ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

УДК 004.94 DOI: https://doi.org/10.30837/2522-9818.2025.3.102

В. Поддубний, О. Сєвєрінов

МОДЕЛЬ АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ З ВИКОРИСТАННЯМ НУЛЬОВОГО ВОДЯНОГО ЗНАКУ НА ОСНОВІ RGB-ЗОБРАЖЕНЬ

Предметом дослідження методи та схеми автентифікації користувачів в інформаційно-комунікаційних мережах. **Мета роботи** – розробка моделі автентифікації користувачів в інформаційно-комунікаційних системах з використанням методу нульового водяного знаку на основі RGB-зображень **завдання:** розгляд основних проблем під час інтеграції систем контролю доступом; розробка моделі автентифікації користувачів з використанням нульового водяного знаку; дослідження потенційних характеристик та висування пропозицій/рекомендацій щодо її використання для автентифікації, побудова графічних схем, що відображають процеси та процедури Для виконання окреслених завдань використовувалися такі **методи**: методи моделювання, методи формального опису **Досягнуті результати:** запропонована вдосконалена модель автентифікації користувачів заснована на алгоритмі нульового водяного знаку, що являється альтернативою існуючим схемам автентифікації в інформаційно комунікаційних системах, досліджені її потенційні характеристики, що підтверджують перспективність розробки, побудовані графічні представлення процесів та процедур **Висновки** під час роботи було коротко розглянуто основні проблеми з якими стикаються власники інформаційно-комунікаційних систем при інтеграції систем автентифікації, запропоновано вдосконалену модель автентифікації за допомогою нульового водяного знаку, в якості нульового водяного знаку використовувався метод заснований на RGB-зображенях з використанням перетворення K-means та DWT, в якості другого фактору використовується пароль. Представлено три режими роботи: реєстрація, автентифікація та зміна ключових даних для автентифікації. Така модель є альтернативою існуючим схемам та можуть потенційно зменшити вартість автентифікації, кількість помилок першого та другого роду у порівняні з аналогічними схемами автентифікації, підвищити зручність автентифікації в інформаційно-комунікаційних системах. Також це розширює множину вибору схем автентифікації що мають власники систем при їх інтеграції.

Ключові слова: цифровий водяний знак; автентифікація; зображення; модель; пароль.

Вступ

Зі зростанням ролі інформаційних технологій та їх активним упровадженням у різні сфери діяльності посилюється необхідність використання засобів автентифікації користувачів, зокрема під час отримання доступу до приміщень, технічних засобів чи інформації в інформаційно-комунікаційних системах. Традиційно такі засоби ґрунтуються на паролях, магнітних картках, біометричних даних або QR-кодах. Одним із шляхів підвищення рівня захисту є поєднання зазначених методів у межах багатофакторної автентифікації [1].

Разом з тим, такі системи характеризуються значними витратами, оскільки вимагають застосування спеціалізованого обладнання (наприклад, зчитувачів відбитків пальців чи інших біометричних сенсорів). Використання карток або кодів також створює додаткові ризики: наявність фізичного носія сигналізує потенційному зловмиснику про його важливість, що стимулює спроби викрадення, копіювання чи підміни даних.

Альтернативним підходом є застосування нульових водяних знаків для побудови систем автентифікації. Ключова перевага цього методу полягає в тому, що критичні дані не змінюються та залишаються невидимими для зловмисника, оскільки він не має змоги визначити їхню наявність. Крім того, реалізація подібних рішень є відносно маловартісною, адже водяний знак може ґрунтуватися на різних типах інформації, для опрацювання якої не потрібне спеціальне обладнання [2, 3].

Основна проблематика застосування нульових водяних знаків у багатофакторній автентифікації полягає у новизні технології та недостатній кількості досліджень у цій сфері. Водночас перспективи її використання видаються обнадійливими, особливо з огляду на інтеграцію з сучасними IoT-засобами. Таким чином виникає необхідність в дослідженні та розробці нових методів автентифікації заснованих на нульовому водяному знакові.

Аналіз проблеми

Автентифікація поділяється за кількістю факторів авторизації (фактор – набір доказів, які пред’являє користувач для підтвердження особи, так вона може бути однофакторною та багатофакторною.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Для забезпечення належного рівня безпеки рекомендується використовувати, як мінімум, двофакторну автентифікацію [4, 5].

Під час побудови систем автентифікації власники систем зустрічаються з наступними проблемами:

– вибору фактору;
– вибору схеми автентифікації.
– вартості;
– безпеки;
– зручності;
– завадозахищеності.

Проблема вибору фактору полягає у визначені які фактори слід використовувати (знання чогось, володіння чимсь, характеристики об'єкту). Різні фактори мають різні характеристики вартості, надійності, зручності ітд. Власнику системи слід визначитись які фактори слід використовувати, як їх поєднувати, інтегрувати в систему тощо.

Проблема вибору схеми автентифікації полягяє у виборі порядку поєднання та впливу факторів, так існують послідовні, паралельні та послідовно-паралельні схеми автентифікації. Власнику системи слід визначитися, в якому порядку використовувати фактори автентифікації та як обчислювати кінцевий результат автентифікації.

Проблема вартості полягає у зменшені показників вартості кожної авторизації, обслуговування системи автентифікації, додаткових матеріалів та засобів для автентифікації кожного користувача.

Проблема безпеки закладається у забезпеченні достатнього рівня достовірності авторизації. Під безпекою розуміється характеристика, яка є сукупністю вірогідностей помилок першого та другого роду, можливостей злому системи зловмисником, викрадення даних, їх підробкою.

Проблема зручності полягає у максимізації суб'єктивних параметрів зручності авторизації (складності дій, швидкості, необхідності запам'ятовувати дані тощо).

Проблема завадозахищеності з'являється в системах, де рівень шуму вищий ніж 0. Вона полягає у мінімізації помилок першого та другого роду при автентифікації через виникнення помилок в обробці чи введенні наборів даних.

Тому під час інтеграції багатофакторної автентифікації власники систем зазвичай не розробляють власні моделі, а використовують наявні, через що виникає необхідність у розробці готових моделей для мінімізації та вирішення наведених вище проблем і створені множини вибору залежно від пріоритетів власників систем.

Аналіз літератури

Схеми автентифікації за допомогою нульових водяних знаків вже відомі. Так, наприклад, в роботі [6] наводиться огляд поточного стану досліджень у сфері автентифікації зображень, зокрема з використанням методів нульового водяного знаку. В роботі [7] подано метод, який є забезпеченням автентичності медичних зображень з використанням схеми НВЗ, що зберігає оригінальність зображення (без вбудовування змін до пікселів). У роботі [8] наводиться приклад використання нульових водяних знаків разом з QR-кодами. Автори пропонують схему автентифікації медичних зображень, яка поєднує НВЗ та QR-код. В роботі [9] автори пропонують гібридний метод, що поєднує цифровий підпис та НВЗ для забезпечення автентичності, цілісності, виявлення маніпуляцій і захисту прав автора для чутливих текстових документів.

Як можна побачити кількість наявних схем автентифікації з використанням НВЗ досить велика, проте дані схеми не підходять для автентифікації користувачів в інформаційно-комунікаційних системах. Схеми автентифікації, що використовують як контейнер тексту, не можуть бути використані для автентифікації користувачів в інформаційно-комунікаційних системах, оскільки користувачу незручно вводити великі текстові дані, а при введенні тексту з носія краще використовувати дані криптографічних перетворень. Дані методи підходять для машинної автентифікації або для підтвердження авторства.

Тому виникає необхідність у вдосконаленні наявних моделей автентифікації користувачів саме для інформаційно-комунікаційних систем, де як одним із факторів використовується цифрове зображення.

Модель багатофакторної автентифікації на основі методу нульового водяного знаку

Проведений аналіз показав, що для вирішення наведених проблем запроваджуються нові методи багатофакторної автентифікації, серед яких розповсюдженості набули методи, засновані на використанні OTP-кодів, адаптивній та поведінковій автентифікації, WebAuthn тощо. Досить новою є автентифікація за допомогою нульових

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

водяних знаків. На сьогодні запропоновано декілька таких методів [10]. Одним із досить простих у використанні є запропонований авторами в роботах [11, 12] метод багатофакторної автентифікації на основі пароля та RGB-зображення.

Метод формування водяного знака детально описаний в роботі [13]. Проте відсутні моделі його використання та аналогічних методів для автентифікації користувачів в інформаційно-комунікаційних системах.

Розглянемо загальну модель використання нульового водяного знака для автентифікації. В такій моделі основні дії користувача такі:

– реєстрація;
– автентифікація;
– зміна ключових даних.

Дії користувача виконуються послідовно, тобто спочатку реєстрація, автентифікація, за необхідності зміна ключових даних. Зміна ключових даних без автентифікаціїх неможлива, в свою чергу автентифікація неможлива без першочергової реєстрації.

Для системи автентифікації за допомогою нульових водяних знаків обрана типова схема для багатьох систем та засобів, які здійснюють процедуру автентифікації. Проте виникає необхідність у деталізації процесів, ключових даних, параметрів та інших даних у разі використання нульового водяного знаку як алгоритму підтвердження правильності автентифікації.

Запропонована модель автентифікації за допомогою нульових водяних знаків зображена на рис. 1.

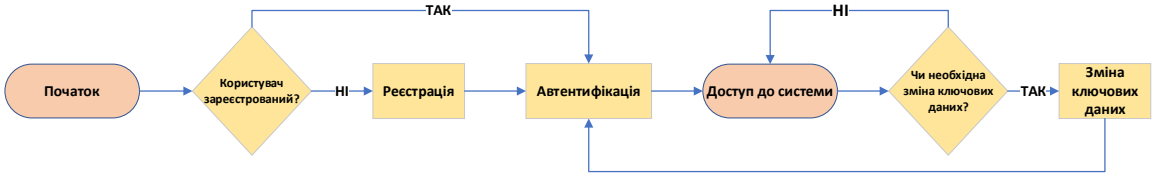

Рис. 1. Модель автентифікації

В роботі [12] розглянуто основні компоненти роботи типової моделі автентифікації з використанням нульового водяного знаку. Тому виникає необхідність у деталізації процедур кожного окремого процесу. Метод формування водяного знаку та розширення ключа не розглядатиметься детально, оскільки він описаний у роботі [13].

У такій системі як ключові дані виступають:

– пароль обраний користувачем;
– цифрове RGB зображення.

Як підтвердження автентифікації використовується результат порівняння сформованого нульового водяного знака з еталонною копією.

Процес реєстрації користувача з використанням запропонованого методу водяного знаку полягає в послідовному виконанні таких кроків:

Крок 1. Користувач обирає ключем довільне зображення O (або генерує його засобами системи, в якій інтегрована схема, у тому числі як генератор зображень може використовуватися штучний інтелект):

$$O \in \{0,\ldots,255\}^{H*W*3}, \quad (1)$$

де $H, W \in \mathbb{N}$ – висота та ширина вхідного зображення, $\mathbb{N} \in \{1,2,3\ldots\infty\}$;

Крок 2. Користувач обирає випадковий пароль доступу $PASS$ залежно від політики паролів організації

$$PASS \in \{0,\ldots,255\}^{L}, \quad (2)$$

де L – кількість символів в паролі;

Крок 3. Користувач вводить в систему (за допомогою засобів зчитування та цифровізації IT) обране зображення O та пароль $PASS$

$$OIT,\ PASSIT; \quad (3)$$

Крок 4. Під час реєстрації генерується нульовий водяний знак W, де вхідні дані – це ключ $PASS$ (або його розгорнутий варіант) та обране зображення O:

$$W = F(O, PASS); \quad (4)$$

Крок 5. Сформований нульовий водяний знак зберігається в базі даних системи як еталонна копія

$$W \to DB. \quad (5)$$

Процес реєстрації користувача в системі з використанням запропонованого методу водяного знака подано на рис. 2.

Для процедури автентифікації на основі запропонованого методу водяного знака обрається стандартна послідовність дій, що складається з таких кроків:

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Крок 1. Користувач вводить в систему IT власний пароль $PASS$ та засобами системи зчитує зображення O, яке він обрав як ключ, аналогічно (3);

Крок 2. Генерується нульовий водяний знак, де вхідні дані – це ключ (або його розгорнутий варіант) та обране зображення:

$$W' = F(O, PASS); \quad (6)$$

Крок 3. Модуль автентифікації порівнює згенерований нульовий водяний знак з еталонним нульовим водяним знаком W з бази даних за допомогою функції порівння S, повертаючи певне значення подібності x:

$$x = S(W', W); \quad (7)$$

Крок 4. Система порівнює коефіцієнт схожості [14] водяного знаку з еталонним нульовим знаком (x) зі встановленим значенням допустимої похибки (y); якщо $x < y$, то користувачеві блокується доступ до системи, а якщо $x \geq y$, – доступ надається

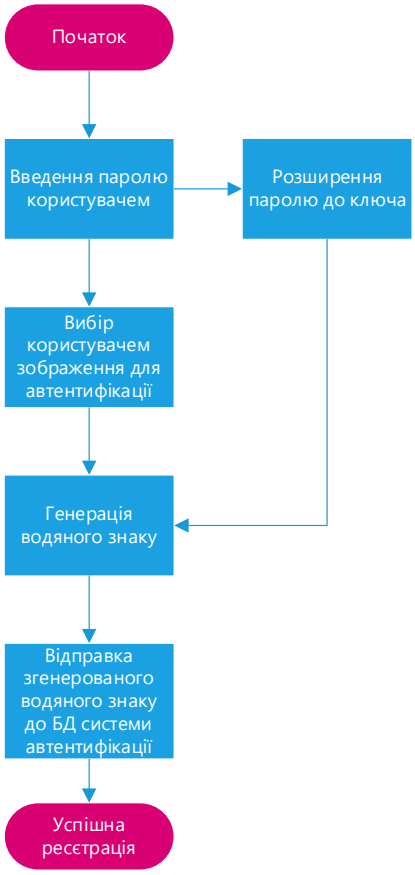

Рис. 2. Процес реєстрації користувача в системі

На рис 3. наведений процес автентифікації користувача за допомогою запропонованої моделі.

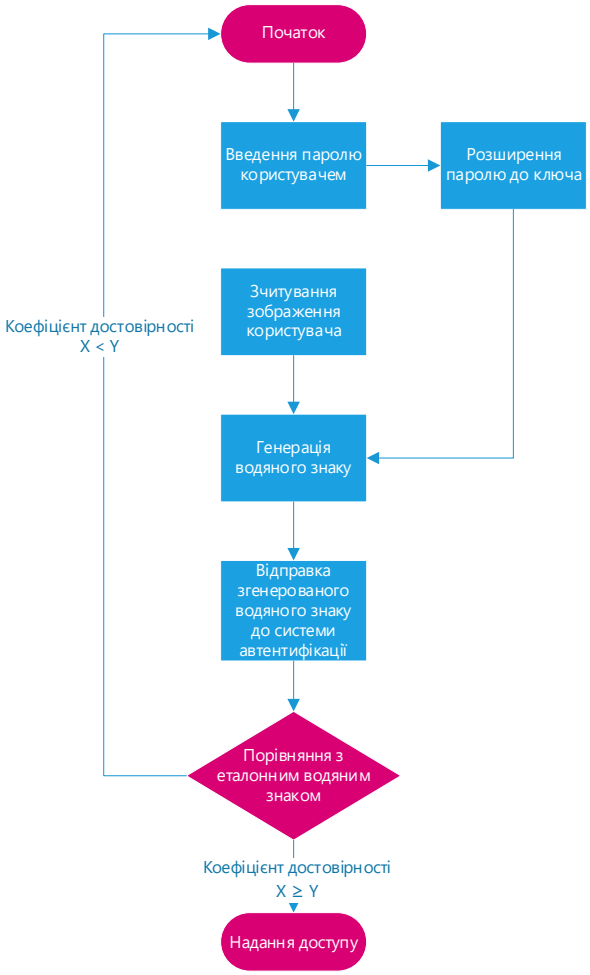

Рис. 3. Процес автентифікації за допомогою запропонованої моделі

Для зміни ключових даних у разі використання запропонованого методу водяного знака пропонується здійснити типові кроки:

Крок 1. Користувач має пройти успішну автентифікацію для надання йому повноважень щодо зміни ключових даних:

$$Auth \Leftrightarrow x \geq y. \quad (8)$$

Крок 2. Користувач після успішної автентифікації має заново ввести нові уключові дані;

$$O' \to IT,\ PASS' \to IT. \quad (9)$$

Крок 3. Метод формування нульового водяного знака здійснює повторне формування водяного знака за новими введеними ключовими даними

$$W' = F(O', PASS'). \quad (10)$$

Крок 4. Новосформований водяний знак записується в базу даних системи автентифікації

$$W' \to DB, \quad (11)$$

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

На рис 4. наведений процес зміни даних автентифікації користувача за допомогою запропонованої моделі.

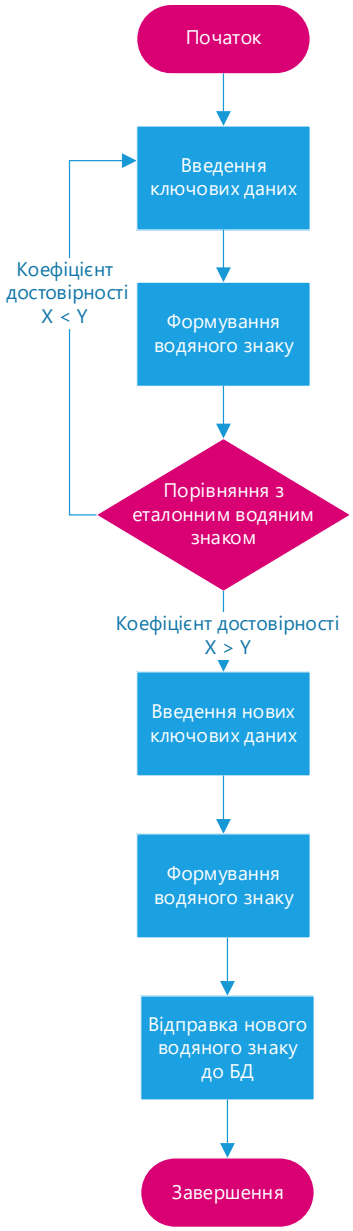

Рис 4. Процес зміни даних користувача за допомогою запропонованої моделі

За умови застосуванні IoT-пристроїв така модель може контролювати доступ до приміщень або певної інформації. Засобом зчитування зображення можуть бути відеокамери, для перетворення цифрового водяного знаку можна використовувати мікроконтролери. Після обчислення перетворення цифрового водяного знака результат передається на сервер доступу організації, яка перевіряє:

1) коректність введеної інформації;

2) чи має користувач з такими даними доступ до певного ресурсу.

Оскільки обробка зображення складніша ніж процес формування та перевірка геш-значення, то рекомендується додатково зберігати геш-значення від паролю $PASS$ в базі даних системи автентифікації DB

$$H(PASS) \to DB \qquad (12)$$

Під час автентифікації перевіряти геш-значення H' від введеного пароля $PASS'$ та між еталонним значенням H перед формуванням водяного знака. Це може пришвидшити процедуру автентифікації, відкидаючи одразу помилки в паролі.

У запропонованому варіанті процедура реєстрації та автентифікації не містить додаткових ідентифікаторів користувача для авторизації (прав доступу, ролей тощо), для використання рольової моделі пропонується застосовувати ідентифікатор у вигляді логіну при записі в базу даних. Таким чином формується комбінація логін–водяний знак. Для невеликих систем, або систем, де не потрібний адміністративний розподіл, може здійснюватися перевірка лише на наявність схожого водяного знака в базі даних.

Потенційні характеристики запропонованої моделі

Розглянемо дану модель с точки зору потенційного вирішення вищезазначених проблем.

Проблема вибору фактора. Дана модель ґрунтується на двох факторах. Це знання чогось – пароль, та володіння чимось – зображення. Тобто вона пропонує вже готове рішення поєднання факторів автентифікації.

Проблема вибору схеми автентифікації. Модель є послідовною, оскільки фактори в ній застосовуються один за одним. Кінцевим результатом застосування є водяний знак, що перевіряється схемою автентифікації. Модель пропонує готову схему поєднання факторів.

Проблема вартості. Розглянемо загальну вартість моделі автентифікації з факторами «занання чогось» та «володіння чимсь»:

$$C = x \cdot z + K_з + K_в + (A_з + A_в) \cdot x, \qquad (13)$$

де $A_з$ – вартість адміністрування системи знання (створення облікових записів, зміна паролів) у розрахунку на одного користувача;

ISSN 2522-9818 (print)
Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33) ISSN 2524-2296 (online)

$A_в$ – вартість адміністрування системи володіння (створення облікових записів, зміна засобів, видача та контроль) у розрахунку на одного користувача;

x – кількість користувачів;

z – вартість одного засобу для користувача;

$K_з$ – вартість комплексу засобів захисту для роботи з знанням (засоби вводу);

$K_в$ – вартість комплексу засобів захисту для роботи з інформацією (засоби зчитування то обробки інформації) [15].

Запропонована модель потенційно знижує z – вартість засобу доступу (носій з інформацією, магнітна картка, ключ тощо), оскільки збереження та розповсюдження цифрового зображення не потребує багатьох ресурсів, це може бути аркуш паперу, особистий телефон співробітника чи зовнішнє інтернет-посилання.

Проблема безпеки. Розглянемо потенційну надійність моделі автентифікації. Математична складність перебору пароля:

$$S(pass) = y^c, \tag{14}$$

де c – кількість символів в паролі; y – розмір алфавіту (діапазон символів, які може набувати пароль).

Потенційні варіації зображення:

$$S(image) = 256^{M \cdot M \cdot 3} = 2^{24M^2}, \tag{15}$$

де 256 – значення яскравості кожного біту; M – розмір зображення; 3 – кількість спектрів (R,G,B).

Дані характеристики зменшуються, оскільки самий метод водяного знака містить колізії та толерантний до утворення шумів та викривлень, тому маючи початкові високі показники надійності сама модель формування водяного знака потребує додаткового вивчення з метою оцінки його криптостійкості.

Проблема зручності. З точки зору користувача, "зручність" це перш за все простота використання. Модель використовує широко розповсюджені паролі, які є зрозумілим та розповсюдженим методом автентифікації, другим фактором виступає цифрове зображення, яке також зрозуміле більшості користувачів. Навіть користувачі, які не мають досвіду роботи з інформаційно-комунікаційними системами можуть зрозуміти принцип використання зображення для автентифікації. Тим самим дана модель має високу зручність та гнучкість у разі використанні її для автентифікації[16, 17].

Проблема завадозахищеності. Дана проблема виникає в мережах з деяким рівнем шуму. Запропонована модель має певну толерантність (як показано в роботі [13], водяний знак може бути розпізнаний з мінімальною кількістю помилок при рівні шуму 13 PSTR [18]). Модель стійка до шумів при:

– зчитуванні зображення в систему автентифікації;

– передачі сформованого водяного знака для перевірки з еталонним водяним знаком.

Тобто не обов'язково $W' = W$ та $O' = O$, якщо система налаштована відповідним чином.

Отже запропонована модель є досить практичною з точки вирішення основних проблем під час вибору моделей автентифікації, та пропонує власникам систем додаткову гнучкість в ході побудови систем автентифікації. Проте деякі аспекти моделі (такі як криптографічна стійкість, практична зручність) потребують додаткового вивчення та дослідження.

Висновок

В роботі запропонована модель багатофакторної автентифікації за допомогою методу нульового водяного знака, заснованого на RGB-зображеннях. Дана розроблена модель є альтернативою існуючим моделям та здатна потенційно зменшити вартість автентифікації, кількість помилок першого та другого роду порівняно з аналогічними схемами автентифікації, підвищити зручність автентифікації в інформаційно-комунікаційних системах. Також це розширює множину вибору схем автентифікації, що мають власники систем. Така модель потенційно вирішує проблеми, які виникають в ході побудові систем автентифікації, проте потребує дослідження з точки зору криптостійкості методу формування нульового знака та практичної зручності.

Перевагою такої моделі є її стійкість до виникнення шумів під час введення ключових даних або передачі результата автентифікації. Додатковими перевагами є: використання двох факторів автентифікації, висока зрозумілість користувачам.

Тому, хоча запропонована модель є перспективною, пропонуються такі вектори дослідження:

– дослідження криптографічної стійкості методу нульового водяного знака, та схеми автентифікації в цілому;

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)

– практична реалізація моделі з метою дослідження швидкодії та вартості ресурсів, необхідних для автентифікації;

– практична реалізація моделі з метою тестування зручності на вибірці користувачів.

Список літератури

1. Lal N. A., Prasad S., Farik M. A Review of Authentication Methods. *International Journal of Scientific & Technology Research*. 2016. Vol. 5, No. 11. P. 246–249. URL: https://www.researchgate.net/publication/311514269_A_Review_Of_Authentication_Methods
2. Arévalo-Ancona R. E., Cedillo-Hernandez M., Ramirez-Rodriguez A. E., Nakano-Miyatake M., Perez-Meana H. Secure Medical Image Authentication Using Zero-Watermarking Based on Deep Learning Context Encoder. *Computación y Sistemas*. 2024. Vol. 28, No. 1. P. 199–210. DOI: 10.13053/cys-28-1-4898
3. Seenivasagam V., Velumani R. A QR Code Based Zero-Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud. *Computational and Mathematical Methods in Medicine*. 2013. Article ID 516465. 10 p. DOI: 10.1155/2013/516465
4. Chapple M. *Implementing Access Control Systems*. Indiana (USA): Wiley, 2020. P. 110–135.
5. Айко О. В., Василенко О. Д., Степаненко В. М. Системи автоматизації контролю доступу на об’єкти. *Всеукраїнська науково-практична конференція студентів, аспірантів та молодих вчених*. 2023. P. 106–108. URL: https://ela.kpi.ua/server/api/core/bitstreams/e4de99d9-a572-452d-8194-3ba4a39f5bb4/content
6. Qi X., Liu Y. Cloud Model Based Zero-Watermarking Algorithm for Authentication of Text Document. *Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security* (Emeishan, China, 2013). 2013. P. 712–715. DOI: 10.1109/CIS.2013.15
7. Hasan B. M. S., Ameen S. Y., Hasan O. M. Image Authentication Based on Watermarking Approach: Review. *Asian Journal of Research in Computer Science And Information Technology*. 2021. Vol. 9, No. 3. P. 34–51. DOI: 10.9734/AJRCOS/2021/v9i330224
8. Arévalo-Ancona, R. E., Cedillo-Hernández, M., Ramírez-Rodríguez, A. E., Nakano-Miyatake, M., Pérez-Meana, H. Secure Medical Image Authentication Using Zero-Watermarking Based on Deep Learning Context Encoder. *Computación y Sistemas*. 2024. Vol. 28, No. 1 P. 199–210. DOI: 10.13053/CyS-28-1-4898
9. Seenivasagam V., Velumani R. A QR Code Based Zero-Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud. *Computational and Mathematical Methods in Medicine*. 2013. Vol. 2013, Article ID 516465, 16 p. DOI: 10.1155/2013/516465
10. Tayan O., Kabir M. N., Alginahi Y. M. A Hybrid Digital-Signature and Zero-Watermarking Approach for Authentication and Protection of Sensitive Electronic Documents. *The Scientific World Journal*. 2014. Article ID 514652. 10 p. DOI: 10.1155/2014/514652
11. Поддубний В., Сєвєрінов О., Непокритов Д. Дослідження ефективності алгоритмів оброблення зображень у схемах нульових водяних знаків. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 1(31). С. 102–114. DOI: 10.30837/2522-9818.2025.1.102
12. Поддубний В. О., Сєвєрінов О. В., Гвоздьов Р. Ю. Використання нульових водяних знаків для підтвердження авторства зображень та багатофакторної автентифікації. *Радіотехніка*. 2024. Вип. 218. С. 35–43. DOI: 10.30837/rt.2024.3.218.02
13. Poddubnyi V., Sievierinov O. Method of User Authentication in Information and Communication Systems Using Zero Watermark. *Innovative Technologies and Scientific Solutions for Industries*. 2025. № 2(32). P. 69–78. DOI: 10.30837/2522-9818.2025.2.069
14. Pal A., Mondal B., Bhattacharyya N., Ghosh S. Similarity in Fuzzy Systems. *Journal of Uncertainty Analysis and Applications*. 2014. Vol. 2. Article 18. DOI: 10.1186/s40467-014-0018-0
15. Altinkemer K., Wang T. Cost and Benefit Analysis of Authentication Systems. *Decision Support Systems*. 2011. Vol. 51, No. 3. P. 394–404. DOI: 10.1016/j.dss.2011.01.005
16. Phillips T. Usability and Security of Different Authentication Methods for an Electronic Health Records System. *Proceedings of the 14th International Conference on Health Informatics (HEALTHINF)*. 2021. 8 p. URL: https://www.academia.edu/125169716/Usability_and_Security_of_Different_Authentication_Methods_for_an_Electronic_Health_Records_System
17. Kruzikova A., Knapova L., Smahel D., Dedkova L., Matyas V. Usable and Secure? User Perception of Four Authentication Methods for Mobile Banking. *Computers & Security*. 2022. Vol. 115. Article 102603. DOI: 10.1016/j.cose.2022.102603

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 3 (33)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

18. Nadipally M. Optimization of Methods for Image-Texture Segmentation Using Ant Colony Optimization. In: *Intelligent Data-Centric Systems: Intelligent Data Analysis for Biomedical Applications*. Academic Press, 2019. Ch. 2. P. 21–47. DOI: 10.1016/B978-0-12-815553-0.00002-1

References

1. Lal, N.A., Prasad, S. Farik, M. (2016), "A review of authentication methods", *International Journal of Scientific & Technology Research*, Vol. 5, No. 11, P. 246–249. URL: https://www.researchgate.net/publication/311514269_A_Review_Of_Authentication_Methods
2. Arévalo-Ancona, R.E., Cedillo-Hernandez, M., Ramirez-Rodriguez, A.E., Nakano-Miyatake, M. Perez-Meana, H. (2024), "Secure medical image authentication using zero-watermarking based on deep learning context encoder", *Computación y Sistemas*, Vol. 28, No. 1, P. 199–210. DOI:10.13053/cys-28-1-4898
3. Seenivasagam, V. & Velumani, R. (2013), "A QR code based zero-watermarking scheme for authentication of medical images in teleradiology cloud", *Computational and Mathematical Methods in Medicine*, 2013, Article ID 516465, 10 p. DOI:10.1155/2013/516465
4. Chapple, M. (2020), *Implementing Access Control Systems*, Indiana (USA): Wiley, P. 110–135.
5. Aiko, O.V., Vasylenko, O.D. Stepanenko, V.M. (2023), "Systems for access control automation at facilities" ["Systemy avtomatyzatsii kontroliu dostupu na ob'yekty"], *Vseukrainska naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh*. P. 106-108. available at: https://ela.kpi.ua/server/api/core/bitstreams/e4de99d9-a572-452d-8194-3ba4a39f5bb4/content
6. Qi, X. Liu, Y. (2013), "Cloud model based zero-watermarking algorithm for authentication of text document", *Proceedings of the 2013 Ninth International Conference on Computational Intelligence and Security* (Emeishan, China), P. 712–715. DOI:10.1109/CIS.2013.15
7. Hasan, B.M.S., Ameen, S.Y. and Hasan, O.M. (2021), "Image Authentication Based on Watermarking Approach: Review", *Asian Journal of Research in Computer Science and Information Technology*, № 9(3), P. 34–51. DOI:10.9734/AJRCOS/2021/v9i330224
8. Arévalo-Ancona, R.E., Cedillo-Hernández, M., Ramírez-Rodríguez, A.E., Nakano-Miyatake, M. and Pérez-Meana, H. (2024), "Secure Medical Image Authentication Using Zero-Watermarking Based on Deep Learning Context Encoder", *Computación y Sistemas*, 28(1), P. 199–210. DOI:10.13053/CyS-28-1-4898
9. Seenivasagam, V. and Velumani, R. (2013), "A QR Code Based Zero-Watermarking Scheme for Authentication of Medical Images in Teleradiology Cloud", *Computational and Mathematical Methods in Medicine*, Article ID 516465, 16 p. DOI:10.1155/2013/516465
10. Tayan, O., Kabir, M.N. Alginahi, Y.M. (2014), "A hybrid digital-signature and zero-watermarking approach for authentication and protection of sensitive electronic documents", *The Scientific World Journal*, Article ID 514652, 10 p. DOI:10.1155/2014/514652
11. Poddubnyi, V., Sievierinov, O. & Nepokrytov, D. (2025), "Research of the effectiveness of image processing algorithms in zero-watermarking schemes", ["Doslidzhennia efektyvnosti alhorytmiv obroblennia zobrazhen u skhemakh nulovoho vodianoho znaka"], *Suchasnyi stan naukovykh doslidzhen ta tekhnolohii v promyslovosti*, No. 1(31), P. 102–114. DOI:10.30837/2522-9818.2025.1.102
12. Poddubnyi, V.O., Sievierinov, O.V. & Hvozdiov, R.Yu. (2024), "Using zero watermarks for image copyright protection and multifactor authentication" ["Vykorystannia nul′ovykh vodianykh znakiv dlia pidtverdzhennia avtorstva zobrazhen′ ta bahatofaktornoï avtentyfikatsii"], *Radiotekhnika*, Issue 218, P. 35–43. DOI:10.30837/rt.2024.3.218.02
13. Poddubnyi, V. Sievierinov, O. (2025), "Method of user authentication in information and communication s ystems using zero watermark", *Innovative Technologies and Scientific Solutions for Industries*, No. 2(32), P. 69–78. DOI:10.30837/2522-9818.2025.2.069
14. Pal, A., Mondal, B., Bhattacharyya, N. Ghosh, S. (2014), "Similarity in fuzzy systems", *Journal of Uncertainty Analysis and Applications*, Vol. 2, Article 18. DOI:10.1186/s40467-014-0018-0
15. Altinkemer, K. Wang, T. (2011), "Cost and benefit analysis of authentication systems", *Decision Support Systems*, Vol. 51, No. 3, P. 394–404. DOI: 10.1016/j.dss.2011.01.005
16. Phillips, T. (2021), "Usability and security of different authentication methods for an electronic health records system", *Proceedings of the 14th International Conference on Health Informatics (HEALTHINF)*. 8 p. available at: https://www.academia.edu/125169716/Usability_and_Security_of_Different_Authentication_Methods_for_an_Electronic_Health_Records_System

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 3 (33)*

17. Kruzikova, A., Knapova, L., Smahel, D., Dedkova, L. Matyas, V. (2022), "Usable and secure? User perception of four authentication methods for mobile banking", *Computers & Security*, Vol. 115, Article 102603. DOI: 10.1016/j.cose.2022.102603
18. Nadipally, M. (2019), "Optimization of methods for image-texture segmentation using ant colony optimization". In: *Intelligent Data-Centric Systems: Intelligent Data Analysis for Biomedical Applications*. Academic Press, Ch. 2, P. 21–47. DOI: 10.1016/B978-0-12-815553-0.00002-1

Надійшла (Received) 05.04.2025

Відомості про авторів / About the Authors

Поддубний Вадим Олександрович – аспірант, Харківський національний університет радіоелектроніки, кафедра безпеки інформаційних технологій, Харків, Україна; e-mail: vadym.poddubnyi@nure.ua; ORCID ID: https://orcid.org/0000-0002-4380-491X

Сєвєрінов Олександр Васильович – кандидат технічних наук, Харківський національний університет радіоелектроніки, доцент кафедри безпеки інформаційних технологій, Харків, Україна; e-mail: oleksandr.sievierinov@nure.ua; ORCID ID: https://orcid.org/0000-0002-6327-6405

Poddubnyi Vadym – PhD Student, Kharkiv National University of Radio Electronic, Department of Information Technology Security, Kharkiv, Ukraine.

Sievierinov Oleksandr – PhD (Engineering Sciences), Kharkiv National University of Radio Electronic, Associate Professor at the Department of Information Technology Security, Kharkiv, Ukraine.

USER AUTHENTICATION MODEL USING ZERO WATERMARKING BASED ON RGB IMAGES

The subject of the research is the methods and schemes of user authentication in information and communication networks. **The aim of the work** is to develop a user authentication model in information and communication systems using the zero-watermarking method based on RGB images. **Objectives**: to examine the main issues arising during the integration of access control systems; to develop a user authentication model using zero-watermarking; to study potential characteristics and put forward proposals/recommendations for its application in authentication; to construct graphical schemes that illustrate processes and procedures. **Methods used**: modeling methods and formal description methods. **Results achieved**: an improved user authentication model based on the zero-watermarking algorithm has been proposed as an alternative to existing authentication schemes in information and communication systems; its potential characteristics have been studied, confirming the prospects of the development; graphical representations of processes and procedures have been constructed. **Conclusions**: in the course of the work, the main problems faced by owners of information and communication systems during the integration of authentication systems were briefly reviewed; an improved authentication model using zero-watermarking was proposed. The zero-watermarking method is based on RGB images employing K-means clustering and DWT, while a password is used as the second factor. Three operating modes are presented: registration, authentication, and modification of key authentication data. This model serves as an alternative to existing schemes and can potentially reduce the cost of authentication, lower Type I and Type II error rates compared to similar authentication schemes, and improve the convenience of authentication in information and communication systems. It also expands the range of authentication schemes available to system owners during integration.

Keywords: digital watermarking; authentication; image; model; password.

Бібліографічні описи / Bibliographic descriptions

Поддубний В.О., Сєвєрінов О.В. Модель автентифікації користувачів з використанням нульового водяного знаку на основі RGB-зображень. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 3 (33). С. 102–110. DOI: https://doi.org/10.30837/2522-9818.2025.3.102

Poddubnyi, V., Sievierinov, O. (2025), "User authentication model using zero watermarking based on RGB images", *Innovative Technologies and Scientific Solutions for Industries*, No. 3 (33), P. 102–110. DOI: https://doi.org/10.30837/2522-9818.2025.3.102