Метою роботи є розробка комбінованого стеганографічного методу для захисту авторського права на цифрові зображення з застосуванням ЦВЗ, стійкого до стиснення.

В основі розробленого методу лежить комбінований підхід DWT-SVD як найбільш збалансований інструмент, що забезпечує одночасну візуальну невидимість (прозорість) вбудованого водяного знаку та його робастність (стійкість) до атак стиснення. Алгоритм вбудовування передбачає перехід зображення-контейнера в колірний простір YCbCr, де модифікації піддається лише канал яскравості (Y). До цього каналу застосовується дискретне вейвлет-перетворення на базі фільтра Хаара, що дозволяє виділити низькочастотну область апроксимації (LL), яка містить основну енергетичну складову зображення. Паралельно з цим, авторський водяний знак (логотип) піддається криптографічному скремблюванню за допомогою хаотичного перетворення Арнольда. Це перетворює впізнаваний підпис на візуальний шум, який неможливо відновити без знання секретного ключа. Математичне ядро системи реалізує модифікацію сингулярних чисел матриці LL-піддіапазону контейнера шляхом додавання до них сингулярних чисел зашифрованого знаку з певним коефіцієнтом інтенсивності α. Для реалізації «напівсліпої» схеми вилучення програма автоматично генерує та зберігає файл матричних ключів формату .npz. Це дозволяє проводити верифікацію авторства без наявності оригінального зображення, використовуючи лише захищене фото та збережені ортогональні матриці.

Експериментальні дані розробленого методу підтвердили його високу ефективність. PSNR = 41,8 дБ, що свідчить про ідеальну візуальну стійкість вбудованого ЦВЗ. Тестування на робастність продемонструвало, що водяний знак зберігає свою структуру та залишається впізнаваним після агресивного стиснення JPEG з фактором якості до 20%.

1. Мокін В. Б., Капшук О. В. Методи та засоби стеганографічного захисту інформації : монографія. Вінниця : ВНТУ, 2021. 180 с. URL: https://ir.lib.vntu.edu.ua/

Розробка безпечної системи таємного голосування

УДК 004.056.5

Володимир Гудиш [1], Валерій Трушевський [2]

Львівський національний університет імені Івана Франка, [1]volodymyr.hudysh@lnu.edu.ua, [2]valeriy.trushevsky@lnu.edu.ua

Голосування є ключовим механізмом народного волевиявлення в демократичному суспільстві. Проте сучасні виклики, зокрема пандемія COVID-19, повномасштабне збройне вторгнення Росії в Україну та вимушена міграція мільйонів громадян як всередині країни, так і за кордон, унеможливили або суттєво ускладнили участь у традиційному виборчому процесі. Ці обставини актуалізували запит на системи дистанційного електронного голосування як засіб забезпечення конституційного права на волевиявлення за будь-яких умов.

Більшість наявних рішень змушені балансувати між конкуруючими вимогами. Традиційні паперові системи не забезпечують математично доведеної верифікованості результатів, а процес підрахунку голосів залишається непрозорим для незалежних спостерігачів. Сучасна криптографія виборів демонструє фундаментальну напругу між верифікованістю результатів та захистом від примусу [6]: системи, що ставлять абсолютний пріоритет на верифікованості, як правило, надають виборцю докази, якими може скористатися зловмисник або роботодавець. Водночас повне усунення будь-якої верифікованості перетворює криптографію на "чорну скриньку", якій виборець змушений сліпо довіряти. Тому завданням є не вибір одного з полюсів, а свідоме позиціювання на цьому спектрі: досягнення достатнього рівня верифікованості при одночасному збереженні анонімності та недопущенні можливості довести конкретний вибір виборця стороннім особам.

З метою вирішення зазначених проблем розроблено безпечну систему таємного голосування, яка забезпечує анонімність виборця, верифікованість результатів та захист від широкого спектру криптографічних і мережевих атак без необхідності довіряти будь-якому окремому компоненту системи. Запропоновано та реалізовано систему з елементами підходу Zero Trust, що поєднує: гомоморфне шифрування ElGamal на еліптичній кривій SECP256R1 [1] для агрегації голосів без розшифрування; три незалежні рівні доказів з нульовим розголошенням (ZKP): диз'юнктивний OR-доказ коректності голосу, Sum-доказ одиничного вектора бюлетеня [9] та доказ коректності дешифрування Чаума–Педерсена [2]; сліпі підписи за RFC 9474 (RSABSSA-SHA384-PSS-Randomized) [3] для унеможливлення зв'язування виборця з бюлетенем; порогове дешифрування за схемою Шаміра (2-з-3) [4] із захистом ключових часток у HashiCorp Vault з шифруванням Fernet [7]; а також окремий клієнтський застосунок із вбудованим Tor для анонімної маршрутизації трафіку.

Система складається з трьох незалежних серверів та клієнтського застосунку. *Main Server* (Python/Flask) відповідає за автентифікацію виборців і ведення публічного Bulletin Board. *Validator Server* (TypeScript/Node.js, бібліотека @cloudflare/blindrsa-ts) верифікує право голосу та видає сліпий підпис, не маючи змоги асоціювати його з конкретним виборцем. *Election Agency* (Python/Flask) верифікує ZKP-докази і сліпий підпис та публікує агреговані результати. Клієнтський застосунок (Python/customtkinter) надсилає бюлетень безпосередньо до Election Agency через Tor (.onion-адреса) [8], повністю виключаючи Main Server з ланцюжка передачі голосу.

Бюлетень формується як unit vector — масив шифротекстів ElGamal, де кожна позиція містить зашифроване значення 0 або 1. Sum-доказ гарантує, що сума елементів вектора дорівнює рівно 1 [9]. Tracking Code, що є хешем SHA-384 від JSON-об'єкта бюлетеня, обчислюється на стороні клієнта і публікується на Bulletin Board: виборець у будь-який момент може переконатися у врахуванні свого голосу (Individual Verifiability). На етапі підрахунку Election Agency виконує гомоморфне додавання шифротекстів окремо для кожного кандидата, збирає частки приватного ключа з двох серверів і розшифровує агреговані суми. Для кожного кандидата публікується Decryption Proof — доказ рівності

дискретних логарифмів (Чаум–Педерсен) [2], що підтверджує коректне використання приватного ключа. Будь-який аудитор може самостійно відтворити агрегацію з Bulletin Board і верифікувати кожен доказ без знання приватного ключа (Universal Verifiability).

Усі сервери функціонують за протоколом HTTPS. Реєстрація виборців захищена підтвердженням електронної пошти та CAPTCHA. Передбачено rate limiting для захисту від DoS-атак. Схема 2-з-3 за Шаміром із зберіганням часток у HashiCorp Vault [7] унеможливлює компрометацію ключа при доступі до одного сервера.

Розроблена система реалізує ключові складові End-to-End Verifiability — Individual Verifiability та Universal Verifiability: виборець підтверджує врахування голосу через Tracking Code і Bulletin Board; математика гарантує чесність розшифрування через Chaum–Pedersen Decryption Proof [2, 5]. Застосування мережі Tor та сліпих підписів RFC 9474 [3] забезпечує анонімність виборця навіть за умови компрометації окремих вузлів інфраструктури.

1. National Institute of Standards and Technology. Digital Signature Standard (DSS). FIPS PUB 186-5. NIST, 2023. 36 p.
2. Chaum D., Pedersen T. Wallet databases with observers. CRYPTO 1992. Lecture Notes in Computer Science, vol. 740. – Springer, 1993. – P. 89–105.
3. Denis F. et al. RFC 9474: RSA Blind Signatures. – IETF, 2023. URL: https://www.rfc-editor.org/rfc/rfc9474 (дата звернення: 01.05.2026).
4. Shamir A. How to share a secret. Communications of the ACM. – 1979. – Vol. 22, №11. – P. 612–613.
5. Cortier V., Galindo D., Glondu S., Izabachène M. Election verifiability for Helios under weaker trust assumptions. ESORICS 2014. Lecture Notes in Computer Science, vol. 8713. – Springer, 2014. – P. 347–364.
6. Jafar U., Ab Aziz M.J., Shukur Z. Blockchain for Electronic Voting System — Review and Open Research Challenges. Sensors. – 2021. – Vol. 21, №17. – P. 5874.
7. Python Cryptography Library. Fernet (symmetric encryption). — URL: https://cryptography.io/en/stable/fernet/
8. The Tor Project. About Tor. — URL: https://support.torproject.org/about-tor/
9. Cramer R., Gennaro R., Schoenmakers B. A secure and optimally efficient multi-authority election scheme. Eur. Trans. Telecommun. – 1997. – Vol. 8, №5. – P. 481–490.

Модель гібридної системи виявлення вторгнень на основі криптографічних перетворень та методів штучного інтелекту

УДК 621.395.7 (043.2)

Аліна Давлетова[1]

Західноукраїнський національний університет, [1]a7davletova@gmail.com