KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN

OPINION

by Assoc. Prof. DSc Pavel Stoyanov Petrov, University of Economics - Varna, Faculty of Informatics, Department of Informatics

for the dissertation of **Tsvetelina Rosenova Ivanova** on the topic **"Research of cryptographic function for protection of sound files"**, presented for obtaining the educational and scientific degree "Doctor" in Professional Field 4.6. Informatics and Computer Science

The opinion was prepared based on the Law on the Development of Academic Staff in the Republic of Bulgaria (ZRASRB), Rules for Implementation of the Law on the Development of Academic Staff in the Republic of Bulgaria (PPZRASRB), Rules of The Konstantin Preslavsky University of Shumen (KPUS) - 26.11.2021, Order of the Rector of the KPUS №RD-16-003/24.03.2022 and Decision of the Scientific Jury.

Dissertation characteristics and the significance of the developed problem

The dissertation is 105 pages long and includes an introduction - a general description of the dissertation, three chapters, a conclusion, and a bibliography of 140 sources. There are 18 figures and 28 tables included.

The Introduction establishes the relevance and significance of the dissertation's topic in relation to the need to improve the reliability of digital information and communication channels for data transmission, as well as the use of various audio encryption algorithms. The following goal has been set up: develop and test a function for encrypting audio files in order to improve information security by using mathematical functions from chaos theory that are subjected to various filtering. To accomplish this goal, there are three main tasks. The research object, subject, and methods are also presented.

The current state of the problem of audio file protection is reviewed in Chapter One. There are discussions about cryptography and sound files. The use of chaotic systems to model pseudo-random generators is proposed in Chapter Two. The proposed pseudo-random generators, which are based on a chaotic attractor, a chaotic function, and two Zaslavsky functions, were tested experimentally. The developed function for audio file protection is examined in Chapter Three through various tests on various parameters.

In the form of a description of the contributions, the Conclusion summarizes the main findings of the study. There are also suggestions for future work.

The dissertation's problem is significant: issues related to the development and analyses of new information protection algorithms are critical for increasing the reliability of digital channels for audio data transmission. From a scientific standpoint, research into a cryptographic algorithm based on pseudo-random generators and using chaos theory functions is of some interest, and it could be of great practical importance. In this sense, research in this field is beneficial, and the author's proposals are both theoretical and practical.

The Dissertation Abstract is 31 pages long and accurately reflects the dissertation's content.

Evaluation of results and contributions

The author has 6 publications on the topic and demonstrates in-depth knowledge of the state of the problems on the dissertation topic. The dissertation's findings have been validated in peer-reviewed journals; there are five registered publications in Scopus with an H-index of 2, which not only meet but also exceed the minimum requirements of the Regulations for ZRASRB implementation. In the future, I recommend more publications as a first author, both collectively and individually.

I accept the dissertation's contributions as significant and useful - one scientific and five scientifically applied.

Critical assessments, remarks, and recommendations

- The text is broken up into numerous sub-sections, some of which are only one page or one paragraph long (1.1.1, 1.1.3, 1.3.1, 1.3.3, 1.4.3, etc.). To avoid the feeling of reading a reference book, these parts could be enlarged with a smoother transition and connection between them. Also, subdivisions with only one sub-item should be avoided (3.1.1).
- Several styles of bibliographic description are noticed when designing the bibliography. All publications should follow the same style. When indicating Internet sources, indicate when they were available / used, as it is relatively easy to delete and change content in the Internet space. Although an attempt was made to arrange the sources in alphabetical order, there are some shifts, such as sources 15-24 and others. Sources 107 and 120 are nearly identical.

Conclusion

The criticisms and suggestions made do not take anything away from the dissertation's accomplishments, and I appreciate the dissertation's achievements. I believe Tsvetelina Rosenova Ivanova has presented a study that meets the requirements of ZRASRB and PPZRASRB, as well as the rules of KPUS for awarding the educational and scientific degree "Doctor," and I propose to the Scientific Jury to give Tsvetelina Rosenova Ivanova the educational and scientific degree "Doctor" in PF 4.6. Informatics and computer science.

Date: 09.05.2022 г. Member of the Jury:

/Assoc. Prof. DSc Pavel Petrov/