

# Detecting Hidden Information from a Spread Spectrum Watermarked Signal by Genetic Algorithm

Saeed Sedghi *Student member*, Habib Rajabi Mashhadi, Morteza Khademi

**Abstract**—Spread spectrum audio watermarking (SSW) is one of the most secure techniques of audio watermarking. SSW hides information by spreading their spectrum which is called watermark and adding to a host signal as a watermarked signal. Spreading spectrum is done by a pseudo-noise (PN) sequence. In conventional SSW approaches, receiver must know PN sequence used at the transmitter and location of watermark in watermarked signal for detecting hidden information. It is contributed a high secure feature for this method since any unauthorized user who doesn't access this information couldn't detect hidden information. In this paper a novel approach based on genetic algorithm is proposed for recovering PN sequence and detecting location of watermark signal without any information from the transmitter. Using this approach unauthorized users could detect hidden information.

## I. INTRODUCTION

Genetic algorithm (GA) has established itself as one of the most powerful and applicable optimization methods. Because of its high flexibility and robustness beside its simplistic implementation procedure, the GA has been employed for a large number of applications in signal processing areas as a powerful optimization tool [1]. Successful operation of GA is widening its applications in signal processing. In this paper, another application of GA in digital watermarking is introduced.

In recent years, digital watermarking has received considerable attention from the security and cryptographic research communities. There has been a growing interest in the domain since 1996. Digital watermarking is a technique of hiding information into innocuous-looking cover media objects as a host, so that no one can perceive existence of this information without complicated tests. It is intended to provide a degree of copyright protection as use of digital media mushrooms [2].

Depending on type of cover media, watermarking is classified into image watermarking and audio watermarking. This paper deals with audio watermarking.

Numerous audio watermarking techniques have been proposed. The most important ones are LSB [3], Phase

coding [4], Echo hiding [5] and spread spectrum watermarking [6].

Spread spectrum watermarking (SSW) is one of the most promising watermarking technologies. It is designed such that, bandwidth spectrum of embedded hidden information occupies bandwidth of host signal as much as possible [7]. It could be achieved by spread spectrum techniques. Spread spectrum is techniques that spreads spectrum of data through a pseudo-random-noise (PN) sequence.

Hidden information, whose spectrum is spread by PN sequence, is called watermark signal. Adding watermark signal to host signal results watermarked signal. Since a watermarked signal contains hidden information whose spectrum is spread over the entire bandwidth of host and its energy density is reduced, the quality of watermarked signal could not be distinguished from the quality of host signal. So, existence of hidden information in watermarked signal is not detectable.

Spread spectrum watermarking has some interesting properties which are very useful for detection of hidden information in the receiver. These properties have been derived from PN properties [8]. One of the most important properties is correlation property of PN sequence. Due to this property, detection of hidden information is possible if the receiver knows the PN sequence used at the transmitter side and exact location of watermark in watermarked signal. The essential knowledge's for detection, results high secure transmission of information against any unauthorized user who doesn't access to the PN sequence and location of watermark. So, PN sequence could be considered as a secret key. This key is only available at the receiver and no other one can access to this key.

In this paper using GA a computational approach is presented such that makes it possible to detect hidden information, whereas the receiver has no knowledge of the transmitter's spreading sequence. Employing this approach, security of SSW technology fails and for having high secure feature of SSW some additional modification must be proposed.

The rest of the paper is organized as follows. In section II, the spread spectrum watermarking and properties of PN sequence are described. In section III recovering PN sequence from a received watermarked signal using GA is presented. Section IV describes detection of the watermark signal by genetic algorithm. Section V represents simulation results. Conclusions are given in section VI.

Saeed Sedghi is graduate student with the Department of Electrical Engineering, Ferdowsi University, Mashhad, Iran. (Email: saeed\_se2001@yahoo.com).

Habib Rajabi Mashhadi is with the Department of Electrical Engineering, Ferdowsi University, Mashhad, Iran, (Email: h\_mashhadi@ferdowsi.um.ac.ir).

Morteza Khademi is with the Department of Electrical Engineering, Ferdowsi University, Mashhad, Iran, (Email: [khademi@ferdowsi.um.ac.ir](mailto:khademi@ferdowsi.um.ac.ir)).

## II. SPREAD SPECTRUM WATERMARKING

Many algorithms for audio watermarking have been proposed to embed hidden information into a host signal unperceivable. Watermarking methods could be characterized by a number of defining features [2]: perceptual transparency (imperceptibility of watermark), capacity (extreme bit rate of watermark), robustness (against common signal processing manipulations), security (against unauthorized users) and Computational complexity (cost). Any watermarking method has some weakness features and some strong ones. Depending on situation of watermarking application for transmission of hidden information, proper method should be selected.

SSW is one of the most interesting and powerful methods for embedding hidden information into a host signal. It is felt to have high degree of robustness, security and perceptual transparency. In this paper we show the SSW approach has weak security. We show this by means of an attack based on genetic algorithm

For explaining high security of SSW in conventional methods, a brief description of embedding procedures by this algorithm is essential.

Most of the watermarking algorithms encode hidden information into a watermark signal before embedding into a host signal. The encoding is essential for ensuring inaudibility and robustness of watermark in watermarked signal

1. Encoding process in spread spectrum watermarking is spreading spectrum of hidden information by PN sequence.

A PN sequence is a zero mean periodic binary sequence with a noise like waveform whose elements are equal to  $+\delta$  or  $-\delta$  and called chip. It is generated by a feedback shift register that is made up of  $m$  flip-flops [9]. Thus, maximum period of PN is  $2^m - 1$ . A PN sequence which has the period of  $2^m - 1$  is called maximal length PN sequence.

There are two choices for spreading spectrum of hidden information: direct sequence spread spectrum and frequency hopping spread spectrum. Direct sequence spread spectrum (DSSS) is the most suitable technique for SSW [2]. DSSS spreads spectrum of hidden information through multiplying data by PN sequence as (1).

$$w(n) = p(n)m(n) \quad (1)$$

Where  $w(n)$  represents watermark signal,  $p(n)$  represents PN sequence and  $m(n)$  represents hidden information.

Note that clock rate of PN sequence which is called chip rate, is a period of PN sequence times more than bit rate of hidden information, i.e. each bit of hidden information stays constant over a period, or block of PN sequence. It can be expressed as (2):

$$N = Rc/Rb \quad (2)$$

Where  $N$  is period of PN,  $Rc$  is the chip rate of PN sequence and  $Rb$  is bit rate of hidden information.

So, watermark signal is blocks of PN sequences whose elements during one period are multiplied by  $+1$  or  $-1$  according to the bit value of hidden information. Figure 1, illustrates a watermark signal.

Watermarked signal is the result of adding watermark and host signal:

$$S(w,x) = \lambda w(n) + x(n) \quad (3)$$

Where  $S$  represents watermarked signal,  $\lambda$  represents amplitude of watermark and  $x$  represents host signal.

In this case, the energy density of hidden information is reduced since its spectrum is spread over the whole bandwidth of host signal and does not make any perceiving distortion to host.

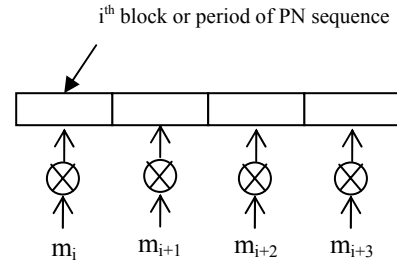


Fig. 1. A watermark signal by 4 blocks of PN sequence, each block contains one period of PN and represents one bit of hidden information.

Extraction of hidden information from a received watermarked signal is completed by using correlation property of PN sequence. Cross correlation between two maximal length PN sequences is as (4) [8]:

$$C(P_a, P_b) = \frac{1}{N} \sum_{i=0}^{N-1} P_a(i)P_b(i) = \begin{cases} 1, & \text{if } a = b \\ -1/N, & \text{otherwise} \end{cases} \quad (4)$$

Where  $P_a(n)$  and  $P_b(n)$  represent two different maximal length PN sequences and  $N$  represents period of PN sequence.

Equation (4) expresses that computing the correlations between watermarked signal and PN sequences used for spreading at the transmitter, and comparing the correlations with a threshold, determines whether watermark is present in the signal or not.

Computing correlation between received watermarked signal and PN sequence is as follows:

$$C(p_b, s) = C(x, p_b) + C(w, p_b) = C_x + C_w \quad (5)$$

$$C_x = \sum_{i=0}^{N-1} x(i) p_b(i) \quad (6)$$

$$C_w = m \sum_{i=0}^{N-1} p_a(i) p_b(i) \quad (7)$$

Where  $s$  represents watermarked signal,  $p_b$  represents PN sequence used at the receiver,  $x$  represents host signal,  $w$

represents watermark signal,  $p_a$  represents PN sequence used at the transmitter and  $N$  represents period of PN sequence.

Considering the correlation property of PN sequence,  $C_x$  will be very small in comparison with  $C_w$  if PN sequence incorporated for computing cross correlation is the PN sequence used at the transmitter. It is due to the fact that multiplying host signal by PN spreads spectrum of host and de-spread spectrum of hidden information. For detecting hidden information thus, the receiver must have some knowledge from transmitter: exact PN sequence used for spreading spectrum and location of watermark in watermarked signal. This will guaranty that an unauthorized user who doesn't have any information about PN sequence and location of watermark couldn't have access to hidden information. It leads to a high secure feature for SSW technology. Finally it should be mentioned that for synchronization between receiver and transmitter some extra bits must be considered as synchronization bit in payload. SSW watermarking proposed in [11] uses 1152 chips for spreading spectrum of 18 synchronization bit. It decreases capacity of watermark signal.

### III. RECOVERING PN SEQUENCE

Recovering PN sequence from a spread spectrum watermarked signal with no knowledge of the PN sequence or its location is very hard and almost impossible since there are vast regions for the solutions set. For instance, to recover a PN sequence with a chip period equal to 63 bits,  $2^{63}$  PN sequences must be generated.

In this section, with an assumption of knowing exact location of watermark in watermarked signal, recovering PN sequence is described. In section 4 a novel algorithm for detecting location of watermarked signal will be explained.

In [12] an approach for detecting hidden information from an image spread spectrum embedded signal is proposed this approach detects abrupt jumps in the statistics of watermarked signal to recover PN sequence. Proposed algorithm which is based on hypothesis tests for detection of abrupt jump in the statistics is very complicated and its performance suffers from for low frequency embedding.

Recovering PN sequence could be considered as an unconstrained optimization problem. We have a set of feasible solution and would like to minimize a cost function by a global optimization.

The set of feasible solutions are sequences with period of PN sequence and elements of  $+\delta$  and  $-\delta$ . Defining a cost function for this problem should be based on a very useful property of SSW in detection which is correlation property of PN sequence. So, our cost function is cross correlation between generated sequence and watermarked signal.

In [13] an interesting method for recovering PN sequence of spread spectrum signal with a predefined SNR is proposed. This approach uses GA with fitness function of cross correlation between estimated PN sequence and spread spectrum. However, spread spectrum watermarking is more complicated than a single spread spectrum signal since in

SSW, spread spectrum hidden information is like a white Gaussian noise for host signal.

Note that computing cross correlation between sequences of our solutions set and watermarked signal for only one block of SSW signal, won't converge to the PN sequence used at the transmitter, since energy of host signal is at least 12 dB more than energy of watermark and have a strong effect on maximizing cross correlation (i.e. optimization algorithm converges to a sequence that maximizes correlation with the host). As a solution to this problem, several consequence blocks of watermark (i.e. several bits of hidden information) should be considered in computation of cross correlation. In this case watermark signal has stronger effect than host signal on maximizing cross correlation function.

Finding the global optimization by Searching over the entire of our solutions set as mentioned above, is the subject of deterministic methods like covering methods, tunneling methods, zooming methods, etc. These methods find the global minimum by an exhaustive search over the entire solutions set. For instance the basic idea for covering method is to cover the feasible solutions set by evaluating the objective function at all points [10]. these algorithms have high reliability and accuracy is always guaranteed, but they have a slower convergence rate [14].

Taking vast regions of our solution set into account, we need efficient optimization algorithms that have a high reliability and fast converging rate. Many stochastic optimization algorithms have been proposed such as genetic algorithm, simulated annealing, ant colony, etc. however GA has proved that is the most successful and powerful one for a wide range of applications and strike an attractive balance between reliability and converging rate.

Genetic algorithms are based loosely on natural evolution and were introduced by Holland in 1975 [15]. GA uses three operators for converging to global optimization: selection based on fitness evaluation, reproduction and replacement. The population comprises a group of chromosomes from which candidates can be selected for the solution of a problem. After evaluating fitness of each chromosome based on an objective function, chromosomes will be selected to produce the offspring by cross over and mutation operations. The chromosomes in the current population are then replaced by their offspring and this cycle will be repeated [1]. Generation of populations will be repeated until a desired termination is reached.

The GA used in this paper has the following properties:

- A- **String chromosomes and code:** String chromosomes incorporated in our GA are sequences generated with period of  $N$  and elements of  $+\delta$  and  $-\delta$ . Initialization is placing  $+\delta$  and  $-\delta$  into chromosome bits by random.
- B- **Fitness evaluation:** Our Cost function is the same as defined above, cross correlation between string chromosomes and watermarked signal. Fitness evaluation is according to maximizing cost function.
- C- **Population size:** Although large population size will cover more regions of solution and increases reliability

of GA for converging to global maximum, leads to low efficiency. Hence, there is a trade off here. The best amount of population size is 100 for this paper which is attained by experience.

- D- **Type of cross-over:** Multi-point cross over will lead to better converges in comparison with single point cross over.
- E- **Mutation probability:** A typically recommended value for the mutation rate (i.e. mutation probability) is  $1/L$ , Where L is the length of each chromosome. We have found empirically that a much higher rate (of .1) gives better results for our problem. This large probability for mutation is due to the fact that the regions for exploring global maximum are very vast and we need larger mutation to greater innovation in GA.
- F- **The maximum number of generations:** The maximum number of generations for converging to global maximum depends on period of PN sequence. Table I illustrates maximum number of generations for different periods.
- G- **Elitism:** The benefits of elitism are well documented and we adopt a simple elitism strategy in our work. This operation in GA avoids destruction of the best offspring in each generation which may result by mutation. Since we have used a large probability of mutation, using this operation is useful.

Table II summarizes GA parameters used for recovering PN sequence.

Table I.

Number of generations for different PN sequences

<i>Period of PN (chip)</i>	<i>Maximum number of generation</i>
15	10
31	30
63	75
127	500
255	20000

Table II.

GA parameters

<i>GA parameters</i>	<i>assignment</i>
Population size	100
Type of cross over	Multi point
Mutation probability	.1
Number of generation	See table I
Number of chromosome bits	Period of PN sequence

Convergence of GA to the PN sequence used at the transmitter is illustrated in figure2. In this figure, cross correlation between 5 blocks of estimated PN sequence with the period of 63 chips and watermarked signal for any

generation is shown. Since, our fitness function is absolute amount of cross correlation between estimated PN sequence in each generation and watermarked signal, increasing cross correlation expresses improvement of fitness evaluation for generations. By employing elitism in our GA, improvement of each generation is guaranteed. After 75 generations, the largest cross correlation is attained which is near 5, due to using 5 blocks for estimation.

Finally note that although, mutation may destroy the best offspring in each generation, using elitism operator this problem will be solved.

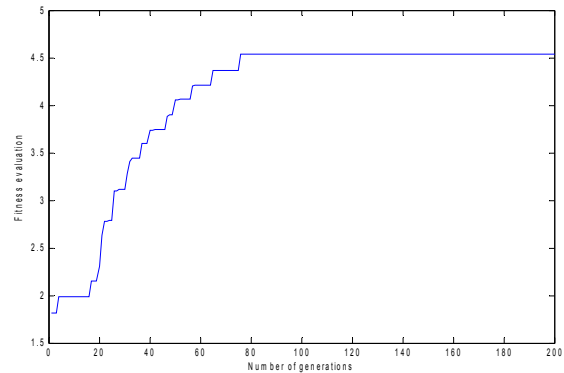


Fig. 2. Fitness of the best individual versus number of generations

### III. DETECTING LOCATION OF WATERMARK

In section III, knowing exact location of watermark signal for recovering PN sequence had been assumed. Since it is not known when the watermark in a watermarked signal starts, it is crucial that the detector locks to the received watermarked signal to recover PN sequence. Conventional SSW techniques add some bits to payload as synchronization bits to make detection of watermark possible [11].

In this context, the present paper proposes a computational approach based on genetic algorithm for detecting exact location of watermark signal. The approach incorporates the same GA that employed for recovering PN sequence.

This problem can be considered as an optimization problem whereas our cost function is the place where cross correlation between blocks of estimated PN sequence by GA and watermarked signal has the nearest amount to the number of blocks. Attending to correlation property of PN sequence, only the blocks contain PN sequence (i.e. watermark signal) in a watermarked signal converge to global optimization. Therefore this problem could be solved by combining covering method and GA.

Figure 3 illustrates procedures of this approach. Lag which represents chip distance between estimated PN sequence and watermark, will be increased one chip if the correlation function between blocks of watermarked and estimated PN sequence by GA, is not near enough to number of blocks (e.g. four blocks in figure3). Figure 4 illustrates block diagram of this approach.

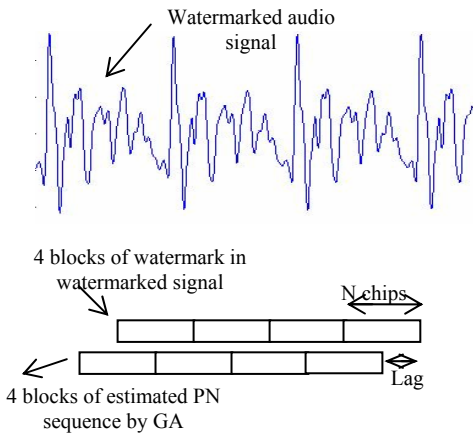


Fig. 3. Cross correlation between 4 blocks of estimated PN sequence and watermark.

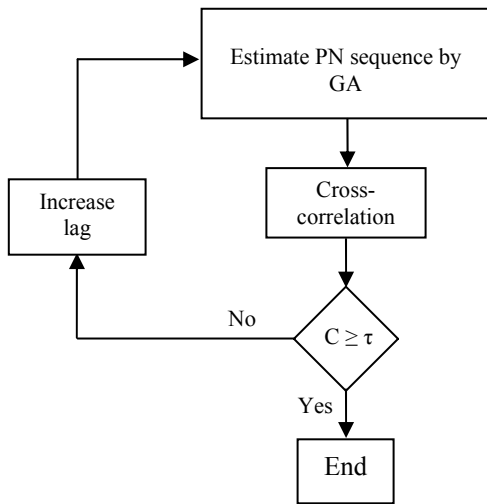


Fig. 4. Block diagram of detecting watermark location

## V. MAIN RESULTS

The most important disadvantage of GA is the time duration for converging to global optimization. Converging time in GA depends on fitness function for evaluation. For the problem of recovering PN sequence, sequences with different period have different converging time. Converging times for sequences with different periods, is given in table III. Comparing them show that converging time increases exponentially as period of PN sequences increase.

Table III.

Converging optimization time for PN sequences with different period

<i>Period of PN sequence (chip)</i>	<i>Converging Time (second)</i>
15	5.516
31	15.71
63	69.75
127	429.906
255	34677.97

Table III shows that the greater PN sequence is, the more difficult situations for recovering PN sequence and the more secure SSW will be result. However, greater period of PN decreases capacity of SSW algorithm for embedding hidden information. Typical period of maximal length PN sequence used for SSW are 31 and 63 chip.

Simulation results for detection of watermark location are presented in Figure 5. This figure, illustrates cross correlation between estimated PN sequence by GA and watermarked signal, in different portions of watermarked signal. Lag represents distance between starting point of watermark and estimated PN sequence. As it is shown in figure, zero lag (i.e. exact location of watermark) has the largest cross correlation.

Figure 6, illustrates cross correlation between estimated PN sequence and watermarked signal, when watermark signal does not exists in this portion of watermarked signal. As is shown, Cross correlation is very small in comparison with number of blocks.

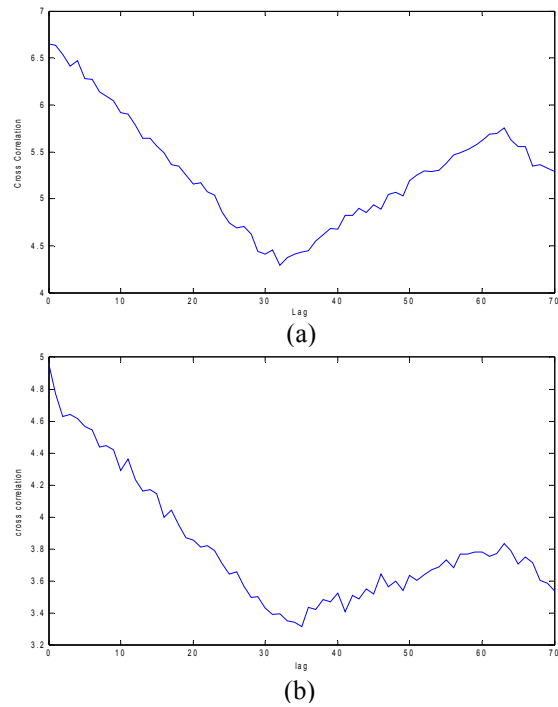


Fig. 5. Cross correlation between estimated PN sequence and watermarked signal with different lags for a) 127 chips and b) 63 chips

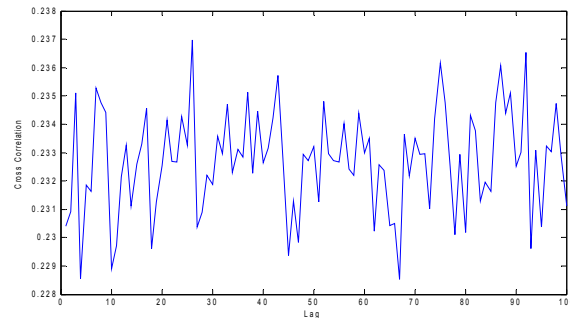


Fig. 6. Cross correlation in the portion of watermarked that watermark does not exist

These figures show that by investigating correlation property of PN sequence, and finding the largest cross correlation, location and starting point of watermark signal in a watermarked signal could be detected.

## VI. CONCLUSIONS

A novel approach based on GA for detecting hidden information from a spread spectrum watermarked proposed. To the knowledge of the authors, this is the first application of GA for audio watermarking and widens application of GA in the area of signal processing.

Using proposed approach, essential knowledge at the receiver for detecting hidden information which is PN sequence used at the transmitter and its location could be detected. Our works shows that the security of SSW can be compromised by a genetic algorithm based attack. Work is needed to make SSW secure.

Simulation results presented in previous section shows capability of GA for detecting hidden information. Converging time table shows that greater period of PN, greater time for converging to PN sequence used at the transmitter and more difficult situation for detecting hidden information.

In this paper knowing period of PN sequence, has been assumed. In the situation whereas no knowledge about period of PN sequence exists, this algorithm must be applied for different period of estimated PN sequence. Note that Typical period of maximal length sequence for SSW are 31 and 63 chips.

## REFERENCES

- [1] K. S. Tang, K. F. Man, S. Kwong and Q. He, "Genetic algorithms and their applications," *IEEE signal processing magazine*, 1996.
- [2] N. Cvejic, T. Seppanen "algorithms for audio watermarking and steganography" *PHD thesis, oulu university of technology*, June 2004.
- [3] K. Gopulan "Audio steganography using bit modification", *Proc.IEEE, intl.Conf. Acoustic Speech and signal proc.*, 2003.
- [4] R. Ansari, H. Malik, A. Khikhar "Data-hiding in audio using frequency-selective phase alteration" *Proc.IEEE, intl.Conf. Acoustic Speech and signal proc.*, 2004.
- [5] H. Joong, Y. H. Choi, "a novel echo-hiding scheme with forward backward kernels" *Circuits and Systems for Video Technology, IEEE Transactions on* Volume 13, Issue 8, Aug. 2003.
- [6] Z. Liu, A. Inue, "Spread spectrum watermarking of audio signals" *IEEE Transactions on circuits and system for video technology* Volume. 13, NO. 8, AUGUST, 2003.
- [7] W. Bender, D. Gruhl, N. Morimoto, and A. Lu. "Techniques for data hiding," *I.B.M. Systems Journal*, 35(3 & 4):313-336, 1996.
- [8] Z. Liu, Y. Kobayashi, S. Sawato, and A. Inoue, "A robust audio watermarking method using sine function patterns based on pseudo-random sequences," in *Proc. Pacific Rim Workshop on Digital Steganography*, 2002.
- [9] S. Haykin, "communication systems," 4<sup>th</sup> edition, John Wiley & Sons, Inc, 2001.
- [10] J. S. Arora, O. A. Elwakeil and A. Chahande, "Global optimization methods for engineering applications: a review," *optimal design laboratory*, 1995.
- [11] M. Haggmuller, G. Kubin, "speech watermarking for air traffic control", *euro control experimental centre*, EE Note NO.05/05, 2004.
- [12] S. Trivedi and R. Chandramouli, " Secret Key Estimation in Sequential Steganography," *IEEE Transaction on signal processing, Volume 53, NO. 2, FEBRUARY 2005*.
- [13] V. R. Asghari and M. Ardebilipour, "Spread Spectrum Code Estimation by Genetic Algorithm," *International Journal of signal processing, VOL 1, Number 4, 2004*.
- [14] K. Yen and L. Hanzo, " Genetic Algorithm Assisted Joint Multiuser Symbol Detection and Fading Channel Estimation for Synchronous CDMA Systems," *IEEE Transaction on selected areas in communication, VOL. 19, NO. 6, JUNE 2001*.
- [15] J. H. Holland, *Adaptation in Natural and Artificial Systems. Ann Arbor, MI: Univ. Michigan Press*, 1975.