МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

Вінницький національний медичний університет ім. М.І. Пирогова

кафедра біологічної фізики, медичної апаратури та інформатики

МАТЕРІЛИ ІІІ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

«МЕДИКО-ТЕХНІЧНА СПІВПРАЦЯ ЗАРАДИ ПЕРЕМОГИ: АКТУАЛЬНІ ЗАВДАННЯ МЕДИЧНОЇ, БІОЛОГІЧНОЇ ФІЗИКИ ТА ІНФОРМАТИКИ»

5-6 квітня 2024 року

м.Вінниця

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ

Вінницький національний медичний університет
ім. М.І. Пирогова

МАТЕРІАЛИ ІІІ ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

«МЕДИКО-ТЕХНІЧНА СПІВПРАЦЯ ЗАРАДИ ПЕРЕМОГИ: АКТУАЛЬНІ ЗАВДАННЯ МЕДИЧНОЇ, БІОЛОГІЧНОЇ ФІЗИКИ ТА ІНФОРМАТИКИ»

5-6 квітня 2024 року

м. Вінниця

УДК 577.35+004
ISBN 978-617-7417-21-6 (електронне видання)

Медико-технічна співпраця заради перемоги: Актуальні завдання медичної, біологічної фізики та інформатики. Матеріали доповідей та виступів III всеукраїнської науково-практичної конференції з міжнародною участю 5-6 квітня 2024 року Вінниця. – Вінниця: Едельвейс. – 230 с.

УДК 577.35+004
ISBN 978-617-7417-21-6 (електронне видання)

Збірник містить матеріали доповідей та виступів учасників III всеукраїнської науково-практичної конференції з міжнародною участю «Медико-технічна співпраця заради перемоги: Актуальні завдання медичної, біологічної фізики та інформатики» яка зареєстрована на сайті Наукові заходи для ЗВО – Інститут модернізації змісту освіти (imzo.gov.ua) в розділі наукові заходи для ЗВО, перелік проведення наукових конференцій з проблем вищої освіти і науки в системі Міністерства освіти і науки України на 2024 рік ПЕРЕЛІК - Зміни 2024 (1).pdf - Google Диск за номером 921. Конференція відбулась в Вінницькому національному медичному університеті ім. М.І. Пирогова 5-6 квітня 2024 року. У поданих матеріалах висвітлюється широке коло актуальних проблем розвитку теоретичних та практичних аспектів, пов'язаних з використанням технічних засобів та інформаційних технологій в галузях медицини та біології.. Збірник призначено для науковців, викладачів закладів вищої освіти, аспірантів, магістрів, здобувачів, і студентів.

Матеріали подані в авторській редакції. Автори опублікованих матеріалів несуть повну відповідальність за підбір, точність наведених фактів, цитат, даних, власних імен, посилань, грамотність, літературний стиль та інші відомості. Редколегія залишає за собою право скорочувати та редагувати подані матеріали. Рукописи не повертаються. Організатори конференції та члени редколегії не завжди поділяють думки учасників (авторів).

Рекомендовано до друку Вченою радою Вінницького національного медичного університету ім. М.І. Пирогова (протокол № 10 від 31.05.2024 р.)

ОРГАНІЗАТОРИ КОНФЕРЕНЦІЇ

Вінницький національний медичний університет ім. М.І. Пирогова

Вінницький національний технічний університет

Національний медичний університет ім. О.О.Богомольця

Донецький національний університет ім. Василя Стуса

ОРГАНІЗАЦІЙНИЙ КОМІТЕТ КОНФЕРЕНЦІЇ

Голова: Олег Власенко, проректор з наукової роботи ЗВО «ВНМУ ім. М.І. Пирогова», д.м.н., професор

Члени: Анатолій КУЛИК, Сергій ПАВЛОВ, Вальдемар ВУЙЦІК, Andrzej Jerzy SMOLARZ, Orken MAMYRBAYEV, Валентина ВАСИЛЕНКО, Роман КВЄТНИЙ, Олександр ЧАЛИЙ, Ольга ДОЦЕНКО, Юрій ТРІУС, Володимир ЛУЖЕЦЬКИЙ, Ірина ЖУРАВСЬКА, Олег АВРУНІН, Наталія ТИТОВА, Юрій ДОБРОВОЛЬСЬКИЙ, Олександр НІКОЛЬСЬКИЙ.

Метою конференції є висвітлення здобутків вчених України при розроблюванні, використанні і впровадженні технічних засобів та інформаційних технологій в галузях медицини та біології.

Напрями роботи конференції

- Актуальні проблеми біологічної фізики.
- Медична інженерія. Телемедицина.
- Моделювання та комп'ютерна діагностика.
- Захист інформації в медичних інформаційних системах.
- Математичні аспекти в задачах біології та медицини.
- Специфічні питання педагогіки для студентів медичного та біологічного профілю.
- Метрологічне забезпечення медико-біологічного обладнання.
- Отримання, оброблення та аналіз медичних і біологічних зображень і сигналів.

ШИФРУВАННЯ МЕДИЧНИХ ЗОБРАЖЕНЬ

Олександр РОМАНЮК[1] ,Володимир МАЙДАНЮК[1], Сергій ПАВЛОВ[1], Наталія ТІТОВА[2], Сергій РОМАНЮК[2]
[1]Вінницький національний технічний університет
[2]Національний університет «Одеська політехніка»
rom8591@gmail.com

Шифрування медичних зображень – це важливий напрямок захисту конфіденційності пацієнтів і забезпечення безпеки медичних даних. Оскільки медичні зображення, такі як рентген, МРТ, УЗД та інші, містять чутливу інформацію про здоров'я особи, їх необхідно захищати від несанкціонованого доступу, змінення або розголошення.

Медичні зображення можуть бути різних типів, зокрема:

- Рентгенівські знімки використовуються для візуалізації кісток і певних органів.
- Комп’ютерна томографія (КТ) дає детальні зображення внутрішніх органів.
- Магнітно-резонансна томографія (МРТ) використовує магнітні поля для створення детальних зображень м'яких тканин.
- Ультразвукове дослідження (УЗД) використовує звукові хвилі для візуалізації органів і плода під час вагітності.
- Позитронно-емісійна томографія (ПЕТ) використовується для виявлення метаболічних змін в тканинах.

Медичні зображення використовуються для: діагностики захворювань; планування лікування; відстеження прогресу лікування; медичних досліджень.

Існують різні методи шифрування медичних зображень, які забезпечують цю захищеність [1]:

Симетричне шифрування використовує один і той же ключ для шифрування та дешифрування даних. Цей метод швидкий, але вимагає безпечного обміну ключем між відправником і отримувачем.

Асиметричне шифрування використовує пару ключів – відкритий та приватний. Відкритий ключ може бути відомий широкому колу осіб для шифрування даних**,** але дешифрувати інформацію може лише власник приватного ключа. Цей метод безпечніший для обміну даними через ненадійні мережі, але він повільніший порівняно з симетричним шифруванням.

Гібридне шифрування Комбінує симетричне та асиметричне шифрування, використовуючи сильні сторони обох методів. Зазвичай, симетричний ключ шифрується за допомогою асиметричного шифрування, щоб безпечно передати його між відправником і отримувачем.

Хешування може використовуватись для верифікації цілісності зображень, переконуючись, що вони не були змінені під час передачі.

Фрактальне шифрування медичних зображень є одним із передових методів криптографії, який використовує математичні властивості фракталів для забезпечення безпеки даних. Фрактали — це складні геометричні фігури, які відзначаються самоподібністю на різних масштабних рівнях, і ця властивість може бути використана для створення дуже складних систем шифрування.

Фрактальне шифрування базується на ідеї, що фрактали можуть відтворювати зображення з високим ступенем деталізації, використовуючи відносно прості математичні моделі. Фрактали – це об'єкти або структури, що володіють властивістю самоподібності, тобто вони виглядають майже однаково на будь-якому рівні збільшення. Під час шифрування медичного зображення, алгоритм фрактального шифрування перетворює дані зображення на фрактальний код, який є складним для розшифрування без знання ключа [2].

Фрактальне шифрування базується на ітераційних алгоритмах і використовує самоподібність фракталів для трансформації зображення. Воно включає такі етапи:

1. Розбиття зображення на частини: Медичне зображення розділяється на менші фрагменти або блоки.
2. Пошук самоподібних ділянок: Для кожного фрагмента знаходяться області в зображенні, які можна апроксимувати за допомогою фрактальних трансформацій.
3. Застосування фрактального кодування: Кожен фрагмент зображення кодується за допомогою фрактальних трансформацій, що дозволяє отримати набір параметрів (фрактальний код) для кожного блоку [3,4].
4. Шифрування фрактальних кодів: Отримані фрактальні коди можуть бути додатково зашифровані за допомогою традиційних методів шифрування для підвищення рівня безпеки.

Ключ шифрування у цьому випадку генерується на основі параметрів фрактальних перетворень, які визначають, як зображення буде змінено. Цей метод може включати масштабування, поворот та інші трансформації, які застосовуються до різних частин зображення згідно з фрактальними правилами.

Завдяки складності фрактальних структур, система шифрування може виявитися дуже стійкою до спроб дешифрування без наявності ключа.

Фрактальне шифрування може бути ефективним для великих зображень, оскільки фрактальні правила можуть застосовуватися локально, не вимагаючи обробки всього зображення цілком. Деякі методи фрактального шифрування можуть одночасно зі шифруванням стискати зображення, зменшуючи вимоги до простору для зберігання. Генерація фрактальних ключів і процес шифрування/дешифрування можуть бути обчислювально вимогливими, особливо для великих зображень.

Для використання фрактального шифрування необхідні спеціалізовані алгоритми та програмне забезпечення. Оскільки фрактальне шифрування є досить новим і нішевим напрямком, відсутні універсальні стандарти для його застосування.

Для шифрування медичних зображень використовуються різні програми та платформи, деякі з яких спеціалізуються саме на медичних даних, тоді як інші є більш універсальними рішеннями для шифрування. Ось декілька прикладів програм, які можуть бути використані в цій сфері:

DICOM (Digital Imaging and Communications in Medicine) - міжнародний стандарт для зберігання, обміну та передачі медичних зображень. DICOM включає механізми безпеки для шифрування та захисту медичних зображень [5].

GnuPG (GNU Privacy Guard) - безкоштовний інструмент відкритого коду, який дозволяє шифрувати дані та створювати цифрові підписи. GnuPG підтримує асиметричне шифрування, що робить його придатним для безпечного обміну даними, включаючи медичні зображення[6].

TrueCrypt/VeraCrypt - програмне забезпечення для шифрування на рівні диску, яке може захищати медичні зображення збережені на локальних дисках, зовнішніх накопичувачах або USB-пристроях. VeraCrypt є форком (розгалуженням) TrueCrypt і пропонує покращену безпеку[7].

Microsoft BitLocker - Вбудований інструмент шифрування в деяких версіях Windows, який забезпечує шифрування всього диску. BitLocker може захистити дані на жорстких дисках, включаючи медичні зображення, від несанкціонованого доступу[8].

OpenSSL - Потужний інструментарій відкритого коду для роботи з криптографічними протоколами SSL і TLS. OpenSSL може використовуватися для шифрування даних перед їхньою передачею через мережу, включаючи шифрування медичних зображень [9].

FileVault - Вбудована система шифрування в MacOS, яка забезпечує шифрування всього диску. FileVault захищає інформацію на комп'ютерах Mac, включаючи медичні зображення [10].

Ці та інші інструменти допомагають забезпечити конфіденційність і безпеку медичних зображень та інших чутливих даних пацієнтів. Важливо вибрати таке рішення, яке відповідає специфічним потребам і вимогам в сфері охорони здоров'я, а також дотримується відповідних нормативних і законодавчих вимог.

Інновації та нововведення в сфері шифрування медичних зображень відображають постійне прагнення забезпечити кращий захист конфіденційності пацієнтів та ефективність управління даними в охороні здоров'я. Ось кілька напрямків, де спостерігаються інновації.

Квантове шифрування використовує принципи квантової механіки для створення майже непорушного шифру. Воно забезпечує високий рівень безпеки за рахунок квантового розподілу ключів, який дозволяє двом сторонам обмінюватися шифрувальними ключами таким чином, що будь-яка спроба перехоплення ключа змінює його стан, роблячи перехоплення очевидним [11].

Блокчейн-технології пропонують новий підхід до безпечного зберігання та обміну медичними зображеннями. Завдяки децентралізованій природі блокчейну, дані можуть бути захищені від несанкціонованого доступу, модифікації та видалення. Шифрування даних перед їх записом у блокчейн додатково збільшує рівень безпеки [12].

Гомоморфне шифрування дозволяє проводити обчислення над зашифрованими даними без необхідності їх дешифрування. Це означає, що медичні зображення можуть бути аналізовані та оброблені у зашифрованому вигляді, забезпечуючи неперервний захист даних. Це особливо важливо для захисту конфіденційності при дистанційному діагностуванні або колаборативних дослідженнях [13].

Штучний інтелект (ШІ) може бути застосований для розробки більш ефективних та безпечних методів шифрування медичних зображень. ШІ може аналізувати великі обсяги даних для ідентифікації потенційних загроз безпеці та автоматично адаптувати шифрувальні механізми для посилення захисту. Крім того, ШІ може оптимізувати процеси шифрування та дешифрування для покращення швидкості та ефективності [14].

Розподільне шифрування та децентралізоване зберігання забезпечують новий рівень захисту для медичних зображень, розподіляючи зашифровані дані між кількома серверами або вузлами. Це знижує ризик втрати даних або несанкціонованого доступу, оскільки атакувати потрібно одночасно кілька вузлів для доступу до повної інформації. Крім того, цей метод може підвищити доступність даних, оскільки інформація зберігається в декількох місцях.

Технології розпізнавання візерунків і машинного зору можуть бути інтегровані з системами шифрування для автоматизованого визначення та шифрування конфіденційних частин медичних зображень, таких як особисті ідентифікатори пацієнтів або особливо чутливі медичні дані. Це дозволяє захищати важливу інформацію без необхідності шифрування всього зображення, що може спростити подальшу обробку та аналіз [15].

Хоча технологія розширеної реальності (AR) не є прямо пов'язаною з шифруванням, вона може використовуватися для створення додаткового шару безпеки при перегляді медичних зображень. Наприклад, AR може відображати конфіденційну інформацію на медичних зображеннях лише при певних умовах або використовувати біометричні дані для автентифікації користувачів перед наданням доступу до чутливих даних [16].

Штучний інтелект може використовуватися не лише для оптимізації процесів шифрування, але й для створення адаптивних систем шифрування, які здатні самостійно виявляти та реагувати на змінні загрози безпеці. Системи можуть навчатися з часом, ідентифікуючи нові вектори атак та автоматично адаптуючи методи шифрування для забезпечення найкращого захисту даних.

Біометричне шифрування використовує унікальні біометричні дані, такі як відбитки пальців, риси обличчя або райдужку ока, для генерації криптографічних ключів. Це забезпечує високий рівень особистої ідентифікації та безпеки, роблячи шифрування медичних зображень

значно більш індивідуалізованим і безпечним. Однак, це також ставить під сумнів питання конфіденційності та управління біометричними даними [17, 18].

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Майданюк, В. П. Основи теорії інформації та кодування : [Електронний ресурс] / Майданюк В. П., Романюк О. Н., Тужанський С. Є. – Вінниця : ВНТУ, 2022. – 133 с.
2. Свинчук О.В., Барабаш О.В., Олімпієва Ю.І., Ільїн О.Ю. Застосування фрактальних функцій для шифрування даних в системах захисту інформації / ISSN 2412-4338 Телекомунікаційні та інформаційні технології. 2020 № 1(66). – С. 15-24.
3. Maydaniuk V. P., Arseniuk I. R., Lishchuk O. O. Increasing the Speed of Fractal Image Compression Using Two-Dimensional Approximating Transformations / Journal of engineering sciences Журнал інженерних наук Web site: http://jes.sumdu.edu.ua DOI: 10.21272/jes.2019.6(1).e3 Volume 6, Issue 1 (2019). URL:https://essuir.sumdu.edu.ua/bitstream-download/123456789/71732/1/Maydaniuk_JES_2019.pdf;jsessionid=556835563BA701D321655D28CDDD5510/.
4. Майданюк В. П. Аспекти оптимізації швидкості фрактального ущільнення зображень / В. П. Майданюк, О. О. Ліщук, Д. С. Король // Оптико-електронні інформаційно-енергетичні технології. - 2017. - № 1. - С. 24-32.
5. DICOM. URL: https://uk.wikipedia.org/wiki/DICOM.
6. GNU Privacy Guard. URL:https://uk.wikipedia.org/wiki/GNU_Privacy_Guard.
7. VeraCrypt. URL: https://uk.wikipedia.org/wiki/VeraCrypt.
8. BitLocker. URL: https://uk.wikipedia.org/wiki/BitLocker.
9. OpenSSL. URL: https://www.openssl.org.
10. FileVault. URL: https://uk.wikipedia.org/wiki/FileVault.
11. Квантова криптографія. URL: https://uk.wikipedia.org/wiki/Квантова_криптографія.
12. Блокчейн у медицині. URL: https://blog.whitebit.com/uk/blockchain-in-medicine/.
13. Гомоморфне шифрування. URL: https://uk.wikipedia.org/wiki/Гомоморфне_шифрування.
14. Криптографія, блокчейн, ШІ: як технології захищають ваші кошти у банку. URL:https://proit.org.ua/kriptoghrafiia-blokchiein-shi-iak-tiekhnologhiyi-zakhishchaiut-vashi-koshti-u-banku/.
15. Штучний інтелект і машинний зір: можливості технологій. URL: https://aiconference.com.ua/uk/news/iskusstvenniy-intellekt-i-mashinnoe-zrenie-vozmognosti-tehnologiy-97504.
16. Імерсивні технології. URL:https://uk.wikipedia.org/wiki/Імерсивні_технології.
17. Луценко М. С., Кузнецов О. О., Прокопович-Ткаченко Д. І., Звєрєв В. П., Уварова А. О. Порівняльний аналіз біометричних криптосистем / Прикладна радіоэлектронска, 2018, Том 17, № 3, 4. С. 182-191.
18. Писаренко Т.В. Аналіз світових технологічних трендів у військовій сфері: монографія [Електронний ресурс]/Т. Писаренко, Т. Кваша, Т. Гаврис та ін.,за заг. редакцією Т. В. Писаренко. – К.: УкрІНТЕІ, 2021.- 110с. URL:https://mon.gov.ua/storage/app/media/innovatsii-transfer-tehnologiy/2021/09/30/Analiz.svit.tekhn.trend.viysk.sferi-2021.30.09.pdf.