Examiner's report of doctoral thesis

Author: Nguyễn Thanh Dũng

Title: Secure Encryption via Deterministic Chaos

Examiner: doc. RNDr. PaedDr. Eva Volná, PhD.
University of Ostrava

Objectives of the thesis and their fulfilment

A given doctoral thesis is focussed on possibilities of evolutionary algorithms, which are applied to enhance the quality of recovered signal in chaotic secure communication system. The Pecora and Carroll, Active-Passive Decomposition method and Feedback method are used to achieve the synchronization of chaos communication. Differential evolution algorithm and Self-Organising Migrating Algorithm are used as the evolutionary algorithms to find the unknown parameters of receiver chaotic systems. Chosen methods can be considered as fully competent and it is sufficient for purposes and objectives of the PhD thesis. The given thesis has fulfilled its main objectives and its topic is up to date.

Benefits in the field of knowledge

The synchronization error always exist in the communication system, therefore application of evolutionary algorithms to improve the quality of communication chaos is required. The author's new proposal demonstrated that the synchronization qualities of chaotic secure communication, which were achieved by estimated parameters via evolutionary algorithms, is always better than that of original. Next, it is possible to state that all realized simulations gave satisfactory results and thus evolutionary algorithms are successful in solving this difficult problem.

The proposed procedures and methodologies are supported by several publications of the doctoral student. In the years 2009-2012, he published 9 articles in journals and at international conferences and workshops.

Benefits in the field of social practice

The author created a pilot application, which introduced a method of improving the efficiency of chaotic communication schemes. It is obvious that the proposal is based on good author's knowledge and experience with an implementation of similar problems in practice.

Formal arrangement

The doctoral thesis has 105 pages. The whole thesis is written in English. The thesis is written and structured in a logical and well arranged way. Its text is presented at an appropriate level of expertise and it is compact, only some of the images are not of adequate quality.

Questions and comments

1. I miss a more detailed state of art. Could you briefly specify whether a given issue has been solved by other softcomputing methods too?
2. Could you specify your contribution in multi-authors publications?

Conclusion

The submitted thesis fulfils the requirements for a doctoral thesis, both in terms of theoretical - methodological level, so the usefulness in practice. The thesis contains the original results.

I recommend the thesis to the defence before the relevant commission. Based on the thesis, I suggest the academic and scientific degree "Doctor Philosophiae" (Ph.D. abbreviation) to confer to Nguyễn Thanh Dũng after successfully defending of his thesis.

Ostrava, 20 September 2012

Doc. RNDr. PaedDr. Eva Volná, PhD.

Review of Ph.D. work

Secure Encryption Via Deterministic Chaos

Study-branch: Technical Cybernetics
Author: Nguyễn Thanh Dũng
Supervisor: Prof. Ing. Ivan Zelinka, PhD.
Reviewer: Doc. Mgr. Roman Jašek, Ph.D.

About Work and Main Aims of this Work are these:

The evolutionary algorithms are applied to enhance the quality of recovered signal in chaotic secure communication system that is the core objective of this dissertation. The synchronization error between the transmitter and the receiver in communication systems is used to design the cost function.

The parameters of chaotic dynamic model are estimated by evolutionary algorithms via minimizing the synchronization errors. By this way, the quality of recovered signal is increased when the synchronization error approaches to minimum value. The Pecora and Carroll method (PC method), Active-Passive Decomposition method (APD method) and Feedback method-three synchronization methods are used to achieve the synchronization of chaos communication. Differential evolution algorithm (DE) and Self-Organising Migrating Algorithm (SOMA) are used as the evolutionary algorithms to find the unknown parameters of receiver chaotic systems. The synchronizations of identical chaos are executed: Synchronization of three dimensional Lotka-Volterra systems via PC method, synchronization of four dimensional Qi systems via APD method, synchronization of four dimensional Liu systems via Feedback method. The powerful of EA on this problem are also proven via the synchronization of 5 and 6 dimensional chaotic systems.The application of EA is used for designing the control function in the synchronization between two difference chaotic systems.Based on the optimum results from evolutionary algorithms, the estimated values are used to reconstruct the receiver chaotic systems. The optimal quality of synchronization is achieved by using the estimated parameters. The synchronization between the transmitter and the receiver chaotic system is used to retrieve the transmitted information in Chaotic Masking Scheme (CMS). The quality of chaotic secure communication is enhanced with estimated parameters.

Advantages in knowledge

In any communication system, there are synchronization errors. The choice of evolutionary algorithms, therefore, in my opinion, an innovative contribution.

Outputs of the author confirmed that their implementation was appropriately chosen procedure.

Advantages in terms of social practice

The author created a pilot program that introduced a method to improve the efficiency of chaotic communication systems. It is clear that the proposal is based on the author's good knowledge and experience in implementing similar problems in practice.

Presentation

Dissertation is 105 pages, has a good and clear structure. Nedostačná image quality is to reduce the overall level of work.

High quality publication outputs are the author, in which their practices interpetuje (in 2009-2012 was issued 9 articles in journals and at international conferences and workshops).

Questions and comments

First Where else could you use outputs of your work? Where do you see the evolutionary algorithms as a tool of competitive advantage?

Conclusion

The submitted thesis fulfils the requirements for a doctoral thesis, both in terms of theoretical - methodological level, so the usefulness in practice. The thesis contains the original results.

I recommend the thesis to the defence before the relevant commission. Based on the thesis, I suggest the academic and scientific degree "Doctor Philosophiae" (Ph.D. abbreviation) to confer to Nguyễn Thanh Dũng after successfully defending of his thesis.

26. 9. 2012

Review of PhD work of Mr. Ing. Nguyễn Thanh Dũng named „*Secure Encryption Via Deterministic Chaos*"

Doc. Dr. Ing. Tomáš Brandejský, FTSci CTU in Prague

From the formal viewpoint, the work written in English language consists of 83 pages of original text extended by such parts like Acknowledgements, Abstract (in both English and Czech languages), lists of Contents, Figures, Tables and Symbols and Abbreviations. The work is naturally divided into 3 parts and 15 chapters. The separate parts are Introduction, Theory and Experiment. These chapters are named Introduction and State of Art, The Aims of Dissertation, Secure Communication Based on Chaos, Synchronization Methods, Chaotic Systems, Evolutionary Algorithms, Design of Experiment – Cost function, Synchronization of 3D Lotka-Volterra System via Pecora and Carroll method, Synchronization of 4D Qi Chaotic System via Active-Passive Decomposition method, Synchronization of 4D Liu Chaotic System via Feedback method, Synchronization of 5D Lorenz Chaotic System, Six Dimensional Example: Synchronization of 6D Lorenz Chaotic System, Synchronization of Two Different Chaotic Systems, Application on Chaotic Secure Communication System and Discussions and Conclusions.
The first chapter named Introduction and State of Art consists of two pages and it describes problem domain and structure of the work. There are also listed presented experiments.
Within the second chapter The Aims of Dissertation, which is one page long, the main objectives of the work are summarised.

The chapter Secure Communication Based on Chaos opens second – Theoretical - part of the work. It contains three pages and explains general structure of chaotic system, Chaos Shift Keying and Chaotic Masking Scheme chaotic communication methods.
Fourth chapter named Synchronization Methods also consists of three pages and it introduces fundamental synchronization methods as it is Pecora and Carroll method, Active-Passive Decomposition method and Feedback method.
As the topic tells, the next chapter describes Chaotic Systems. This chapter introduces systems used in the following experiments, namely they are Lorenz system, Rössler system, Lü system, Lotka-Volterra system, Lorenz – Stenflo system, Qi system, Liu system, Roy and Musielak 5D extension of Lorenz system and Kennamer 6D extension of the same system.
The sixth chapter named Evolutionary Algorithms introduces applied used in experiments described in the work (by my mean, they are not used to simulate anything – chapter 6, page 34, line 2). They are differential evolution and SOMA.

The last and the largest part of thesis is Experiment Section. It starts with the chapter Design of Experiment – Cost function. Within this chapter, cost function, used HW and SW equipment and DE and SOMA algorithm parameters are described.
The chapter Synchronization of 3D Lotka-Volterra System via Pecora and Carroll method presents experiments with this system. Unfortunately, the synchronization of the

some systems using another method is not compared (the similar remark might be written also in same following experiments).
The ninth chapter Synchronization of 4D Qi Chaotic System via Active-Passive Decomposition method describes experiments with another system using different synchronization method.
The tenth chapter describes Synchronization of 4D Liu Chaotic System via Feedback method.
The next one outlines Synchronization of 5D Lorenz Chaotic System. The following chapter brings Six Dimensional Example: Synchronization of 6D Lorenz Chaotic System.
Chapter named Synchronization of Two Different Chaotic Systems brings problem of synchronization of two non-identical chaotic systems. The chapter demonstrates on example of synchronization of Rössler and Lü systems that the synchronization between different systems is impossible.
The chapter Application on Chaotic Secure Communication System discusses results of experiments with respect to application in secure communication.
The last chapter Discussions and Conclusions then brings comparison of synchronization methods and used evolutionary techniques.

The work is written in good English. Its structure corresponds to requirements to PhD work. I found some errors in language, but they are not significant and I am not native speaker.

Mistakes and problems found in the text:

Ch. 3.2, 1st line: When there is defined acronym, the original words are written with capitals.

Many chapters are too short that they should be sub-chapters.

What is the sense of chapter 7, when the following chapters confirm meaning that for different chaotic system synchronization methods there are needed different cost functions?

In the experiment description, there is not described if these experiments were performed only once or repeatedly. Does it mean that results produced by DE and SOMA algorithms with presented parameters are so repeatable, that it has no sense to discuss problem of experiment repetition?

What is the influence of signal/noise ratio (ratio of chaotic system signal and transmitted signal) on efficiency or suitability of communication methods?
And what about transmitted/chaotic signal average values differences? These problems were not discussed in the work.

Achievement of aims defined in the work

- The goals of the work were presented in chapter 2 as:

- To simulate several examples of identical chaos synchronization (3, 4, 5, 6-dimensional chaos systems).
- To simulate the using of EA for synchronization between two difference chaos systems.
- To simulate a synchronization via PC, APD and Feedback methods.
- To prove that EA are able to estimate the unknown parameters of chaos systems.
- To optimum cost function with SOMA and DE, enhancing the quality of chaos synchronization.
- To test a performance of EA in CMS scheme.

It is possible to confirm that these goals were satisfied with respect to above presented remarks.

Quality of state of art discussion of solved problem in the work
State of art is discussed in chapter 1 (and particularly also in the following chapters). This discussion is adequate to solved problem.

Theoretical asset of PhD work
The work is practically oriented as concludes numbers of pages devoted to theoretical and practical parts of the work. The work also brings summarised information about many chaotic systems.

Practical asset of PhD work
From the practical viewpoint, the work brings results of many experiments with synchronization of chaotic systems of different types using many Synchronization Methods.

The suitability of used methods
The used methods are standard research methods and they are suitable to solved problem.

The way how the used methods were applied
These methods were well applied and results are applicable in the further research.

PhD student proved adequate knowledge in given subject.

I recommend the work for defence.

In Prague 24th September

Doc. Dr. Ing. Tomáš Brandejský