КОМБІНОВАНИЙ МЕТОД ЗАХИСТУ АУДІОДАНИХ НА ОСНОВІ RSA-ШИФРУВАННЯ ТА LSB-СТЕГАНОГРАФІЇ В ЗОБРАЖЕННЯХ

Федюшин О.І., Безсонов М.В.
Харківський національний університет радіоелектроніки, Харків, Україна

Захист аудіоінформації є актуальною задачею в умовах стрімкого розвитку засобів цифрової комунікації. Голосові повідомлення, аудіозаписи та інші акустичні дані нерідко містять конфіденційну інформацію, що потребує надійного захисту від несанкціонованого доступу та перехоплення. Існуючі методи захисту — симетричне шифрування (AES, ГОСТ), асиметричні криптосистеми (RSA, ECC) та стеганографія — зазвичай застосовуються окремо, що суттєво знижує загальний рівень захисту. Комбінування криптографічних і стеганографічних підходів дозволяє досягти синергетичного ефекту: криптографія забезпечує конфіденційність даних, тоді як стеганографія приховує сам факт передачі захищеної інформації [1]. Водночас питання практичної реалізації таких комбінованих методів для аудіоданих із збереженням прийнятної обчислювальної складності залишається актуальним. RSA є однією з найбільш відомих та досліджених асиметричних криптосистем, заснованих на обчислювальній складності задачі факторизації великих чисел [2]. Класична схема RSA передбачає вибір двох великих простих чисел p і q, обчислення модуля $n = p \cdot q$ та функції Ейлера $\varphi(n) = (p-1)\cdot(q-1)$. Відкритий ключ e обирається як взаємно просте з $\varphi(n)$ число, а закритий ключ d обчислюється як мультиплікативний обернений елемент e за модулем $\varphi(n)$, тобто задовольняє умову $e \cdot d \equiv 1 \pmod{\varphi(n)}$. Для ефективного обчислення d застосовується розширений алгоритм Евкліда (Extended GCD), що дозволяє знайти обернений елемент за $O(\log n)$ кроків [3].

Метою доповіді є розробка та аналіз комбінованого методу захисту аудіоданих, що поєднує RSA-шифрування на основі кольорового RGB-представлення аудіобайтів з LSB-стеганографією в зображеннях-контейнерах, а також оцінка криптостійкості та обчислювальної ефективності запропонованого підходу. У роботі розроблено та реалізовано систему захисту аудіоданих, що складається з двох взаємодоповнювальних рівнів захисту: криптографічного та стеганографічного. Загальна схема роботи системи передбачає наступну послідовність операцій. Перший рівень — криптографічне перетворення аудіоданих. На вхід системи подається аудіофайл у форматі WAV. Після зчитування файлу отримується масив байтів, кожен з яких набуває значень від 0 до 255. Для підготовки до шифрування кожен байт перетворюється на рядковий запис у форматі шестизначного HEX-кольору виду #XXXXXX. При цьому до запису додається випадкове символьне «сіль» (salt) з множини {a, b, c, d, e}, що заповнює незадіяні позиції до шести символів. Позиція значущого числа в рядку (на початку або в кінці) також визначається випадково (гейт). Такий підхід обфусковує розподіл значень вихідних байтів та ускладнює статистичний аналіз.

Отримані рядки інтерпретуються як HTML-кольори, з яких витягуються компоненти Alpha (A), Red (R), Green (G) та Blue (B). Кожна компонента шифрується окремо за формулою RSA:

$$c = m^{\wedge}e \bmod n$$

де m — значення компоненти кольору (0–255), e — відкрита експонента, $n = p \cdot q$ — модуль RSA. Оскільки значення m обмежені діапазоном [0, 255], а n може бути відносно невеликим, результат шифрування c не завжди вкладається у байтовий діапазон [0, 255]. У разі переповнення ($c \geq 256$) оригінальне значення m записується без шифрування, а індекс цієї позиції фіксується в окремому списку «позицій винятків». Це забезпечує коректну зворотну операцію дешифрування без втрати даних.

Закритий ключ d обчислюється за розширеним алгоритмом Евкліда. На відміну від класичного перебору, що використовується в деяких навчальних реалізаціях RSA, застосування Extended GCD гарантує знаходження оберненого елементу за детермінований час. У разі, якщо $\text{GCD}(e, \varphi(n)) \neq 1$, алгоритм повертає -1, що сигналізує про неможливість обчислення оберненого елементу для обраної пари $(e, \varphi(n))$. Алгоритм генерації e перебирає прості числа від 10-значного генератора та перевіряє взаємну простоту з $\varphi(n)$, фіксуючи до 80 кандидатів та обираючи мінімальний, що підвищує безпеку та відтворюваність генерації ключів.

Сформований масив зашифрованих байтів містить: послідовно записані індекси позицій винятків (по 4 байти кожен), маркер-роздільник (байт 254), кількість позицій винятків, поточну довжину масиву даних, та безпосередньо зашифровані компоненти кольорів. Значення d передається або зберігається окремо як закритий ключ і не включається до контейнера в незахищеному вигляді. Для зворотного перетворення (дешифрування) кожна компонента обробляється за формулою:

$$m = c^{\wedge}d \bmod n$$

При цьому для індексів із списку винятків оригінальне значення відновлюється безпосередньо, оминаючи операцію піднесення до степеня.

Другий рівень - стеганографічне приховування. Зашифрований масив байтів вбудовується у зображення-контейнер (формат PNG) методом найменш значущого біта (LSB). Реалізований алгоритм вбудовування спочатку кодує у молодших бітах пікселів 4-байтне ціле число - довжину прихованого повідомлення, а потім послідовно вбудовує всі біти зашифрованого масиву. Кожен піксель контейнера модифікується лише в одному молодшому біті (RGB-компоненти), що забезпечує мінімальне візуальне спотворення. У разі, якщо розмір повідомлення перевищує ємність наявного зображення, контейнер автоматично масштабується з використанням інтерполяції HighQualityBicubic до мінімального необхідного розміру, після чого виконується повторна перевірка ємності.

Алгоритм декодування виконує зворотню процедуру: послідовно зчитуються молодші біти пікселів контейнера, з яких спочатку відновлюється довжина повідомлення, а потім — масив зашифрованих байтів. Після

витягування даних зі стеганоконтейнера виконується RSA-дешифрування та зворотне перетворення з кольорового представлення в аудіобайти.

Запропонований метод реалізовано у вигляді API-сервісу на платформі .NET із використанням бібліотеки NAudio для роботи з аудіофайлами та System.Drawing для обробки зображень. Контролер надає ендпоінти для шифрування (Encrypt) та дешифрування (Decrypt) аудіоданих. Вхідні дані передаються у вигляді бінарних потоків, а результати повертаються у вигляді оброблених байтових масивів разом з діагностичними метаданими (значення e, d, проміжні розміри буферів).

Аналіз безпеки запропонованого методу показує, що дворівневий захист суттєво ускладнює несанкціоноване відновлення вихідних аудіоданих. Зловмисник, який перехопив стеганоконтейнер, стикається з необхідністю спочатку виявити сам факт приховування інформації (що ускладнюється мінімальними змінами LSB-вбудовування), а потім вирішити задачу RSA-дешифрування без знання закритого ключа *d* та параметрів *p, q* [4, 5] Додаткове рандомізоване «засолення» вхідних байтів перед шифруванням ускладнює атаки на основі відомого відкритого тексту. Обчислювальна складність одного акту шифрування одного байту визначається складністю операції *m^e mod n*, яка при розумному виборі параметрів становить O(log e · log² n).

Серед обмежень слід зазначити, що застосування RSA до окремих байтів (8-бітових значень) є нетиповим підходом і ефективним лише за умови вибору *n* у межах, що допускають значення ciphertext ≥ 256 для деяких входів, що і відстежується механізмом індексів-винятків. Вибір великих *p* та *q* збільшує безпеку, але також збільшує частку позицій-винятків, для яких шифрування фактично не застосовується. Оптимальний вибір параметрів RSA для 8-бітового вхідного простору є відкритим питанням, що потребує подальшого дослідження. Таким чином, запропонований комбінований метод захисту аудіоданих забезпечує двохрівневу безпеку завдяки поєднанню асиметричного шифрування на основі кольорового представлення аудіобайтів та LSB-стеганографії в зображеннях. Практична реалізація у вигляді .NET-сервісу підтверджує працездатність підходу та його придатність для захисту конфіденційних аудіоповідомлень у цифрових системах.

Список літератури

1. Kodlubovskyi D. Data hiding in images using combined steganography and cryptography. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/688.

2. Rivest R., Shamir A., Adleman L. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM. 1978. Vol. 21, No. 2. P. 120–126.

3. Knuth D. E. The Art of Computer Programming. Vol. 2: Seminumerical Algorithms. 3rd ed. Addison-Wesley, 1997. 764 p.

4. Mustafa Sabah. Combination of Steganography and Cryptography. URL: https://iopscience.iop.org/article/10.1088/1757-899X/518/5/052003/pdf.

5. Chan C.-K., Cheng L. M. Hiding data in images by simple LSB substitution. Pattern Recognition. 2004. Vol. 37, No. 3. P. 469–474. cryptography. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/688.