УДК 681.3

В.В. Ларін, Д.С. Гаврилов, Д.І. Комолов, К.В. Яливець

Харківський університет Повітряних Сил імені Івана Кожедуба, Харків

МЕТОД ЗАХИСТУ НИЗЬКОЧАСТОТНИХ СКЛАДОВИХ В АЛГОРИТМІ КОДУВАННЯ JPEG

В роботі викладено адаптивно-селективний алгоритм, який спирається на захисті низькочастотних компонент за допомогою симетричного криптоалгоритма ГОСТ 28147-89. Алгоритм забезпечує виконання завдання захисту відеоінформації при передачі з борту безпілотного літального апарату на наземні системи комплексів повітряної розвідки з необхідною оперативністю, достовірністю та скритністю.

Ключові слова: *відеоінформація, захист, низькочастотні компоненти, безпілотній літальний апарат.*

Вступ

Постановка проблеми досвід ведення бойових дій в зоні антитерористичної операції (АТО) показав, що під час ведення повітряної розвідки за допомогою безпілотного літального апарату (БПЛА) відеоінформація може бути перехоплена противником. Виконання завдання БПЛА по розвідці місцевості умовно можна поділити на три основні етапи (фази) φ: початкова фаза польоту (зліт та вихід на маршрут), розвідка території противника та кінцева фаза польоту(повернення на контрольовану територію). На початковій та кінцевій фазі польоту БПЛА пролітає над контрольованою нашими військами територію, на якій знаходяться наші позиції та техніка. Тож, імовірність спостерігання за союзними військами на початковій і кінцевій фазі польоту близьке до 1, а на ворожій імовірність прямує до 0.

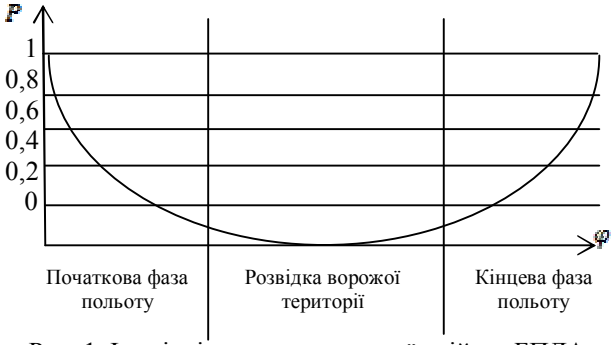

Рис. 1. Імовірність виявлення своїх військ БПЛА під час польоту

Рис. 1 вказує на необхідність захисту відеоінформаційного потоку, який передається з борта на диспетчерський пункт від несанкціонованого доступу з виконанням умов по оперативності, скритності та достовірності для авторизованого користувача.

Аналіз останніх досліджень і публікацій показав, що при використання цифрового відеозв'язку загальна затримка в каналі зв'язку не повинна перевищувати 150 мс. Під сумарною затримкою будемо розуміти не лише шифрування/дешифрування даних, але й компресію, передачу, прийом, декомпресію та відображення [1]. Тож, чим менше додаткових часових трат вносить шифрування/ дешифрування, тим краще ми зможемо забезпечити оперативність передачі даних. Також вдалось з'ясувати, що інформаційна місткість низькочастотних компонент в 2 та більше разів перевищує високочастотні компоненти. Низькочастотні компоненти містять інформацію про плавне змінювання кольору на зображенні, а високочастотні про різке (контури об'єктів) [2, 3]. Отже, захист лише низькочастотних елементів надасть нам змогу обмежити коло доступу до важливої для нас інформації не витрачаючи час та обчислювальні ресурси на шифрування другорядних даних.

Формулювання мети статті: обґрунтування імовірності забезпечення захисту відеоінформації від несанкціонованого доступу з забезпеченням достовірності, оперативності та скритності.

Постановка задачі

Під достовірністю будемо розуміти суму імовірністей правильного відтворення шифрованої та відкритої інформації для авторизованого користувача, яка може варіюватися від [0; 2]. Для задоволення потреб у якості відтворення значення $P_{заг}$ має бути близьким до 2, причому

$$P_{заг} = P_{ш} + P_{в},$$

$$P_{ш} = \max_{1 \le i \le M} \{P_{ш_i}\},$$

де $P_{ш}$ – імовірність правильного відновлення шифрованих даних; $P_{ш_i}$ – ймовірності правильного відновлення шифрованої частини інформаційної частини, у разі використання зловмисником і-го методу крипто аналізу;

$$P_{в} = \max_{1 \le i \le M} \{P_{в_i}\},$$

де $P_{в}$ – імовірність правильного відновлення відкритого тексту; $P_{в_i}$ – ймовірності правильного відновлення відкритої інформаційної частини, у разі використання зловмисником і-го методу криптоаналізу.

Також мінімальний час впродовж якого обраний алгоритм буде виконувати свої захисні властивості.

$$T_б = \min_{1 \le i \le M} \{T_{б_i}\},$$

де $T_{б_i}$ – безпечний час функціонування алгоритму, який реалізує і-й метод крипто аналізу.

Під скритністю будемо розуміти пікове відношення сигнал/шум для авторизованого користувача.

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

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

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

Отже, для задоволення потреб авторизованого користувача розроблений алгоритм повинен задовольняти таким умовам:

$$P_{заг} \to 1;\ h_{ав} \to 1;\ T(W_{ст})_д \le \min\{T(W)_{вим}; T_{доп}\},$$

а для несанкціонованого:

$$P_{заг} \to 0; \qquad h_{несанкц.} \to 0.$$

Виклад основного матеріалу

Розробляючи селективно-адаптивний алгоритм шифрування основаного на алгоритмі кодування JPEG (рис. вдалось класифікувати зображення. Дана операція стала можливою після дискретно-косинусного перетворення (ДКП), коли низькочастотні компоненти знаходяться у верхній лівій частині блоку, та їх розмір не перевищує 4х4 (16 елементів), які можуть нести інформацію про контури об'єкти на зображенні.

$$P_{дкп} = \sum_{i=1}^{4} \sum_{j=1}^{4} a_{ij} \Big/ 16$$

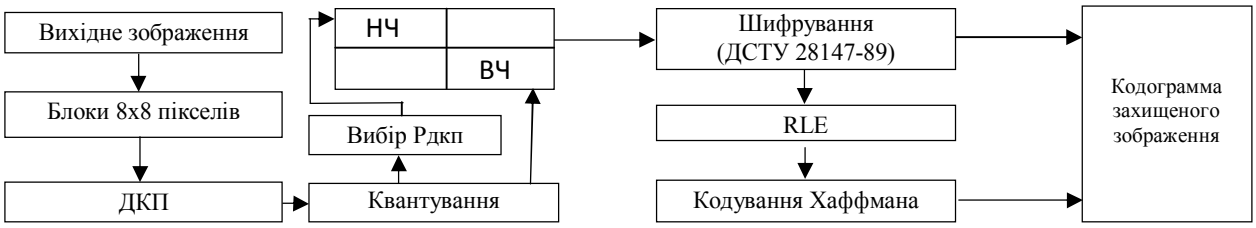

Рис. 2. Адаптивно-селективний метод захисту зображення з використанням заданого рівня шифрування низькочастотної складової зображення

– слабонасичені зображення

$$ДР_{слабо.насич.} \to n_1 = [1;6];$$

– середньонасичені зображення

$$ДР_{серед.насич.} \to n_2 = [7;10];$$

– сильнонасичені зображення

$$ДР_{сильн.насич.} \to n_3 = [11;16].$$

Для визначення до якого саме класу відноситься зображення після ДКП введемо операцію визначення порогу за умовою:

$$P_{дкп} = \begin{cases} n_1 \to P_{дкп} \in ДР_{слаб.насич.}; \\ n_2 \to P_{дкп} \in ДР_{серед.насич}; \\ n_3 \to P_{дкп} \in ДР_{сильн.насич}. \end{cases}$$

Саме визначення зображення за класом дає змогу захистити необхідну та достатню кількість інформації. Ця кількість інформації надає змогу захистити інформацію від сторонніх осіб не збільшивши, значною мірою, час на обробку даних.

Висновки

В статті обґрунтовано необхідність захисту відеоінформаційного ресурсу та можливість виконання цієї умови шляхом захисту лише низькочастотних компонентів з використанням адаптивно-селективного методу в алгоритмі JPEG. Розроблений метод справляється з поставленою задачею та виконує захист зображень від несанкціонованого доступу противника з відповідністю умовам по достовірності, оперативності та скритності. Даний метод може використовуватися при обробці даних на борту літального апарату для забезпечення захисту державного відеоінформаційного ресурсу та збереження державної таємниці.

Список літератури

1. Фахрутдинов Р.Ш. Метод защиты видеоданных с различной степенью конфиденциальности / Р.Ш. Фахрутдинов. – СПб,: 2012. – 125 с.

2. Ватолин Д. Метод сжатия данных. Устройство архиваторов, сжатия изображений и видео / Д. Ватолин, А. Ратушняк, М. Смирнов. – М.: ДИАЛОГ-МИФИ , 2003. – 463 с .

3. Красильников Н.Н. Цифровая обработка изображений / Н.Н. Красильников. – М. Вузовская книга, 2011. – 320 с.

Надійшла до редколегії 20.05.2015

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

МЕТОД ЗАЩИТЫ НИЗКОЧАСТОТНЫХ СОСТАВЛЯЮЩИХ В АЛГОРИТМЕ КОДИРОВАНИЯ JPEG

В.В. Ларин, Д.С. Гаврилов, Д.И. Комолов, К.В. Яливец

В работе изложен адаптивно - селективный алгоритм основанный на защите низкочастотных компонент с помощью симметричного криптоалгоритма ГОСТ 28147-89. Данный алгоритм обеспечивает выполнение задачи защиты видеоинформации при передачи с борта беспилотного летательного аппарата на наземные системы комплексов воздушной разведки с требуемой оперативностью, достоверностью и скрытностью.

Ключевые слова: *видеоинформация, защита, низкочастотные компоненты, беспилотный летательный апарат.*

SAVE LOW-FREQUENCY ELEMENT IN ALGORITHM COMPRESSING JPEG

V.V. Larin, D.S. Gavrilov, D.I. Komolov, K.V. Yalivets

In the work relation adaptive- selective algorithm. Base is algorithm this is save low-frequency element use symmetrical coder GOST 28147-89. This algorithm provide save videoinformation to broadcast from unmanned airplane to command post with necessary speed, authentic and reserve.

Keyword*: videoinformation, save, save low-frequency element, unmanned airplane.*