АНОТАЦІЯ

Радченко Є. О. Алгоритмічне та програмне забезпечення систем захисту мультимедійних даних користувачів мережі Інтернет. − Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня доктора філософії з галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення. – Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Київ, 2020.

Мультимедійні дані складають значну частку даних, що передаються через мережу Інтернет та зберігаються у різноманітних хмарних сховищах. Частина цих мультимедійних даних є приватними даними користувачів (особисті фотографії, відео та аудіозаписи). Водночас, спостерігається тенденція збільшення кількості користувачів у соціальних мережах та месенджерах, в результаті чого переважна більшість користувачів мережі Інтернет має певну долю власних персональних даних на серверах різноманітних компаній. Ця персональна інформація є конфіденційною і не має розповсюджуватися без згоди власника. Проте, відомі випадки використання персональних мультимедійних даних, опублікованих у приватних бесідах соціальних мереж та месенджерах, з метою таргетування рекламних оголошень. Отже, зберігаючи дані поза локальним комп’ютером, користувач втрачає повний контроль за доступом до цих даних. Проблема передачі конфіденційних мультимедійних даних існує і у телемедицині, де передбачене використання комп’ютерних та телекомунікаційних технологій для обміну медичною інформацією у вигляді зображень та відео (наприклад, рентгенівські знімки, відеозаписи ендоскопічного обстеження тощо). При передачі конфіденційних даних пацієнта через мережу Інтернет існує ймовірність витоку інформації, а передача медичних даних у відкритому вигляді є неприпустимою з правової точки зору.

Для захисту конфіденційних даних користувачів мережі Інтернет можуть використовуватись різноманітні методи, включаючи методи стеганографічного захисту. Перевагою стеганографічного захисту є те, що він дозволяє приховати сам факт існування конфіденційної інформації, що дозволяє використовувати стеганографічні методи для забезпечення конфіденційності у звичайних месенджерах, соціальних мережах, тощо. Для підвищення рівня захисту мультимедійних даних доцільно використовувати крипто-стеганографічні методи, які передбачають попереднє шифрування даних перед їх стеганографічним вбудовуванням.

Під час реалізації методів захисту мультимедійних даних у вигляді програмного продукту необхідно враховувати не лише рівень захисту даних, а також інші вимоги, виконання яких є важливим для зручної роботи користувача. Основною з цих вимог є висока швидкість оброблення користувацьких даних. Аналіз існуючого програмного забезпечення свідчить про те, що на сьогодні спостерігається потреба у розроблені нових програмних продуктів, які дозволятимуть користувачам мережі Інтернет забезпечувати конфіденційність своїх мультимедійних даних. При цьому необхідно забезпечити зручність та простоту розроблення таких програмних продуктів для різних галузей застосування та різних груп користувачів. З урахуванням цих особливостей та потреб постає актуальна **науково-практична проблемна задача** розроблення універсальної архітектури програмної системи захисту мультимедійних даних, а також програмних компонентів, що реалізують нові крипто-стеганографічні методи захисту мультимедійних даних користувачів.

Метою дисертаційної роботи є підвищення ефективності програмних засобів крипто-стеганографічного захисту мультимедійних даних користувачів мережі Інтернет за рахунок вдосконалення архітектури програмної системи захисту та розроблення нових алгоритмічно-програмних методів крипто-стеганографічного захисту мультимедійних даних, що забезпечують надійність

захисту та підвищення швидкодії процедур оброблення мультимедійних даних користувача.

У першому розділі дисертаційної роботи здійснено комплексний аналіз методів та програмних засобів стеганографічного захисту персональних мультимедійних даних у мережі Інтернет. Проведений аналіз показав необхідність розроблення нових програмних рішень для захисту мультимедійних даних користувачів мережі Інтернет та дозволив сформулювати вимоги до програмного забезпечення процесів захисту мультимедійних даних.

У другому розділі запропоновано алгоритмічне забезпечення крипто-стеганографічного захисту мультимедійних даних, а саме, розроблено три методи крипто-стеганографічного захисту: метод на основі схеми відповідності бітів, метод на основі дерева Хаффмана та метод на основі псевдовипадкового вбудовування.

У третьому розділі розроблено універсальну архітектуру програмної системи крипто-стеганографічного захисту мультимедійних даних; запропоновану архітектуру реалізовано у вигляді програмного забезпечення з використанням методу на основі схеми відповідності бітів, методу на основі дерева Хаффмана та методу на основі псевдовипадкового вбудовування.

У четвертому розділі досліджено запропоновану архітектуру, зокрема, здійснено порівняльний аналіз розроблених алгоритмічно-програмних методів крипто-стеганографічного захисту мультимедійних даних за часом виконання, стеганографічною стійкістю та стійкістю до статистичних атак.

У дисертаційній роботі отримано ряд **нових наукових результатів**, зокрема, **уперше** запропоновано універсальну архітектуру програмної системи захисту мультимедійних даних користувачів мережі Інтернет, використання якої дозволяє спростити процес розроблення програмного забезпечення систем захисту мультимедійних даних та яка, на відміну від існуючих, забезпечує

можливість використання довільних методів крипто-стеганографічного захисту даних і отримання мультимедійних даних з різних програмних середовищ.

Уперше запропоновано алгоритмічно-програмний метод крипто-стеганографічного захисту мультимедійних даних, характерною рисою якого є можливість поєднання з іншими методами LSB-стеганографії для підвищення їх стеганографічної стійкості та який, на відміну від відомих, ґрунтується на застосуванні процедури шифрування на основі схеми відповідності бітів і логічної функції, що дозволяє забезпечити захист мультимедійних даних та підвищити швидкодію процедури вбудовування стегоданих у понад 5 разів.

Уперше розроблено алгоритмічно-програмний метод крипто-стеганографічного захисту мультимедійних даних, який, на відміну від відомих, ґрунтується на використанні процедури побудови дерева Хаффмана на основі зображення-ключа, що дозволяє підвищити рівень захисту конфіденційних графічних даних від підбору ключів та статистичних стегоатак у середньому у 17,4 разів.

Уперше розроблено алгоритмічно-програмний метод крипто-стеганографічного захисту мультимедійних даних, визначальною рисою якого є застосування процедури псевдовипадкового вбудовування даних із застосуванням двох генераторів псевдовипадкових чисел, та який характеризується високою стійкістю до підбору ключів за рахунок зростання ентропійних характеристик та змінної кількості ключів, що дозволяє забезпечити захист мультимедійних даних.

За матеріалами дисертації опубліковано 6 наукових праць, зокрема, 3 наукових статті, з яких 2 статті опубліковано у закордонних фахових виданнях третього квартиля (Q3), які реферуються базою Scopus, та 1 стаття опублікована у науковому виданні, що входить до наукових фахових видань України, і 3 публікації у матеріалах науково-технічних конференцій.

Ключові слова: прикладне програмне забезпечення, програмна система, архітектура програмного забезпечення, захист мультимедійних даних, крипто-стеганографічні методи.

SUMMARY

Radchenko Y. Algorithmic support and software of Internet user's multimedia data protection systems. − Qualifying scientific work, the manuscript.

PhD thesis in the field of knowledge 12 Information technologies in a specialty 121 Software engineering. – National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, 2020.

Multimedia data make up a significant proportion of data transmitted over the Internet and stored in various cloud storage. Some of this multimedia data is private user data (personal photos, videos and audio recordings). At the same time, there is a tendency to increase the number of users in social networks and messengers, as a result the vast majority of Internet users have some of their own personal data on the servers of various companies. This personal information is confidential and should not be disclosed without the consent of the owner. However, there are known cases of using personal multimedia data published in private conversations in social networks and messengers to target advertisements. Therefore, by storing data outside the local computer, the user loses complete control over access to this data. The problem of confidential multimedia data transmission also exists in telemedicine, where computer and telecommunication technologies are used to exchange medical information in the form of images and videos (for example, X-rays, endoscopic videos, etc.). When transmitting confidential patient data over the Internet, there is a possibility of information leakage, but the transfer of medical data in the open is legally unacceptable.

A variety of methods can be used to protect the confidential data of Internet users, including steganographic protection methods. The advantage of steganographic

protection is that it allows to hide the fact of the existence of confidential information, which allows to use steganographic methods to ensure confidentiality in regular messengers, social networks, and so on. To increase the level of multimedia data protection, it is advisable to use crypto-steganographic methods, which provide data pre-encryption before steganographic embedding.

When implementing methods of multimedia data protecting in the form of a software product, it is necessary to take into account not only the level of data protection, but also other requirements, the fulfillment of which is important for the user's convenience. The main of these requirements is the high speed of user data processing. Analysis of existing software shows that today there is a need to develop new software products that will allow Internet users to ensure the confidentiality of their multimedia data. It is necessary to ensure the convenience and simplicity of developing such software products for different applications and different user groups. Taking into account these features and needs, there is an urgent **scientific and practical problem** of developing an universal architecture of the software system for multimedia data protection, as well as software components that implement new crypto-steganographic methods for user`s multimedia data protection.

The purpose of the dissertation is to increase the efficiency of software for Internet users multimedia data crypto-steganographic protection by improving the architecture of the software protection system and developing new algorithmic and software methods for multimedia data crypto-steganographic protection.

In the first section of the dissertation a comprehensive analysis of methods and software for steganographic protection of personal multimedia data on the Internet is given. The analysis showed the need to develop new software solutions for the Internet users multimedia data protection and allowed to formulate software requirements for multimedia data protection processes.

The second section proposes algorithmic support for multimedia data crypto-steganographic protection, namely, developed three methods of crypto-steganographic protection: a method based on the bit correspondence scheme, a method based on the Huffman tree and a method based on pseudo-random embedding.

In the third section the universal architecture of the software system for multimedia data crypto-steganographic protection was developed; the proposed architecture is implemented in the form of software using a method based on the bit correspondence scheme, a method based on the Huffman tree and a method based on pseudo-random embedding.

The fourth section examines the proposed architecture, in particular, a comparative analysis of the developed algorithmic and software methods of multimedia data crypto-steganographic protection by embedding time, steganographic stability and resistance to statistical attacks.

The dissertation provides a number of new scientific results, in particular, the universal architecture of the software system for Internet user's multimedia data protection, which simplifies the process of software development of multimedia data protection systems and provides the ability to use arbitrary methods of crypto-steganographic data protection and provide multimedia data from different software environments, has been **proposed for the first time**.

An algorithmic software method of multimedia data crypto-steganographic protection, the characteristic feature of which is the possibility of combining with other methods of LSB-steganography to increase their steganographic stability and which, unlike the known ones, relies on the encryption procedure based on bit correspondence scheme and logic function that allows to protect multimedia data and increase the speed of embedding procedure in more than 5 times, has been **developed for the first time**.

An algorithmic software method of crypto-steganographic multimedia data protection which, unlike the known ones, is based on the use of the Huffman tree

procedure based on the key-image, which allows to increase the level of protection of confidential graphic data agains the key search in 17.4 times, has been **developed for the first time**.

An algorithmic software method of multimedia data crypto-steganographic protection, the defining feature of which is the application of pseudo-random data embedding procedure using two pseudo-random number generators, and which is characterized by high resistance to the key search due to increasing entropy characteristics and variable number of keys that enables multimedia data protection, has been **developed for the first time**.

Based on the dissertation, 6 scientific works **were published**, in particular, 3 scientific articles, 2 articles of which were published in foreign professional publications of the third quartile (Q3), which are referenced by Scopus, and 1 article was published in a scientific publication included in scientific professional publications of Ukraine, and 3 publications were published in the materials of scientific and technical conferences.

Keywords: application software, software system, software architecture, multimedia data protection, crypto-steganographic methods.

Список публікацій здобувача / List of publications of the applicant:

- статті в закордонних фахових виданнях третього квартиля (Q3), які реферуються базою Scopus / articles in foreign professional journals of the third quartile (Q3) which are referenced by the Scopus (2):

1. Radchenko Ye., Dychka I., Sulema Ye., Suschuk-Sliusarenko V., Shkurat O. Steganographic Protection Method Based on Huffman Tree. Advances in Intelligent Systems and Computing. Springer Verlag, Germany, 2019. Vol. 902, P. 283–292. ISSN : 21945357.

2. Hu Zh., Dychka I., Sulema Ye., Radchenko Ye. Graphical Data Steganographic Protection Method Based on Bits Correspondence Scheme. International Journal of Intelligent Systems and Applications (IJISA). China, 2017. Vol. 9. No. 8, P. 34–40. ISSN : 20749058.

- стаття в науковому фаховому журналі України / article in Ukrainian professional journal (1):

3. Сулема Є.С., Радченко Є.О. Метод стеганографічного захисту мультимедійних даних на основі процедури псевдовипадкового вбудовування. Наукові вісті КПІ, 2020. № 1, С. 40–47.

- матеріали науково-технічних конференцій / materials of the scientific conferences (3):

4. Радченко Є.О., Сулема Є.С. Спосіб стеганографічного захисту графічних даних на основі схеми відповідності бітів та аналізу візуальних властивостей контейнера. Матеріали доповідей Шостої Міжнародної науково-практичної конференції з сучасних проблем кодування, захисту й ущільнення інформації. Вінниця, Україна, 2017. С. 51–53.

5. Радченко Є. О., Сулема Є. С. Метод стеганографічного захисту WAV-файлів. Збірник тез доповідей 12-ї наукової конференції магістрантів та аспірантів «Прикладна математика та комп'ютинг» (ПМК-2019). НТУУ «КПІ». 2019. С. 99–104.

6. Sulema Ye. S., Radchenko Ye. O. Algorithm of graphical data stegonagraphic protection based on bits difference transform. Збірник тез доповідей 8-ї наукової конференції магістрантів та аспірантів «Прикладна математика та комп'ютинг» (ПМК-2016). НТУУ «КПІ». 2016. С. 254–258.