УДК 004.9 **doi: 10.26906/SUNZ.2025.2.203-209**

А. С. Шандиба, В. І. Сітніков, О. С. Ніколаєв, Д. О.Кібірєв

Харківський національний університет радіоелектроніки, Харків, Україна

НАНЕСЕННЯ ЦИФРОВИХ ВОДЯНИХ ЗНАКІВ З ВИКОРИСТАННЯМ ХАОТИЧНИХ КАРТ

Анотація. У сучасному цифровому середовищі питання охорони авторських прав та безпеки інформації стають надзвичайно важливими. Одним з дієвих способів захисту мультимедійного контенту є технологія цифрових водяних знаків, яка дає змогу ідентифікувати та відстежувати незаконне використання цифрових файлів. Водночас, традиційні способи нанесення водяних знаків мають певні недоліки, що стимулює пошук нових рішень. Метою дослідження є створення способу впровадження цифрових водяних знаків з використанням хаотичних карт, задля збільшення захищеності знаків від впливів і змін. Предметом дослідження є методи та технології цифрового водяного маркування (стеганографії), що використовують хаотичні карти для підвищення надійності, захищеності та непомітності вбудовуваної інформації в цифрові об'єкти. Об'єктом дослідження виступають цифрові зображення (або мультимедійні об'єкти), на які наноситься водяний знак із застосуванням алгоритмів на основі хаотичних карт, що забезпечує захист авторських прав, аутентифікацію та цілісність інформації. Для досягнення поставленої мети було розглянуто наступні завдання: проаналізовано ключові методи нанесення цифрових водяних знаків, розглянуто характеристики хаотичних карт та потенціал їх застосування при створенні водяних знаків, розглянуто алгоритм для вбудовування цифрових водяних знаків, використовуючи хаотичні карти. У цій роботі розглянуто теоретичні засади цифрових водяних знаків, проведено аналіз існуючих методів їх нанесення, а також детально вивчено можливість застосування хаотичних карт у цій сфері. Запропоновано методику використання хаотичних карт для генерування ключів і вбудовування водяних знаків. Проаналізовано сильні та слабкі сторони цього підходу, а також окреслено перспективи майбутніх досліджень у цій галузі.

Ключові слова: хаотичні карти, алгоритм, кіберзагрози, зображення, стеганографія, захист, водяні знаки.

Вступ

Цифрові водяні знаки (ЦВЗ) — це приховані дані, які впроваджуються в цифрові медіа (зображення, відео, аудіо, тексти) для ідентифікації власника та запобігання несанкціонованому копіюванню чи редагуванню. Вони зазвичай невидимі або малопомітні для звичайного користувача, але можуть бути виявлені спеціалізованими засобами. Основна функція ЦВЗ – захист авторських прав та забезпечення безпеки інформації в цифровому просторі.

З розвитком інформаційних технологій та збільшенням обсягів цифрового контенту, постає потреба в нових способах захисту. Звичайні методи захисту, як-от паролі чи шифрування, можуть бути легко зламані або обійдені. Натомість, цифрові водяні знаки є більш надійним методом, оскільки вони не лише захищають вміст, але й дозволяють відстежувати його походження, підтверджувати автентичність, а також виявляти джерела несанкціонованого розповсюдження.

Сучасний цифровий світ вимагає ефективних інструментів захисту авторських прав і боротьби з піратством. З ростом популярності інтернет-платформ і можливостей швидкого розповсюдження цифрового контенту виникає серйозна загроза незаконного використання та копіювання файлів. Нанесення цифрових водяних знаків — один із найефективніших методів забезпечення захисту файлів від таких загроз. Водночас, це дозволяє зберігати цілісність та автентичність даних, адже водяний знак може бути невід'ємною частиною файлу, яку неможливо безпечно видалити або змінити без виявлення.

Хаотичні карти — це математичні структури, що базуються на принципах хаотичної динаміки, які використовуються в криптографії для генерування складних, непередбачуваних послідовностей, які можна використовувати для захисту даних. Хаос, як явище, характеризується високою чутливістю до початкових умов, що дозволяє створювати складні та стійкі до атак системи. У криптографії хаотичні карти застосовуються для створення випадкових чисел, генерування ключів та інших задач, де потрібна висока ступінь непередбачуваності.

Властивості хаотичних карт, як-от детермінованість, чутливість до умов і здатність генерувати складні структури, роблять їх ідеальними для використання в сучасних системах безпеки. Ці карти можуть служити основою для створення водяних знаків, оскільки дозволяють вбудовувати захищені дані таким чином, що їх неможливо легко виявити чи видалити без порушення цілісності файлу.

Використання хаотичних карт для нанесення цифрових водяних знаків відкриває нові можливості для підвищення стійкості та надійності захисту. Завдяки їхнім властивостям можна створювати водяні знаки, які є надзвичайно стійкими до атак і важко виявляються чи змінюються без пошкодження самого файлу. Хаотичні карти можуть бути використані для генерації ключів, які застосовуються для вбудовування водяних знаків у цифрові файли.

Завдяки таким властивостям, як висока непередбачуваність та складність, хаотичні карти можуть забезпечити додатковий рівень безпеки, захищаючи водяні знаки від атак, спрямованих на їхнє виявлення або видалення. Цей підхід дозволяє значно підвищити ефективність захисту авторських прав та безпеки цифрових файлів, особливо в умовах постійного розвитку технологій кіберзагроз.

Аналіз наукових робіт засвідчує наявність численних методів накладання цифрових водяних знаків, включаючи стеганографічні та криптографічні

стратегії. Розвідки свідчать про високий ступінь захисту цифрових водяних знаків при використанні хаотичних систем.

Різні моделі хаотичних карт демонструють ефективність у формуванні унікальних ключів для вбудовування водяних знаків. Зокрема, дослідження Cox I. J. [6] і Kalker та Haitsma [11] висвітлюють, що цифрові водяні знаки, побудовані на хаотичних картах, мають посилену стійкість до атак. До того ж, праці Zhang та Wang [9] та O'Connor та Hunt [8] досліджують потенціал застосування хаотичних систем у криптографії та їх ефективність у генерації випадкових послідовностей. Зважаючи на це, використання хаотичних карт здатне значно покращити безпеку цифрових водяних знаків.

Теоретичні основи цифрових водяних знаків

Цифрові водяні знаки – це непомітні чи майже непомітні відомості, вшиті в цифрові файли задля їхнього захисту від несанкціонованого використання та підтвердження авторства. Принцип їхньої роботи полягає в тому, що водяний знак містить конкретну інформацію, яка може бути зашифрованою або вбудованою у вигляді додаткових даних, що суттєво не впливають на властивості файлу, як-от його розмір або якість. Процес вбудовування цифрового водяного знака складається з декількох етапів:

1. Генерування водяного знака – створення унікального ідентифікатора або коду, що буде вбудований у файл.
2. Вбудовування водяного знака – введення водяного знака в окремі частини файлу без видимого впливу на його структуру. Це може бути досягнуто через зміни певних пікселів у зображенні, частотних складових у звукових або відеофайлах або навіть символів у текстових файлах.
3. Витягування водяного знака – процес вилучення водяного знака з файлу для перевірки його автентичності або власності, що зазвичай потребує наявності секретного ключа або певних алгоритмів для розшифрування водяного знака.

Цифрові водяні знаки можуть бути видимими або прихованими для користувача, а також можуть використовувати різні способи вбудовування – від простих методів зміни значень пікселів до більш складних криптографічних підходів. Цифрові водяні знаки можна класифікувати за різними критеріями. Ось основні типи:

1. Стеганографічні водяні знаки:

Призначення: використовуються для прихованого вбудовування інформації в цифрові файли.

Метод: водяний знак вбудовується в такі елементи файлу, як пікселі зображень, бітові потоки в аудіо- та відеофайлах або текстові файли. Стеганографічні водяні знаки не впливають на зовнішній вигляд чи якість файлу, що робить їх майже непомітними для користувача.

Застосування: використовуються для прихованої ідентифікації файлів, захисту від копіювання, а також для забезпечення конфіденційності та аутентичності.

2. Криптографічні водяні знаки:

Призначення: використовуються для забезпечення безпеки та достовірності інформації шляхом шифрування водяного знака.

Метод: водяний знак вбудовується в дані файлу, при цьому він шифрується або підписується з використанням криптографічних алгоритмів. Для вилучення водяного знака необхідно мати відповідний криптографічний ключ або сертифікат.

Застосування: використовуються в галузі цифрових підписів, авторських прав, юридичних та фінансових документах, де важливо забезпечити підтвердження достовірності та походження інформації.

3. Змішані водяні знаки:

Призначення: комбінують як стеганографічні, так і криптографічні методи для досягнення більш високого рівня захисту.

Метод: водяний знак може бути одночасно зашифрованим і прихованим у даних. Це дозволяє додати додатковий рівень безпеки, оскільки втрата одного з рівнів захисту (наприклад, виявлення стеганографічного водяного знака) не впливає на цілісність або безпеку водяного знака в цілому.

Традиційні методи нанесення водяних знаків охоплюють такі підходи, як зміна пікселів зображення, використання частотних компонентів аудіо чи відеофайлів або інші техніки, які впливають на дані файлу.

Переваги традиційних методів:

1. Легкість впровадження: багато методів нанесення водяних знаків прості у реалізації та не вимагають великих обчислювальних ресурсів.
2. Низькі витрати на впровадження: технології, засновані на традиційних методах, зазвичай дешевші у впровадженні і не потребують складних апаратних або програмних рішень.
3. Широкий спектр застосувань: ці методи можуть бути застосовані до різних типів файлів, таких як зображення, відео, аудіо, а також текстові документи.

Недоліки традиційних методів:

1. Вразливість до атак: традиційні водяні знаки часто виявляються вразливими до різноманітних атак, як-от спроби видалення чи модифікації, зокрема через зміни в форматах файлів чи стиснення.
2. Зниження якості файлу: для деяких методів нанесення водяних знаків, як-от зміна пікселів або частотних компонентів, існує ризик погіршення якості файлу (особливо це стосується зображень та відео).
3. Обмеження на кількість водяних знаків: у деяких випадках можна вбудовувати лише обмежену кількість водяних знаків у файл, що може обмежити їхню ефективність для масового захисту контенту.

Традиційні методи нанесення водяних знаків мають свої переваги, але й суттєві обмеження, які потребують нових технологічних рішень для підвищення безпеки та ефективності. Хаотичні карти, як один із таких підходів, пропонують можливості для створення більш стійких та захищених водяних знаків. **.** Схема загального принципу роботи хаотичної карти наведена на рис. 1.

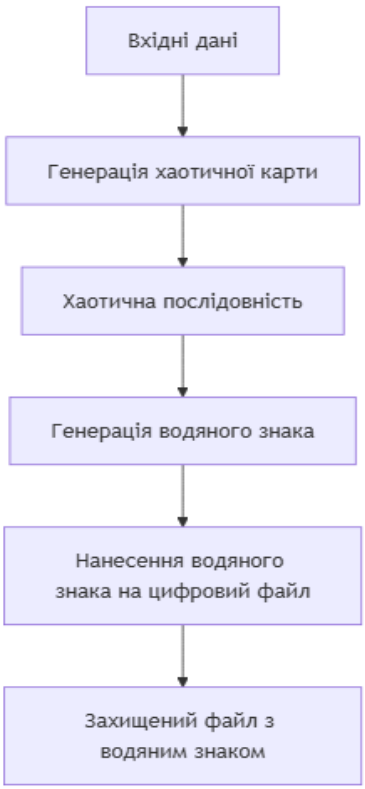

Рис. 1. Схема загального принципу роботи хаотичної карти

Хаотичні карти: Теоретичні основи

Хаотичні системи – це динамічні системи, що вирізняються залежністю від початкових параметрів; незначні зміни в цих параметрах можуть спричинити значні відмінності у поведінці системи в майбутньому. Вони мають високий рівень непередбачуваності, що робить їх особливо цінними для використання в криптографії та захисті даних. Хаотичні системи часто застосовуються для створення псевдовипадкових послідовностей, які є необхідними для забезпечення надійності криптографічних алгоритмів.

Хаотичні карти (або динамічні карти) представляють собою окремий різновид хаотичних систем. Вони є математичними моделями, що описують, як змінюється значення певної величини в результаті повторюваних операцій за заданими правилами або функціями.

Для хаотичних карт характерна здатність демонструвати надзвичайно складну та непередбачувану поведінку навіть за простих початкових умов.

Основні риси хаотичних карт:

1. Чутливість до початкових параметрів: Як і у звичайних хаотичних системах, навіть незначні зміни у вхідних параметрах можуть привести до принципово інших результатів.

2. Детермінованість: Незважаючи на випадковий вигляд хаотичної поведінки, система залишається детермінованою, тобто її поведінка визначається математичними рівняннями.

3. Портованість: властивість означає, що хаотична система в процесі свого розвитку може набувати певної структурованої форми, зберігаючи при цьому високу чутливість до початкових умов.

4. Перехідна та лінійна стабільність: Хаотичні карти можуть мати як стабільні, так і перехідні стани, що робить їх корисними у ситуаціях, де важливо забезпечити певну стабільність або передбачуваність на тривалий період часу.

Математичні моделі хаотичних карт базуються на повторюваних функціях, які генерують складні та непередбачувані послідовності. Одним з найбільш популярних підходів до створення хаотичних карт є використання атракторів та фазових просторів.

Математична модель хаотичної карти може включати функції, що визначають еволюцію системи з плином часу. Такі функції зазвичай мають вигляд:

$$x_{n+1} = f(x_n), \quad (1)$$

де x_n — це значення на n-му кроці, а $f(x_n)$ — це функція, що визначає зміну значення на наступному етапі.

Поширені функції, які використовуються для побудови хаотичних карт, можуть включати логістичні функції, функції Лоренца, або навіть більш складні моделі на основі фрактальних властивостей. Результат таких функцій, як правило, має складну динамічну поведінку, що характеризується хаосом та непередбачуваністю.

В криптографії хаотичні карти можуть використовуватися для генерації псевдовипадкових послідовностей, що є основою для створення криптографічних ключів, а також для шифрування та розшифрування даних. Моделі хаотичних карт можуть забезпечувати високий ступінь випадковості, необхідний для забезпечення надійної безпеки в криптографічних системах. Наприклад, для генерації псевдовипадкових чисел або секретних ключів хаотичні системи можуть використовуватися через процеси, які володіють певними властивостями детермінованого хаосу. Як хаотичні карти можуть бути використані для генерації ключів або вбудовування водяних знаків:

1. Генерація криптографічних ключів: Хаотичні карти можуть бути використані для генерації криптографічних ключів завдяки їх властивостям, які дозволяють створювати складні та непередбачувані послідовності. Наприклад, можна використати хаотичну карту для генерування чисел, що згодом використовуються як криптографічний ключ у системах шифрування або для хешування. Оскільки хаотичні карти можуть генерувати велику кількість різноманітних, непередбачуваних варіантів чисел, вони забезпечують високий рівень безпеки.

2. Вбудовування водяних знаків: Хаотичні карти також можуть використовуватися для вбудовування цифрових водяних знаків у файли. У цьому випадку алгоритм хаотичної карти може визначати, де і як водяний знак буде інтегровано в цифровий файл (наприклад, зображення, аудіофайл чи відео). Оскільки поведінка хаотичних карт чутлива до початкових умов, водяний знак можна розташувати у файлі таким чином, щоб він був майже непомітним, але в той же час достатньо стійким до спроб видалення або зміни.

Процес вбудовування водяного знака за допомогою хаотичних карт може включати:

1. Генерацію хаотичних послідовностей, які визначають місце і спосіб інтеграції водяного знака в дані файлу.

2. Шифрування водяного знака за допомогою результатів хаотичної системи, що додає додатковий рівень захисту.

3. Вилучення водяного знака з файлу шляхом застосування зворотного процесу, заснованого на тій самій хаотичній карті, яка використовувалася для його вбудовування.

Завдяки своїй непередбачуваності та чутливості до початкових умов хаотичні карти є дуже ефективним інструментом для захисту цифрових файлів через водяні знаки, а також для підвищення надійності криптографічних систем.

Нанесення цифрових водяних знаків з використанням хаотичних карт

Нанесення цифрових водяних знаків із застосуванням хаотичних мап є передовим підходом до захисту цифрових файлів, що ґрунтується на властивостях хаотичних систем для створення непередбачуваних і стійких до змін водяних знаків. Ключовим компонентом цього підходу є використання математичних моделей хаотичних мап для визначення точок і методів, через які відбуватиметься вбудовування водяного знака в цифрові дані.

Метод вбудовування водяних знаків із застосуванням хаотичних мап передбачає такі етапи:

1. Генерація хаотичної послідовності: Застосовується функція хаотичної мапи для створення послідовності чисел, що визначають, де і як буде вбудовуватися водяний знак. Ця послідовність є чутливою до початкових умов, що забезпечує високий рівень безпеки та непередбачуваність водяного знака.

2. Вибір точок вбудовування: Хаотична послідовність використовується для визначення місць у цифровому файлі (наприклад, пікселях зображення, бітах звукових файлів), де водяний знак буде вбудовуватися. Цей підхід дає змогу мінімізувати помітність водяного знака, водночас залишаючи його достатньо стійким до спроб маніпулювання даними.

3. Вбудовування водяного знака: Після вибору точок вбудовування водяний знак інтегрується в цифровий файл, зазвичай шляхом модифікації бітових чи піксельних значень. Завдяки використанню хаотичних мап, зміни в даних мінімальні, що дає змогу водяному знаку залишатися непомітним для звичайного спостерігача, але достатньо стійким.

4. Шифрування водяного знака: Для додаткової безпеки водяний знак може бути зашифрований за допомогою хаотичної мапи. Це додає рівень захисту від несанкціонованих спроб змінити або видалити водяний знак.

5. Витягування водяного знака: Для того щоб отримати водяний знак із зашифрованого файлу, необхідно застосувати зворотний процес, використовуючи той самий алгоритм хаотичної мапи. Точне знання початкових умов і параметрів мапи дає змогу правильно відновити водяний знак.

Розглянемо алгоритми для генерації хаотичних мап та їх використання для вбудовування та витягування водяних знаків (рис. 2, 3).

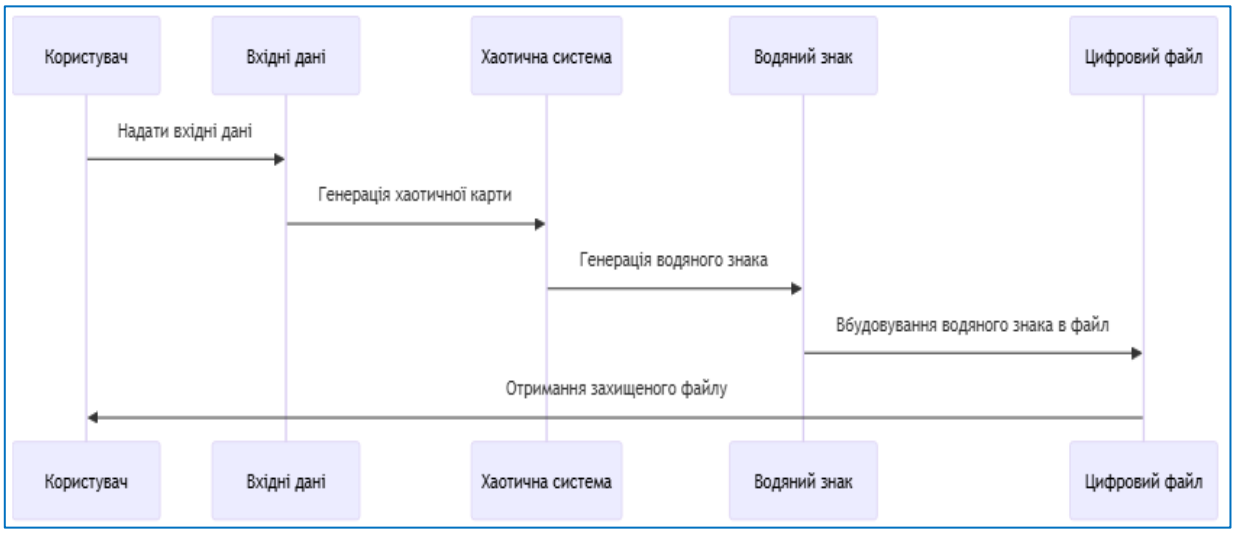

Рис. 2. Алгоритм генерації хаотичної карти

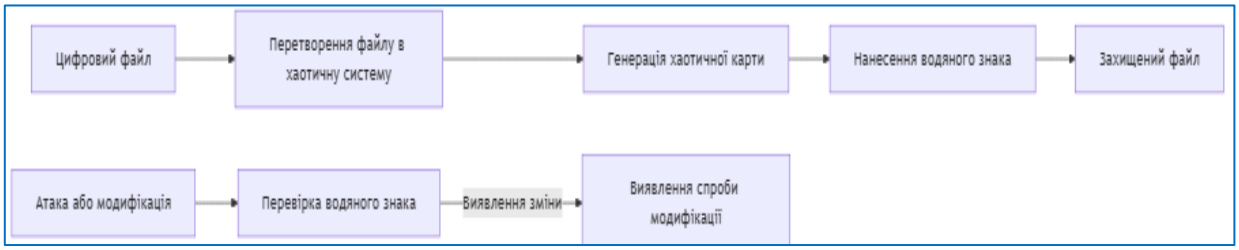

Рис. 3. Моделювання вбудовування водяного знака за допомогою хаотичної карти

Алгоритм Логістичної мапи (Logistic Map): Логістична мапа є одним з основних прикладів хаотичних мап і може бути використана для генерації послідовностей чисел, що визначатимуть точки вбудовування водяних знаків. Алгоритм базується на рівнянні: $x_{n+1}=r \cdot x_n \cdot (1-x_n)$, де x_n – поточне значення, а r – параметр, що впливає на ступінь хаосу в системі. За допомогою цього рівняння можна генерувати послідовності чисел, які можуть бути використані для визначення точок вбудовування водяного знака в цифровий файл.

Алгоритм Бенсона (Benson Map): Бенсонова мапа є ще одним типом хаотичної мапи, що використовується для генерації послідовностей чисел з високою чутливістю до початкових умов. Завдяки своїй структурі, Бенсонова мапа може бути використана для вбудовування водяних знаків у різні типи файлів, зокрема зображення та звукові файли.

Фрактальні мапи: Фрактальні мапи використовують властивості фракталів для створення хаотичних послідовностей. Вони можуть застосовуватися для вбудовування водяних знаків у вигляді структур, що повторюються на різних масштабах, роблячи водяний знак ще більш стійким до спроб модифікації.

Алгоритм Коса (Coupled Map Lattice): Алгоритм Коса є прикладом хаотичної системи, що використовує багатовимірні мапи для створення хаотичних послідовностей. Це дає змогу отримати складніші структури для водяних знаків і поліпшити їхню стійкість до атак.

Приклади програмного забезпечення або реалізацій, що застосовують хаотичні мапи для цієї мети:

Chaotic Watermarking System: Деякі програмні системи для вбудовування водяних знаків використовують хаотичні мапи для генерації ключів та визначення точок вбудовування. Програмне забезпечення може застосовувати алгоритм Логістичної мапи для створення псевдовипадкових послідовностей, що керують процесом вбудовування та витягування водяних знаків.

X-Watermark: Це програмне забезпечення, що використовує фрактальні та хаотичні мапи для створення водяних знаків у зображеннях. Застосовує комбіновані методи хаотичних мап і фракталів для збільшення стійкості водяного знака до атак.

Watermarking by Chaotic Maps: Це науковий проєкт або бібліотека, що реалізує методи вбудовування водяних знаків у цифрові файли з використанням хаотичних мап. Алгоритми побудовано на різних математичних моделях хаотичних систем, як-от Логістична мапа або Бенсонова мапа.

Digital Watermarking Toolkits: Деякі розроблені бібліотеки, як-от OpenCV або Matlab, можуть бути налаштовані для застосування хаотичних мап у процесі вбудовування водяних знаків. Такі бібліотеки дають змогу розробникам адаптувати хаотичні алгоритми до своїх специфічних потреб у захисті даних. Завдяки використанню хаотичних мап, процес нанесення водяних знаків набуває високого рівня безпеки, стійкості до атак і непередбачуваності. Це забезпечує захист цифрових файлів від несанкціонованого використання і копіювання, зберігаючи водночас мінімальний вплив на якість та видимість водяного знака.

Переваги та виклики використання хаотичних карт

Проаналізувавши класичні підходи і підходи з використанням хаотичних карт можна виділити такі основні переваги і недоліки.

Переваги застосування хаотичних карт проти традиційних методів водяного знакування:

1. Висока захищеність від атак: Хаотичні карти надають значно кращий захист від спроб видалення чи зміни водяних знаків. Оскільки ці системи демонструють надзвичайну чутливість до початкових умов, будь-яка зміна будь-якого параметра або компоненту в структурі карти суттєво впливає на кінцевий результат, що ускладнює відновлення чи розпізнавання водяного знака без точних знань про його вихідні умови.
2. Непередбачуваність: Хаотичні карти генерують випадкові, непередбачувані послідовності, що робить їх відтворення чи зломування надзвичайно складним без правильних параметрів. Це значно ускладнює несанкціоноване вилучення водяних знаків, створених за допомогою хаотичних систем, на відміну від більш стандартних методів, де водяний знак може бути визначений за певними шаблонами.
3. Мінімальний вплив на якість даних: Завдяки застосуванню хаотичних карт, водяний знак може бути вбудований в такі області, що їх неможливо виявити візуально, і вони практично не впливають на якість цифрового файлу. На відміну від традиційних методів, які можуть впливати на візуальні або звукові характеристики файлів, хаотичні карти дозволяють уникнути помітних спотворень.
4. Гнучкість та адаптивність: Хаотичні карти пропонують гнучкість у використанні різних математичних моделей, що дозволяє адаптувати методи водяного знакування під конкретні потреби безпеки та специфікації. Це надає можливість обирати відповідні алгоритми для різних типів файлів, таких як зображення, аудіо, відео або текстові документи.
5. Підвищена стійкість до маніпуляцій: Хаотичні карти демонструють добру адаптацію до змін вхідних даних, тому навіть у випадку часткового пошкодження або маніпуляцій, цифровий водяний знак залишатиметься незмінним. Це робить хаотичні системи привабливішими за традиційні підходи, де незначні зміни можуть призвести до втрати водяного знаку.

Проблеми, що виникають при використанні хаотичних карт: стабільність, чутливість та атаки:

1. Стабільність алгоритмів: Оскільки хаотичні карти сильно залежать від початкових умов та параметрів, їх застосування потребує особливої уваги до стабільності. Незначні зміни в параметрах можуть викликати великі відхилення у результатах генерації хаотичних послідовностей, що може вплинути на ефективність вбудовування водяних знаків. Для забезпечення високої стабільності необхідне ретельне налаштування алгоритмів.
2. Чутливість до змін: Хаотичні карти можуть бути надзвичайно чутливими до найдрібніших змін.

Навіть незначні зміни у даних (наприклад, спроба стиснення або зміна формату файлу) можуть пошкодити водяний знак або зробити його невидимим. Це становить серйозну проблему, особливо коли необхідно витягнути водяний знак з пошкоджених файлів або після стиснення даних.

3. Складність відновлення водяного знака: Вилучення водяного знака за допомогою хаотичних карт може бути дуже складним завданням, особливо без точного знання початкових умов і параметрів карти. Це ускладнює процес відновлення водяного знака у разі змін або атак, що може бути проблематичним для правоохоронних органів чи власників авторських прав.

4. Обмеження на обчислювальні ресурси: Алгоритми, що використовують хаотичні карти, можуть бути обчислювально складними і потребувати значних ресурсів для генерації послідовностей та вбудовування водяних знаків. Це може призвести до проблем із продуктивністю в режимі реального часу для деяких додатків, особливо при обробці великих обсягів даних.

Пропозиції щодо вдосконалення методів на основі хаотичних карт

1. Оптимізація алгоритмів: Щоб покращити стабільність та ефективність хаотичних карт у нанесенні водяних знаків, важливо оптимізувати обчислювальні алгоритми. Це зменшить потребу в обчислювальних ресурсах та збереже високу стійкість до атак.

2. Розробка адаптивних алгоритмів: Створення адаптивних методів вбудовування водяних знаків на основі хаотичних карт, здатних враховувати зміни параметрів даних або умов середовища, підвищить їх стійкість до атак і змін. Це може включати використання багатокрокових або гібридних методів, які поєднують хаотичні карти з іншими криптографічними техніками.

3. Використання мульти-хаотичних карт: Застосування кількох різних хаотичних карт або комбінованих моделей хаосу може покращити стійкість водяного знака до різних типів атак. Використання різних моделей дозволить більш ефективно адаптувати водяний знак до різних типів файлів і знижує ризик успішного відновлення водяного знака без відомих параметрів.

4. Впровадження технологій з машинним навчанням: Використання машинного навчання для адаптації та оптимізації процесу вбудовування водяних знаків може допомогти покращити точність та надійність водяних знаків на основі хаотичних карт. Це дозволить створити системи, що автоматично підлаштовуються під зміни вхідних даних та зменшують уразливість до змін та атак.

5. Інтеграція з багаторівневими системами захисту: Для підвищення рівня безпеки водяних знаків можна використовувати хаотичні карти в поєднанні з іншими технологіями, такими як криптографія з відкритим ключем або цифрові підписи. Це забезпечить додатковий рівень захисту та ускладнить процес нанесення водяних знаків для потенційних зловмисників.

Conclusions

Внаслідок аналізу застосування хаотичних карт у контексті впровадження цифрових водяних знаків, можна виділити кілька ключових спостережень. Хаотичні карти, що демонструють властивості непередбачуваності та залежності від початкових умов, забезпечують посилений захист від різноманітних впливів, як-от спроби зміни або видалення водяного знака. Завдяки складності відтворення без точних параметрів генерації, такі методи забезпечують більш надійний захист авторських прав та цілісності даних, у порівнянні з традиційними підходами.

Проте, існують й певні виклики, особливо ті, що стосуються чутливості хаотичних карт до змін вхідних даних, а також обмежень у обчислювальних ресурсах. Для підтримки їх стабільності й ефективності, необхідна оптимізація алгоритмів та їх адаптація до різних умов експлуатації.

Підтвердження чи спростування ефективності цієї технології.

Використання хаотичних карт у технологіях цифрових водяних знаків демонструє значний потенціал для створення більш складних та захищених методів захисту цифрової інформації. Хаотичні системи, які мають здатність формувати унікальні та комплексні послідовності, можуть значно покращити стійкість до атак та несанкціонованих спроб вилучення водяного знака. Разом з тим, потреба у налаштуванні та оптимізації алгоритмів створює певні труднощі у практичній реалізації цих технологій, проте переваги у порівнянні з традиційними підходами свідчать про їх високу ефективність.

Перспективи подальшого розвитку. Наступні дослідження в цій сфері можуть бути зосереджені на кількох ключових напрямках. Першим є вдосконалення методів генерації хаотичних карт для досягнення більшої стабільності при мінімальних обчислювальних витратах. Це розширить сферу застосування цих методів у реальних додатках, мінімізуючи вимоги до ресурсів.

Другим важливим напрямом є інтеграція хаотичних карт з іншими сучасними криптографічними методами, такими як цифрові підписи або методи з відкритими ключами, що дасть змогу розробляти більш надійні та багаторівневі системи захисту. Крім того, використання машинного навчання для адаптації алгоритмів до змін у даних може суттєво поліпшити якість та стійкість водяних знаків.

Потенціал застосування цих методів у сучасних системах безпеки. Методи впровадження водяних знаків на основі хаотичних карт мають великий потенціал у сучасних технологіях забезпечення безпеки. Їх можна використовувати для захисту авторських прав у медіаіндустрії, у фінансових технологіях для забезпечення цілісності транзакцій, а також у галузях, які вимагають високого рівня конфіденційності даних, наприклад, у сфері охорони здоров'я та державної безпеки. З огляду на розвиток квантових обчислень та нових криптографічних стандартів, хаотичні карти можуть стати важливим компонентом для забезпечення довгострокового захисту інформації.

СПИСОК ЛІТЕРАТУРИ

1. Anderson, Ross J. Security engineering: a guide to building dependable distributed systems. John Wiley & Sons, 2010. url: https://www.cl.cam.ac.uk/archive/rja14/book.html
2. Diffie, Whitfield, and Martin E. Hellman. "New directions in cryptography." Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman. 2022. 365-390. doi: https://doi.org/10.1145/3549993.355000
3. J. Chen and B. C. Schafer, "Watermarking of Behavioral IPs: A Practical Approach," *2021 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, Grenoble, France, 2021, pp. 1266-1271, doi: 10.23919/DATE51398.2021.9474071.
4. Kadian, P., Arora, S.M. & Arora, N. Robust Digital Watermarking Techniques for Copyright Protection of Digital Data: A Survey. Wireless Pers Commun 118, 3225–3249 (2021). doi: https://doi.org/10.1007/s11277-021-08177-w
5. Lawnik, M.; Berezowski, M. New Chaotic System: M-Map and Its Application in Chaos-Based Cryptography. Symmetry 2022, 14, 895. doi: https://doi.org/10.3390/sym14050895
6. Shih, Frank Y. Digital watermarking and steganography: fundamentals and techniques. CRC press, 2017. doi: https://doi.org/10.1201/9781315121109
7. Cox, Ingemar J., et al. "A review of watermarking principles and practices 1." Digital signal processing for multimedia systems (2018): 461-485. url: http://www.wirelesscommunication.nl/wireless/articles/98_bookchapterwatermarking.pdf
8. Hamadi, S. J., & Emad A. Mohammed. (2024). Chaotic Systems in Cryptography: An Overview of Feature-Based Methods. Al-Salam Journal for Engineering and Technology, 4(1), 164–172. doi: https://doi.org/10.55145/ajest.2025.04.01.016
9. Zhang, B.; Liu, L. Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics 2023, 11, 2585. doi: https://doi.org/10.3390/math11112585
10. Menezes, Alfred J., Paul C. Van Oorschot, and Scott A. Vanstone. Handbook of applied cryptography. CRC press, 2018. doi: https://doi.org/10.1201/9780429466335
11. Aberna, P., Agilandeeswari, L. Digital image and video watermarking: methodologies, attacks, applications, and future directions. Multimed Tools Appl 83, 5531–5591 (2024). https://doi.org/10.1007/s11042-023-15806-y
12. Naik, R.B., Singh, U. A Review on Applications of Chaotic Maps in Pseudo-Random Number Generators and Encryption. Ann. Data. Sci. 11, 25–50 (2024). https://doi.org/10.1007/s40745-021-00364-7

Received (Надійшла) 12.03.2025
Accepted for publication (Прийнята до друку) 20.05.2025

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Шандиба Антон Сергійович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Anton Shandyba – student, Department of Electronic Computers, Kharkiv National University of Radio Electronics, Ukraine;
e-mail: anton.shandyba@nure.ua; ORCID Author ID https://orcid.org/0009-0000-7697-0634.

Сітніков Віталій Ігорович – асистент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Vitalii Sitnikov – Assistant of Department of Electronic Computers, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: vitalii.sitnikov1@nure.ua; ORCID Author ID: https://orcid.org/0009-0005-3087-6104.

Ніколаєв Олексій Євгенович – студент кафедри електронних обчислювальних машин, Харківський національний університет радіоелектроніки, Харків, Україна;
Alexey Nikolayev – student, Department of Electronic Computers, Kharkiv National University of Radio Electronics, Ukraine;
e-mail: oleksii.nikolaiev@nure.ua; ORCID Author ID https://orcid.org/0009-0008-5741-4702.

Кібірєв Денис Олексійович – аспірант кафедри безпеки інформаційних технологій, Харківський національний університет радіоелектроніки, Харків, Україна;
Denis Kibirev – PhD student, Department of Information Technology Security, Kharkiv National University of Radio Electronics, Kharkiv, Ukraine;
e-mail: oleksii.leha@nure.ua; ORCID Author ID: https://orcid.org/0009-0008-9869-4261.

Digital watermarking using chaotic maps

Anton Shandyba, Vitalii Sitnikov, Alexey Nikolayev, Denis Kibirev

Abstract. In today's digital environment, the issues of copyright protection and information security are becoming increasingly important. One of the effective methods for protecting multimedia content is digital watermarking technology, which enables the identification and tracking of unauthorized use of digital files. At the same time, traditional watermarking methods have certain drawbacks, which encourages the search for new solutions. The aim of this research is to develop a method for implementing digital watermarks using chaotic maps, in order to enhance the resilience of watermarks against tampering and alterations. The subject of the research is the methods and technologies of digital watermarking (steganography) that utilize chaotic maps to improve the reliability, security, and invisibility of embedded information within digital objects. The object of the research is digital images (or multimedia objects) to which a watermark is applied using chaotic map-based algorithms, ensuring copyright protection, authentication, and data integrity. To achieve the set goal, the following tasks were undertaken: an analysis of key digital watermarking methods, an examination of the characteristics of chaotic maps and their potential in watermark creation, and a review of an algorithm for embedding digital watermarks using chaotic maps. This work explores the theoretical foundations of digital watermarking, analyzes existing embedding methods, and thoroughly investigates the potential application of chaotic maps in this domain. A methodology for using chaotic maps to generate keys and embed watermarks is proposed. The strengths and weaknesses of this approach are analyzed, and prospects for future research in this area are outlined.

Keywords: chaotic maps, algorithm, cyber threats, image, steganography, protection, watermarks.