Review

Ph.D. Candidate : Ing. Volodymyr Lynnyk, ČVUT Praha
Dissertation Topic: Chaos based communication systems

General
Chaotic systems are extremely sensitive to initial conditions and this feature can be very helpful in the field of cryptography. Various encryption schemes use chaotic systems for encryption key generation and this key is then, for example, used for pixel permutation and pixel diffusion, in the case of pattern encryption. But chaotic systems and their maps can be used directly for encryption purpose. Images, multimedia and signal in general providing the most information to a person. For this reason the question appears as to which way can be signal be secured against unauthorized reading e.g. in medicine or military fields. Position permutation and diffusion of the pixels belongs to basic methods of encryption. Their combination leads to better security against known attacks and is very often has found practical usage. However, these methods remains open for various encryption algorithms and that is why the knowledge of chaotic systems can be useful. These systems are extremely sensitive to initial conditions and thus they are suitable candidates in the field of cryptography. Many papers have been written on this theme for that very reason.

Content and structure
The doctoral dissertation dissusses Chaos based communication from a theoretical viewpoint. The thesis consists of 4 chapters including Introduction, Preliminary knowledge, Chao-based communication, Generalized Lorenz system and Conclusion. The thesis also contains results of candidates research in the form of 10 publications.
Based on the state of art, it can be stated that the selected topic represents a well known and properly investigated area of chaos encryption.

Formal quality and defined aims
The quality of the candidates thesis can be evaluated from a graphical and formal point of view. In the graphical point of view it can be stated, that the level of quality is very good, however the formal quality has one drawbacks - aims are not clearly defined in thesis.

Selected topic and methods
In the thesis, the candidate used rigirous and theoretical methods and its research follows standard scientific processes.

Question and remarks
In the proposed thesis I would have following questions and suggestions (as discovered during review) :

1. Aims are not clearly defined in proposed thesis. Can you please clarify what aims has been used in your thesis and how they were fullyfied?
2. Fig. 2.13 is weakly printed ony with a few points. Is that picture complete?
3. Page 37. Please clarify claiming “Its security is not proven”.

4. Remark – numbering of the references in the text is not sequential. According to common rules, it should be like [1], [2],… instead of [65; 74; …] as is on p.1 and in whole thesis.

Conclusion

I have to state that the Ph.D. thesis, proposed by candidate Ing. Volodymyr Lynnyk meet scientific criteria. According to my opinion, the proposed thesis are suitable and fully meet criteria for defence process.
My conclusion is that I recommend proposed thesis for defense.

prof. Ing. Ivan Zelinka, Ph.D.
Department of Informatics and Artificial Intelligence
Faculty of Applied Informatics
Tomas Bata Univerzity in Zlin
Nad Stranemi 4511
Zlin 76001