Codebook Code Division Multiple Access Image Steganography

Dušan LEVICKÝ, Stanislav ŠURIN

Dept. of Electronics & Multimedia Communications, Technical University of Košice,
Park Komenského 13, 041 20 Košice, Slovak Republic

Dusan.Levicky@tuke.sk, Stanislav.Surin@tuke.sk

Abstract. *In this paper, a new modification of spread spectrum image steganography (SSIS) is presented. The proposed modification of SSIS hides and recovers a message of substantial length within digital image while maintaining the original image size and dynamic range. An embedded message can be in the form of text, image, or any other digital signal.*

Our method is based on CDMA SSIS technique. To increase the information capacity of the stego channel and decrease a distortion of a cover image, a new modification of CDMA using a codebook (in the following referred to as Codebook CDMA (CCDMA)) is suggested.

Keywords

Steganography, spread spectrum, CDMA, information hiding, PN sequences, codebook.

1. Introduction

The word steganography literally means covered writing as derived from Greek. It includes a vast array of methods of secret communications that conceal the existence of the message. Among these methods there are invisible inks, microdots, character arrangement (other than the cryptographic methods of permutation and substitution), digital signatures, covert channels and spread-spectrum communications.

Steganography is the art of concealing the existence of information within seemingly innocuous carriers. Steganography can be viewed as akin to cryptography. Both have been used throughout recorded history as means to protect information. At times these two technologies seem to converge while the objectives of the two differ. Cryptographic techniques "scramble" messages so if intercepted, the messages cannot be understood. Steganography, in an essence, "camouflages" a message to hide its existence and makes it seem "invisible" thus concealing the fact that a message is being sent altogether. An encrypted message may draw suspicion while an invisible message will not.

The main goal of this paper is to present a novel framework that allows increasing the capacity of image channel using modified CDMA spread spectrum approach in the DCT-domain.

This paper is organized as follows. In Section 2, the principles of spread spectrum image steganography are briefly discussed. In Section 3, our proposal of a new modified CDMA scheme is explained. Then, Section 4 describes implementation of modified CDMA SSIS in the DCT-domain. Finally, Section 5 analyzes the obtained results and compares the modified CDMA with the standard CDMA approach in SSIS.

2. Spread Spectrum Image Steganography

The SSIS [1] is a data hiding/secret communication steganographic system, which uses digital imagery as a cover signal. SSIS provides the ability to hide a significant quantity of information bits within digital images while avoiding detection by an observer.

Spread spectrum was originally developed for military (radar and communications) use in several countries. Since its declassification, it has found civilian application, particularly in code-division multiple-access (CDMA) communications, the system used for cellular telephony.

In spread spectrum, a narrowband signal (the message to be transmitted) is modulated by a broadband carrier signal, which broadens (spreads) the original, narrowband spectrum; hence the term "spread spectrum." The following properties of spread spectrum are particularly well-suited for steganography.

Antijamming (AJ)

The antijamming (AJ) property results from the fact that an attacker does not know the privileged information that the sender and an authorized receiver possess. As a result, the attacker must jam the entire spectrum of the broadband signal. The jammer has limited power, however, so it can only jam each frequency with low power. Hence, the sender and receiver have an effective signal-to-jammer advantage called the processing gain.

Low probability of intercept (LPI)

The low probability of intercept (LPI) property is a consequence of spreading: a large signal power is distributed over the entire frequency spectrum, so only a small amount of power is added at each frequency. Often, the increase is below the noise floor, so an attacker may not even detect the transmission of a spread-spectrum signal.

Pseudo-noise (PN)

For security, the carrier is often a pseudo-noise (PN) signal, meaning that it has statistical properties similar to those of a truly random signal, but it can be exactly regenerated with knowledge of privileged information. For example, the carrier could be the output of a random-number generator that has been initialized with a particular seed, and only the owner knows the seed.

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.

3. Proposal of a Codebook CDMA Image Steganography (CCDMAIS)

Code division multiple access (CDMA) [5] is a modulation and multiple-access scheme based on spread-spectrum communication.

In a CDMA system, each signal consists of a different pseudorandom binary sequence called the spreading code that modulates a carrier, spreading the spectrum of the waveform. A large number of CDMA signals share the same frequency band. If CDMA is viewed in either the frequency or time domain, the multiple access signals overlap with each other. However, the use of statistically orthogonal spreading codes separates the various signals in the code space.

A CDMA receiver separates the signals by means of a correlator that uses the particular binary sequence to despread the signal and collect energy of the desired signal.

A pseudorandom noise (PN) sequence is used to spread the spectrum. The sample rate of the spreading sequence called the chip rate is chosen so that the bandwidth of the filtered signal is several times the bandwidth of the original signal.

There exists a large set of PN sequences, e.g. m-sequences, Gold sequences, PN sequences, Kasami sequences, Walsh sequences, Hadamard sequences. The last two of them represent orthogonal codes.

Creating of a codebook of PN codes

In similarity with real CDMA systems, each bit from a binary word is equivalent to a signal from one user. An 8-bit binary word represents simultaneous transmission of eight channels; each channel has assigned its own spreading sequence. A binary word is represented as a combination of PN sequences. The number of used sequences is equal to the number of bits in the binary word. The spreading is depicted in Fig.1. This way, for encoding of an 8-bit binary word we will need to use 8 different PN sequences.

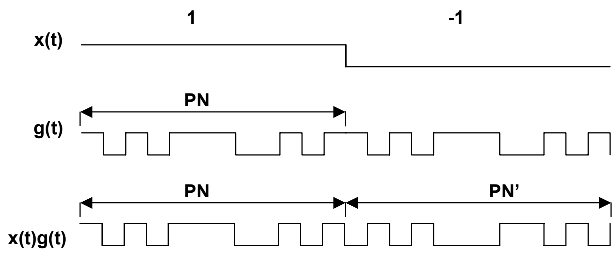


Fig. 1. Spread-spectrum example using direct sequencing, x(t) binary data waveform to be transmitted, g(t) code sequence, x(t)g(t) transmitted sequence

It can be said that each PN sequence carry one bit of information (Fig.1 shows differences between transmittion of binary values 1 and 0).

In the following we will explain our original modification of this scheme. Let's consider creating of a codebook that will assign a different binary word named *codeword* to a different combination of PN sequences. As will be seen later, thus we are able to increase the bit/PNsequence rate.

We begin with a simple example to illustrate our discussion.

Let's have three different PN sequences denoted as PN1, PN2, and PN3. As was mentioned above, in the standard CDMA these are capable of a 3-bit codeword representation, e.g. a binary word 101 can be coded as a combination PN1+PN2'+PN3 where PN2' denotes the PN2 sequence phase shifted by 180^0 (for binary sequences, phase shifting by 180^0 means mapping of bit $0 \to 1$ and bit $1 \to 0$, i.e. amplitude inversion). Tab.1 shows all the possible combinations of these sequences.

PN1 PN2 PN3		PN1’ PN2’ PN3’	
PN1’ PN2 PN3		PN1 PN2’ PN3’	
PN1 PN2’ PN3		PN1’ PN2 PN3’	
PN1 PN2 PN3’		PN1’ PN2’ PN3	
PN1 PN2	PN1 PN2’	PN1’ PN2	PN1’ PN2’
PN1 PN3	PN1 PN3’	PN1’ PN3	PN1’ PN3’
PN2 PN3	PN2 PN3’	PN2’ PN3	PN2’ PN3’
PN1		PN1’	
PN2		PN2’	
PN3		PN3’	

Tab. 1. Possible combinations of three PN sequences denoted as PN1, PN2, PN3, and their inverse forms PN1’, PN2’, PN3’.

The grey area shows all the possible combinations in CDMA system. Comparing to the similarity with real CDMA systems, the rest of the table is equivalent to the situation, when not all signals are present (some users do not transmit). It represents all the possible subsets, which can be created from the set of PN1, PN2, and PN3.

The total number of all the combinations is 26 in this case. Supposing we create a table (*codebook*) where a different codeword will be assigned to each combination of sequences; this way we are able to encode up to 26 different binary words or $\lfloor \log_2 26 \rfloor = 4$ bits, where $\lfloor \cdot \rfloor$ means rounding to the nearest lower integer.

The total number of codewords one can create from N PN sequences can be obtained as a summation of the following combinations (the first number tells how many sequences are chosen from the set of all N sequences):

1 of N: $2\ {}_N C_1 = 2N$

2 of N: $2\ {}_N C_2 + {}_N C_1\ {}_{N-1} C_1$

3 of N: $2\left({}_N C_3 + {}_N C_2\ {}_3 C_1\right)$

4 of N: $2\left({}_N C_4 + {}_N C_3\ {}_2 C_1\right) + {}_N C_2\ {}_3 C_2$

…

i (i is odd) of N:

$$2\left({}_N C_i + {}_N C_{i-1}\ {}_{N-(i-1)} C_1 + {}_N C_{i-2}\ {}_{N-(i-2)} C_2 + \ldots + {}_N C_{\frac{i+1}{2}}\ {}_{N-\left(\frac{i+1}{2}\right)} C_{\frac{i+1}{2}-1}\right)$$

j (j is even) of N:

$$2\left({}_N C_j + {}_N C_{j-1}\ {}_{N-(j-1)} C_1 + {}_N C_{j-2}\ {}_{N-(j-2)} C_2 + \ldots\right) + {}_N C_{\frac{j}{2}}\ {}_{N-\frac{j}{2}} C_{\frac{j}{2}}$$

…

N of N: 2^N

where ${}_N C_k$ is defined as follows

$${}_N C_k = \binom{N}{k} = \frac{N!}{k!(N-k)!}$$

Following the above mentioned example, the following combinations can be created from the set of $N = 3$ PN sequences:

1 of 3: $2\ {}_3 C_1 = 6$

(PN1, PN2, PN3, PN1’, PN2’, PN3’)

2 of 3: $2\ {}_3 C_2 + {}_3 C_1\ {}_2 C_1 = 12$

(PN1 PN2, PN1 PN3, PN2 PN3, PN1 PN2’, PN1 PN3’, PN2 PN3’, PN1’ PN2, PN1’ PN3, PN2’ PN3, PN1’ PN2’, PN1’ PN3’, PN2’ PN3’)

3 of 3: $2^3 = 8$

(PN1 PN2 PN3, PN1’ PN2 PN3, PN1 PN2’ PN3, PN1 PN2 PN3’, PN1’ PN2’ PN3’, PN1 PN2’ PN3’, PN1’ PN2 PN3’, PN1’ PN2’ PN3)

The comparison of an increase of the number of bits per one PN sequence is depicted in Fig.2.

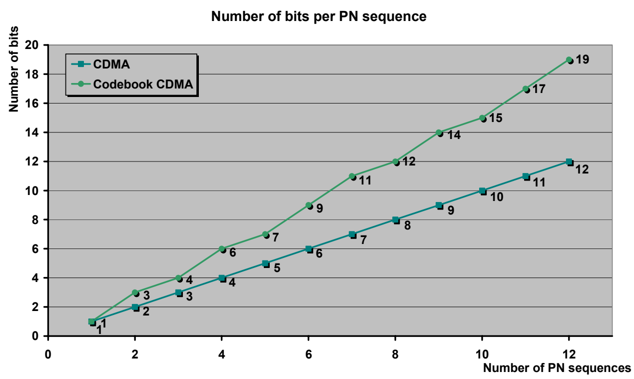


Fig.2. Comparison of the number of bits we are able to transmit using CDMA or CCDMA system

4. Implementation of CCDMA SSIS in the DCT-Domain

The discrete cosine transform is a real domain transform, which represents the entire image as coefficients of different frequencies of cosines (which are the basis vectors for this transform). The formula for a 2-D DCT is as follows:

$$F(u,v) = \frac{1}{4} K_u K_v \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left(u\pi \frac{2x+1}{2N}\right) \cos\left(v\pi \frac{2y+1}{2N}\right) \quad (1)$$

where

$$K_u = \frac{1}{\sqrt{2}} \text{ if } u = 0 \text{ or } K_u = 1 \text{ if } u = 1,$$

$$K_v = \frac{1}{\sqrt{2}} \text{ if } v = 0 \text{ or } K_v = 1 \text{ if } v = 1 .$$

The image is coded via DCT by taking 8 x 8 blocks of the image, which are then transformed individually. The 2D DCT of an image gives the result matrix such that top left corner represents the lowest frequency coefficient while the bottom right corner is the highest frequency. DCT also forms the basis of the JPEG image compression algorithm, which is one of the most widely used image data storage formats [2]. The DCT approaches are able to withstand some forms of attacks very well.

Generally speaking, the message has to be added to frequencies of high energy in order to be resistant to noise. In our system, the AC coefficients from middle frequencies having the smallest quantization step sizes in the JPEG quantization table were selected (according to Fig.3).

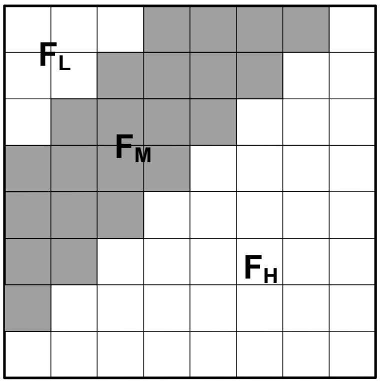


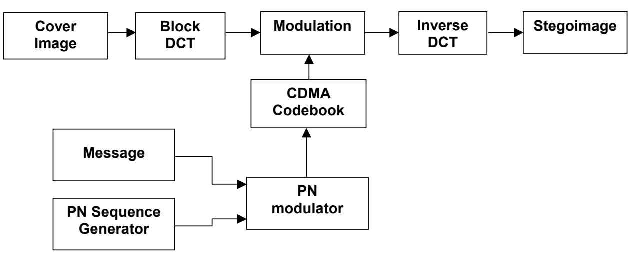
Fig.3. Definition of DCT regions

For each 8x8 block of the image, the DCT for the block is first calculated. In that block, the middle frequency components F_M (with indexes of their position *x,y*) are added to the PN sequence S, multiplied by a gain factor *α*

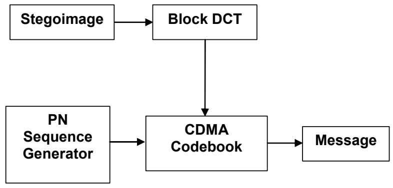
$$F_{S_{x,y}}(u,v) = \begin{cases} F_{x,y}(u,v) + \alpha F_{x,y}(u,v), & u,v \in F_M \\ F_{x,y}(u,v), & u,v \notin F_M \end{cases} . \quad (2)$$

We choose working in the block DCT domain because DCT has good energy compaction capability and it is feasible to incorporate the HVS (*Human Visual System*) characteristics [3, 4].

The proposed system is depicted in Fig.4.



(a) Encoder



(b) Decoder

Fig.4. Codebook CDMA SSIS block scheme.

5. Experimental Results

The tests were performed with a gray standard testing image Lena of size 256x256 pixels (containing 64 kB).

In evaluating the stegoimage quality we make use of root-mean-squared error (RMSE) and peak-signal to noise ratio (PSNR) as error metrics. Denoting the original *N* x *N* image by *C* and stegoimage by *S*, RMSE is given by

$$RMSE = \sqrt{\frac{1}{N^2}\sum_{i=1}^{N}\sum_{j=1}^{N}\left[C(i,j) - S(i,j)\right]^2} . \quad (3)$$

PSNR (in dB) is computed using

$$PSNR = 20\log_{10}\left(\frac{255}{RMSE}\right). \quad (4)$$

First, for comparison reasons we present a result of the standard CDMA approach to image steganography in the DCT-domain (Fig. 5).

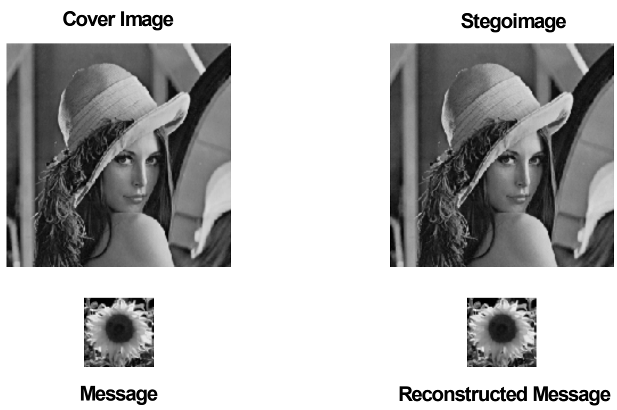


Fig. 5. The original image, the stegoimage, and the message.

As a message, a 6 kB image was used (see Fig.5). This message was inserted in the middle and higher frequencies of 8x8 block DCT-domain. Each bit of the message was spread by one of the Hadamard spreading sequences of 8-bit length. We used 7 different parallel sequences for encoding in our scheme, which results in necessity of transmittion of 7021 combinations.

As the results show the stegoimage has perceptively no striking differences comparing with the original image. The obtained PSNR was 47.46 dB. The message was reconstructed without error using decorrelation detector [6]. The obtained payload was 0.76 bits/pixel.

The following figure shows the same cover image with a hidden message using a codebook.

Fig. 6. The image with a hidden message using CCDMA SSIS.

CCDMA enabled us to hide larger amount of data; in this case we were able to include 7.16 kB of message data using only 6 different Hadamard spreading sequences of the length 8 bits. As can be seen from Tab.1, for creating of the codebook we can use subsets of 4 combinations. A total number of 5041 combinations needed to be transmitted with following subsets of PN combinations (resulting from stego data histogram analysis):

- 861 words consisting of one PN combinations,
- 1693 words consisting of two PN combinations,
- 2389 words consisting of three PN combinations,
- 98 words consisting of four PN combinations.

This results in smaller amount of included energy and, finally, it affects the PSNR. In this case, the obtained PSNR was 50.88 dB and payload 0.87 bits/pixel. One spreading sequence carried in average 3.42 bits of information. Another very important fact is that we obtain much lower MAI (multiple access interference) resulting in higher error resilience and simplification of decoding process.

In both cases the gain factor α was set to 0.42.

6. Conclusions

In this paper, a new method called CCDMAIS based on a creating of a codebook for CDMA system for more effective usage of PN sequences was proposed. Usage of the codebook enables to increase a capacity of a cover image, as was presented in the previous section.

An analysis of possibilities of HVS model usage as well as CDMA techniques in wavelet domain are left as a future line of research. This way, suppression of perceptible distortion and an increase of image capacity are expected.

Acknowledgements

The work presented in this paper was supported by the Grant of the Ministry of Education and the Academy of Science of the Slovak Republic VEGA under Grant No. 1/1057/04.

References

[1] MARVEL, L. M., BONCELET, CH. G., RETTER, CH. T. Spread spectrum image steganography. *IEEE Trans. On Image Processing,* vol. 8, no. 8, Aug. 1999, p.1075 – 1083.

[2] LEVICKÝ, D., FORIŠ, P., KLENOVIČOVÁ, Z., ŠURIN, S. Súčasný stav a perspektívy využitia digitálnych vodoznakov. In *Cofax – Telecommuniations 2004, 10th International Scientific Conference,* 2004, p. 165 - 168.

[3] LEVICKÝ, D., FORIŠ, P. Human visual system models in digital image watermarking, *Radioengineering,* vol. 13, no. 4, p. 38-43.

[4] HERNÁNDEZ, J. A., AMADO, M., PÉREZ-GONZÁLEZ, F. DCT-domain watermarking techniques for still images: Detector performance analysis and a new structure. *IEEE Trans. Image Processing*, vol. 9, no. 1, Jan. 2000, p. 55 – 68.

[5] SKLAR, B. *Digital Communications: Fundamentals and Applications.* Prentice Hall, 2001.

[6] MOSHAVI, S. Multi-user detection for DS-CDMA communications. *IEEE Comm. Magazine*, Oct. 1996, p. 124 – 136.

About Authors...

Dušan LEVICKÝ was born in Slanec, Slovakia, in 1948. He received the M.Sc. and PhD. Degrees at the Technical University of Košice, and now he is professor at the Dept. of Electronics and Multimedia Communications, Technical University, Košice. His research interests include multimedia digital image processing and cryptography.

Stanislav ŠURIN was born in Stropkov, Slovakia, in 1978. Following his education at the Faculty of Informatics and Electrical Engineering, Košice, he is currently working towards the PhD. degree on steganography and spread spectrum communications with the Multimedia Communications Group at the Dept. of Electronics and Multimedia Communications, Technical University, Košice. His research interests include steganography, image processing, CDMA systems, and spread spectrum communications.