Detecting Hidden Information from Watermarked Signal using Granulation Based Fitness Approximation

M. Davarynejad[1], S. Sedghi[2], M. Bahrepour[2], Chang Wook Ahn[3], M. Akbarzadeh[4], C. A. Coello Coello[5]

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 adds it to a host signal as a watermarked signal. Spreading spectrum is done by a pseudo-noise (PN) sequence. In conventional SSW approaches, the receiver must know the PN sequence used at the transmitter as well as the location of the watermark in watermarked signal for detecting hidden information. This method is attributed high security features, since any unauthorized user who does not access this information cannot detect any hidden information. Detection of the PN sequence is the key factor for detection of hidden information from SSW. Although PN sequence detection is possible by using heuristic approaches such as evolutionary algorithms, due to the high computational cost of this task, such heuristic tends to become too expensive (computationally speaking), which can turn it impractical. Much of the computational complexity involved in the use of evolutionary algorithms as an optimization tool is due to the fitness function evaluation that may either be very difficult to define or be computationally very expensive. This paper proposes the use of fitness granulation to recover a PN sequence with a chip period equal to 63, 127, 255 bits. This is a new application of authors' earlier work on adaptive fitness function approximation with fuzzy supervisory. With the proposed approach, the expensive fitness evaluation step is replaced by an approximate model. The approach is then compared with standard application of evolutionary algorithms; statistical analysis confirms that the proposed approach demonstrates an ability to reduce the computational complexity of the design problem without sacrificing performance.

1 Faculty of Technology, Policy and Management, Delft University of Technology, email: M.Davarynejad@tudelft.nl

2 Department of Computer Science, University of Twente, email: {s.sedghi@utwente.nl, m.bahrepour@utwente.nl}

3 School of Information and Communication Engineering, Sungkyunkwan University, email: cwan@skku.edu

4 Electrical Engineering Department, Ferdowsi University of Mashhad, email: akbarzadeh@kiaeee.org

5 CINVESTAV-IPN (Evolutionary Computation Group), Departmento de Computación, Av. IPN No. 2508, Col. San Pedro Zacatenco, Mexico D.F. 07300, email: ccoello@cs.cinvestav.mx

1 Introduction

In recent years, digital watermarking has received considerable attention from the security and cryptographic research communities. Digital watermarking is a technique for hiding information bits into an innocuous-looking media object, which is called host, so that no one can suspect of the existence of hidden information. It is intended to provide a degree of copyright protection such as the use of digital media mushrooms [1]. Depending on the type of the host signal used to cover the hidden information, watermarking is classified into image watermarking and audio watermarking. In this paper we focus our results to audio watermarking but the approach is also applicable to image watermarking.

Numerous audio watermarking techniques have been proposed, the most important being: LSB [2], Phase coding [3], Echo hiding [4] and spread spectrum watermarking (SSW) [5]. The latter, SSW, is recognized as the most promising watermarking method because of its high robustness against noise and its high perceptual transparency. The main idea of SSW is adding spread spectrum of hidden information to the spectrum of the host signal. Spreading the spectrum of hidden information is performed by a pseudo-random noise sequence.

The detection of hidden information from the received watermark signal is performed by the exact PN sequence used for spreading the spectrum of hidden information. Therefore, the receiver should access the PN sequence for detection. This essential knowledge for detection, results in a highly secure transmission of information against any unauthorized user who does not have access to the PN sequence and location of the watermark. Hence, the PN sequence can be regarded as a secret key which is shared between the transmitter and the receiver.

In [6], a GA is presented in such a way that it is possible to detect hidden information, whereas the receiver has no knowledge of the transmitter's spreading sequence. Repeated fitness function evaluations for such a complex problem is often the most prohibitive and limiting feature of this approach. For the problem of recovering the PN sequence, sequences with different periods have different converging times. The studies have shown that the converging time increases exponentially as the period of the PN sequences increases [6]. So the approach fails by losing the validity of information. To alleviate this problem, a variety of techniques for constructing approximation models– often referred to as metamodels – have been proposed. For computationally expensive optimization problems such as detection of hidden information, it may be necessary to perform an exact evaluation and then use an approximate fitness model that is computationally efficient.

A popular subclass of fitness function approximation methods is fitness inheritance where fitness is simply transmitted (or "inherited") [7, 8]. A similar approach named "Fast Evaluation Strategy" (FES) has also been suggested in [9] for fitness approximation where the fitness of a child individual is the weighted sum of its parents. Other common approaches based on learning and interpolation from known fitness values of a small population, (e.g. low-order polynomials and the least square estimations [10], artificial neural networks (ANN), including multi-layer perceptrons

[11] and radial basis function networks [12], support vector machine (SVM) [13], etc.) have also been employed.

In this paper, the concept of fitness granulation is applied to exploit the natural tolerance of evolutionary algorithms in fitness function computations. Nature's "survival of the fittest" principle is not about exact measures of fitness; instead, it is about rankings among competing peers. By exploiting this natural tolerance for imprecision, optimization performance can be preserved by computing fitness only selectively and by preserving this ranking (based on fitness values) among individuals in a given population. Also, fitness is not interpolated or estimated; rather, the similarity and indistinguishability among real solutions is exploited.

In the proposed algorithm, as explained in detail by its authors in [14, 15], an adaptive pool of solutions (fuzzy granules) with an exactly computed fitness function is maintained. If a new individual is sufficiently similar to a known fuzzy granule, then that granule's fitness is used instead as a crude estimate. Otherwise, that individual is added to the pool as a new fuzzy granule. In this fashion, regardless of the competition's outcome, fitness of the new individual is always a physically realizable one, even if it is a "crude" estimate and not an exact measurement. The pool size as well as each of the granule's radius of influence is adaptive and will grow/shrink depending on the utility of each granule and the overall population fitness. To encourage fewer function evaluations, each granule's radius of influence is initially large and is gradually shrunk at later stages of evolution. This encourages more exact fitness evaluations when competition is fierce among more similar and converging solutions. Furthermore, to prevent the pool from growing too large, granules that are not used are gradually eliminated. This fuzzy granulation scheme is applied here as a type of fuzzy approximation model.

The paper is organised as follows: Section 2 presents a brief overview of the proposed granulation based fitness approximation method. For future details, readers are referred to [15] were the proposed method is described in more details and an example is also provided in addition to some supporting simulation. An auto-tuning strategy for determining the width of membership functions (MFs) is presented in [16], which removes the need for exact parameter determination, without obvious influence on convergence speed. In Section 3, the spread spectrum watermarking and the properties of the PN sequence are described. In Section 4, the recovering of the PN sequence from a received watermarked signal using GA and granulation based fitness approximation is presented. Some supporting simulation results and discussion thereof are presented in Section 5. Finally, some conclusions are drawn in Section 6.

2 AFFG Framework - The Main Idea

The proposed adaptive fuzzy fitness granulation (AFFG) aims to minimize the number of exact fitness function evaluations by creating a pool of solutions (fuzzy granules) by which an approximate solution may be sufficiently applied to proceed with the evolution. The algorithm uses Fuzzy Similarity Analysis (FSA) to produce and update an adaptive competitive pool of dissimilar solutions/granules. When a new solution is introduced to this pool, granules compete by a measure of similarity to win the new solution and thereby to prolong their lives in the pool. In turn, the new individual simply assumes fitness of the winning (most similar) individual in this pool. If none of the granules is sufficiently similar to the new individual, i.e. their similarity is below a certain threshold, the new individual is instead added to the pool after its fitness is evaluated exactly by the known fitness function. Finally, granules that cannot win new individuals are gradually eliminated in order to avoid a continuously enlarging pool. The proposed algorithm is briefly discussed below. For further details, readers are referred to [14, 15] where the proposed method is described in more details and an example is provided, in addition to some supporting simulation.

After a random parent population is initially created, a set of fuzzy granules that is initially empty is shaped. The average similarity of new solutions to each granule is then computed. This is influenced by granule enlargement/shrinkage. The fitness of each new solution is either calculated by exact fitness function computing or is estimated by associating it to one of the granules in the pool if there is a granule in the pool with a similarity value higher than a predefined threshold. Depending on the complexity of the problem, the size of this pool can become excessive and computationally cumbersome by itself. To prevent such unnecessary computational effort, an interesting and advantageous approach is introduced in [15].

The distance measurement parameter is completely influenced by granule enlargement/shrinkage in widths of the produced MFs. In [12], the combined effect of granule enlargement/shrinkage is based on the granule fitness and it needs to adjust two parameters. These parameters are problem dependent and it seems critical to set up a procedure in order to avoid this difficulty. In order to removes the need for exact parameter determination of AFFG approach, an auto-tuning strategy is presented in [16].

3 Spread Spectrum Watermarking

SSW is the algorithm that has high robustness (surviving hidden information after noise addition), high transparency (high quality of watermarked signals after addition of hidden information) and high security (against unauthorized users) from the watermarking features point if view. SSW borrows the idea of spread spectrum communication to hide information by embedding the bits of information into a host signal. The embedding processes employ a pseudorandom noise (PN) sequence. A PN

sequence is a zero mean periodic binary sequence with a noise defined by a waveform whose bits are equal to +1 or –1 [17].
Each bit of hidden information w(i) is multiplied by all the bits of a period of a pseudorandom noise (PN), p(n) sequence to generate each block of the watermark signal w(i).

$$w(i) = p(n)\ m(i) \tag{1}$$

A watermark signal is the sequence of all the watermark blocks as w = (w1,…,wk). The watermarked signal s(w,x) is produced as:

$$S(w,\ x) = \lambda\ w(n) + x(n) \tag{2}$$

Then, the watermarked signal s(w,x) is sent to the receiver.
The extraction of hidden information from a received watermarked signal is performed using the correlation property of the PN sequence. Cross correlation C(.,.) between two PN sequences pa and pb is as (3) [18]:

$$C(P_a,\ P_b) = \frac{1}{N}\sum_{i=0}^{N-1}(P_a(i)\ P_b(i)) = \begin{Bmatrix} i, & if\ a=b \\ -1/N, & otherwise \end{Bmatrix} \tag{3}$$

Hence, cross correlation between a watermarked signal and a PN sequence is as follows:

$$C(S,p') = C(w,p') + C(m.p,p') = \begin{Bmatrix} C(w,p') + m & if\ p=p' \\ C(w,p') - \frac{m}{N} & Otherwise \end{Bmatrix} \tag{4}$$

Equation (4) expresses that by calculating the correlations between the received watermarked signal and the employed PN sequence at the transmitter, and comparing the result with a threshold, determines the bit of hidden information.

4 Recovering PN Sequence

Recovering the PN sequence from a spread spectrum watermarked signal where no information about the PN sequence or its location is known would be very hard since there are vast regions for the solutions set. For instance, in order to recover a PN sequence with a period equal to 63 bits, 263 PN sequences must be generated.
In this section, with the assumption that knowing the exact location of the watermark in the watermarked signal, we describe the recovering of the PN sequence.

In [19], an approach for detecting the hidden information from an image spread spectrum signal is proposed. This approach detects abrupt jumps in the statistics of watermarked signal to recover the PN sequence. The proposed algorithm, which is based on hypothesis tests for detection of abrupt jumps in the statistical values is very complicated and its performance suffers from for low frequency embedding.

Recovering the PN sequence could be considered as an unconstrained optimization problem. We have a set of feasible solutions to minimize a cost function using a global optimizer. The set of feasible solutions are sequences with periods of PN sequences and elements of +1 and –1. Defining a cost function for this problem should be based on a very useful property of SSW in detection which is the correlation property of the PN sequence. So, our cost function is the cross correlation between the generated sequence and the watermarked signal.

In [20], an interesting method for recovering the PN sequence of a spread spectrum signal with a predefined SNR, is proposed. This approach uses a GA with a fitness function defined in terms of the cross correlation between the estimated PN sequence and the spread spectrum. However, the spread spectrum watermarking is more complicated than a single spread spectrum signal since in SSW, the spread spectrum hidden information is like a white Gaussian noise for a host signal.

Note that computing the cross correlation between sequences of our solutions set and watermarked signal for only one block of SSW signals, will not converge to the PN sequence used at the transmitter, since the energy of the host signal is at least 12 dB more than the energy of the watermark and it has a strong effect on maximizing the cross correlation (i.e., an optimization algorithm converges to a sequence that maximizes the 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 the computation of the cross correlation. In this case, the watermark signal has a stronger effect than the host signal on maximizing the cross correlation function.

Finding the global optimization by searching over the entire set of our solutions, as mentioned above, is the subject of deterministic methods such as 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 the covering method is to cover the feasible solutions set by evaluating the objective function at all points [21]. These algorithms have high reliability and accuracy is always guaranteed, but they have a slower convergence rate [22].

Since our solutions set is vast, we need efficient optimization algorithms that have a high reliability and fast convergence rate. Many stochastic optimization algorithms have been proposed such as the genetic algorithm, simulated annealing, ant colony, etc.; however the GA has shown to be one of the most successful and powerful search engines for a wide range of applications and strikes an attractive balance between reliability and convergence rate.

5 Empirical Results

The empirical study consisted on comparing the GA performance, as a function optimizer, and the proposed granulation techniques with fuzzy supervisory (AFFG-FS). Since in [16], by numerous simulations, it has been shown that AFFG-FS, with its fuzzy supervisory technique, removes the need for exact parameter determination without obvious influence on convergence speed, we did not take into account the original AFFG.

Since the GA was used as a function optimizer, we chose roulette wheel with elitism as the selection method, in order to keep track of the best solution found. The GA was implemented with one-point crossover. The population size was set to 20 with the elite size of 2. The mutation and crossover rate used was 0.01 and 1.0, respectively. Ten runs of each experiment were executed.

For AFFG-FS, the number of individuals in the granule pool is varied between 10, 20 and 50. The report results were obtained by achieving the same level of fitness evaluation for both the canonical GA and the proposed methods.

The average convergence trends of the standard GA, AFFG-FS are summarized in Figures 1-3. All the results presented were averaged over 10 runs. As shown in the Figures, the search performance of the AFFG-FS is superior to the standard GA even with a small number of individuals in the granule pool.

We also studied the effect of varying the number of granules N_G on the convergence behavior of AFFG-FS. It can be shown that AFFG-FS is not significantly sensitive to N_G. However, a further increase of N_G, slows down the rate of convergence due to the imposed computational complexity.

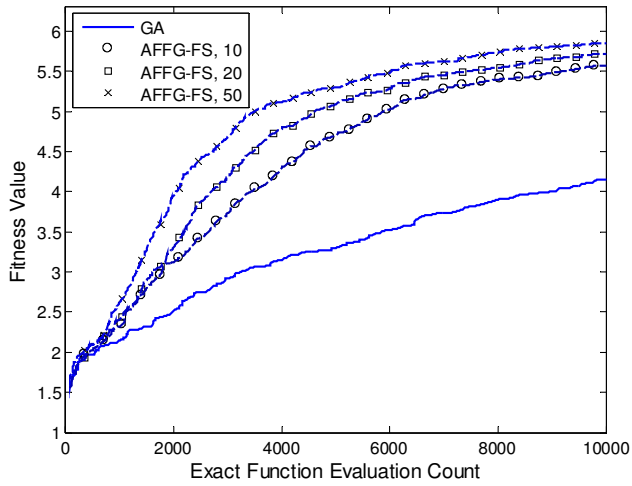

Figure 1: Cross correlation between estimated PN sequence with the period of 255 chips and the watermarked signal

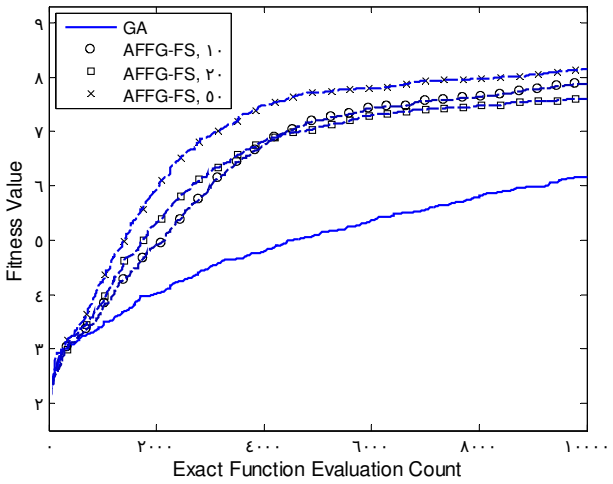

Figure 2: Cross correlation between estimated PN sequence with the period of 127 chips and the watermarked signal

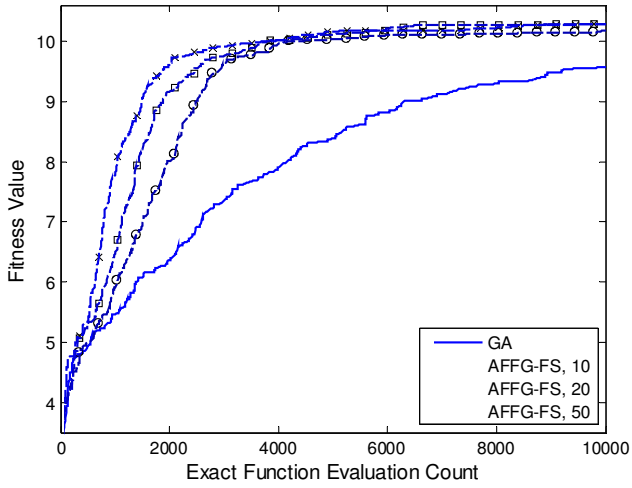

Figure 3: Cross correlation between estimated PN sequence with the period of 63 chips and the watermarked signal

6 Concluding Remarks

One of the most secure techniques of audio watermarking is spread spectrum audio watermarking. The key factor for detection of hidden information from SSW is the PN sequence. Here, an intelligent guided technique via an adaptive fuzzy similarity analysis is adopted in-order to accelerate the process of evolutionary based recovering of PN sequence. A fuzzy supervisor such as the auto-tuning algorithm is introduced in order to avoid the tuning of parameters used in this approach.
A comparison is provided between simple GA, FES and the proposed approach. Numerical results showed that the proposed technique is capable of optimizing functions of varied complexity efficiently. Furthermore, in comparison with our previous work, it can be shown that AFFG and AFFG-FS are not significantly sensitive to N_G , and small N_G values can still produce good results. Moreover, the auto-tuning of the fuzzy supervisor removes the need for exact parameter determination without an obvious influence on convergence speed.

Acknowledgments

The last author acknowledges support from CONACyT project no. 45683-Y.

References

1. N. Cvejic, T. Seppanen “Algorithms for Audio Watermarking and Steganography”, PHD thesis, oulu university of technology, June 2004.
2. K. Gopulan “Audio steganography using bit modification”, Proceedings of the 2003 International conference on Acoustic Speech and signal Processing, 2003.
3. R. Ansari, H. Malik, A. Khikhar “Data-hiding in audio using frequency-selective phase alteration”, Proceedings of the IEEE International conference on Acoustic Speech and signal Processing, 2004.
4. H. Joong, Y. H. Choi, “a novel echo-hiding scheme with forward backward kernels” IEEE Transactions on Circuits and Systems for Video Technology, Volume 13, No 8, Aug 2003.
5. Z. Liu, A. Inue, “Spread spectrum watermarking of audio signals”, IEEE Transactions on Circuits and System for Video Technology, Volume 13, NO. 8, Aug 2003.
6. Saeed Sedghi, Habib Rajabi Mashhadi, Morteza Khademi. "Detecting Hidden Information from a Spread Spectrum Watermarked Signal by Genetic Algorithm", IEEE Congress on Evolutionary Computation, pp. 480-485, July 16-21, 2006
7. J.-H. Chen, D. Goldberg, S.-Y. Ho, and K. Sastry, “Fitness inheritance in multiobjective optimization”, Proceedings of the 2002 International conference on Genetic and Evolutionary Computation Conference, pp. 319–326, 2002.
8. Margarita Reyes-Sierra , Carlos A. Coello Coello, “Dynamic fitness inheritance proportion for multi-objective particle swarm optimization”, Proceedings of the 8th annual conference on Genetic and Evolutionary Computation, July 08-12, 2006, Seattle, Washington, USA
9. Mehrdad Salami , Tim Hendtlass, “The Fast Evaluation Strategy for Evolvable Hardware”, Genetic Programming and Evolvable Machines, Volume 6, NO. 2, p.139-162, June 2005.

10. R. Myers and D. Montgomery. “Response Surface Methodology”, John Wiley & Sons, Inc., New York, 1995.
11. Y.-S. Hong, H.Lee, and M.-J. Tahk, “Acceleration of the convergence speed of evolutionary algorithms using multi-layer neural networks”, Journal of Engineering Optimization, Volume 35, NO 1, pp. 91–102, 2003.
12. Won, K. S. and Ray, T., “A Framework for Design Optimization using Surrogates”, Journal of Engineering Optimization, pp. 685-703, 2005.
13. Gunn S.R., “Support Vector Machines for Classification and Regression”, Technical Report, School of Electronics and Computer Science, University of Southampton, (Southampton, U.K.), 1998.
14. M. Davarynejad, "Fuzzy Fitness Granulation in Evolutionary Algorithms for Complex Optimization", M.Sc. Thesis. Ferdowsi University of Mashhad, Department of Electrical Engineering, 2007.
15. M. Davarynejad, M.-R. Akbarzadeh-T, N. Pariz, “A Novel General Framework for Evolutionary Optimization: Adaptive Fuzzy Fitness Granulation”, Proceedings of the 2007 IEEE International Conference on Evolutionary Computing, pp. 951-956, Singapore, September 25-28, 2007.
16. M. Davarynejad, M.-R. Akbarzadeh-T, Carlos A. Coello Coello, "Auto-Tuning Fuzzy Granulation for Evolutionary Optimization", IEEE World Congress on Evolutionary Computation, pp. 3572-3579, June 2008.
17. S. Haykin, “Communication Systems,” 4th edition, John Wiley & Sons, Inc, 2001.
18. Z. Liu, Y. Kobayashi, S. Sawato, and A. Inoue, “A robust audio watermarking method using sine function patterns based on pseudorandom sequences”, in Proceedings of the Pacific Rim Workshop on Digital Steganography, 2002.
19. S. Trivedi and R. Chandramouli,” Secret Key Estimation in Sequential Steganography”, IEEE Transaction on Signal Processing, Volume 53, NO. 2, Feb 2005.
20. V. R. Asghari and M. Ardebilipour, “Spread Spectrum Code Estimation by Genetic Algorithm,” International Journal of Signal Processing, Volume 1, NO 4, 2004.
21. J. S. Arora, O. A. Elwakeil and A. Chahande, “Global optimization methods for engeering applications: a review”, optimal design laboratory, 1995.
22. 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, Volume. 19, NO. 6, June 2001.