images," in *Information Hiding, First International Workshop, Lecture Notes in Computer Science*, R. Anderson, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1174, pp. 207–226.
[7] L. M. Marvel and C. G. Boncelet, Jr., "Capacity of the additive steganographic channel," submitted for publication.
[8] R. van Schyndel, A. Tirkel, and C. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Processing*, 1994, vol. 2, pp. 86–90.
[9] R. B. Wolfgang and E. J. Delp, "A watermark for digital images," in *Proc. IEEE Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, vol. 111, pp. 219–222.
[10] R. Machado, http://www.fqa.com/romana/romanasoft/stego.html.
[11] E. Milbrandt, http://members/iquest.net/˜mrmil/stego/html, Oct. 1997.
[12] C. I. Podilchuk and W. Zeng, "Digital image watermarking using visual models," in *Human Vision and Electronic Imaging II*, vol. 3016, B. E. Rogowitz and T. N. Pappas, Eds. SPIE, 1997, pp. 100–111.
[13] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Transparent robust image watermarking," in *Proc. Int. Conf. Image Processing*, Lausanne, Switzerland, Sept. 1996, vol. 111, pp. 211–214.
[14] K. Tanaka, Y. Nakamura, and K. Matsui, "Embedding secret information into a dithered multi-level image," in *Proc. IEEE Military Communications Conf.*, Monterey, CA, 1990, pp. 216–220.
[15] P. Davern and M. Scott, "Fractal based image steganography," in *Information Hiding, First International Workshop, Lecture Notes in Computer Science*, R. Anderson, Ed. Berlin, Germany: Springer-Verlag, 1996, vol. 1174, pp. 279–294.
[16] M. D. Swanson, B. Zhu, and A. H. Tewfik, "Robust data hiding for images," in *Proc. IEEE Digital Signal Processing Workshop*, Loen, Norway, Sept. 1996, pp. 37–40.
[17] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," NEC Res. Inst., Tech. Rep. 128, Aug. 1995.
[18] A. K. Jain, *Fundamentals of Digital Image Processing.* Englewood Cliffs, NJ: Prentice-Hall, 1989.
[19] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, *Spread Sprectrum Communications, Volume I.* Rockville, MD: Computer Science, 1985.
[20] B. Schneier, *Applied Cryptography-Protocols, Algorithms, and Source Code in C.* New York: Wiley, 1996.
[21] F. Hartung and B. Girod, "Fast public-key watermarking of compressed video," in *Proc. IEEE Int. Conf. Image Processing*, Santa Barbara, CA, Oct. 1997.
[22] J. S. Lee, "Digital image enhancement and noise filtering by use of local statistics," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. PAMI-2, pp. 165–168, Mar. 1980.
[23] J. B. Bednar and T. L. Watt, "Alpha-trimmed means and their relationship to the median filters," *IEEE Trans. Acoust., Speech, Signal Processing*, vol. ASSP-32, pp. 145–153, Feb. 1984.
[24] C. T. Retter, "Decoding binary expansions of low-rate Reed–Solomon codes far beyond the BCH bound," in *Proc. 1995 IEEE Int. Symp. Information Theory*, Whistler, B.C., Canada, Sept. 1995, p. 276.
[25] M. Bossert and F. Hergert, "Hard- and soft-decision decoding beyond the half minimum distance—An algorithm for linear codes," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 709–714, Sept. 1986.
[26] L. Harcke and G. Wood, "Laboratory and flight performance of the Mars pathfinder (15,1/6) convolutionally encoded telemetry link," Nat. Aeronaut. Space Admin., NASA Code 624-04-00-MN-20 TDA Progress Rep. 42-129, 1997.

Lisa M. Marvel (M'91) received the B.S.E. degree from the University of Pittsburgh, Pittsburgh, PA, in 1992, and the M.S. and Ph.D. degrees in electrical engineering from the University of Delaware, Newark, in 1996 and 1999, respectively.

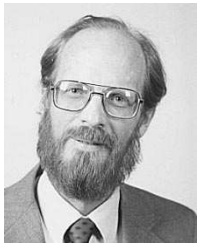
She is currently a Research Scientist at the U.S. Army Research Laboratory, Aberdeen Proving Ground, MD. Her research interests include steganography, digital communications, and image and signal processing.

Dr. Marvel received the General Electric Fellowship for graduate studies in 1993 and the 1994 George W. Laird Fellowship at the University of Delaware College of Engineering.

Charles G. Boncelet, Jr. (S'82–M'84) received the B.S. degree in applied and engineering physics from Cornell University, Ithaca, NY, in 1980, and the M.S. and Ph.D. degrees in electrical engineering and computer science from Princeton University, Princeton, NJ, in 1982 and 1984, respectively.

He worked briefly for IBM and ATT Bell Laboratories. Since 1984, he has been on the Faculty of Electrical Engineering at the University of Delaware, Newark. In 1992, he held an appointment as a Visiting Associate Professor of electrical and computer engineering at the University of Michigan, Ann Arbor. In 1995, he was promoted to Professor and was awarded a joint appointment in the Department of Computer and Information Sciences. Current research interests include multimedia, computer networks, information theory, data compression, and signal and image processing. He has published more than 70 papers in refereed journals and technical conferences. He has supervised eight Ph.D. and 15 M.S. students.

Dr. Boncelet was Conference Co-chair, 1991 and 1992, for SPIE conferences on nonlinear imaging, CD-ROM Publications Chair of the 1995 ICIP, General Chair of the 1998 ARL/ATIRP Annual Conference, and since 1997, he has been a member of the IEEE Signal Processing Society Publications Board. He is a Member of SIAM and the Delaware Academy of Science.



Charles T. Retter (M'75) received the B.S.E.E. degree from Drexel University, Philadelphia, PA, in 1968, the M.S.E.E. degree from Northeastern University, Boston, MA, in 1972, and the Ph.D. degree in electrical engineering from the Johns Hopkins University, Baltimore, MD, in 1975.

From 1968 to 1978, he was with Raytheon Corporation, NASA/Goddard Space Flight Center, and Gaertner Research, Inc. From 1978 to 1985, he was with the Data General Corporation in central-processor development, the department described in Tracy Kidder's book, *Soul of a New Machine*. During this time, he was working on his new machine, the Nova 4/C. He later led the team that designed the Eclipse S/280. From 1985 to 1992, he was an Associate Professor in the Department of Electrical and Computer Engineering, Northeastern University. Since 1993, he has been with the Army Research Laboratory, Aberdeen Proving Ground, MD. His research interests are in the areas of error-correcting codes, computer security, and computer architecture. He is the author of many papers about error-correcting codes, co-author of a textbook on computer architecture, and has three patents involving computer design.

Dr. Retter is a member of ACM and Sigma Xi.