УДК 621.397

О.Г. Оксіюк[1], Д.С. Гаврилов[2], П.М. Гуржій[3], Б.О. Демідов[2]

[1] *Київський національний університет ім. Тараса Шевченка, Київ*
[2] *Харківський національній університет Повітряних Сил ім. Івана Кожедуба, Харків*
[3] *Військовий інститут телекомунікацій та інформатизації, Київ*

# МЕТОД ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ НА ОСНОВІ БАГАТОРІВНЕВОЇ СЕЛЕКТИВНОЇ ОБРОБКИ В ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

*Проаналізовано алгоритм JPEG на наявність значущих компонент на кожному з етапів обробки даних. Запропоновано багаторівневу схему селективної обробки базового кадру для забезпечення конфіденційності переданої інформації за відведений час.*

***Ключові слова:*** *захист, кадр, безпілотний літальний апарат.*

## Вступ

**Постановка проблеми в загальному вигляді.** В сучасних збройних конфліктах та в зонах проведення антитерористичних операцій (АТО) активного застосування на тактичному рівні отримали безпілотні літальні апарати (БПЛА). При цьому частка застосування БПЛА збільшується щорічно. Дана тенденція зберігається завдяки високій ефективності виконання завдань по повітряній розвідці. Функціонально БПЛА призначені як для здобування інформації про положення та сили противника, так і про положення, сили та рівень замаскованості союзних військ. З комерційної точки зору більш вигідним є не побудова власних БПЛА, а перехоплення даних, що передаються з борта БПЛА при виконанні завдання. З даних міркувань актуальним є завдання забезпечення конфіденційної передачі даних з борта БПЛА на пункт дистанційного управління. Одним з можливих підходів до вирішення цього завдання може бути застосування алгоритмів селективної обробки з виділенням значущої інформації та її подальшим шифруванням. Даний підхід здатен обробляти дані за час, менший ніж при послідовній схемі обробки даних, завдяки чому забезпечується оперативність передачі актуальної інформації.

**Аналіз останніх досліджень і публікацій.** Питанню селективної обробки даних на основі алгоритму JPEG присвячена достатня кількість публікацій [2–5; 7; 10], проте запропоновані методи забезпечують той чи інший рівень захисту на одному з етапів обробки даних, та мають недоліки як пропущення інформації, так і захист надлишкових даних.

**Формулювання мети статті.** Завданням досліджень є удосконалення методів захисту кадру за рахунок застосування багаторівневого аналізу та захисту значущих компонент.

При цьому процес передачі даних має відповідати наступним вимогам:

- оперативність;
- конфіденційність;
- достовірність.

Так як метод, що розробляється, має передавати інформацію переважно тактичного рівня, яка характеризується короткостроковим життям (від декількох хвилин до десятків годин), ключовим критерієм є здатність запропонованого методу виконувати поставлене завдання за визначений короткий проміжок часу. Виходячи з того, що оперативність передачі даних залежить від об'єму даних, що обробляються $W_{ст}$, часу роботи шифратора $T_ш$ /дешифратора $T_{дш}$, компресора $T_к$ /декомпресора $T_{дк}$ та часу передачі по каналах зв'язку $T_п$, загальний час на обробку та доставку даних $T(W_{ст})_д$ визначається за виразом:

$$T(W_{ст})_д = T_к + T_ш + T_п + T_{дш} + T_{дк}.$$

Таким чином, умова оперативної передачі даних виконується за умови:

$$T(W_{ст})_д \le \min\left\{T(W)_{вим}; T_{доп}\right\},$$

де $T(W)_{вим}$ – час, за який, по вимогам системи передачі даних, має відбутися обробка та передача даних об'єму W; $T_{доп}$ – час процесу обробки та передачі даних, який є допустимим для нормального функціонування системи.

Під конфіденційністю С будемо розуміти властивість інформації, яка полягає в неможливості несанкціонованому користувачу V заволодіти інформацією I, яка належить авторизованому користувачу A.

$$C = \begin{cases} I \in A, \\ I \notin V. \end{cases}$$

Рівень достовірності будемо визначати за допомогою пікового відношення сигнал/шум для авторизованого користувача.

$$h_{ав} = 20\ell g\left(\frac{255}{\sqrt{\sum_{i=1}^{Z_{стр}}\sum_{j=1}^{Z_{стб}}(a_{ij}-a'_{ij})^2 / Z_{стр}\cdot Z_{стб}}}\right),$$

де $a_{ij}$, $a'_{ij}$ – відповідність вихідного та відновленого значення $(i;j)$-го елемента; $Z_{стр}$, $Z_{стб}$ – кількість рядків та стовпців в кадрі зображення.

При цьому отримана інформація $I_{отр}$ вважається достовірною, якщо виконується вимога:

$$I_{отр} = I_{пер},$$

де $I_{пер}$ – інформація, що передавалась.

## Виклад основного матеріалу

Розробляючи багаторівневий селективний алгоритм захисту базового кадру, проведений аналіз вказав, що сучасні методи селективної обробки даних на основі алгоритму JPEG забезпечують той чи інший рівень захисту аналізуючи дані лише за одним з параметрів. Так на етапі перетворення з кольорового простору RGB в кольоровий простір YCrCb значущою інформацією є компонента яскравості, виділення якої не є додатковою операцією. При цьому блоковий експрес аналіз дозволяє виділити блоки, що несуть інформацію, від блоків, що її не несуть за незначний в порівнянні з методами, що працюють на наступних етапах, час. Проте ймовірність пропуску інформації даного методу не задовольняє вимоги по захисту. Для усунення цього недоліку пропонується застосування аналізу на етапі ДКП. Запропоновано використовувати адаптивний метод, викладений в роботі [10], який приймає за значущу інформацію низькочастотні компоненти та шифрує їх в обсязі, який залежить від класу (насиченості) блоку.

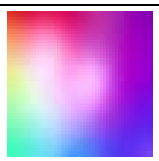
Адаптація запропонованого в роботі [10] методу полягає в тому, що рівень насиченості блоку, за даними дослідження, можливо оцінити за кількістю логічної «1» в порівнянні з логічним «0» блоці (табл. 1), де відношення «1» до «0» визначається наступним чином:

$$K = \frac{n_1}{n_0} * 100\%,$$

де K – показник, який визначає наявність контурів в блоці; $n_1$ – кількість «1» в блоці; $n_0$ – кількість «0» в блоці.

Таблиця 1

Результати проведеного досліду

| |  |  |  |  |  |
|---|---|---|---|---|---|
| розмір блоку | 8 × 8 | 8 × 8 | 8 × 8 | 8 м 8 | 8 × 8 |
| ймовірність появи «1» | 0,0059 | 0,2928 | 0,2749 | 0,4668 | 0,4761 |
| ймовірність появи «0» | 0,9941 | 0,7079 | 0,75251 | 0,5332 | 0,5239 |
| відношення "1" до "0" (К), % | 0,5935 | 41,3617 | 36,5311 | 87,5468 | 90,8761 |
| клас блоку | без контуру | з поступовим переходом | | з контуром | |

Останнім рівнем захисту є кластерне кодування та шифрування на основі змінних таблиць статистичних взаємозв'язків.

До переваг даного методу можна віднести:

1. Яскраво виражена значуща інформація буде відфільтрована та закодована на першому етапі, що дозволить не затрачати час на її обробку на наступних етапах;
2. У разі пропуску інформації більш ретельний аналіз по низькочастотним компонентам дозволить забезпечити необхідний рівень захисту;
3. Кластерне кодування та шифрування змінними таблицями статистичних взаємозв'язків дозволить з збереженням рівня компресії підвищити рівень захисту даних.

В загальному вигляді блок-схема симетричного алгоритму прийме вигляд рис. 1.

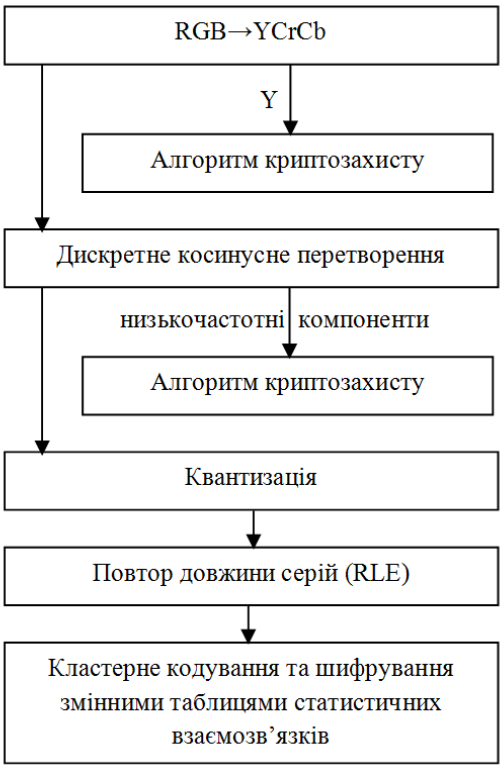



Рис. 1. Блок-схема багаторівневого методу селективної обробки даних

## Висновки

У результаті проведених досліджень визначено особливості інформативних даних на кожному етапі алгоритму JPEG. Запропоновано багаторівневу схему обробки базового кадру для передачі даних відеоінформації з борта БПЛА на пункт дистанційного управління, що забезпечить оперативну, конфіденційну передачу даних на тактичному рівні.

## Список літератури

*1. Gavrulov D. The analysis of template method of video processing / V. Larin, P. Krasnikov, D. Gavrulov // Proceedings of 2015 1st International Conference on Advanced Information and Communication Technologies-2015 (AICT'2015), Lviv, Ukraine, October 29 – November 1, 2015. – P. 87-89.*

*2. Grangetto M. Multimedia Selective Encryption by Means of Randomized Arithmetic Coding / M. Grangetto, E. Magli, G. Olmo // IEEE Transactions on Multimedia. – 2006. – T. 8.*

*3. Qiao L. A New Algorithm for MPEG Video Encryption / L. Qiao, K. Nahrstedt // International Conference on Imaging Science, Systems, and Technologies (CISST '97). 1997.*

*4. Spanos G.A. Security for Real-Time MPEG Compressed Video in Distributed Multimedia Applications / G.A. Spanos, T.B. Maples // IEEE 15th International Phoenix Conference on Computer Communications. – 1996.*

*5. Гаврилов Д.С. Метод захисту низькочастотних складових в алгоритмі кодування JPEG / В.В. Ларин, Д.С. Комолов, К.В. Ялівець, Д.С. Гаврилов // Системи обробки інформації. – Х.: ХУПС, 2015. – Вип. 9(134). – С. 121-123.*

*6. Баранник В.В. Метод повышения информационной безопасности в системах видеомониторинга кризисных ситуаций: монография / В.В. Баранник, Ю.Н. Рябуха. – Черкассы, 2015. – 143 с.*

*7. Barannik V.V. The model of avalanche-relating effect in the process of images reconstruction in the combined cryptosemantic systems on the polyadic presentation / V.V. Barannik, V.V. Larin, S.A. Sidchenko // Наукоємні технології. – 2010. – № 1(5). – С. 68-70.*

*8. Бараннік В.В. Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку / А.В. Власов, В.В. Бараннік, Р.В. Тарнополов // Наукоємні технології. – 2014. – № 1(21). – С. 55-60.*

*9. Баранник В.В. Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления / В.В. Баранник, А.В. Власов, С.А. Сидченко, А.Э. Бекиров // Информационно-управляющие системы на ЖД транспорте. – 2014. – №3. – С. 24-31.*

*10. Бараннік В.В. Селективний метод шифрування видеопотоку в телекомуникаційних системах на основі приховування базового І-кадру / В.В. Бараннік, Д.І. Комолов, Ю.М. Рябуха // Наукоємні технології. – № 2. – 2015. – С. 14-23.*

*Надійшла до редколегії 12.01.2017*

**Рецензент**: д-р техн. наук проф. В.В. Бараннік, Харківський національний університет Повітряних Сил ім. Івана Кожедуба, Харків.

### МЕТОД ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВИДЕОИНФОРМАЦИОННОГО РЕСУРСА НА ОСНОВЕ МНОГОУРОВНЕВОЙ СЕЛЕКТИВНОЙ ОБРАБОТКИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ

А.Г. Оксиюк, Д.С. Гаврилов, П.Н. Гуржий, Б.А. Демидов

*Проанализировано алгоритм JPEG на наличие значимых компонент на каждом из этапов обработки данных. Предложено многоуровневую схему селективной обработки базового кадра для обеспечения конфиденциальной передачи информации за отведенное время.*

***Ключевые слова:*** *защита, кадр, беспилотный летательный аппарат.*

### METHOD SAFETY VIDEOINFORMATION RESOURCES THROUGH A TIERED SELECTIVE TREATMENT IN TELECOMMUNICATION SYSTEMS

O.G. Ocsiuk, D.S. Havrylov, P.M. Guzhiy, B.O. Demidov

*JPEG algorithm has been analyzed for the presence of significant components at each stage of processing. It has been purposed scheme of selective treatment of the base frame to ensure the confidentiality of transmitted information in the allotted time.*

***Keywords:*** *protection, frame, drone.*