

БУЙБАРОВА М.Ф.,
ВИНОГРАДОВ Ю.М.,
ПРИЙМАК В.Ю.,

МЕТОД ЗАХИЩЕНОЇ РЕАЛІЗАЦІЇ ПЕРЕТВОРЕНЬ ФУР'Є НА ВІДДАЛЕНИХ РОЗПОДІЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

У статті пропонується метод захищеної реалізації Дискретного Перетворення Фур'є (ДПФ) та Швидкого Перетворення Фур'є (ШПФ) на віддалених процесорних засобах хмарних систем. Метод забезпечує захист від доступу до даних при їх передачі та під час їх обробки на віддалених комп'ютерних системах. Метод базується на використанні потокового шифрування і використання адитивного маскуванню відліків сигналу. Детально описані процедури шифрування даних і їх дешифрування після обробки. Наведено числові приклади шифрування та дешифрування даних для ДПФ та ШПФ. Теоретично та експериментально доведено ефективність запропонованого методу.

This paper proposes a method for protected implementation of Discrete Fourier Transform (DFT) and Fast Fourier Transform (FFT) at remote processors of cloud systems. Proposed method ensures protection of data against unauthorized access during network transmission and during processing on remote computer systems. The method is based on stream encryption and using of additional masking for signals. The proposed procedure for data encryption and decryption after processing are described in details. A numerical example for encryption and decryption for both DFT and FFT are given. The effectiveness of proposed method is proved theoretically and experimentally.

Ключові слова: Розподілені віддалені обчислення, хмарні обчислення, захищені обчислення, швидке перетворення Фур'є, обробка сигналів.

Вступ

Однією з фундаментальних операцій комп'ютерної обробки інформації є Дискретне Перетворення Фур'є (ДПФ). Ця операція лежить в основі технологій обробки сигналів, зокрема, зображень та звуків. ДПФ перетворює послідовність цифрових вимірів сигналу через певні проміжки часу в спектральне представлення сигналу, у вигляді набору амплітуд та фаз синусоїд, сума яких відтворює сигнал. Зрозуміло, що, чим більше синусоїд задіяні в представленні сигналу, тим вища якість представлення сигналу. З іншого боку, чим більше синусоїд використовується для відтворення сигналу, тим більший об'єм обчислень потребує реалізація ДПФ.

Для сучасного етапу розвитку інформаційних технологій характерним є динамічне розширення інтерфейсу між зовнішнім світом та засобами комп'ютерної обробки інформації. Домінуючу роль у цьому процесі відіграють засоби цифрової обробки сигналів, в основі яких лежить ДПФ. Це означає, що коло застосування ДПФ ширшає з кожним роком, як і вимоги до якості перетворення. Потужний імпульс розширенню використання ДПФ надає розповсюдження систем відео нагляду. Ці системи широко викорис-

товуються в технологічних процесах, системах регулювання, а також, є технологічною основою боротьби з проявами тероризму. Характерним для таких систем є те, що вони працюють в середовищі Інтернет у реальному часі, а це, в свою чергу, диктує жорсткі вимоги до швидкості реалізації ДПФ. Таким чином, важливою проблемою є пошук резервів для прискорення реалізації ДПФ.

Одним із таких резервів, який може бути використаний для швидшого обчислення ДПФ, є прогресивні хмарні технології. Вже на сьогоднішній день хмарні технології, які надають доступ користувачеві Інтернету до практично необмежених обчислювальних ресурсів, активно залучаються для вирішення широкого кола важливих для практики задач. З іншого боку, саме головні переваги хмарних технологій: обчислювальна потужність та загальнодоступність є причиною недоліків і проблем. Гостро постає питання стійкості віддаленої обчислювальної системи до втручання зловмисників та захищеності оброблюваної інформації.

Проведений аналіз показав, що для більшості практичних застосувань ДПФ, дані, які оброблюються, носять конфідентційний характер. Тому, аби залучати хмарні технології для ДПФ,

необхідно, в першу чергу, вирішити проблему захищеної реалізації ДПФ на невідконтрольних користувачеві обчислювальних потужностях.

Таким чином, наукова задача організації захищеної реалізації ДПФ на віддалених обчислювальних потужностях є важливою та актуальною для сучасного етапу розвитку інформаційних технологій.

Аналіз відомих технологій захищеної віддаленої обробки сигналів

Задачі обробки сигналів являються одними з найбільш масовими задачами комп'ютерних технологій. Значна частина їх виконується в реальному часі. Поява прогресивних технологій обробки інформації в хмарах, які надають для вирішення прикладних задач практично необмежені обчислювальні потужності, стимулювала інтенсивні дослідження в напрямку захищеної реалізації віддаленої обробки сигналів.

Головною проблемою, на вирішення якої направлені виконані до теперішнього часу дослідження, полягає в використанні спеціальних методів шифрування, які б дозволяли отримувати коректний результат шляхом дешифрування результатів віддаленої обробки зашифрованих даних. З наведеного слідує, що не існує універсальних методів шифрування даних перед їх віддаленою обробкою, які не залежать від операцій обробки сигналів. Це означає, що для кожного виду обробки сигналів слід окремо розробляти метод шифрування та дешифрування.

Зокрема, в роботі [1] запропоновано методи захищеної реалізації масових операцій обробки зображень – медіанної та середньоарифметичної фільтрації. В основі цих методів покладено інтервальне шифрування точок зображення перед передачею його для обробки в хмарних системах. Метод забезпечує виконання медіанної фільтрації на віддалених відкритих комп'ютерних системах, закриваючи при цьому доступ до справжнього зображення.

Проведений аналіз показав, що метод інтервального шифрування запропонований в роботі для задач захищеної організації фільтрації на віддалених комп'ютерних потужностях не може бути ефективно застосований для виконання операцій перетворення Фур'є. Специфіка цих операцій вимагає розробки спеціальних методів їх захищеної реалізації.

Важливість реалізації захищеного дискретного перетворення Фур'є та актуальність питань, які вирішуються за допомогою перетворення

Фур'є зумовили інтенсивні дослідження цієї тематики.

Зокрема, в роботі [2] пропонується метод шифрування даних, над якими віддалено виконується ДПФ. При цьому, для шифрування даних використовуються алгоритми на основі модулярного експоненціювання. Це дає змогу гнучко регулювати рівень захищеності віддаленої реалізації ДПФ. Крім того, в розробці запропоновані ефективні механізми контролю правильності віддаленого ДПФ на невідконтрольних обчислювальних платформах. Разом з тим, використання в якості механізму шифрування модулярного експоненціювання помітно ускладнює вибір ключів та має наслідком значну обчислювальну складність реалізації ДПФ, яка в декілька разів перевищує складність простої реалізації ДПФ. Крім того, значну складність становить проблема генерації ключів в запропонованому методі, яка потребує також значних обчислювальних ресурсів. Якщо припустити, що ключі використовуються багаторазово, то це призводить до суттєвого зменшення рівня захищеності, через те, що відкриває зловмиснику значно ширші можливості для злому коду шифру. Використання ж одноразових ключів в запропонованій розробці має наслідком витрати значних за обсягом обчислювальних ресурсів, більших, ніж безпосереднє обчислення ДПФ.

Таким чином, основним недоліком відомого методу реалізації захищеного ДПФ на віддалених обчислювальних платформах, є значна обчислювальна складність реалізації ДПФ в хмарі, що не дозволяє виконувати ці обчислення в реальному часі. Крім того значною є складність генерації ключів, яка виконується безпосередньо користувачем.

Ціллю розробки є створення методу захищеної реалізації ДПФ та ШПФ на віддалених розподілених комп'ютерних системах, яка не потребує значних за обсягом обчислювальних ресурсів і дозволяє реалізувати обчислення в режимі реального часу.

Реалізація захищеного ДПФ та ШПФ

Вхідними даними для ДПФ є масив x_0, x_2, \dots, x_{n-1} вимірних значень сигналу через фіксовані проміжки часу. В результаті перетворення отримується вихідний масив n комплексних чисел y_0, y_2, \dots, y_{n-1} , компоненти яких являють амплітуду та фазу синусоїд, сума яких відтворює заданий вхідний сигнал.

$$\forall k \in \{0, 1, \dots, n-1\}: y_k = \sum_{l=0}^{n-1} x_l \cdot W_n^{lk}, \quad (1)$$

де $W_n = e^{-j \frac{2\pi}{n}}$

Для реалізації захищеного обчислення формули (1) пропонується наступна організація дій користувача:

1. Генерація випадкових комплексних чисел m_0, m_2, \dots, m_{n-1} , що являють собою послідовність масок.

2. Формування маскованої послідовності $x'_0, x'_2, \dots, x'_{n-1}$ шляхом додавання послідовності масок до вхідної послідовності:

$$\forall l \in \{0, 1, \dots, n-1\}: x'_l = x_l + m_l$$

Отриману послідовність користувач відправляє на хмару, де над цією послідовністю виконується ДПФ, а результуюча послідовність y'_k відправляється назад користувачеві.

3. Формування інверсної послідовності $x''_0, x''_2, \dots, x''_{n-1}$ шляхом віднімання послідовності масок від вхідної послідовності:

$$\forall l \in \{0, 1, \dots, n-1\}: x''_l = x_l - m_l$$

Отриману послідовність користувач відправляє на хмару, де над цією послідовністю виконується ДПФ, а результуюча послідовність y''_k відправляється назад користувачеві.

4. Користувач формує вихідну послідовність ДПФ на власній обчислювальній платформі шляхом поелементного обчислення середнього арифметичного отриманих з хмари двох послідовностей y'_k та y''_k .

$$\forall k \in \{0, 1, \dots, n-1\}: y_k = \frac{y'_k + y''_k}{2} \quad (2)$$

Конструктивність запропонованої організації захищеного обчислення ДПФ може бути доведено наступним чином.

Перша результуюча послідовність y'_k може бути представлена у вигляді:

$$\forall k \in \{0, 1, \dots, n-1\}:$$

$$y'_k = \sum_{l=0}^{n-1} (x_l + m_l) \cdot W_n^{lk} = \sum_{l=0}^{n-1} x_l \cdot W_n^{lk} + \sum_{l=0}^{n-1} m_l \cdot W_n^{lk}$$

Друга результуюча послідовність y''_k може бути представлена у вигляді:

$$\forall k \in \{0, 1, \dots, n-1\}:$$

$$y''_k = \sum_{l=0}^{n-1} (x_l - m_l) \cdot W_n^{lk} = \sum_{l=0}^{n-1} x_l \cdot W_n^{lk} - \sum_{l=0}^{n-1} m_l \cdot W_n^{lk}$$

Відповідно, користувач, формуючи середнє арифметичне двох отриманих послідовностей за формулою (2) отримує наступну послідовність:

$$\forall k \in \{0, 1, \dots, n-1\}:$$

$$y_k = \frac{y'_k + y''_k}{2} = \frac{\sum_{l=0}^{n-1} x_l \cdot W_n^{lk} + \sum_{l=0}^{n-1} m_l \cdot W_n^{lk}}{2} + \frac{\sum_{l=0}^{n-1} x_l \cdot W_n^{lk} - \sum_{l=0}^{n-1} m_l \cdot W_n^{lk}}{2} = \sum_{l=0}^{n-1} x_l \cdot W_n^{lk}$$

Варто зазначити, що запропонований метод може бути застосований також для реалізації захищеного Швидкого Перетворення Фур'є (ШПФ). Дійсно, у кожній з послідовностей y'_k

та y''_k , доданок $\sum_{l=0}^{n-1} x_l \cdot W_n^{lk}$ може бути обчислений за допомогою ШПФ за наступним алгоритмом[3]:

Вхідна послідовність x_l розкладається на дві

$\frac{n}{2}$ -відлікові послідовності:

$$x_l^1 = x_{2l}, \quad l = 0, 1, \dots, \frac{n}{2} - 1$$

$$x_l^2 = x_{2l+1}, \quad l = 0, 1, \dots, \frac{n}{2} - 1$$

Тоді (1) можна переписати наступним чином:

$$\forall k \in \{0, 1, \dots, \frac{n}{2} - 1\}:$$

$$y_k = \sum_{l=0}^{\frac{n}{2}-1} x_l^1 \cdot W_n^{lk} + \sum_{l=0}^{\frac{n}{2}-1} x_l^2 \cdot W_n^{lk} = \sum_{l=0}^{\frac{n}{2}-1} x_{2l} \cdot W_n^{2lk} + \sum_{l=0}^{\frac{n}{2}-1} x_{2l+1} \cdot W_n^{(2l+1)k} \quad (3)$$

Оскільки

$$W_n^2 = \left(e^{-j \left(\frac{2\pi}{n} \right)} \right)^2 = e^{-j \left(\frac{2\pi}{\frac{n}{2}} \right)} = W_{\frac{n}{2}}$$

То формулу (3) можна тотожно перетворити:

$$\forall k \in \{0, 1, \dots, \frac{n}{2} - 1\}:$$

$$y_k = \sum_{l=0}^{\frac{n}{2}-1} x_{2l} \cdot W_n^{2lk} + \sum_{l=0}^{\frac{n}{2}-1} x_{2l+1} \cdot W_n^{(2l+1)k} = \sum_{l=0}^{\frac{n}{2}-1} x_{2l} \cdot W_{\frac{n}{2}}^{lk} + W_n^k \cdot \sum_{l=0}^{\frac{n}{2}-1} x_{2l+1} \cdot W_{\frac{n}{2}}^{lk} =$$

$$= \sum_{l=0}^{\frac{n}{2}-1} \chi_l^1 \cdot W_{\frac{n}{2}}^{lk} + W_n^k \cdot \sum_{l=0}^{\frac{n}{2}-1} \chi_l^2 \cdot W_{\frac{n}{2}}^{lk}$$

Тобто,

$$\forall k \in \{0, 1, \dots, \frac{n}{2}-1\}: y_k = \gamma_k^1 + W_n^k \gamma_k^2 \quad (4)$$

де γ_k^1 та γ_k^2 – ДПФ послідовностей χ_l^1 та χ_l^2 відповідно.

Формула (4) визначає y_k тільки для $k \in [0; \frac{n}{2}-1]$. Необхідно визначити y_k для

$k \in (\frac{n}{2}-1; n-1]$. Враховуючи, що функції γ_k^1 та

γ_k^2 періодичні з періодом $\frac{n}{2}$, а

$$W_n^{k+\frac{n}{2}} = W_n^k \cdot W_n^{\frac{n}{2}} = W_n^k \cdot e^{-j\left(\frac{2\pi n}{n \cdot 2}\right)} = -W_n^k,$$

то на проміжку $k \in (\frac{n}{2}-1; n-1]$ y_k визначається як:

$$\forall k \in \{0, 1, \dots, \frac{n}{2}-1\}:$$

$$y_{k+\frac{n}{2}} = \gamma_{k+\frac{n}{2}}^1 + W_n^{k+\frac{n}{2}} \gamma_{k+\frac{n}{2}}^2 = \gamma_k^1 - W_n^k \gamma_k^2$$

Тобто:

$$y_k = \begin{cases} \gamma_k^1 + W_n^k \gamma_k^2, & k \in [0; \frac{n}{2} - 1] \\ \gamma_k^1 - W_n^k \gamma_k^2, & k \in (\frac{n}{2} - 1; n - 1] \end{cases}$$

В свою чергу, кожна з послідовностей γ_k^1 та γ_k^2 також може бути розкладена на дві $\frac{n}{4}$ -відлікові послідовності. Процес зменшення розміру ДПФ може рекурсивно продовжуватися до тих пір, поки не залишаться тільки 2-відлікові послідовності, тобто, остаточно, вхідну послідовність x_l можна розкласти на $\frac{n}{2}$ -відлікових послідовності.

Запропонована організація захищеного виконання ДПФ ілюструється наступним прикладом:

Нехай довжина вхідної послідовності складає 8 відліків, які наведені в другому стовпчику таблиці 1. В разі прямого виконання ДПФ за формулою (1), результуюча послідовність має вигляд наведений в третьому стовпчику таблиці 1. Згідно з першим пунктом запропонованого методу, користувач генерує 8 комплексних масок, які містяться в четвертому стовпчику таблиці 1.

Згідно з наступними кроками запропонованого методу, користувач формує масковану послідовність x'_l та інверсну масковану послідовність x''_l (які знаходяться відповідно у другому та третьому стовпчику таблиці 2).

Табл. 1. Цифрова діаграма прямого виконання ДПФ

l	x_l	y_l	m_l
0	5.2	18.90	-2.3 + j·1.1
1	3.7	12.14 + j·15.11	7.1 - j·2.4
2	-6.6	-0.40 + j·5.09	4.8 + j·1.6
3	4.1	6.05 - j·14.68	-3.2 + j·1.9
4	-3.9	-12.89	6.4 + j·4.3
5	1.7	6.05 + j·14.68	3.3 - j·2.5
6	8.3	-0.40 - j·5.10	-5.9 + j·7.2
7	6.4	12.14 - j·15.11	-1.5 - j·0.8

Табл. 2. Цифрова діаграма виконання захищеного ДПФ

l	x_l'	x_l''	y_l'	y_l''	$\frac{y_l' + y_l''}{2}$
1	$2.9 + j \cdot 1.1$	$7.5 - j \cdot 1.1$	$27.6 + j \cdot 10.39$	$10.2 - j \cdot 10.39$	18.9
2	$10.8 - j \cdot 2.4$	$-3.4 + j \cdot 2.4$	$3.70 - j \cdot 2.11$	$20.57 + j \cdot 32.33$	$12.14 + j \cdot 15.11$
3	$-1.8 + j \cdot 1.6$	$-11.4 - j \cdot 1.6$	$-1.19 - j \cdot 13.4$	$0.39 + j \cdot 23.59$	$-0.40 + j \cdot 5.09$
4	$0.9 + j \cdot 1.9$	$7.3 - j \cdot 1.9$	$1.05 - j \cdot 6.83$	$11.06 - j \cdot 22.54$	$6.05 - j \cdot 14.68$
5	$2.5 + j \cdot 4.3$	$-10.3 - j \cdot 4.3$	$-15.6 + j \cdot 18.1$	$-10.19 - j \cdot 18.1$	-12.89
6	$5.0 - j \cdot 2.5$	$-1.6 + j \cdot 2.5$	$-14.10 + j \cdot 4.11$	$26.22 + j \cdot 25.26$	$6.05 + j \cdot 14.68$
7	$2.4 + j \cdot 7.2$	$14.2 - j \cdot 7.2$	$10.79 + j \cdot 6.6$	$-11.6 - j \cdot 16.80$	$-0.40 - j \cdot 5.10$
8	$4.9 - j \cdot 0.8$	$7.9 + j \cdot 0.8$	$10.94 - j \cdot 7.96$	$13.33 - j \cdot 22.25$	$12.14 - j \cdot 15.11$

Далі відбувається виконання ДПФ над отриманими послідовностями на віддалених комп'ютерних системах. Звідти користувач отримує вихідні замасковані послідовності y_l' та y_l'' , значення яких наведено у четвертому та п'ятому стовпчиках таблиці 2. Для одержання вихідної послідовності y_l користувач виконує поелементне знаходження середнього арифметичного отриманих послідовностей. Результат цієї операції відображено в останньому стовпчику таблиці 2. Порівнявши останній стовпчик таблиці 2, де знаходяться значення вихідної послідовності, обраховані за допомогою запропонованого методу захищеної реалізації ДПФ

та третій стовпчик таблиці 1, де знаходяться значення вихідної послідовності, обраховані прямим ДПФ, видно, що ці значення співпадають.

Для цього ж прикладу можна простежити схему реалізації захищеного ШПФ. Аналогічно з реалізацією ДПФ, користувач створює дві послідовності x_l' та x_l'' , шляхом додавання та віднімання послідовності масок m_l до вхідної послідовності x_l . Далі, відповідно до запропонованого методу, відбувається обчислення ШПФ для послідовностей. Схему отримання послідовностей y_l' та y_l'' показано на рисунку 1 та на рисунку 2 відповідно.

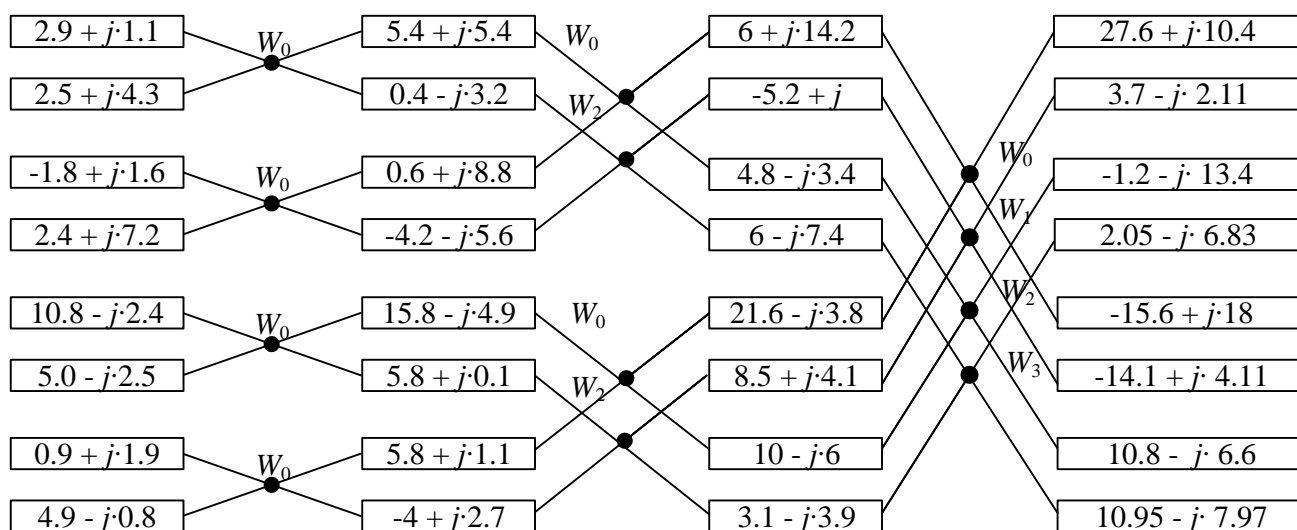


Рис. 1. Схема виконання ШПФ маскованої послідовності

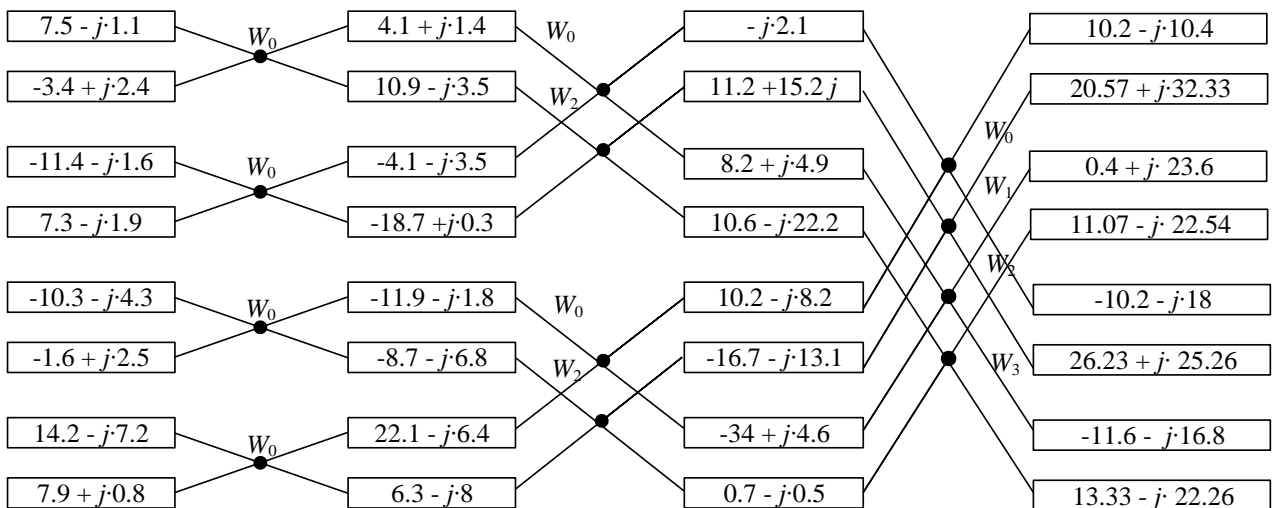


Рис. 2. Схема виконання ШПФ маскованої інверсної послідовності

Оцінка ефективності

Ефективність запропонованого методу захищеної реалізації перетворень Фур'є на віддалених обчислювальних потужностях оцінюється:

- зменшенням обчислювальної складності операцій, що виконуються безпосередньо користувачем на його обчислювальній платформі.
- рівнем захищеності вихідних даних та результатів перетворення Фур'є;

При виконанні ДПФ повністю на обчислювальній платформі користувача, кількість операцій множення, як слідує з формули (1) становить $4 \cdot n^2$, а кількість операцій додавання – $2 \cdot n^2$. Враховуючи, що згідно з [3] тривалість операцій процесорного множення в η раз більша за тривалість операції процесорного додавання, то час T_k виконання ДПФ користувачем може бути представлено у вигляді формули:

$$T_k = (4(\eta \cdot n)^2 + 2n^2) \cdot \tau_\delta = 4\left(\eta^2 + \frac{1}{2}\right)n^2 \cdot \tau_\delta \approx 4\eta^2 \cdot n^2 \cdot \tau_\delta,$$

де τ_δ – час виконання процесорного додавання.

При реалізації запропонованого методу користувач виконує операції додавання випадкової послідовності (n операцій додавання), віднімання випадкової послідовності (n операцій додавання), а також обчислення середнього арифметичного одержаних результатів (n операцій додавання і n операцій зсуву). Оскільки операція зсуву виконується значно швидше операції до-

давання, то можна вважати, що час виконання користувачем ДПФ T'_k за запропонованим варіантом оцінюється наступним чином:

$$T'_k = 3n \cdot \tau_\delta$$

Таким чином застосування запропонованого методу дозволяє зменшити час виконання ДПФ користувачем в q раз, причому чисельне значення q визначається наступною формулою:

$$q = \frac{T_k}{T'_k} = \frac{4}{3}\eta^2 \cdot n \quad (5)$$

Згідно з даними [4] для сучасних процесорів Intel значення $\eta \approx 10$, розмірність – n перетворення Фур'є для типових систем обробки зображень становить 10^2 . Таким чином, згідно (5), використання запропонованого методу забезпечує прискорення обробки зображень користувачем приблизно на 4 порядки. проведені експериментальні дослідження показали, що реальне збільшення швидкодії перетворення Фур'є становить близько $5 \cdot 10^3$. Це свідчить про високу ефективність застосування запропонованого методу захищеної реалізації перетворень Фур'є на віддалених комп'ютерних системах на основі хмарних технологій.

Основна ціль запропонованого методу полягає в тому, щоб практично унеможливити доступ до вихідних даних та результатів перетворення Фур'є, що виконується на віддалених обчислювальних потужностях.

Несанкціонований доступ до даних користувача може бути реалізовано як на стадії їх передачі по мережі Інтернет, так і безпосередньо на віддалених комп'ютерних системах, що виконують обчислення, пов'язані з перетворенням Фур'є.

Рівень захищеності даних овіється об'ємом обчислювальних ресурсів, потрібних зловмиснику для незаконного доступу до даних.

При застосуванні запропонованого методу для одиночної операції ДПФ або ШПФ вимога забезпечення захищеності операндів та результатів не забезпечується, оскільки зловмисних, перехопивши послідовності $x_0', x_1', \dots, x_{n-1}'$ та $x_0'', x_1'', \dots, x_{n-1}''$ достатньо просто відновить значення вхідної послідовності x_0, x_1, \dots, x_{n-1} для перетворення Фур'є шляхом поелементного обчислення середнього арифметичного двох перехоплених послідовностей.

Проте аналіз практичних застосувань операції ДПФ та ШПФ для обробки зображень та звукових сигналів [3] показує, що реально виконується потік вказаних операцій. Тобто практично завжди виконується послідовність з h операцій ДПФ або ШПФ. При виконанні вказаного потоку запропонований метод передбачає:

- використання для кожної з h операцій ДПФ або ШПФ окремих послідовностей масок;

- генерацію користувачем секретних, не співпадаючих між собою послідовностей v_1, v_2, \dots, v_h та w_1, w_2, \dots, w_h , $\forall l \in \{1, 2, \dots, h\}$: $v_l \in \{1, 2, \dots, h\}$, $w_l \in \{1, 2, \dots, h\}$ відправки на віддалені обчислювальні потужності вхідних даних для кожної з h операцій ДПФ або ШПФ. Вказані послідовності визначають порядок отримання результатів користувачем.

- обчислення згідно формули (2) результату l -ї операції ДПФ або ШПФ виконується користувачем після отримання відповідних результатів від віддалених обчислювальних потужностей.

Відповідно, зловмиснику, для того, щоб відновити вхідні дані потоку операцій ДПФ або ШПФ співставити пару вхідних послідовностей з потоку $2 \cdot h$ посилок даних користувача. Очевидно, що для цього потрібно перебрати, в середньому, $2 \cdot h^2$ пар, для кожної з яких необхідно виконати дві операції ДПФ або ШПФ, що потребує $4 \cdot n^2$ операцій процесорного множення для ДПФ і $2 \cdot n \cdot \log_2 n$ операцій процесорного множення для ШПФ.

Таким чином, для отримання незаконного доступу до даних одного перетворення Фур'є, що виконується на віддалених комп'ютерних потужностях, потрібний об'єм ресурсів оцінюється часом виконання $8 \cdot h^2 \cdot n^2$ операцій процесорного множення. Враховуючи, що в реальних системах [3], значення $n \approx 10^3$, а $h \approx 10^4$, то об'єм ресурсів для отримання незаконного доступу оцінюється часом виконання 10^{15} операцій процесорного множення, що для більшості застосувань робить злам запропонованого механізму захисту практично недоцільним.

Висновки

У результаті виконаних досліджень, досягнута поставлена ціль – розроблено оригінальний метод захищеної реалізації потоку операцій ДПФ та ШПФ на віддалених обчислювальних потужностях в рамках хмарних технологій.

Запропонований метод по суті реалізує потік шифрування даних, що відправляються користувачем на віддалені комп'ютерні системи, де безпосередньо виконуються ДПФ та ШПФ, а також, дешифрування отриманих результатів. Детально розроблено методику застосування запропонованого методу для ДПФ та ШПФ, теоретично доведено конструктивність розроблених процедур.

Головною перевагою запропонованого методу є простота операцій шифрування та дешифрування даних, що забезпечує низький рівень витрат обчислювального часу на виконання операцій, пов'язаних з захистом інформації.

Теоретично доведено, що запропонований метод захищеної реалізації потоку операцій ДПФ та ШПФ забезпечує достатній для задач практики рівень захищеності даних та результатів перетворення Фур'є, що виконуються на віддалених обчислювальних потужностях та передаються по відкритим каналам Інтернет.

Теоретично та експериментально доведено, що використання запропонованого методу забезпечує підвищення швидкості обробки зображень та звукових сигналів на 3-4 порядки.

Запропонований метод може бути ефективно використаний для потокової обробки зображень в реальному часі, зокрема, в системах обробки супутникових зображень, а також в інтелектуальних системах відеоспостереження.

Список посилань

1. Марковський О.П. Захищена реалізації захисту зображень в GRID-системах / О.П. Марковський, М.В. Невдащенко, А.М. Білашевська // Вісник НТУУ «КПІ». Інформатика, управління та обчислювальна техніка – К.: Век+, – 2014. – № 61. – 180 с.
2. Bianchi T. On the Implementation of the Discrete Fourier Transform in the Encrypted Domain/ T. Bianchi, A. Piva, M. Barni // IEEE Transactions on Information Forensics and Security. – 2009. – Vol.4. – P. 86-97.
3. Смит С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников / Смит Стивен; пер. с англ. А.Ю.Линовича, С.В.Витязева, И.С.Гусинского. – М.:Додэка XXI, 2012. — 720 с.
4. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы. Шестое издание / Б. Брэй; пер. с англ. А.В.Жукова.- Санкт-Петербург: БХВ-Петербург, 2005.-1328 с.