

КРИПТОГРАФІЧНА СИСТЕМА З ВИКОРИСТАННЯМ АВТОЕНКОДЕРУ ТА СИМЕТРИЧНОГО ШИФРУВАННЯ ДЛЯ ЗАДАЧІ ШИФРУВАННЯ МЕДИЧНИХ ЗОБРАЖЕНЬ

Прохоров П.А., Добровольський Ю.Г.

***Чернівецький Національний Університет
імені Юрія Федьковича, м. Чернівці***

Згідно низки нормативних актів та законів України будь-яка медична інформація охороняється законом, а отже медичні заклади потребують використання систем що забезпечують високий рівень захисту такої інформації.

Основним недоліком використання класичних примітивів симетричного та асиметричного шифрувань при роботі з медичними зображеннями є те, що вони проектувались для захисту текстової інформації, невизначеність змісту та об'єму якої є джерелом випадковості для таких примітивів та ускладнює перехоплювачу її дешифрування. Проте, медичні зображення одного класу (наприклад рентгенівські знімки певної кінцівки) будуть мати певні повторювані та/або схожі геометричні патерни, що характеризують певну патологію або її відсутність [1]. Таким чином виникає потреба у додатковій обробці таких зображень для підвищення криптостійкості шифрованих зображень.

Одним з вирішень цього питання є використання нейронних мереж типу Автоенкодер [2]. Таким чином, якщо додати кодування зображення частиною мережі Енкодер перед шифруванням та декодувати частиною Декодер після дешифрування то ми отримуємо додатковий рівень криптостійкості через те що до алгоритму шифрування зображення поступає вже у закодованому вигляді. Схему роботи такої криптосистеми можна побачити на рисунку 1.



Рисунок 1 – Криптосистема з Автоенкодером та симетричним шифруванням

Література:

1. Alsman Y. et al. Hybrid Encryption Scheme for Medical Imaging using AutoEncoder and Advance Encryption Standard: *Electronics*. 2022. 11(23), 3967. DOI: <https://doi.org/10.3390/electronics11233967>
2. Chen Y., Tang C., Te R. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion: *Signal Processing*. 2020. Volume 167, Issue C. DOI: <https://doi.org/10.1016/j.sigpro.2019.107286>