Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

УДК 004.94
DOI: https://doi.org/10.30837/2522-9818.2025.2.069

В. Поддубний, О. Сєвєрінов

МЕТОД АВТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ІЗ ЗАСТОСУВАННЯМ НУЛЬОВОГО ВОДЯНОГО ЗНАКА

Предметом дослідження є системи контролю доступом в інформаційно-комунікаційних мережах. **Мета роботи** – розроблення методу автентифікації користувачів в інформаційно-комунікаційних мережах як системи контролю доступом з використанням нульового водяного знака. **Завдання:** розроблення методу автентифікації користувачів із застосуванням нульового водяного знака; тестування запропонованого методу; висування пропозицій та рекомендацій щодо подальшого впровадження методу автентифікації. Для виконання окреслених завдань використовувалися такі **методи**: комп'ютерне моделювання запропонованого методу для дослідження його характеристик; емпіричні методи – упровадження методу та спостереження за результатами перетворень; статистичні методи – обчислення показників нормальної кореляції та пікового значення сигнал / шум, коефіцієнтів Спірмена. **Досягнуті результати:** уперше запропоновано метод автентифікації користувачів в інформаційно-комунікаційній системі, оснований на унікальному алгоритмі нульового водяного знака; сформовано пропозиції щодо подальшого впровадження методу; протестовано розроблений метод. **Висновки.** У межах роботи запропоновано метод автентифікації, оснований на алгоритмі нульового водяного знака, для використання як системи контролю доступом на промислових підприємствах. Метод було протестовано, результати тестування доводять його роботоспроможність та ефективність. Запропонований метод потенційно може зменшити вартість двофакторної автентифікації в умовах розгортання систем автентифікації у великих підприємствах.

Ключові слова: системи контролю доступу; нульовий водяний знак; метод; автентифікація; зображення.

Вступ

Нульові водяні знаки – це технологія, що використовується для забезпечення авторства цифрових зображень. Проте новизна цієї технології зумовлює безліч проблем за умови їх практичного застосування. Так, наприклад, нульові водяні знаки наразі досить погано працюють у використанні в подібних зображеннях (зокрема в медицині) [1].

Одним із можливих варіантів застосування нульових водяних знаків є завдання автентифікації користувачів. Ця робота спрямована на демонстрацію методу нульового водяного знака для використання в схемі двофакторної автентифікації. Така схема будується на двох факторах, а саме: знання чогось (пароль), володіння чимось (зображення). Додатковим фактором є знання того, чи є фото основною інформацією, оскільки зловмисник не може чітко визначити ключову інформацію. Ця схема є експериментальною через досить обмежене вивчення нульових водяних знаків для автентифікації та потребує доопрацювання й подальшого дослідження алгоритмів і методів.

Запропонований метод може бути використаний у схемах автентифікації на промислових підприємствах для автентифікації користувачів як системи контролю доступом. Метод має деякі переваги порівняно з поширеними методами багатофакторної автентифікації, зокрема: відсутність персональної інформації (на відміну від біометрії), відсутність спеціальних токенів чи карток, використання як мінімум двох факторів, висока мобільність та зручність для користувача. Перелічені переваги роблять його більш дешевою альтернативою для автентифікації користувачів в інформаційно-комунікаційних системах.

Аналіз проблеми

У багатьох вимогах і практиках використання багатофакторної автентифікації (як мінімум двофакторної) необхідне для забезпечення надійного підтвердження особистостей користувачів. Так, наприклад, відповідно до наказу Адміністрації Держспецзв'язку від 24.06.2024 № 317 "Про визначення Базового профілю безпеки інформації", використання двофакторної автентифікації призначене для ідентифікації та автентифікації користувачів, які мають привілейовані облікові записи [2].

Стандарт IEC 62443, що встановлює вимоги промислової інформаційної безпеки, також рекомендує впровадження багатофакторної

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

автентифікації для підвищення рівня безпеки доступу користувачів [3].

Системи контролю доступом – необхідний елемент, що забезпечує автентифікацію користувачів для доступу до приміщень чи засобів. Системи контролю доступом необхідні, оскільки традиційні системи фізичного доступу вже не задовольняють вимоги з безпеки та контролю [4]. Великі підприємства зазвичай потребують більш складних і коштовних систем контролю доступу через значну кількість приміщень та персоналу. Особливо це актуально для впровадження двофакторної автентифікації [5]. Методи та схеми двофакторної автентифікації під час розгортання в промислових підприємствах зазвичай потребують виділення значної кількості фінансів та людських годин, оскільки постає необхідність додаткових засобів (сканерів біометрії, токенів, карток, адміністрування).

У роботі [6] запропоновано загальну схему автентифікації, основану на алгоритмі нульового водяного знака. Більш деталізований опис цієї схеми подано в праці [7]. Крім того, в ній проаналізовано перетворення цифрових зображень з метою їх використання в алгоритмах нульового водяного знака в процесі автентифікації. Одними з найкращих алгоритмів є, зокрема, *DWT* та *K-means*, тому було прийнято рішення використати *DWT* як перетворення першого рівня, а *K-means* – другого рівня.

Метод застосовує як контейнер RGB-зображення, що описано в роботі [8]. У цій праці описано метод цифрового знака та його використання.

Розроблення методу автентифікації із застосуванням нульового водяного знака є перспективним завданням у зв'язку з можливістю зниження вартості автентифікації користувачів на виробничих підприємствах, адже водяний знак не потребує спеціалізованих носіїв інформації чи спеціальних сканерів для її оброблення. Запропонований метод інтегрується в системи контролю доступом та призначений для автентифікації користувачів за умови їх доступу до контрольованих об'єктів.

Алгоритми оброблення цифрових зображень

Дискретне вейвлет-перетворення (DWT) – це вейвлет-перетворення, для якого вейвлети дискретно відбираються. Як і в інших вейвлет-перетвореннях, ключовою перевагою, на відміну від перетворення Фур'є, є часова роздільна здатність: воно фіксує як частоту, так і інформацію про місце розташування (місце розташування в часі).

DWT розділяє зображення на високочастотні та низькочастотні компоненти.

LL – низькочастотний піддіапазон, що використовується для подальших перетворень.

LH – піддіапазон, що виділяє горизонтальні особливості оригінального зображення.

HL – піддіапазон, що виділяє вертикальні особливості оригінального зображення.

HH – піддіапазон, що виділяє діагональні особливості оригінального зображення [7].

На рис. 1 показаний приклад перетворення *DWT* (перетворення Хаара) для монохромного зображення.

Рис. 1. Приклад перетворення Хаара

У статистиці та машинному навчанні кластеризація k-середніх – це метод кластерного аналізу, метою якого є розподілення n спостережень на k кластерів, у яких кожне спостереження належить до кластера з найближчим середнім.

Він подібний до алгоритму очікування-максимізації для сумішей Гаусса тим, що обидва вони намагаються знайти центри природних кластерів у даних, а також у підході ітераційного уточнення, який використовують ці алгоритми.

Алгоритм передбачає кілька кроків.

1. K точок розміщуються в просторі, що є об'єктами, які групуються. Ці точки – початкові центроїди групи.

2. Кожен об'єкт призначається до групи, яка має найближчий центроїд.

3. Коли всі об'єкти будуть призначені, перераховується положення K центроїдів.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

4. Повторюються кроки 2 і 3, доки центроїди не перестануть рухатися. Це призводить до поділу об'єктів на групи, з яких можна обчислити показник, що потрібно мінімізувати.

Приклад використання перетворення зображено на рис. 2 [10].

Рис. 2. Приклад перетворення *K-means*

Опис методу

Наведемо порядок формування водяного знака (W).

1. Користувач має в розпорядженні зображення (O) та пароль $(PASS)$.

2. Алгоритм нульового знака отримує зображення в цифровому вигляді та пароль.

3. Зображення (O) розкладається на спектри, отримуючи зображення $(O_r,\ O_g,\ O_b)$. Ці зображення є матрицями значень пікселів від 0 до 255.

4. Після розкладання зображення $(O_r,\ O_g,\ O_b)$ підлягають перетворенню *DWT* (як представник *DWT*-перетворень використовується перетворення Хаара). Перетворення здійснюється поблоково для блоків 8×8. Перетворення *DWT* формує набір значень: LL, LH, HL, HH, з яких використовується лише LL (формуючи для кожного спектра LL_r, LL_g, LL_b).

5. Для кожного LL_r, LL_g, LL_b виконується перетворення *K-means*, формуючи, відповідно, K_r, K_g, K_b. Параметри перетворення *K-means*: кількість кластерів – 5, толерантність – 0.05.

6. Паралельно відбувається формування матриці з паролем, для цього пароль *PASS* перетворюється за допомогою функції гешування *SHA*512, формуючи геш H_{pass}.

7. Геш H_{pass} записується у вигляді вектора з 64 значень V_h.

8. Вектор V_h записується 64 рази, формуючи матрицю $Matrix_{pass}$. Отримана матриця має розмір 64×64.

9. Матриця $Matrix_{pass}$ перемножується поблоково (розмір блоку становить) на матриці K_r, K_g, K_b, формуючи M_r, M_g, M_b.

10. Формується параметр b для *Swish*-перетворення, значення формується з байтів гешу H_{pass}. Для цього обирається 10, 20, 30 та 40-й байт, формуючи цим значення int, $\left(\left(int/int_{max}\right)+1\right)\cdot10$.

11. Для кожного значення з матриць M_r, M_g, M_b виконується *Swish*-перетворення, унаслідок чого формуються S_r, S_g, S_b.

12. S_r, S_g, S_b додаються, формуючи кінцеву матрицю W.

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Цей водяний знак зберігається в базі даних системи контролю доступом як "еталонне значення", з яким відбуваються порівняння під час автентифікації. Тобто формування водяного знака – це реєстрація користувача в системі. У подальшому під час повторної авторизації користувач проходить процедуру формування водяного знака з наданими параметрами (пароль і зображення), а система контролю доступом порівнює цей водяний знак з еталонним.

Для підвищення швидкості перевірки можна окремо перевіряти геш-значення паролю, оскільки швидкість формування функції гешу значно вища, ніж швидкість роботи алгоритму нульового водяного знака. Проте в такому разі необхідно використовувати інший алгоритм гешування, що різниться від *SHA*-512, оскільки компрометація гешу зменшить стійкість методу (тому що зловмисник буде знати коефіцієнти *Swish* -перетворення).

На рис. 3 зображена загальна схема роботи методу автентифікації з використанням алгоритму нульового водяного знака.

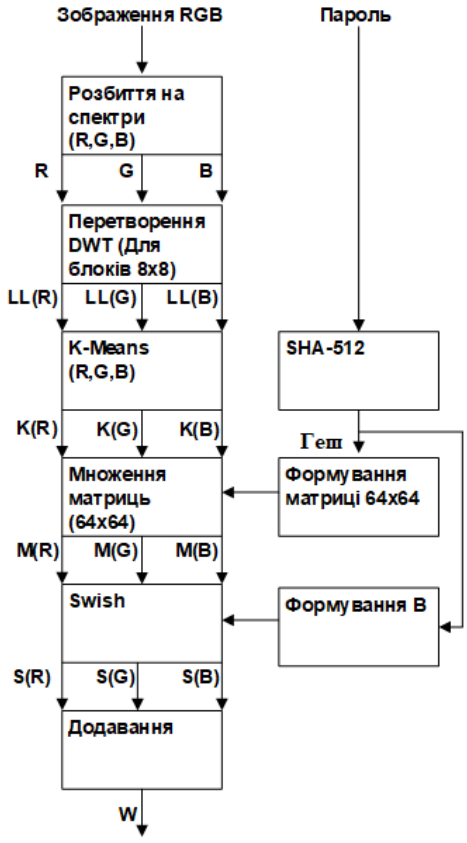

Рис. 3. Схема роботи методу автентифікації з використанням нульового водяного знака

У методі застосовано -функцію, що описується виразом

$$F(x)=\frac{x}{1+e^{-bx}}, \qquad (1)$$

де b – константа або параметр, який залежить від типу моделі. У запропонованому методі цей параметр здається частиною геш-значення.

У методі автентифікації це перетворення виконує функцію згладжування різких змін параметрів зображення. Також *Swish* виконує роль ускладнення оберненості методу внаслідок того, що пошук оберненої функції $\left(F(x)'\right)$ є в декілька разів складнішим завданням, оскільки потребує знаходження похідної або обчислення значень для кожного x та b. Ці значення формуються з гешу паролю, роблячи метод більш залежним до його змін [11].

Тестування

Для тестування методу використано такі метрики:

– нормальна кореляція (коефіцієнт Пірсона);

– коефіцієнт Спірмена.

Кореляція Пірсона (або *NCC*) – це статистичний метод, що застосовується для вимірювання ступеня зв'язку (нормальної кореляції) між двома наборами змінних. Кореляція Пірсона описується такою формулою [12]:

$$r=\frac{\sum_{i=1}^{i}(x_i-\bar{x})(y_i-\bar{y})}{\sqrt{\sum_{i=1}^{i}(x_i-\bar{x})^2}\sqrt{\sum_{i=1}^{i}(y_i-\bar{y})^2}}, \qquad (2)$$

де x, y – елементи наборів, що порівнюються;

$\bar{x}$, $\bar{y}$ – середні значення наборів даних.

Значення r перебуває в діапазоні від –1 до 1. Що ближче значення до 0, то менша подібність наборів даних (відсутність лінійної кореляції). За умови $r=1$ – ідеальна позитивна кореляція, якщо $r=-1$ – ідеальна негативна кореляція.

Коефіцієнт Спірмена – непараметрична міра статистичної залежності між двома змінними, що оцінює, наскільки добре взаємозв'язок між ними може бути описаний монотонною функцією. Коефіцієнт Спірмена для набору даних визначається як [11]

$$p=1-\frac{6\sum_{i=1}^{n}(x_i-y_i)^2}{n\left(n^2-1\right)}, \qquad (3)$$

де n – кількість пар спостережень;

x, y – ранги змінних, що порівнюються.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

Значення p перебувають у діапазоні від –1 до 1. Що ближче значення p до 1, то більша залежність між наборами даних. Якщо $p=1$ – ідеальна монотонна залежність.

Результатом роботи методу є матриця значень. Для оцінювання схожості двох матриць використовується така формула:

$$p_w = p_{row} \cdot p_{col}, \quad (4)$$

де p_{row} – коефіцієнт Спірмена для рядків;

p_{col} – коефіцієнт Спірмена для стовпців.

Коефіцієнт *pcol* обчислюється як

$$p_{col} = \sum_{1}^{l}\left(1-\frac{6\sum_{i=1}^{n}(x_i-y_i)^2}{n\left(n^2-1\right)}\right), \quad (5)$$

де l – кількість стовпців.

Тобто обчислюється сума коефіцієнтів для кожного рядка матриці x та y. Аналогічним чином обчислюється *prow:*

$$p_{row} = \sum_{1}^{m}\left(1-\frac{6\sum_{i-1}^{n}(x_i-y_i)^2}{n\left(n^2-1\right)}\right), \quad (6)$$

де m – кількість рядків.

Для тестування методу автентифікації за допомогою нульового знака було обрано 50 зображень 256×256 пікселів, 50 зображень 512×512 пікселів, 50 зображень 1280×1280 пікселів [14–16].

Зображення для тестування деформувалися програмним чином за допомогою

– кристалізації (розмір кристала $=4$);

– гауссового розмиття $(sigma=3)$;

– додавання шуму (випадкове значення в діапазоні яскравості пікселя $+25/-25$);

– додавання тексту (текст різного кольору, масштабований залежно від розміру зображення).

Приклад спотворення зображення показано на рис. 4.

Рис. 4. Приклад спотворення зображення

Між оригінальним і спотвореним зображенням були виміряні показники *NCC* та *PSTR* [17]. На рис. 5 наведений графік показників *PSTR* для зображень 512×512 пікселів.

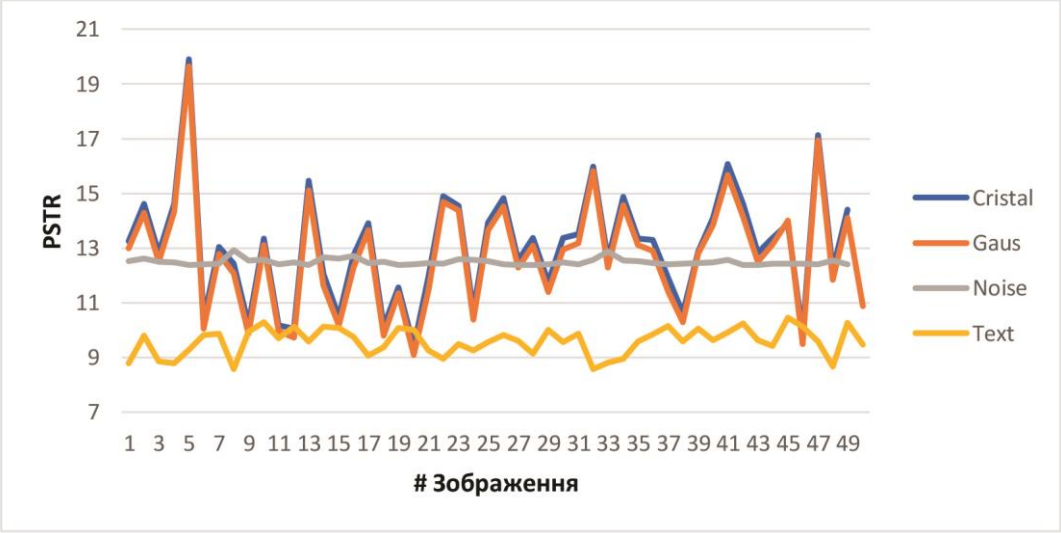

Рис. 5. Графік *PSTR* для спотворених зображень

ISSN 2522-9818 (print)
ISSN 2524-2296 (online)
Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

Як можна побачити, вимірювання проводилися на зображеннях, спотворених в одному діапазоні значень. Це було здійснено з метою переконатися в роботоспроможності методу на різних типах зображень і на різних типах спотворень, адже навіть за умови однакового рівня та методу словотворення різні зображення спотворюються по-різному. Найбільш рівномірний графік для шуму, оскільки шум додається до кожного пікселя залежно від сусідніх пікселів та яскравості самого пікселя. Найбільш нестабільним (таким, чиї показники варіюються в більшому діапазоні) видом спотворення є кристалізація та гауссове розмиття, оскільки за цих видів спотворення відбуваються зміни на основі груп пікселів на зображенні.

Тестування відбувалося способом порівняння результату формування водяного знака для оригінального й спотвореного зображення. Як пароль використовувалося значення "1111".

Тестування відбувалося в такому порядку:

– формувалися водяні знаки для оригінального зображення $[W_o]$;

– формувалися водяні знаки для спотворених зображень $[W_d]$;

– перевірялися водяні знаки W_o та W_d за допомогою коефіцієнта Спірмена та Пірсона.

Загалом було сформовано 150 оригінальних водяних знаків та 600 спотворених.

Після цього випадково обрані зображення Wx_o з $[W_o]$ було порівняно з іншими $[W_o]$ з метою перевірки спроможності водяного знака розрізняти неоднакові зображення.

В описаному методі автентифікація успішна, якщо водяний знак з певною достовірністю ідентичний еталонному водяному знаку, що зберігається в системі контролю доступом. Цей коефіцієнт встановлюється залежно від наявних шумів в інформаційно-комунікаційній системі та ступеня довіри, необхідному власникам.

Після проведення попередніх тестів визначено "коефіцієнт достовірності" – суму значень коефіцієнтів Пірсона та Спірмена, коли прийнято вважати, що водяний знак достовірний. Обране значення коефіцієнта становило 1.4, процедура вибору полягала в порівнянні результатів перевірок зображень і знаходженні параметра, за якого зберігається оптимальна відповідність між помилками першого та другого роду. Тобто для системи із середнім шумом $PSTR$=13 всі значення, менші за 1.4, відкидаються як недостовірні (зображення надто пошкоджені, або подано інше зображення). За такого сценарію автентифікація є невдалою, користувач не пройшов перевірку. Якщо значення вище ніж 1.4 – автентифікація успішна, користувач пройшов перевірку.

Цей коефіцієнт може встановлюватися залежно від системи. Що він вищий, то меншу кількість шумів може ігнорувати водяний знак, то менша кількість помилок другого роду та більша першого роду. Що вищий коефіцієнт, то більшу кількість шумів може ігнорувати метод, то менша кількість помилок першого роду та більша другого роду.

У системах без виникнення шумів цей коефіцієнт може дорівнювати сумі максимального значення коефіцієнтів Пірсона та Спірмена – 2.0.

У табл. 2 наведені результати тестувань, а саме скільки зображень пройшли поріг, що встановлює "коефіцієнт достовірності". Останній стовпець таблиці подає відомості про перевірку методу між зображенням Wx_o та набором $[W_o]$ з метою виявлення здатності методу розрізняти неоднакові зображення (автентифікація з хибними параметрами).

Таблиця 1. *Результати тестувань*

Розмір зображення	**Кристалізація**	**Гауссове розмиття**	**Шум**	**Додавання тексту**	**Порівняння випадкового Wx_o з набором $[W_o]$**
256×256	100%	100%	100%	92%	0%
512×512	98%	100%	98%	92%	0%
1280×1280	100%	100%	100%	100%	0%

Як можна побачити, метод має досить високу стійкість до пошкоджень, до того ж не втрачає здібності розрізняти зображення (навіть схожі) один від одного. Найменший показник проходження тесту під час модифікації "додавання тексту". Це пов’язано з типом шумів, що генерує спотворення.

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

На рис. 6 подано графік "коефіцієнта достовірності" для зображення розміром 512×512 із спотворенням "кристалізація". Як можна побачити, одне зображення не пройшло перевірку, тобто його структура була надто пошкоджена.

На рис. 7 продемонстровано графік "коефіцієнта достовірності" для перевірки між різними зображеннями для зображення розміром 512×512. Як можна побачити, жодне зображення не пройшло перевірку.

Рис. 6. Результати тестування для зображення розміром 512×512 з типом пошкодження "кристалізація"

Рис. 7. Результати тестування для зображення розміром 512×512 для перевірки зображень

Висновки

У роботі запропоновано метод автентифікації користувачів з використанням нульового водяного знака, основаного на перетворенні Хаара та *K-means*. У цьому методі також застосовується *Switch* -функція та функція гешування *SHA*-512.

Метод протестовано на неоднакових зображеннях з різними типами шуму, характеристиками та роздільною здатністю. Запропонований метод автентифікації на основі нульового водяного знака має певну стійкість до пошкоджень і водночас може розрізнити неоднакові зображення або схожі одне на одного (оскільки ми можемо встановити порогове значення

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)

достовірності). За умови встановлення значення коефіцієнта достовірності 1.4 в процесі тестувань 600 зображень з рівнем шуму від 9 до 20 PSTR метод успішно розпізнав 98.3% зображень (лише 1.7% зображень пошкоджено настільки, що користувач не пройшов автентифікацію з правильними атрибутами доступу). Під час тестування подібності між зображеннями (150 перевірок) метод успішно розпізнав 0% зображень (тобто жоден користувач не автентифікувався з хибними атрибутами доступу).

Метод призначений для застосування в мережах для двофакторної автентифікації, найкраще його впроваджувати в мережах промисловості (*Industry* 4.0) для автентифікації користувачів (у системах контролю доступом), оскільки цей метод стійкий до шумів та спотворень. Застосування запропонованого методу є більш дешевим, ніж упровадження методів автентифікації за допомогою біометричних даних чи автентифікації за допомогою токенів або смарт-карток, оскільки не потребує спеціалізованого обладнання. Порівняно з автентифікацію з використанням біометричних даних, перевагою є також те, що ключова інформація модифікована й не є чутливою, що містить персональні дані. Додатковою перевагою методу вважаємо те, що зловмисник не може напряму визначити, чи є зображення X ключовими даними, чи ні. Це робить метод більш стійким, на відміну від використанням QR-кодів.

Оскільки запропонований метод є досить новим, то потребує більшого тестування на значній кількості статистичної інформації та детального криптоаналізу.

Список літератури

1. Roček A., Javorník M., Slavíček K. et al. Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging. *Journal of Digital Imaging*. 2021. Vol. 34. P. 204–211. DOI: 10.1007/s10278-020-00396-0
2. Адміністрація Держспецзв'язку. Про визначення Базового профілю безпеки інформації: Наказ від 24.06.2024 № 317. URL: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-24-06-2024-317-pro-viznachennya-bazovogo-profilyu-bezpeki-informaciyi
3. Міжнародна електротехнічна комісія. EN IEC 62443. Security for industrial automation and control systems URL: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
4. ChappleM., Implementing Access Control Systems, Indiana, USA, 2020, P. 110-135. URL: https://eforum.lntu.edu.ua/index.php/jurnal/article/download/1506/1433/
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* URL: https://ela.kpi.ua/server/api/core/bitstreams/e4de99d9-a572-452d-8194-3ba4a39f5bb4/content
6. 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: https://doi.org/10.30837/rt.2024.3.218.02
7. Поддубний В., Сєвєрінов О., Непокритов Д. Дослідження ефективності алгоритмів оброблення зображень у схемах нульового водяного знака. Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 1(31). С. 102–114. DOI: 10.30837/2522-9818.2025.1.102
8. Poddubnyi V., Gvozdov R., Sievierinov O., Sukhoteplyi V., Bulba S., Lysytsia D. A Zero-Watermarking Algorithm for Use in RGB and Monochrome Images. 2024 *IEEE 5th KhPI Week on Advanced Technology (KhPIWeek)*. P. 1–5. DOI: https://doi.org/10.1109/KhPIWeek61434.2024.10878081.
9. Sethi N., Krishna R., Arora R.P. Image Compression Using Haar Wavelet Transform. Computer Engineering and Intelligent Systems. Vol. 2, No. 3. URL: https://scispace.com/pdf/image-compression-using-haar-wavelet-transform-1q7fxnv973.pdf
10. Accord.NET Framework. KMeans Class URL: http://accord-framework.net/docs/html/T_Accord_MachineLearning_KMeans.htm
11. Ramachandran P., Zoph B., Le Q.V. Swish: A Self-Gated Activation Function. URL: https://arxiv.org/pdf/1710.05941v1.pdf.
12. Berman J. J. Data Simplification. Chapter 4 - Understanding Your Data. 2016. P. 135–187. ISBN 9780128037812
13. McClenaghan E. Spearman Rank Correlation. Technology Networks. 2024. URL: https://www.technologynetworks.com/tn/articles/spearman-rank-correlation-385744
14. The USC-SIPI Image Database URL: https://sipi.usc.edu/database/

Сучасний стан наукових досліджень та технологій в промисловості. 2025. № 2 (32)
ISSN 2522-9818 (print)
ISSN 2524-2296 (online)

15. Nasa Image and Video Library URL: https://images.nasa.gov/
16. Lorem Picsum URL: https://picsum.photos/
17. Nadipally M. Optimization of Methods for Image-Texture Segmentation Using Ant Colony Optimization. *Intelligent Data-Centric Systems: Intelligent Data Analysis for Biomedical Applications*. Academic Press, 2019. Ch. 2. 2019. P. 21–47. DOI:10.1016/B978-0-12-815553-0.00002-1

References

1. Roček, A., Javorník, M., Slavíček, K. et al. (2021), "Zero Watermarking: Critical Analysis of Its Role in Current Medical Imaging", *Journal of Digital Imaging*, Vol. 34, P. 204–211. DOI: 10.1007/s10278-020-00396-0
2. "State Special Communications Service Administration" (2024), *Order on the definition of the Basic information security profile: Order No. 317 dated 24.06.2024* ["Administratsiia Derzhspetszviazku. Pro vyznachennia Bazovoho profiliu bezpeky informatsii: Nakaz vid 24.06.2024 № 317"]. available at: https://cip.gov.ua/ua/docs/nakaz-administraciyi-derzhspeczv-yazku-vid-24-06-2024-317-pro-viznachennya-bazovogo-profilyu-bezpeki-informaciyi
3. "International Electrotechnical Commission (n.d.)", *EN IEC 62443. Security for industrial automation and control systems*. [Online]. available at: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
4. "ChappleM., Implementing Access Control Systems", Indiana, USA, 2020, P. 110-135. available at: https://eforum.lntu.edu.ua/index.php/jurnal/article/download/1506/1433/
5. Aiko, O.V., Vasylenko, O.D., Stepanenko, V.M. "Systems for Access Control Automation at Facilities", *All-Ukrainian Scientific and Practical Conference of Students, Postgraduates and Young Scientists* ["Systemy avtomatyzatsii kontroliu dostupu na ob'yekty. Vseukrainska naukovo-praktychna konferentsiia studentiv, aspirantiv ta molodykh vchenykh"]. available at: https://ela.kpi.ua/server/api/core/bitstreams/e4de99d9-a572-452d-8194-3ba4a39f5bb4/content
6. Poddubnyi, V.O., Sievierinov, O.V., Hvozdiov, R.Y. (2024), "Using Zero Watermarks for Image Authorship and Multifactor Authentication", *Radiotekhnika*, No. 218, P. 35–43. DOI: https://doi.org/10.30837/rt.2024.3.218.02
7. Poddubnyi, V., Sievierinov, O., Nepokrytyov, D. (2025), "Efficiency Study of Image Processing Algorithms in Zero Watermarking Schemes", *Modern State of Scientific Research and Technologies in Industry* ["Suchasnyi stan naukovykh doslidzhen ta tekhnolohii v promyslovosti"], No. 1(31), P. 102–114. DOI: 10.30837/2522-9818.2025.1.102
8. Poddubnyi, V., Gvozdov, R., Sievierinov, O., Sukhoteplyi, V., Bulba, S., Lysytsia, D. (2024), "A Zero-Watermarking Algorithm for Use in RGB and Monochrome Images", *2024 IEEE 5th KhPI Week on Advanced Technology (KhPIWeek)*, P. 1–5. DOI: https://doi.org/10.1109/KhPIWeek61434.2024.10878081
9. Sethi, N., Krishna, R., Arora, R.P. "Image Compression Using Haar Wavelet Transform", *Computer Engineering and Intelligent Systems*, Vol. 2, No. 3. available at: https://scispace.com/pdf/image-compression-using-haar-wavelet-transform-1q7fxnv973.pdf
10. "Accord.NET Framework", *KMeans Class*. available at: http://accord-framework.net/docs/html/T_Accord_MachineLearning_KMeans.htm
11. Ramachandran, P., Zoph, B., Le, Q.V. "*Swish: A Self-Gated Activation Function*". 2017. available at: https://arxiv.org/pdf/1710.05941v1.pdf
12. Berman, J.J. (2016), "*Data Simplification. Chapter 4 Understanding Your Data*", P. 135–187. ISBN 9780128037812
13. McClenaghan, E. (2024), "Spearman Rank Correlation", *Technology Networks*. available at: https://www.technologynetworks.com/tn/articles/spearman-rank-correlation-385744
14. "University of Southern California, *The USC-SIPI Image Database*". available at: https://sipi.usc.edu/database/
15. NASA (n.d.), *NASA Image and Video Library*. [Online]. Available at: https://images.nasa.gov/
16. Lorem Picsum, "*Free Placeholder Image Service*". available at: https://picsum.photos/
17. Nadipally, M. (2019), "Optimization of Methods for Image-Texture Segmentation Using Ant Colony Optimization", *Intelligent Data-Centric Systems: Intelligent Data Analysis for Biomedical Applications*, Academic Press, Ch. 2, P. 21–47.

Надійшла (Received) 13.04.2025

ISSN 2522-9818 (print)
ISSN 2524-2296 (online) *Innovative technologies and scientific solutions for industries. 2025. No. 2 (32)*

Відомості про авторів / About the Authors

Поддубний Вадим Олександрович – Харківський національний університет радіоелектроніки, аспірант кафедри 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 – Kharkiv National University of Radio Electronic, PhD Student at the 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.

METHOD OF USER AUTHENTICATION IN INFORMATION AND COMMUNICATION SYSTEMS USING ZERO WATERMARK

The subject access control systems is information and communication networks. **The purpose** is to develop a user authentication method for information and communication systems as an access control system using a zero watermarking algorithm. **Objectivs**: develop a user authentication method based on zero watermarking, test the proposed method, provide suggestions and recommendations for the further application of the authentication method. To accomplish the defined tasks, the following **methods** computer simulation of the proposed method to study its characteristics; empirical methods – applying the method and observing the transformation results; tatistical methods – calculating indicators such as Pearson correlation coefficients, peak signal-to-noise ratio (PSNR), and Spearman's rank correlation coefficients. **Results achieved**: novel user authentication method based on a unique zero watermarking algorithm was proposed for the first time within an information and communication system. Suggestions for further application of the method were formulated, and the method was successfully tested. **Conclusions.** During the study, an authentication method based on a zero watermarking algorithm was proposed, designed to be used as an access control system at industrial enterprises. The method was tested, and the test results confirm its operability and effectiveness. This method has the potential to reduce the cost of two-factor authentication when deploying authentication systems in large enterprises.

Keywords: ccess control systems; zero watermarking; method; authentication; image.

Бібліографічні описи / Bibliographic descriptions

Поддубний В. О., Сєвєрінов О. В., Метод автентифікації користувачів в інформаційно-комунікаційних системах із застосуванням нульового водяного знака. *Сучасний стан наукових досліджень та технологій в промисловості*. 2025. № 2 (32). С. 69–78. DOI: https://doi.org/10.30837/2522-9818.2025.2.069

Poddubnyi, V., Sievierinov, O. (2025), "Method of user authentication in information and communication systems using zero watermark", *Innovative Technologies and Scientific Solutions for Industries*, No. 2 (32), P. 69–78. DOI: https://doi.org/10.30837/2522-9818.2025.2.069