Efficient Steganography Using Spread Spectrum with Integrity Verification

B.Sai Venkatesh,
SASTRA University, Thanjavur-613402, Tamilnadu, India
sai_venky30@yahoo.com

ABSTRACT:

Data hiding techniques are growing stronger day by day, and with even stronger detection techniques, a powerful way of hiding and retrieving data is the need of the hour. In this paper, we first discuss basic steganographic techniques in general and spread spectrum steganography in particular. Then we propose a steganographic method which hides data efficiently using Spread Spectrum techniques and also introduces Verification codes to check the integrity of the message at the receiver side. Finally, we look at the advantages of this system over others.

Keywords: Steganography, Spread Spectrum, DCT, Encryption, ECC.

1. INTRODUCTION

The main aim of this paper is to bring in a method of steganography, which satisfies essential data hiding requirements such as robustness, security, capacity and also detects any thwarting or tampering in the midway, hence assuring a strong, safe and secure communication using steganography.

2. OVERVIEW OF STEGANOGRAPHY:

Steganography, which literally means "covered writing", is the art of secret Communication. *Steganos* is Greek for "covered" and *graphein* is Greek for "to write". Its purpose is to hide the very presence of communication as opposed to cryptography whose goal is to make communication unintelligible to those who do not posses the right keys. Three different aspects in information-hiding systems contend with each other:

1. Capacity – amount of information that can be hidden in the cover medium.
2. Security – eavesdropper inability to detect hidden information.
3. Robustness – amount of modification the stego medium can withstand before an adversary can destroy hidden information.

Image steganography is defined as hiding a secret message within an image in such a way that others cannot discern the presence or contents of the hidden message. For example, a message might be hidden within an image by changing the Least Significant Bits (LSB) to be the message bits. By embedding a secret message into a carrier image, a stego-image is obtained. It is important that the stego-image does not contain any easily detectable artefacts due to message embedding that could be detected by electronic surveillance. One could utilize those artefacts to detect images that contain secret messages. Once this is achieved, the steganographic tool becomes useless.

A steganographic system consists of :

- Identifying cover's medium redundant bits.
- Embedding process which creates a *stego medium* by replacing the redundant bits with hidden message data

To send a hidden message, for example,

1. Alice creates a new image with digital camera
2. Alice supplies the steganographic system with her shared secret and message
3. The steganographic systems uses the shared secret to determine how the hidden message should be encoded in the redundant bits
4. The result is the stego image that Alice sends to Bob
5. When Bob receives the image, he uses the shared secret and the agreed steganographic system to retrieve the hidden message

For each color component, the JPEG image format uses a Discrete Cosine Transform (DCT) to transform successive 8x8 pixel block of the image into 64 DCT coefficients each.

To make an efficient image steganography, it has to satisfy the conditions as followed[4-9]: First, the stego image must be inconspicuous so that the attacker could not suspect the existence of the secret information. Secondly, in order to send more information, more data must be able to be inserted into the cover image. Thirdly, the secret

information must have confidentiality even though the attacker may suspect the existence of the information. Even though such conditions are considered, a powerful attacker may find the secret information by some process. The secret message can be forged or deleted by the attacker in order to become a malicious sender. Then the receiver, who received the message, will believe that the stego image was sent from the sender and will confide the changed message extracted from the stego image.

1. LSB embedding – Here the last 1,2,3 or more LSBs of an image are replaced by the encrypted message. However this is easily identifiable by visual attacks and statistical tests such as Chi square test.
2. Transform Domain based embedding – Here the image is first transformed using discrete cosine transform(DCT) , wavelet or some other transform techniques. Tests are available for detecting these techniques as well.
3. Spread Spectrum technique- Here the data to be transmitted is well distributed over the frequency spectrum. Its amplitude generally reduces, sometimes even below the level of noise and hence difficult to detect. Hence it is highly secure and robust.

3. SSIS – SPREAD SPECTRUM IMAGE STEGANOGRAPHY:

SSIS is a quite mature process, and its aim is to achieve low detectability, ease of extraction, high data rate and good robustness to removal. It is based on spread spectrum techniques, but it enhances them by adding other encoding steps, acquiring better performance.

Technique basics

The core of SSIS is a spread spectrum encoder. These devices work by modulating a narrow band signal over a carrier. The carrier's frequency is continually shifted using a pseudorandom noise generator feeded with a secret key. In this way the spectral energy of the signal is spread over a wide band, thus decreasing its density, usually under the noise level. To extract the embedded message, the receiver must use the same key and noise generator to tune on the right frequencies and demodulate the original signal. A casual observer won't be able even to detect the hidden communication, since it is under the noise level. The SSIS encoder adds more steps in order to push spread spectrum to its limits:

1. It optionally encrypts the message *m* to be embedded with *key 1*, getting *e*
2. The data stream passes through a Low-Rate ECC (Error Correction Code) encoder, to acquire better robustness against destruction attacks and unwanted noise, becoming *c*.
3. Spread spectrum modulation, using a pseudorandom noise generator fed with *key2*, and get *s*
4. An interleaver and spatial spreader processes *s* using *key3* obtaining *i*
5. The output of the interleaver is added to the image *f*, getting *g*
6. A quantization process is used to preserve the initial dynamic range of the cover image. We'll call it still *g*

We assume that the stego-image is sent through a noisy channel to the receiver and will become *g'*. The decoding process fairly repeats the same steps backwards:

1. It gets an optimal approximation *f'* of the original image *f* using image restoration techniques
2. *f'* is subtracted from the stego image *g'* to reveal an estimate of the embedded data *i'*.
3. *i'* is fed into a keyed deinterleaver, that uses *key3* to construct an approximation of the hidden signal, *s'*.
4. *s'* is demodulated with *key2* to get an estimate of the encoded message, c'
5. c' is decoded through the low-rate ECC to get e'
6. if m was encrypted, then e' is decrypted with *key1* and this will give m'

4. THE PROPOSED SYSTEM:

In this paper we propose a method that uses spread spectrum techniques to improve robustness of a steganographic image and also checks the integrity of a received image by means of verification codes. The whole process can be split into 3 segments as follows:

1. Embedding of secret information in image.
2. Embedding of verification code in image.
3. Extracting information from a received image and verifying its integrity.

1. **EMBEDDING OF SECRET INFORMATION:**

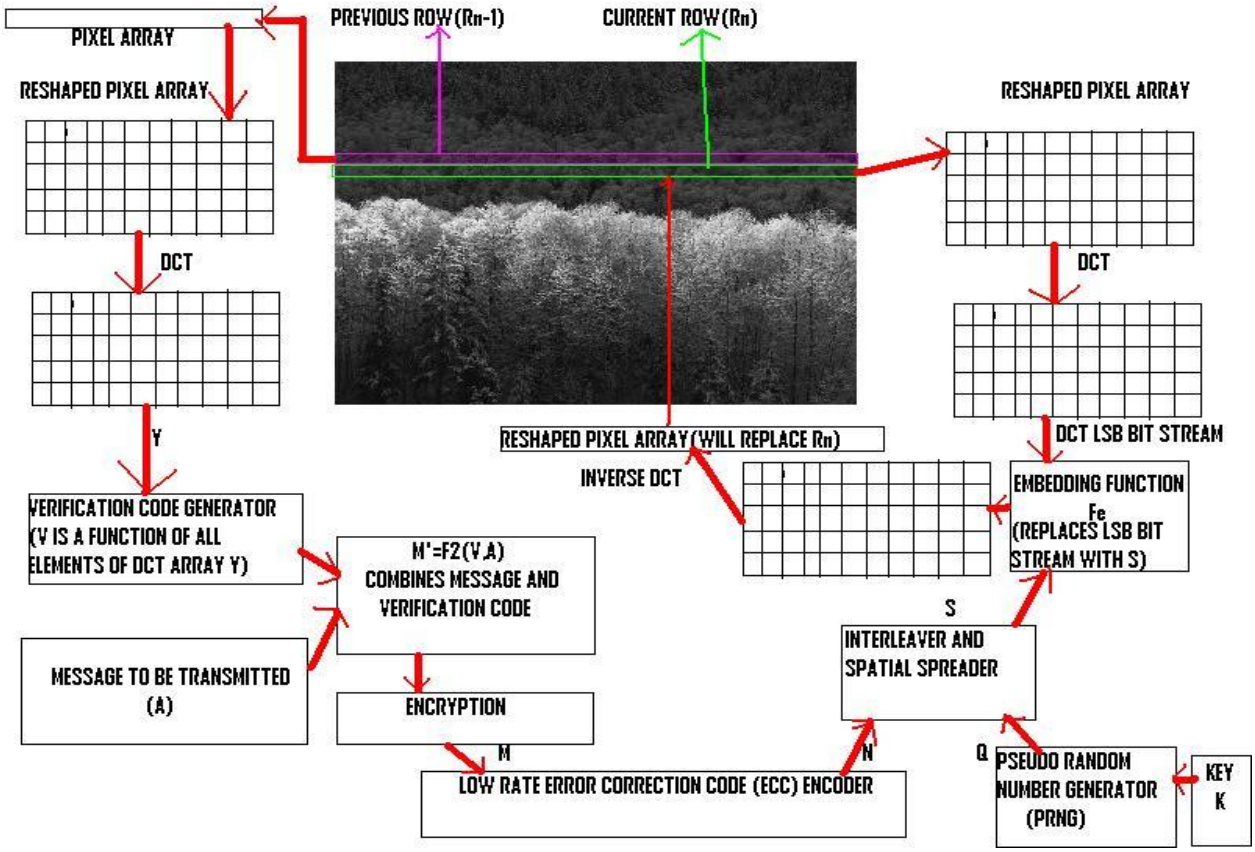
This involves embedding of the secret information, which in this case consists of the message and additional codes/keys in a cover image. The process consists of the following steps:

- Generating the secret information M.
- M is now passed through a low rate Error Correction Code (ECC) encoder to get N. ECC encoder adds redundant bits to reduce the bit rate error, hence making it difficult to detect.
- Using a secret key K, a random order Q is generated using a Pseudo Random Number Generator(PRNG). Though the order Q looks random it is directly related to K and can be found out only if K is available.
- Q and N are fed to an interleaver and spatial spreader which shifts the carrier frequency periodically through various frequencies as indicated by Q. Thus a signal S is generated.
- S is a bit stream which is then used to replace the LSBs of the DCT array of the cover image I. This generates a stego-image X, which may then be quantised.

2.EMBEDDING OF VERIFICATION CODE IN THE IMAGE:

The proposed method assigns individual verification codes in each row, in order to verify the integrity of the whole image, row by row.

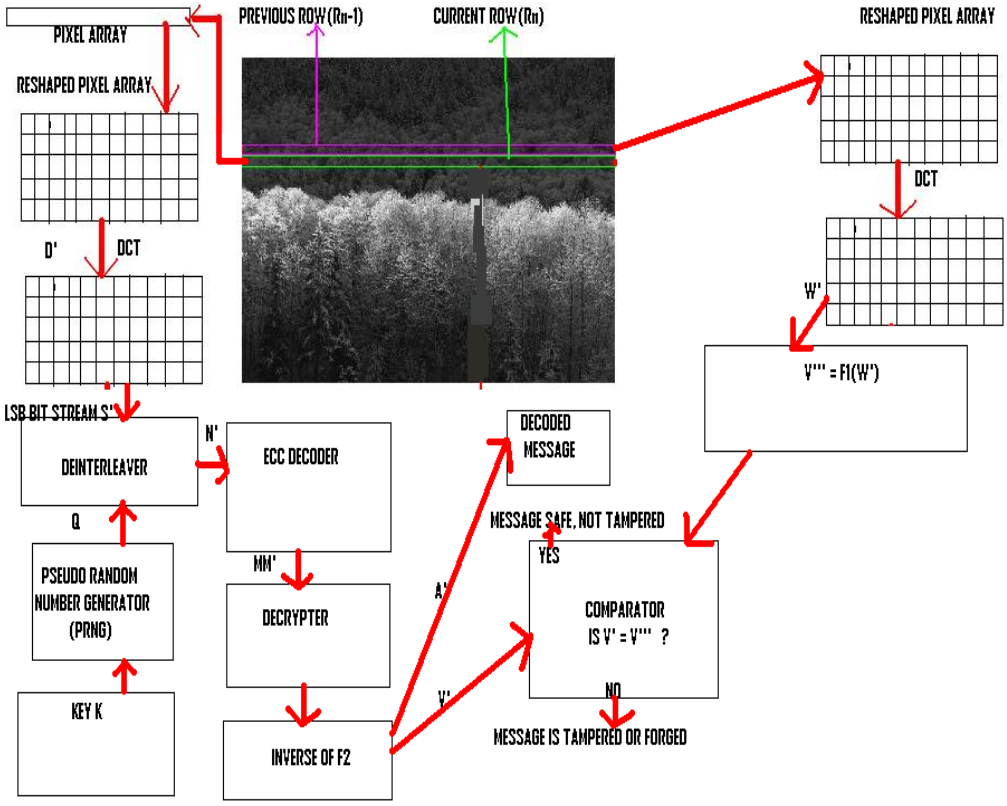
- To generate the verification code for any particular row, the previous row is first broken into a k*n array and its DCT is taken. Then some feature of this array, such as the average of a particular group of numbers within the array, or the Eigen value of the array etc. is taken. This forms the verification code V for the present row.
- V, is then combined with A(the actual message to be transmitted) using a suitable function and is then encrypted using a suitable Algorithm yielding M.



3.EXTRACTING OF INFORMATION AND VERIFICATION OF INTEGRITY:

This is essentially the reverse process of encoding and is done as follows:

- A particular row of the received image S’ is taken and reshaped into a 2D array.
- DCT of this array is taken as D’.
- LSBs of D’ are taken and S’ is generated.
- S’ is now fed to a deinterleaver controlled by a PRNG controlled by key K,and N’ is obtained.
- N” is passed through low rate ECC decoder and MM’ is generated.
- MM’ is now decrypted and F2 inverse is applied to get A’ and V’.
- Now, the previous row is taken and reshaped into an array and a DCT of this is taken as W.
- F1 is applied to W and a code V’’’ is generated.
- If V’=V’’’, then it shows that message has not been tampered or thwarted by intermediate sources. Otherwise, it is a clear indication of message having been destroyed or altered.



4. ADVANTAGES OF THE PROPOSED METHOD OVER OTHER METHODS:

- ★ Since Spread Spectrum is used, the message is well below noise level and hence casual observer cannot detect.
- ★ Decoding is very easy if K is available.
- ★ High robustness.
- ★ Nearly impossible to extract if K is not available.
- ★ There are methods which consider only a few DCT coefficients for the verification code. Hence, if an attacker changes the elements of DCT array, and if he happens to miss these few elements, the receiver still shows safe since these coefficients coincide with the verification code. But since other coefficients have been changed, the message also gets destroyed. But the proposed method avoids this mishap by considering F1 to be dependant on all coefficients of the DCT so that, even if 1 pixel changes, it affects V and hence can be detected.

CONCLUSION:

Through this paper, we have proposed a steganographic system, which is safe, secure and more immune to detections and attacks when compared to the previous systems. Moreover, the system helps us in finding whether the message has been distorted or destroyed either by degradation or by intentional attacks. Thus, a safer communication is ensured

REFERENCES:

[1] K. Nozaki, M. Maeda, K. Tsuda and E. Kawaguchi, A Model of Anonymous Covert Internet Mailing System using Steganography," Proceedings of Pacific Rim Workshop on Digital Steganography(STEG), pp. 7-10, 2002.
[2] E. Kawaguchi, H. Noda and M. Niimi, Image Data Based Steganography," Information Processing Society of Japan(IPSJ MAGAZINE) Vol. 44, No.3, pp. 236-241, 2003.
[3] T. Zhang and X. Ping, A New Approach to Reliable Detection of LSB Steganoraphy in Natural Image," Signal Processing Journal 83, ELSEVIER, pp. 2085-2093, 2003.
[4] D.C. Wu and W.H. Tsai, A Steganographic Method for Images by Pixel-value Differencing," Pattern Recognition Letters 24, ELSEVIER, pp. 1613-1626, 2003.
[5] X. Zhang and S. Wang, Vulnerability of pixel value differencing steganography to histogram analysis and modification for enhanced security," Pattern Recognition Letters, ELSEVIER, Vol. 25, pp. 331-339,2004.
[6] S.J. Wang, Steganography of Capacity Required using Modulo Operator for Embedding Secret Image," Applied Mathematics and Computation 164, ELSEVIER, pp. 99-116, 2004.
[7] C.C. Chang and H.W. Tseng, A Steganographic Method for Digital Images using Side Match," Pattern Recognition Letters, ELSEVIER, Vol.25, pp.1431-1437, 2004.
[8] C.C. Thien and J.C. Lin, A Simple and High-hiding Capacity Method for Hiding Digit-by-digit in Images Based on Modulus Function," Pattern Recognition Journal 36, PERGAMON, pp. 2875- 2881, 2003.
[9] C.K. Chan and L.M. Cheng, \Hiding Data in Images by Simple LSB Substitution," The Journal of The Pattern Recognition Society, PERGAMON, Vol. 37, pp. 469-474, 2004.
[10] Y.R. Park, H.H. Kang, S.U. Shin and K.Y. Kwon, An Image Steganography Using Pixel Characteristics, Lecture Notes in Artificial Intelligence 3802, Springer Verlag, pp. 581-588, 2005.

BIBLIOGRAPHY:

1. Digital Image Processing by Gonzalez and Woods.
2. Integrity verification of secret information in image steganography, by Youngran Park et al.