OPINION

by Prof. PhD Julian Vasilev

University of Economics – Varna,

Professor in professional field 4.6 "Informatics and Computer Science",

validated in the register of academic staff of THE NATIONAL ACADEMY of Sciences "Habilited persons with scientific indicators"

Author of the dissertation work: Tsvetelina Rosenova Ivanova

Theme of the dissertation work: Research of cryptographic function for protection of sound files

Scientific Advisor: Prof. Dr. Sc. Borislav Panayotov Stoyanov

Primary unit that discovered the thesis protection procedure: Department of Computer Informatics at the University of Schummen

Reason for writing the opinion: Order No RD-16-033/24.03.2022 to the Rector of the University of Schumen for the opening of a procedure for the protection and validation of a scientific jury; held the first meeting of the scientific jury on 01.04.2022.

I. Total labour performance

Labour has a total volume of 105 pages. It begins with a general characteristic of the dissertation work, thanks. Continues with 3 chapters, conclusion, bibliography.

The aim of the work is "to construct and study of a function for encrypting audio files in order to improve information security by using mathematical functions from chaos theory, which are subjected to different filtering". The tasks follow the logic of the exhibition.

The object of the study are the pseudo-random sequence generators based on chaotic functions and a cryptographic algorithm to protect sound files.

The subject of the study is the "cryptographic resistance of pseudo-random sequence generators and of sound file protection algorithms".

Chapter One (in a volume of 24 pages) is entitled "Current state of the issue related to information protection". Basic methods in cryptography, different types of algorithms, keys have been studied. A special place is allocated to the random generators of household sequences (item 1.3).

Chapter two (in a volume of 30 pages) is titled "Modeling pseudo-random generators through chaotic systems". Experiments have been done with different input data and in various software tools. The results of the tests are documented correctly.

Chapter Three (in a volume of 18 pages) is entitled "Function for protecting audio files based on Ikeda map".

Each chapter ends with conclusions.

II. Positive moments

The author has mathematical background. There are formulas. A number of diagrams have been made illustrating test results in various software products. The style is scientific. The exhibition follows a common logic.

In a positive way, I take into account the actual experiments carried out and their documentation. **Arduino UNO microcontroller** was used to conduct the experiments.

I accept the **contributions** as achievements of the author.

The **publications** on the dissertation work cover the points for the acquisition of the "Doctor" degree in professional field 4.6 (according to the PPZRASRB). All publications are in English.

The author's concise work (in a volume of 31 pages) represents essential parts of the work.

The PhD student Tsvetelina Ivanova has a profile **in Scopus** (https://www.scopus.com/authid/detail.uri?authorId=57190940003). In Scopus, she has 5 publications, 8 quotes (no autoquotes), h-index: 1 (no autoquotes). For a young scientist, she has shown essential work – both as a number of publications and as a quality of the works themselves.

She participated in **5 scientific projects**.

III. Notes and recommendations. Questions.

When correlation coefficients (e.g. tables 1.3, 3.3) are presented, it is appropriate to give the p-value.

It is good to give the code to Arduino (as an application).

It is good to prepare a reference for the implementation of minimum national requirements for the acquisition of educational and scientific degree "Doctor" in professional field 4.6.

The reference to publications is good to give structured (studies, articles, reports).

Some of the results of the experiments could have been given as applications.

I have the **following questions**:

1. Before proceeding with a correlation analysis, it is appropriate to carry out several checks (related to the initial assumptions of the correlation analysis).

2. Is LaTeX used for the dissertation? Why hasn't Office 365 been used?

3. In some cases, there is "data noise" in encryption. Is there data loss in data encryption?

IV. Conclusion

I believe that the PhD student Tsvetelina Ivanova has shown a skill in developing an independent scientific study of the scale of the dissertation.

Critical remarks and recommendations made do not diminish the contributions made by the author. The formulated notes and recommendations aim to improve the future work of Tsvetelina Ivanova.

As a member of the scientific jury for awarding an educational and scientific degree "Doctor" I give my positive assessment of the willingness of the candidate Tsvetelina Ivanova to acquire the educational and scientific degree "Doctor" in professional field 4.6 "Informatics and Computer Science".

18.04.2022   With respect:

Varna   /Julian Vasilev/