УДК 004.052.42 DOI: 10.31673/2412-4338.2019.049911

Марковський О. П., Гуменюк І. О., Міратаї Аліреза *НТУУ «КПІ ім. Ігора Сікорського», Київ*
Торошанко Я. І., Волощук М. О. *Державний університет телекомунікацій, Київ*

МЕТОД ПРИСКОРЕНОЇ ЗАХИЩЕНОЇ ФІЛЬТРАЦІЇ ЗОБРАЖЕНЬ НА ВІДДАЛЕНИХ КОМП'ЮТЕРНИХ СИСТЕМАХ

У статті пропонується метод пришвидшеної середньоарифметичної фільтрації зображень з залученням віддалених обчислювальних ресурсів (хмарних систем). Запропонований метод реалізує концепцію захищених хмарних обчислень. Він забезпечує захист зображень від незаконного доступу під час надсилання та обчислення в потенційно відкритому середовищі. Показано, що перспективним напрямком організації криптографічного захисту зображень є використання адитивного перетворення зображень. Операції розробленого методу поділяються на дві основні частини. Перша частина – це шифрування та дешифрування зображень, яке потребує відносно незначних обчислювальних ресурсів і може бути виконане з використанням обчислювальних ресурсів користувача. Друга частина – це середньоарифметична фільтрація зображень на віддалених потужних багатопроцесорних системах. Елементи криптографічного захисту запропонованого способу не впливають на результат фільтрації зображень.

В статті представлено математичне підгрунття запропонованого методу. Теоретично отримані результати підтверджені результатами експериментальних досліджень. Запропонована процедура захищеної середньоарифметичної фільтрації зображень детально описана та проілюстрована прикладом. Розроблено рекомендації щодо підвищення ефективності запропонованої процедури середньої арифметичної фільтрації. Проведено порівняльний аналіз запропонованого методу. Теоретично та експериментально доведено, що запропонований метод забезпечує прискорення середньоарифметичної фільтрації зображень приблизно в 4 рази в порівнянні з існуючими методами, що використовують лише обчислювальні ресурси користувача. Розроблений метод орієнтований для використання в системах обробки насамперед аерокосмічних зображень.

Ключові слова: *середньоарифметична фільтрація, захищені обчислення, захищенна обробка зображень, хмарні обчислення, хмарні технології.*

Markovskyi O. P., Humeniuk I. O., Miratаei Alireza *NTUU "Igor Sykorsky KPI", Kyiv*
Toroshanko Ya. I., Voloshchuk M. O. *State University of Telecommunications, Kyiv*

METHOD FOR SPEED UP PROTECTED IMAGE FILTRATION IN CLOUDS

The article proposes a method to speed up the arithmetic mean filtration of images using remote computational resources (cloud systems). The proposed method deals with secure cloud calculations. It provides images protection from illegal access to it during the sending and computing in a potentially insecure environment. It is shown that the perspective direction of organization of cryptographic image protection is the use of additive image conversion. The operations of the elaborated method are divided into two main parts. The first part is the encryption and decryption of images. The processing of the first part needs less computing resources and can be executed using user resources. The second part is arithmetic mean filtration of images, executed on powerful cloud computational resources. The cryptographical protection elements of the proposed method do not make any influence on the result of image filtration.

The article includes the mathematical background of the proposed approach. The results derived theoretically have been confirmed by the results of experimental researches. The proposed procedure of secure arithmetic mean filtration of images is described in detail and illustrated by an example. A recommendation to improve the efficiency of the proposed procedure of arithmetic mean filtration has been worked out. A comparative analysis of the proposed method has been conducted. Theoretically and experimentally it has been proved that the proposed method accelerates arithmetic mean filtration in approximately 4 times compared with the existing methods to speed up this filtration of images using only user computing resources. The developed method is oriented for use in aerospace image processing systems.

Keywords: *arithmetical mean filtration, secure computing, secure image processing, cloud computing, cloud technologies.*

Марковский А. П., Гуменюк И. О., Миратаи Алиреза *НТУУ «КПИ им. Игоря Сикорского», Киев*
Торошанко Я. И., Волощук М. О. *Государственный университет телекоммуникаций, Киев*

МЕТОД УСКОРЕННОЙ ЗАЩИЩЕННОЙ ФИЛЬТРАЦИИ ИЗОБРАЖЕНИЙ НА УДАЛЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ

В статье предлагается метод ускоренной среднеарифметической фильтрации изображений с привлечением удаленных вычислительных ресурсов (облачных систем). Предложенный метод реализует концепцию защищенных облачных вычислений. Он обеспечивает защиту изображений от незаконного доступа при отправке и вычисления в потенциально открытой среде. Показано, что перспективным направлением организации криптографической защиты изображений является использование аддитивного преобразования изображений. Операции разработанного метода делятся на две основные части. Первая часть – это шифрование и дешифрование изображений, которое требует относительно небольших вычислительных ресурсов и может быть выполнено с использованием вычислительных ресурсов пользователя. Вторая часть – это среднеарифметическая фильтрация изображений на удаленных мощных многопроцессорных системах. Элементы криптографической защиты предлагаемого способа не влияют на результат фильтрации изображений.

В статье представлены математическое обоснование предложенного метода. Теоретически полученные результаты подтверждены результатами экспериментальных исследований. Предложенная процедура защищенной среднеарифметической фильтрации изображений подробно описана и проиллюстрирована примером. Разработаны рекомендации по повышению эффективности предложенной процедуры средней арифметической фильтрации. Проведен сравнительный анализ предложенного метода. Теоретически и экспериментально доказано, что предложенный метод обеспечивает ускорение среднеарифметической фильтрации изображений примерно в 4 раза по сравнению с существующими методами, использующими только вычислительные ресурсы пользователя. Разработанный метод ориентирован для использования в системах обработки прежде всего аэрокосмических изображений.

***Ключевые слова**: среднеарифметическая фильтрация, защищенные вычисления, защищенная обработка изображений, облачные вычисления, облачные технологии.*

1. Вступна частина

Постановка задачі. В ході спіралеподібного розвитку комп'ютерних технологій на початку нового тисячоліття людство переходить від персональних комп'ютерів до спільного використання віддалених обчислювальних ресурсів. На відміну від використання ресурсів однієї ЕОМ великою кількістю користувачів в 60-70-х роках минулого століття, спільний доступ здійснюється на принципово новому, більш високому рівні. Революційний прогрес комп'ютерних мереж та багатопроцесорних систем дозволяє реалізувати доступ багатьом користувачам до об'єднаних в планетарному масштабі обчислювальних потужностей в рамках хмарних технологій [1].

Хмарні технології надають широкому колу користувачів доступ до практично необмежених обчислювальних ресурсів. Це дозволяє суттєво розширити клас прикладних задач в галузях науки, техніки та управління, які можуть бути ефективно вирішенні з використанням комп'ютерних засобів. Також, це надає можливості зробити процес вирішення задач більш оперативним і підвищити точність та якість отримуваних результатів. Окрім цього, хмарні технології роблять рентабельним створення суперкомп'ютерів завдяки залученню інвестицій сотень тисяч користувачів, охочих вирішувати на них свої прикладні задачі на комерційній основі [1].

Попри наведені можливості хмарних технологій, наразі широкого розповсюдження набули лише хмарні сховища даних. Основною перепоною широкому використанню хмарних обчислень є незахищеність даних [2, 3]. Існує реальний ризик несанкціонованого доступу до даних в процесі їх передачі та обробки на віддалених, непідконтрольних користувачу, обчислювальних потужностях. Разом з тим, існує широкий клас задач, при вирішенні яких конфіденційність даних стратегічно важлива для користувачів. Зокрема, однією з них є обробка аерокосмічних знімків [4].

Таким чином, задача створення криптографічних механізмів захисту даних, під час їхньої обробки на віддалених обчислювальних потужностях, є актуальною на сучасному етапі розвитку інформаційних технологій.

Аналіз літературних джерел. Одним з найбільш поширених видів обробки зображень є покращення їх якості, шляхом видалення імпульсних завад, які виникають в процесі формування та передачі зображень [5].

Реальне зображення, представляє собою матрицю A з k рядків та h стовбців, кожен елемент якої $a_{x,y}$, $0 \le x \le k$, $0 \le y \le h$, є значенням інтенсивності кольору (кольорів):

$$A = \begin{bmatrix} a_{1,1}\, a_{1,2} \ldots a_{1,h} \\ a_{2,1}\, a_{2,2} \ldots a_{2,h} \\ \ldots\ldots \\ a_{k,1}\, a_{k,2} \ldots a_{k,h} \end{bmatrix}.$$

На практиці кожен елемент зображення $a_{x,y}$ може містити не лише значення вимірів оригінального сигналу, а й випадкові значення частотних імпульсів, що виникають в процесі формування та передачі зображень. Одним із найбільш поширених методів зменшення значення частотних імпульсів в складі зображення є його попередня обробка в формі середньоарифметичної фільтрації.

Суть середньоарифметичної фільтрації полягає в тому, що зображення сканується квадратною апертурою непарного розміру r, і при цьому центральний елемент апертури замінюється на значення середнього арифметичного точок апертури. В результаті фільтрації формується матриця S з істотно меншими значеннями частотних імпульсів:

$$S = \begin{bmatrix} s_{1,1}\, s_{1,2} \ldots s_{1,h} \\ s_{2,1}\, s_{2,2} \ldots s_{2,h} \\ \ldots\ldots \\ s_{k,1}\, s_{k,2} \ldots s_{k,h} \end{bmatrix}$$

При середньоарифметичній фільтрації кожен елемент $s_{x,y}$ відфільтрованого зображення обчислюється як середнє арифметичне значення r^2 елементів поточної апертури:

$$s_{x,y} = \frac{1}{r^2} \sum_{i=x-\frac{r-1}{2}}^{x+\frac{r-1}{2}} \sum_{j=y-\frac{r-1}{2}}^{y+\frac{r-1}{2}} a_{i,j}\,.$$

При фільтрації реального зображення, кількість елементів, які змінюються становить $(k - r + 1) \cdot (h - r + 1)$. Оскільки розмір апертури істотно менший за розмір зображення, можна вважати, що при фільтрації змінюється $k \cdot h$ елементів зображення, тобто використовується $k \cdot h$ апертур.

Технологічно є два методи середньоарифметичної фільтрації [6]. Один з них полягає в тому, що для знаходження кожного елементу відфільтрованого зображення незалежно обчислюється середнє арифметичне елементів поточної апертури. В такому разі, загальний час t_{f1} фільтрації зображення дорівнює:

$$t_{f1} = k \cdot h \cdot (r^2 \cdot t_s + t_d),$$

де t_s – час виконання однієї операції додавання; та t_d – час виконання однієї операції ділення.

Другий метод полягає в тому, що кожна наступна апертура формується на основі попередньої. Перший обчислюваний елемент кожного рядка формується звичним чином, а всі наступні $s_{x,y}$ – шляхом віднімання від попереднього $s_{x,y-1}$ зваженої по r^2 суми першого стовбця попередньої апертури та додавання зваженої суми останнього стовбця поточної апертури:

$$s_{x,y} = s_{x,y-1} - \frac{1}{r^2} \cdot \sum_{i=x-\frac{r-1}{2}}^{i=x+\frac{r-1}{2}} a_{i,y-1-\frac{r-1}{2}} + \frac{1}{r^2} \cdot \sum_{i=x-\frac{r-1}{2}}^{i=x+\frac{r-1}{2}} a_{i,y+-\frac{r-1}{2}} .$$

На рис.1 проілюстровано зв'язок двох сусідніх апертур розміру r=3. Тобто:

$$s_{2,3} = s_{2,2} - \sum_{i=1}^{3} a_{i,1} + \sum_{i=1}^{3} a_{i,4} .$$

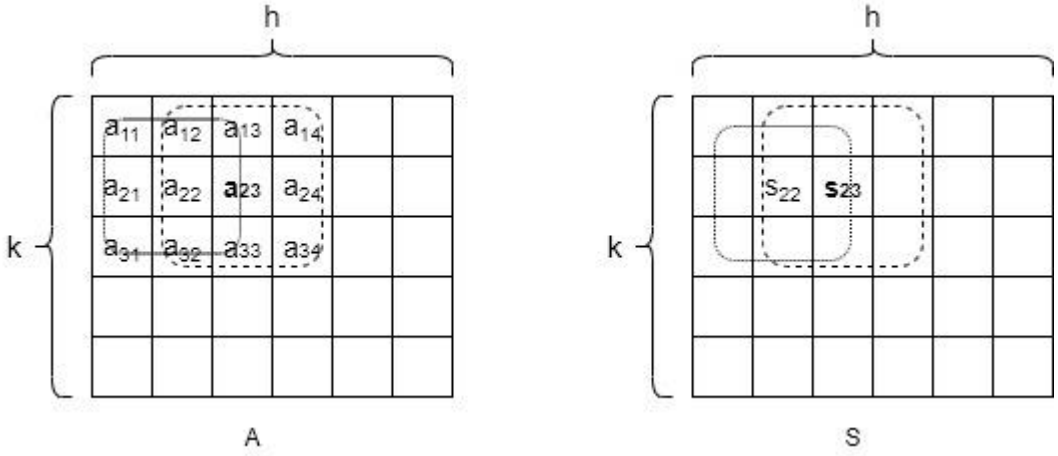

Рис. 1. Приклад виконання середньоарифметичної фільтрації другим методом

Оскільки в реальних системах кількість обчислюваних апертур вимірюється тисячами, то часом обчислення першої апертури кожного рядка можна знехтувати, вважаючи його рівним часу обчислення всіх інших елементів. Тоді час t_{f2} виконання другого методу середньоарифметичної фільтрації дорівнює:

$$t_{f2} = k \cdot h \cdot ((r+2) \cdot t_s + t_d) .$$

Прискорення ς другого методу середньоарифметичної фільтрації в порівнянні з першим становить:

$$\zeta = \frac{t_{f1}}{t_{f2}} = \frac{r^2 \cdot t_s + t_d}{(r+2) \cdot t_s + t_d} .$$

Згідно з оцінками [7]] швидкодії виконання окремих операцій, $\frac{t_d}{t_s} = 30$. При типовому для практичних задач розмірі апертури r = 11, коефіцієнт прискорення ς = 3,5.

Невирішені питання. На основі проаналізованих джерел, можна зробити висновок, що існуючі на даний момент методи прискорення середньоарифметичної фільтрації не здатні забезпечити достатньої для практичних потреб швидкодії. Особливо гостро це стосується задач, для розв'язку яких потрібна швидка обробка потоків зображень [3, 6].

Наразі, найбільш перспективним напрямком вирішення цієї задачі є залучення х віддалених комп'ютерних системах. Проте, при виконанні середньоарифметичної фільтрації в хмарах, не забезпечується необхідний для практичних задач захист зображень від несанкціонованого доступу до них [8]. Таким чином, існує потреба розробки методу захищеної середньоарифметичної фільтрації зображень на віддалених комп'ютерних системах.

Мета та задачі дослідження.

Метою досліджень є прискорення виконання середньоарифметичної фільтрації потоків зображень за рахунок застосування віддалених обчислювальних потужностей.

Для досягнення поставленої мети в ході досліджень розв'язуються наступні наукові задачі:

– розробка методу захищеної групової середньоарифметичної фільтрації зображень, прискорення якої реалізується за рахунок використання високопродуктивних віддалених

обчислювальних потужностей на основі хмарних технологій;

– визначення оптимальної кількості зображень, що оброблюються в межах однієї групи;

– теоретичні та експериментальні дослідження ефективності розробленого методу.

2. Метод прискорення середньоарифметичної фільтрації груп зображень з залученням хмарних технологій

Для досягнення поставленої мети: прискорення фільтрації потоку зображень пропонується використати можливості хмарних технологій, тобто реалізацію більшості обчислень на віддалених комп'ютерних потужностях з забезпеченням надійного захисту зображень від незаконного доступу до них під час передачі та обробки на непідконтрольних користувачеві віддалених системах.

В результаті проведеного аналізу виділено кілька особливостей середньоарифметичної фільтрації. По-перше, оскільки в основі середньоарифметичної фільтрації лежать операції арифметичного додавання та ділення, то найбільш перспективним напрямком захисту зображень під час їх віддаленої середньоарифметичної фільтрації є адитивні перетворення. Суть адитивного маскування полягає в накладанні маскуючого зображення на точки оригінального зображення з подальшим зняттям маски після операції середньоарифметичної фільтрації.

Інша особливість середньоарифметичної фільтрації зображень в реальних системах, полягає в тому, що вони потребують обробки не одиночних зображень, а деякої їх множини $\vartheta = \{A_1, A_2, \ldots A_\eta\}$ [6]. Ця особливість може бути використана для підвищення ефективності захищеної високопродуктивної обробки зображень з залученням хмарних технологій. В якості основного засобу захисту зображень при цьому можна використовувати адитивні перетворення зображень певної групи.

На основі цих особливостей пропонується метод віддаленої захищеної середньоарифметичної фільтрації груп з w оригінальних зображень A_1, A_2, …, A_w. Шифрування групи зображень відбувається в два етапи. Спершу кожне оригінальне зображення A_p, де $p \in \{1, 2, \ldots, w\}$, маскується за допомогою адитивного маскування з отриманням зображення G_p. Другий етап передбачає адитивні перетворення замаскованих зображень G_1, G_2, …, G_w в межах поточної групи з отриманням групи зображень V_1, V_2, …, V_w, які готові до надсилання відкритими каналами та обробки з використанням хмарних технологій.

В результаті віддаленої середньоарифметичної обробки користувач отримує w відфільтрованих зашифрованих зображень Q_1, Q_2, …, Q_w і виконує їхнє зворотне перетворення з отриманням відфільтрованих замаскованих зображень U_1, U_2, …, U_w. Другий етап дешифрування полягає в зніманні масок з зображень U_1, U_2, …, U_w з отриманням відфільтрованих оригінальних зображень S_1, S_2, …, S_w.

Відповідно до запропонованого методу, користувач заздалегідь формує q масок M_1, M_2, …, M_q. Кожна маска M є матрицею з k рядків та h, стовпців, елементами $m_{x,y}$ якої є випадкові значення:

$$M = \begin{bmatrix} m_{1,1}\ m_{1,2} \ldots m_{1,h} \\ m_{2,1}\ m_{2,2} \ldots m_{2,h} \\ \ldots \\ m_{k,1}\ m_{k,2} \ldots m_{k,h} \end{bmatrix}.$$

З залученням власних обчислювальних ресурсів, користувач здійснює середньоарифметичну фільтрацію масок M_1, M_2, …, M_q і отримує їх відфільтровані відповідники D_1, D_2, …, D_q.

Для шифрування користувач обирає w масок M_1, M_2, …, M_w, де $w << q$, і здійснює адитивне маскуванням w оригінальних зображень A_1, A_2, …, A_w, з отриманням G_1, G_2, …, G_w. Тобто на кожне оригінальне зображення A_p накладається маска M_p, шляхом додавання до

кожного елементу $a^p_{x,y}$ відповідного елементу $m^p_{x,y}$, з формуванням зашифрованого зображення G_p:

$$\forall x \in \{1, 2, ..., k\},\ y \in \{1, 2, ..., h\} : g^p_{x,y} = a^p_{x,y} + m^p_{x,y}. \quad (1)$$

Для дешифрування відфільтрованих замаскованих зображень U_1, U_2, …, U_w, користувач знімає з них відповідні заздалегідь відфільтровані маски D_1, D_2, …, D_w. Тобто, він віднімає від кожного елементу $u^p_{x,y}$ зображення U_p, відповідний елемент $d^p_{x,y}$ відфільтрованої маски D_p:

$$\forall x \in \{1, 2, ..., k\},\ y \in \{1, 2, ..., h\} : s^p_{x,y} = u^p_{x,y} - d^p_{x,y}.$$

Формально, обґрунтування запропонованої процедури дешифрування може бути представлене наступними формулами:

$$s^p_{x,y} = u^p_{x,y} - d^p_{x,y} = \frac{1}{r^2} \sum_{i=x-\frac{r-1}{2}}^{x+\frac{r-1}{2}} \sum_{j=y-\frac{r-1}{2}}^{y+\frac{r-1}{2}} g^p_{i,j} - \frac{1}{r^2} \sum_{i=x-\frac{r-1}{2}}^{x+\frac{r-1}{2}} \sum_{j=y-\frac{r-1}{2}}^{y+\frac{r-1}{2}} m^p_{i,j}. \quad (2)$$

Підставивши значення з формули (1) в формулу (2) значення $s^p_{x,y}$ може бути представлене в наступному вигляді:

$$s^p_{x,y} = \frac{1}{r^2} \sum_{i=x-\frac{r-1}{2}}^{x+\frac{r-1}{2}} \sum_{j=y-\frac{r-1}{2}}^{y+\frac{r-1}{2}} (a^p_{i,j} + m^p_{i,j}) - \frac{1}{r^2} \sum_{i=x-\frac{r-1}{2}}^{x+\frac{r-1}{2}} \sum_{j=y-\frac{r-1}{2}}^{y+\frac{r-1}{2}} m^p_{i,j} = \frac{1}{r^2} \sum_{i=x-\frac{r-1}{2}}^{x+\frac{r-1}{2}} \sum_{j=y-\frac{r-1}{2}}^{y+\frac{r-1}{2}} a^p_{i,j}.$$

У запропонованій процедурі маскування, набори масок M_1, M_2, …, M_w та їх відфільтрованих відповідників D_1, D_2, …, D_w використовуються в якості секретних ключів.

Наступним етапом виконання запропонованого методу є адитивне перетворення w замаскованих зображень G_1, G_2, …, G_w.

Суть адитивного перетворення полягає в тому, що над групою з w зображень G_1, G_2, …, G_w здійснюються лінійні операції, з отриманням w зображень V_1, V_2, …, V_w, які оброблюються на віддалених багатопроцесорних системах. В якості адитивного перетворення використовується система Λ лінійних ортогональних перетворень, що може бути представлена в вигляді матриці Λ:

$$\Lambda = \begin{bmatrix} \lambda_{1,1}\ \lambda_{1,2} \ldots \lambda_{1,w} \\ \lambda_{2,1}\ \lambda_{2,2} \ldots \lambda_{2,w} \\ \ldots\ldots \\ \lambda_{w,1}\ \lambda_{w,2} \ldots \lambda_{w,w} \end{bmatrix},$$

де $\forall i, j \in \{1, 2, ..., w\} : \lambda_{ij} \in \{-1, 0, 1\}$, та пов'язана з нею система Γ зворотних лінійних перетворень:

$$\Gamma = \begin{bmatrix} \gamma_{1,1}\ \gamma_{1,2} \cdots \gamma_{1,w} \\ \gamma_{2,1}\ \gamma_{2,2} \cdots \gamma_{2,w} \\ \ldots\ldots \\ \gamma_{w,1}\ \gamma_{w,2} \cdots \gamma_{w,w} \end{bmatrix}.$$

Для обраних систем Λ і Γ при будь-якому векторі $X = \{x_1, x_2, \ldots, x_w\}$ справджується:

$$y_1 = \lambda_{1,1} \cdot x_1 + \lambda_{1,2} \cdot x_2 + \ldots + \lambda_{1,w} \cdot x_w,$$
$$y_2 = \lambda_{2,1} \cdot x_1 + \lambda_{2,2} \cdot x_2 + \ldots + \lambda_{2,w} \cdot x_w,$$
$$y_w = \lambda_{w,1} \cdot x_1 + \lambda_{w,2} \cdot x_2 + \ldots + \lambda_{w,w} \cdot x_w;$$

$$x_1 = \gamma_{1,1} \cdot y_1 + \gamma_{1,2} \cdot y_2 + ... + \gamma_{1,w} \cdot y_w,$$
$$x_2 = \gamma_{2,1} \cdot y_1 + \gamma_{2,2} \cdot y_2 + ... + \gamma_{2,w} \cdot y_w,$$
$$x_w = \gamma_{w,1} \cdot y_1 + \gamma_{w,2} \cdot y_2 + ... + \gamma_{w,w} \cdot y_w.$$

Це означає, що система Γ містить зворотні перетворення відносно системи Λ. Формування матриць Λ і Γ на практиці може здійснюватись заздалегідь з формуванням певної множини перетворень: $\Omega = \{< \Lambda_1,\Gamma_1 >, < \Lambda_2,\Gamma_2 >, \ldots, < \Lambda_\mu,\Gamma_\mu >\}$. Пари сформованних перетворень використовуються в якості секретних ключів.

Приклад вибору ортогональної системи Λ лінійних перетворень для $w = 4$:

$$\Lambda = \begin{bmatrix} \lambda_{1,1} & \lambda_{1,2} & \lambda_{1,3} & \lambda_{1,4} \\ \lambda_{2,1} & \lambda_{2,2} & \lambda_{2,3} & \lambda_{2,4} \\ \lambda_{3,1} & \lambda_{3,2} & \lambda_{3,3} & \lambda_{3,4} \\ \lambda_{4,1} & \lambda_{4,2} & \lambda_{4,3} & \lambda_{4,4} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}.$$

Наведена система Λ є ортогональною в силу того, що лінійна композиція будь-якої підмножини рядків матриці Λ не дорівнює нулю.

Зворотна до Λ ортогональна матриця Γ має наступний вигляд:

$$\Gamma = \begin{bmatrix} \gamma_{1,1} & \gamma_{1,2} & \gamma_{1,3} & \gamma_{1,4} \\ \gamma_{2,1} & \gamma_{2,2} & \gamma_{2,3} & \gamma_{2,4} \\ \gamma_{3,1} & \gamma_{3,2} & \gamma_{3,3} & \gamma_{3,4} \\ \gamma_{4,1} & \gamma_{4,2} & \gamma_{4,3} & \gamma_{4,4} \end{bmatrix} = \begin{bmatrix} -1 & 1 & 1 & 0 \\ 1 & 0 & 0 & -1 \\ 0 & 0 & -1 & 1 \\ 1 & -1 & 0 & 0 \end{bmatrix}.$$

Наприклад, якщо $X = \{x_1, x_2, x_3, x_4\} = \{1, 2, 3, 4\}$, то:

$$y_1 = \lambda_{1,1} \cdot x_1 + \lambda_{1,2} \cdot x_2 + \lambda_{1,3} \cdot x_3 + \lambda_{1,4} \cdot x_4 = x_1 + x_2 + x_3 + x_4 = 10,$$
$$y_1 = \lambda_{2,1} \cdot x_1 + \lambda_{2,2} \cdot x_2 + \lambda_{2,3} \cdot x_3 + \lambda_{2,4} \cdot x_4 = x_1 + x_2 + x_3 = 6,$$
$$y_1 = \lambda_{3,1} \cdot x_1 + \lambda_{3,2} \cdot x_2 + \lambda_{3,3} \cdot x_3 + \lambda_{3,4} \cdot x_4 = x_1 + x_4 = 5,$$
$$y_1 = \lambda_{4,1} \cdot x_1 + \lambda_{4,2} \cdot x_2 + \lambda_{4,3} \cdot x_3 + \lambda_{4,4} \cdot x_4 = x_1 + x_3 + x_4 = 8.$$

Значення X відновлюється зі значень Y з використанням зворотного лінійного перетворення Γ в наступному вигляді:

$$x_1 = \gamma_{1,1} \cdot y_1 + \gamma_{1,2} \cdot y_2 + \gamma_{1,3} \cdot y_3 + \gamma_{1,4} \cdot y_4 = -y_1 + y_2 + y_3 = -10 + 6 + 5 = 1,$$
$$x_1 = \gamma_{2,1} \cdot y_1 + \gamma_{2,2} \cdot y_2 + \gamma_{2,3} \cdot y_3 + \gamma_{2,4} \cdot y_4 = y_1 - y_4 = 10 - 8 = 2,$$
$$x_1 = \gamma_{3,1} \cdot y_1 + \gamma_{3,2} \cdot y_2 + \gamma_{3,3} \cdot y_3 + \gamma_{3,4} \cdot y_4 = -y_3 + y_4 = -5 + 8 = 3,$$
$$x_1 = \gamma_{4,1} \cdot y_1 + \gamma_{4,2} \cdot y_2 + \gamma_{4,3} \cdot y_3 + \gamma_{4,4} \cdot y_4 = y_1 - y_2 = 10 - 6 = 4.$$

Таким чином, запропонований метод захищеної групової середньоарифметичної фільтрації зображень зводиться до виконання наступної послідовності дій:

1) Користувач обирає w зображень $A_1, A_2, \ldots, A_w$, які оброблюються в межах однієї групи.

2) Користувач обирає, з попередньо створених q масок, w масок $M_1, M_2, \ldots, M_w$.

3) Кожне зображення A_p, $p \in \{1, 2, \ldots, w\}$, шифрується маскою M_p за допомогою адитивного маскування, з утворенням w замаскованих зображень $G_1, G_2, \ldots, G_w$.

4) Користувач здійснює перетворення замаскованих зображень $G_1, G_2, \ldots, G_w$, за допомогою системи Λ, і отримує захищенні зображення зображень $V_1, V_2, \ldots, V_w$.

5) Користувач надсилає захищенні зображення $V_1, V_2, \ldots, V_w$ на віддаленні обчислювальні потужності.

6) На віддалених багатопроцесорних системам кожне зображення V_p незалежно оброблюється за допомогою середньоарифметичної фільтрації, з отриманням зображення Q_p.

7) Відфільтроване захищене зображення Q_p передається користувачеві.

8) Користувач, отримавши всю групу зображень Q_1, Q_2, …, Q_w виконує зворотні перетворення системи Г з отриманням w замаскованих відфільтрованих зображень U_1, U_2, …, U_w.

9) Користувач відновлює відфільтровані замасковані зображення U_1, U_2, …, U_w, за допомогою D_1, D_2, …, D_w, з отриманням відфільтрованих оригінальних зображень S_1, S_2, …, S_w.

На рис. 2 схематично зображено порядок обробки зображення запропонованим методом.

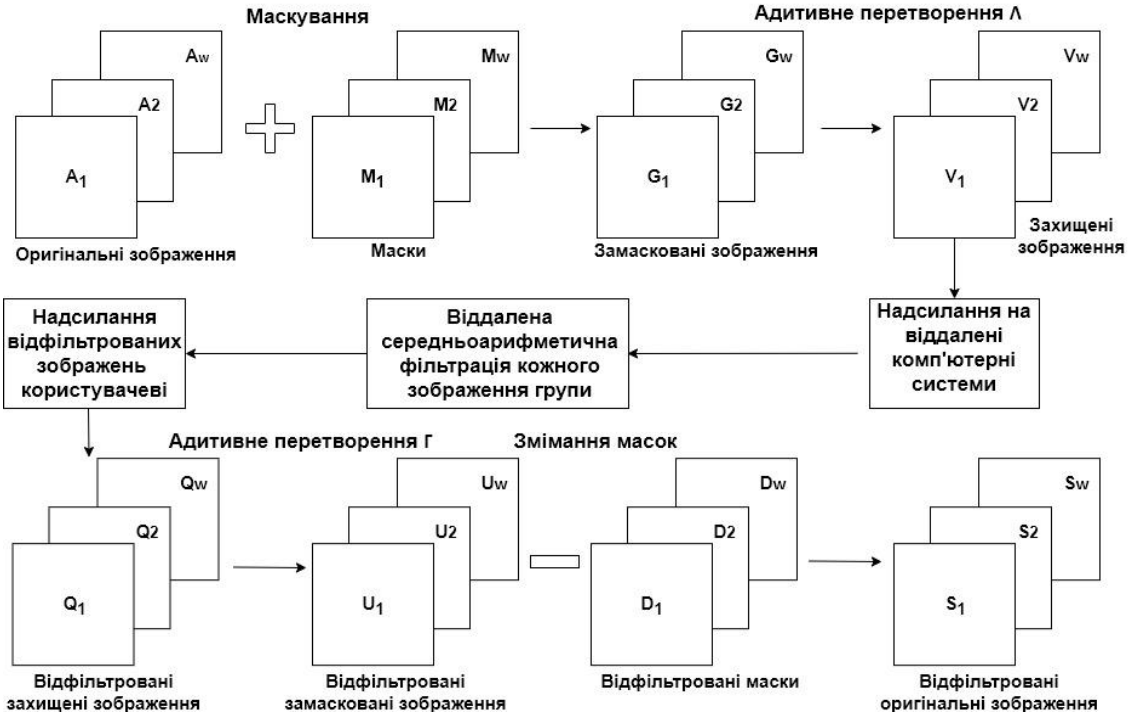

Рис. 2. Схема роботи запропонованого методу захищеної групової середньоарифметичної фільтрації

3. Аналіз ефективності та оптимізація

Оцінку ефективності запропонованого методу захищеної групової середньоарифметичної фільтрації зображень доцільно здійснювати за двома критеріями [9]:

– прискоренням, що забезпечує запропонований метод, в порівнянні з виконанням середньоарифметичної фільтрації зображень на обчислювальних ресурсах користувача;

– рівнем захищеності зображень від несанкціонованого доступу до них в процесі передачі потенційно відкритими каналами та обробки на непідконтрольних користувачу комп'ютерних системах.

Для оцінки рівня захищеності, який забезпечується запропонованим методом, потрібно розглянути кілька ситуацій. Перша з них полягає в тому, що зловмисник має на меті повне відновлення зашифрованих зображень. В запропонованому методі в якості секретного ключа використовується w масок M_1, M_2, …, M_w та пара систем Λ і Г ортогональних лінійних перетворень. Для повного відновлення оригінальних зображень зловмиснику необхідно підібрати систему Λ або зворотну до неї систему Г, а також маски M_1, M_2, …, M_w чи їхні відфільтровані відповідники D_1, D_2, …, D_w. Оскільки в запропонованому методі використовується одна з можливих систем Λ та w з q масок в довільній комбінації, то об'єм ресурсів необхідних для зламу запропонованого методу можна оцінити через об'єм c_{if} ресурсів, потрібних для перебору всіх можливих ключів:

$$c_{if} = c_{im} \cdot c_{is},$$

c_{im} – об'єм ресурсів, потрібних для перебору можливих комбінацій масок;

c_{is} – об'єм ресурсів, потрібних для перебору можливих систем Λ або Г.

В якості оцінки ресурсів c_{is}, що має витратити зловмисник для відновлення вибраної користувачем системи перетворень, може слугувати загальна кількість таких систем. Якщо вважати, що для всіх матриць Λ $\lambda_{ij} \in \{-1, 0, 1\}$, то кількість c_{is} можливих ортогональних систем рівна кількості ортогональних лінійних систем в алгебрі Жегалкіна [10]. Підрахунок c_{is} в залежності від кількості w змінних можна виконати комбінаторними методами. Загальна кількість лінійних булевих функцій від w змінних дорівнює $2^w - 1$ (без урахування їх інверсій). Відповідно, перша функція системи Λ може бути вибрана $2^w - 1 - w$ способами, тобто на роль першої функцій системи Λ підходить будь-яка функція з $2^w - 1$ крім тих, що співпадають зі змінними. Якщо в матриці Λ існує рядок з однією одиничною компонентою, це означає, що одне з зашифрованих зображень V_1, V_2, …, V_w співпадає з оригінальним A_p, тобто одне зображення передається в відкритому вигляді. Оскільки умови задачі захисту виключають можливість передачі зображення в явному вигляді, то кількість можливих лінійних булевих функцій, що можуть використовуватися для адитивного перетворення, зменшується на w.

Друга функція системи Λ може бути вибрана з $2^w - 1 - w$ так, щоб вона не співпадала з першою, тобто $2^w - 2 - w$ способами. Третя функція системи Λ може бути вибрана з $2^w - 1 - w$ так, щоб вона не співпадала з двома раніше обраними та їх лінійною комбінацією, тобто з $2^w - 4 - w$. Аналогічно p-та функція системи Λ, де $p \in \{1, 2, ..., w\}$, може бути вибрана так, щоб не співпадала з будь-якою $2^{p-1} - 1$ лінійних комбінацій раніше обраних $p - 1$ функцій, тобто число варіантів вибору становить $2^w - 2^{p-1} - w$.

Таким чином об'єм c_{is} ресурсів, потрібних для перебору всіх можливих систем Λ або Г може бути обчислений як:

$$c_{is} = \prod_{p=1}^{w} (2^w - w - 2^{p-1}).$$

В таблиці 1 представлено значення об'єму c_{is} ресурсів, потрібних для знаходження системи Λ або Г в залежності від кількості w зображень в межах однієї групи.

Таблиця 1.

Залежність об'єму c_{is} ресурсів, потрібних для знаходження системи Λ або Г від кількості w зображень в групі

w	c_{is}	w	c_{is}
4	3520	8	$4 \cdot 10^{18}$
5	3124550	9	$5{,}8 \cdot 10^{23}$
6	$9{,}4 \cdot 10^{9}$	10	$3{,}3 \cdot 10^{29}$
7	$1 \cdot 10^{14}$	12	$6{,}2 \cdot 10^{42}$

Дані таблиці 1 свідчать про те, що зі збільшенням розміру w групи об'єм перебору різко зростає.

Оцінка об'єму c_{im} ресурсів, потрібних для перебору всіх можливих комбінацій масок може бути виконана з використанням комбінаторних методів. Секретним ключем може бути будь-яка комбінація з w масок M_1, M_2, …, M_w, обраних без повторів з $2^{k \cdot h \cdot n}$ можливих масок, де n – розрядність елементів масок, Тобто, об'єм c_{im} ресурсів може бути обчислений як:

$$c_{im} = \frac{2^{k \cdot h \cdot n}!}{(2^{k \cdot h \cdot n} - w)! w!} = \prod_{\upsilon=0}^{w-1} \frac{2^{k \cdot h \cdot n} - \upsilon}{w - \upsilon}.$$

Відповідно, об'єм c_{if} ресурсів, потрібних для повного відновлення групи з w зображень становить:

$$c_{if} = \prod_{\upsilon=0}^{w-1} \frac{2^{k \cdot h \cdot n} - \upsilon}{w - \upsilon} \cdot \prod_{p=1}^{w} (2^w - w - 2^{p-1}) .$$

Для реальних зображень мінімальне значення $k \cdot h = 1024$, $w = 16$. Тобто, навіть при $w = 1$, обробці одного зображення, об'єм перебору 2^{16384} масок виходить за рамки можливостей технічної реалізації сучасними засобам. Тобто запропонований метод гарантує високий рівень захисту від спроб повного відновлення зображень.

Інший сценарій зламу базується на тому, що зловмисника цікавлять лише основні контури зображення. В такому разі йому достатньо віднайти систему Λ або Г і наближено відновити зображення з використанням статистичних методів. Об'єм ресурсів, потрібних для доступу до w зображень однієї групи можна наближено оцінити через об'єм c_{is} ресурсів, потрібних для знаходження системи Λ або Г. Для цієї ситуації рівень захищенності методу залежить від кількості зображень в одній групі. Зокрема вже при $w \geq 8$, спроби доступу до зображень втрачають доцільність.

Однією з переваг запропонованого методу є можливість зміни рівня захищеності в залежності від класу оброблюваних зображень. З урахуванням того що, запропонований метод передбачає не лише адитивні перетворення, а й маскування, для широкого класу практичних задач оптимальною кількістю зображень в групі є 4.

Для ефективного застосування методу не рекомендується оброблювати суміжні за часом знімки в межах однієї групи.

Ефективність запропонованого методу, в контексті підвищення швидкодії, можна оцінити через коефіцієнт β прискорення. Коефіцієнт β визначається співвідношенням часу t_f середньоарифметичної фільтрації групи зображень лише на ресурсах користувача до часу t_{pf} виконання цієї ж операції за запропонованим методом, тобто з залученням віддалених обчислювальних ресурсів. При цьому, в якості t_f доцільно використовувати час t_{f2} найбільш швидкого варіанту середньоарифметичної фільтрації, тобто обчислювати коефіцієнт β згідно з наступною формулою:

$$\beta = \frac{w \cdot t_{f2}}{t_{pf}} . \qquad (3)$$

Час t_{pf} виконання середньоарифметичної фільтрації w зображень в межах однієї групи згідно з запропонованим методом дорівнює сумарному часу шифрування і дешифрування w зображень однієї групи:

$$t_{pf} = w \cdot t_{mask} + t_{tr} ,$$

де t_{mask} – час накладанння і знімання маски з одного зображення;

t_{tr} – час прямого та зворотного перетворення w зображень в межах однієї групи.

В свою чергу, час t_{mask} накладання і знімання маски з одного зображення визначається сумарним часом виконання однієї операції додавання та однієї операції віднімання для кожного з елементів зображення $t_{mask} = 2 \cdot k \cdot h \cdot t_a$.

За умови що $\lambda_{ij} \in \{-1, 0, 1\}$, w лінійних перетворень системи Λ включають в себе лише операції додавання чи віднімання відповідних елементів w зображень G_1, G_2, …, G_w. Оскільки перетворення системи Г, зворотної до Λ, також є лінійними, то час їхнього виконання є аналогічним. Таким чином час t_{tr} визначається формулою $t_{tr} = 2 \cdot w^2 \cdot k \cdot h \cdot t_a$.

Відповідно, час t_{pf} виконання середньоарифметичної фільтрації w зображень в межах однієї групи згідно до запропонованого методу становить $t_{pf} = 2 \cdot w \cdot k \cdot h \cdot t_a \cdot (1 + w)$.

З урахуванням наведеного вище, формула (3) коефіцієнту β прискорення може бути конкретизована у наступному вигляді:

$$\beta = \frac{w \cdot k \cdot h \cdot ((r+2) \cdot t_a + t_d)}{2 \cdot w \cdot k \cdot h \cdot t_a \cdot (1 + w)} . \qquad (4)$$

З формули (4) слідує, що коефіцієнт β прискорення значною мірою залежить від кількості w зображень в одній групі. Зі збільшенням значення w ефективність запропонованого методу зменшується, але, з іншого боку, стрімко зростає рівень захищенності. Таким чином, вибір значення w потребує вирішення компромісу між прискоренням обробки зображень та рівнем їхньої захищеності. Згідно з проведеними експериментальними дослідженнями оптимальною кількістю зображень в групі для широкого класу прикладних задач становить чотири: $w = 4$.

Таким чином, з врахуванням оцінок [7] швидкодії виконання окремих операцій та того, що при вирішені практичних задач значення апертури становить 11: $r = 11$, наближене значення коефіцієнту β дорівнює 4.

4. Висновки

В результаті проведених теоретичних і експериментальних досліджень, спрямованих на прискорення попередньої обробки зображень методом середньоарифметичної фільтрації, було розроблено метод віддаленої захищеної групової середньоарифметичної фільтрації з залученням високопродуктивних віддалених обчислювальних потужностей. Виявлено, що перспективним напрямком організації криптографічного захисту зображень є використання адитивного перетворення зображень. Доведено, що розроблений метод забезпечує високий рівень захищеності від спроб відновити зображення як підбором ключа, так і статистичною обробкою. Використання запропонованого методу дозволяє підвищити продуктивність середньоарифметичної фільтрації зображень в 4 рази в порівнянні з виконанням цієї операції без залучення віддалених обчислювальних потужностей.

Важлива перевага методу полягає в можливості гнучкої зміни рівня захищеності в залежності від вимог конкретного застосування. Це здійснюється за рахунок зміни кількості зображень в групі. Збільшення кількості зображень, оброблюваних в межах однієї групи, має наслідком стрімке підвищення рівня захищеності, проте зменшує виграш в часі. Розроблений метод орієнтований для використання в системах обробки насамперед аерокосмічних зображень.

Список використаної літератури

1. Tari Z. Security and Privacy in Cloud Computing: Vision, Trends and Chanllenges / Zahir Tari, Xun Yi, Uthpala S. Premarathne, Peter Bertok, and Ibrahim Khalil // IEEE Trans. on Cloud Computing. – 2015. – V.2, №2. – P. 30-38.

2. Pengyao Wang. Rapid processing of remote sensing images based on cloud computing / PengyaoWang,JianqinWang, YingChen, Guangyuan Ni // Future Generation Computer Systems. – 2013. – V.29, №8. – P. 1963-1968.

3. Bardis N. G. Secure Implementation of Modular Exponentiation on Cloud Computing Resources / N. G. Bardis , O. P.Markovskyi // Proceeding of International Conference Applied Mathematics, Computational Science and Systems Engineering. Athens, Greece, October 6-8, – 2017. – P.90-96.

4. Monjur Ahmed. Cloud Computing and Security Issues in the Cloud / Monjur Ahmed, Mohammad Ashraf Hossain // International Journal of Network Security & Its Applications (IJNSA). – 2014. – V.6, №1. – P. 25-36.

5. Sathish V. Cloud-based Image Processing With Data Priority Distribution Mechanism / V. Sathish, T. A. Sangeetha // Journal of Computer Applications. – 2013. – V.6, №1. – P. 6-8.

6. Марковський О. П. Захищена реалізація фільтрації зображень в GRID-системах / О. П. Марковський, М. В. Невдащенко, А. М. Білашевська // Вісник Національного технічного університету України «КПІ». Інформатика, управління та обчислювальна техніка, – Київ: ТОО «ВЕК+». – 2014. – № 61. – С.105-109.

7. Брэй Б. Микропроцессоры Intel. Архитектура, программирование и интерфейсы. Восьмое издание / Б. Брэй. – Санкт-Петербург: БХВ-Петербург, 2015. – 1328 с.

8. Костенко Ю. В., Метод защищенного модулярного экспоненцирования на удаленных компьютерных системах / Ю. В. Костенко, А. П. Марковский, О. В. Русанова // Вісник

Національного технічного університету України «КПІ». Інформатика, управління та обчислювальна техніка. Київ: ТОО «ВЕК+». – 2016. – № 64. – С. 51-54.

9. Буйбарова М. Ф. Метод захищеної реалізації перетворень Фур'є на віддалених розподілених комп'ютерних системах / М. Ф. Буйбарова, Ю. М. Виноградов, В. Ю. Приймак // Вісник Національного технічного університету України «КПІ». Інформатика, управління та обчислювальна техніка. – Київ: ТОО «ВЕК+». – 2016. – № 64. – С. 64-71.

10. Задірака В. К. Комп'ютерна криптологія: підручник / В. К. Задірака, О. С. Олексюк. – Київ: Вища школа. – 2002. – 504с.

References

1. Zahir Tari, Xun Yi, Uthpala S. Premarathne, Peter Bertok, and Ibrahim Khalil. (2015). "Security and Privacy in Cloud Computing: Vision." *Trends and Chanllenges. IEEE Trans. on Cloud Computing,* V.2, No2: 30-38. Print.

2. PengyaoWang, JianqinWang, YingChen, and Guangyuan Ni. (2013). "Rapid Processing of Remote Sensing Images Based on Cloud Computing." *Future Generation Computer Systems.* V.29, No8: 1963-1968. Print.

3. Bardis N. G., and Markovskyi O. P. (2017). "Secure Implementation of Modular Exponentiation on Cloud Computing Resources." *Proceeding of International Conference Applied Mathematics, Computational Science and Systems Engineering. Athens, Greece, October 6-8, 2017*. 90-96. Print.

4. Monjur Ahmed, and Mohammad Ashraf Hossain. (2014). "Cloud Computing and Security Issues in the Cloud." *International Journal of Network Security & Its Applications (IJNSA).* V.6, No1. 25-36. Print.

5. Sathish V., and Sangeetha T. A. (2013). "Cloud-based Image Processing With Data Priority Distribution Mechanism." *Journal of Computer Applications*. V.6, 1: 6-8. Print.

6. Markodskyi O. P., Nevdashenko M. V., and Bilashevska A. M. (2014). "Secure Implementation of Image Filtering in GRID Systems." *Bulletin of the National Technical University of Ukraine "KPI". Informatics, management and computer engineering*, 61: 105-109. Print.

7. Brai B. (2015). "Intel Microprocessors. Architecture." *Programming and Interfaces. St. Petersburg: БХВ BKhV- Petersburg:*1328. Print.

8. Kostenko Yu. V., Markodskyi O. P., and Rusanova O. V. (2016). "Secure Modular Exponential Method on Remote Computer Systems." *Bulletin of the National Technical University of Ukraine "KPI". Informatics, Management and Computer Engineering*, 64: 51-54. Print.

9. Buibarova M. F., Vinohradov Yu. M., and Pryimak V. Yu. (2016). "Method of Secure Implementation of Fourier Transforms on Remote Distributed Computer Systems." *Bulletin of the National Technical University of Ukraine "KPI". Informatics, Management and Computer Engineering*, 64: 64-71. Print.

10. Zadiraka V. K., and Oleksiuk O. S. (2002). *Computer Cryptology*. Kyiv: Vyshcha Shkola: 504. Print.

Автори статті (Authors of the article)

Марковський Олександр Петрович – к.т.н., доцент кафедри обчислювальної техніки (Markovskyi Oleksandr Petrovych – PhD in technic, Associated Professor of Computer Technic Department). Phone: +380 96 710 8534. E-mail: markovskyy@i.ua.

Гуменюк Інна Олександрівна – студентка (Humeniuk Inna Oleksandrivna – student). Phone: +380 68 341 5612. E-mail: humeniuk.inna@gmail.com.

Міратаї Аліреза – аспірант (Mirataei Alireza – post graduate student). Phone: +380 96 160 7125. E-mail: alirezaataei@gmail.com.

Торошанко Ярослав Іванович – к.т.н., доцент кафедри комп'ютерної інженерії (Toroshanko Yaroslav Ivanovych – PhD in Technics, Associated Professor of the Computer Engineering Department). Phone: +380 50 555 5114. E-mail: toroshanko@ukr.net.

Волощук Максим Олегович – студент (Voloshchuk Maksym Olehovych – student). Phone: +380 67 589 3628. E-mail: svp.pb.vvm@gmail.com