Александр В. Винокуров, Алексей А. Задвижкин
Краснодарское высшее военное училище им. генерала армии С.М. Штеменко,
ул. Красина, 6, г. Краснодар, 350063, Россия
e-mail: VAV73@rambler.ru, http://orcid.org/0000-0002-2743-5229
e-mail: z2a82@yandex.ru, http://orcid.org/0000-0002-1116-1921

ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ВИДОВОЙ ИНФОРМАЦИИ ПУТЕМ СОГЛАСОВАННОГО ПРИМЕНЕНИЯ МЕТОДОВ ЕЕ ОБРАБОТКИ И ЗАЩИТЫ

DOI: http://dx.doi.org/10.26583/bit.2019.1.05

Аннотация. Для разрешения противоречия между необходимостью обеспечения требований достоверности видовой информации при ее передаче по радиолиниям в условиях воздействия помех и обеспечения ее защищенности с использованием методов криптографической защиты, предложено согласованное применение методов ее обработки и защиты, которое заключается в сохранении естественной избыточности видовой информации в процессе ее сжатия и в последующем использовании для защиты от ошибок, возникающих в радиолинии. Предлагается концептуально новый подход к рассмотрению подсистемы криптографической защиты информации не как обособленной и индифферентной к вышестоящим и нижестоящим уровням обработки информации части замкнутой системы, а как элемента комплексной системы обработки и защиты информации. В качестве механизма криптографической защиты видовой информации рассматривается сочетание перестановки блоков изображения и наложения гаммы шифра. Такое сочетание классических криптоалгоритмов не размножает ошибки, а искажения отдельных битов, возникающих вследствие воздействия помех в радиолинии, устраняются за счет естественной избыточности видовой информации и помехоустойчивого кодирования. Для проведения корреляционного анализа стойкости комбинированного метода криптозащиты и качественной оценки возможности его применения разработано программное средство. Разработана блок-схема алгоритма синтеза параметров помехоустойчивого кодирования и программное средство, осуществляющее полный перебор параметров алгоритма. Отличительной особенностью программного средства является возможность получения статистических данных для решения оптимизационных задач повышения оперативности прохождения видовой информации или повышения ее достоверности. В качестве примера приведены значения параметров оптимального помехоустойчивого кода для кадра изображения объемом 200 Кб.

Ключевые слова: беспилотные летательные аппараты, видовая информация, избыточность, криптографическая защита, перераспределение избыточности.
Для цитирования: ВИНОКУРОВ, Александр В.; ЗАДВИЖКИН, Алексей А. ПОВЫШЕНИЕ ЗАЩИЩЕННОСТИ ВИДОВОЙ ИНФОРМАЦИИ ПУТЕМ СОГЛАСОВАННОГО ПРИМЕНЕНИЯ МЕТОДОВ ЕЕ ОБРАБОТКИ И ЗАЩИТЫ. Безопасность информационных технологий, [S.l.], p. 46-55, 2019. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1179>. Дата доступа: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.05.

Alexandr V. Vinokurov, Alexey A. Zadvizhkin
Higher Military School named after army General S.M. Schtemenko,
Krasina str., 6, Krasnodar, 350063, Russia
e-mail: VAV73@rambler.ru, http://orcid.org/0000-0002-2743-5229
e-mail: z2a82@yandex.ru, http://orcid.org/0000-0002-1116-1921

Improving the visual information security by consistent application of methods for its processing and protection

DOI: http://dx.doi.org/10.26583/bit.2019.1.05

Abstract. To meet the reliability requirements the visual information transmitted over the radio lines over noisy background must be protected using cryptographic protection methods. That is why an agreed application of processing and protection of visual information has been proposed, which consists in maintaining natural redundancy of visual information in the process of compression and in the subsequent use for protection against the mistakes arising in the radio line. The conceptually new approach to consideration of cryptographic information security subsystem not as a part of the information processing closed system, which is isolated and indifferent with respect to above and below levels, but rather as an

element of a complex processing and information security system is suggested. A combination of the image blocks permutation and a cipher gamma superimposing is considered as a mechanism of cryptographic protection of visual information. Such combination of classical cryptographic algorithms does not multiply the errors, while the distortions of the separate bits arising by the influence of interference in the radio line are eliminated due to natural redundancy of visual information and noise-immune coding. A software tool has been developed to carry out a correlation analysis of the combined cryptoprotection method stability and the qualitative assessment of its use. A block diagram of the algorithm for synthesizing the parameter of noise-immune encoding and a software tool performing a complete enumeration of the algorithm parameters are developed. A distinctive feature of the software is the ability to obtain statistical data for solving optimization problems to increase the efficiency of the passage of visual information and therefore to increase its reliability. As an example, the parameter values of the optimal noise-immune code for an image frame of 200 KB are provided.
Keywords: unmanned aerial vehicles, visual information, redundancy, cryptographic protection, redundancy redistribution.
For citation: VINOKUROV, Alexandr V.; ZADVIZHKIN, Alexey A. Improving the visual information security by consistent application of methods for its processing and protection. IT Security (Russia), [S.l.], p. 46-55, 2019. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1179>. Date accessed: 19 feb. 2019. doi:http://dx.doi.org/10.26583/bit.2019.1.05.

Введение

Современные комплексы с беспилотными летательными аппаратами (БЛА) оснащаются полезными нагрузками для проведения фото- и видеосъемки. Поскольку данные, передаваемые с данных комплексов, могут содержать сведения ограниченного распространения, то для них определены требования нормативных документов по обеспечению безопасности как состояния защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность [1].

Рассмотрим типовую схему этапов обработки и защиты видовой информации, представленную на рис. 1.

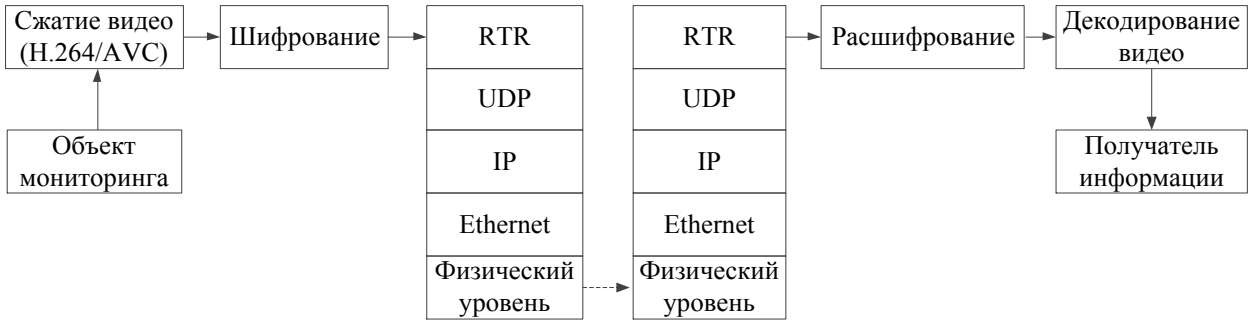

Рис. 1. Структурная схема этапов обработки и защиты видовой информации
(Fig. 1. Block diagram of the stages of processing and protection of visual information)

Выбор стандарта H.264 (рис. 1), обеспечивающего высокую степень сжатия видеопотока при сохранении его высокого качества, обоснован более расширенными возможностями по сравнению с предыдущими стандартами (H.261, H.263), а также тем, что в настоящее время он является основным при разработке программного обеспечения для видеоконференций. Способ сжатия видеоданных, в котором применяется трехмерное косинусное преобразование, рассмотрен в работе [3]. Перспективным методом сжатия видеоинформации является техника, основанная на вейвлет-преобразованиях и широко применяемая в современных Web-камерах в среде Internet [4]. Интерес с точки зрения реализации в аппаратуре БЛА представляет способ обработки видеоинформации, описанный в работе [5].

Анализ рассмотренных, а также других современных методов сжатия видовой информации показывает, что они носят унифицированный характер для сжатия

видеоизображений динамических сцен и являются избыточными для решения конкретной задачи сжатия видеоинформации, поступающей с фотовидеоаппаратуры БЛА. Кроме того, большой объем служебной информации, передаваемой в общем потоке данных на выходе кодера, может составлять более 50 % от общего объема данных [6], при этом качество восстановленных изображений является крайне чувствительным к искажению служебной информации. В работах [7, 8] показано, что применение видеостандарта H.264 приводит к следующим зависимостям качества видеоданных от вероятности битовой ошибки $P_{ош}$:

$P_{ош} \le 3 \cdot 10^{-5}$ – битовые ошибки не влияют на качество принимаемого видео и легко устраняются механизмами защиты от ошибок на канальном уровне;

$P_{ош} \le 10^{-4}$ – обеспечивается превосходное качество видеопотока;

$10^{-4} \le P_{ош} \le 4 \cdot 10^{-4}$ – обеспечивается хорошее качество видеопотока;

$4 \cdot 10^{-4} \le P_{ош} \le 8 \cdot 10^{-4}$ – обеспечивается удовлетворительное качество;

$8 \cdot 10^{-4} \le P_{ош} \le 10^{-3}$– плохое качество видеопотока;

$P_{ош} \ge 10^{-3}$ – очень плохое качество видеопотока.

Невозможность обеспечения требуемого качества видеопотока при увеличении вероятности битовой ошибки обосновывается тем, что естественная избыточность видеоданных устраняется в процессе сжатия (компрессии) и не используется для обеспечения их достоверности при передаче по радиоканалу.

Точность изображений может оцениваться через среднеквадратическую ошибку (СКО, MSE), которая равна среднему квадратов ошибок (разностей пикселей) двух изображений

$$\text{СКО} = \frac{1}{n}\sum_{i=1}^{n}(A_i - B_i)^2, \quad (1)$$

где A_i – пиксели исходного изображения; B_i – пиксели восстановленного изображения.

Для оценки расхождения восстановленных и исходных изображений может использоваться метрика пикового отношения сигнал/шум (PSNR):

$$\text{PSNR} = 20 \ln \frac{\max_i |A_i|}{\text{RMSE}}, \quad (2)$$

где RMSE – корень среднеквадратической ошибки MSE, который равен среднему квадратов ошибок (разностей пикселей) двух изображений:

$$\text{RMSE} = \sqrt{\frac{1}{n}\sum_{i=1}^{n}(A_i - B_i)^2}. \quad (3)$$

Наличие этапа криптографической защиты сжатой видовой информации для обеспечения ее конфиденциальности приводит к необходимости применения дополнительных мер защиты от помех в канале связи. Основным механизмом обеспечения достоверности видовой информации по критерию минимизации вероятности необнаруживаемой ошибки $P_{\text{необ.ош}}$ является применение циклических кодов, обнаруживающих ошибки, и решающей обратной связи для повтора искаженных пакетов.

При условии $P_{\text{необ.ош}} = 0$ отсутствует вероятность трансформации сообщений, и полная группа возможных событий определяется как:

$$P_{\text{пр}} + P_{\text{под}} = 1, \quad (4)$$

где $P_{\text{пр}}$ – вероятность правильного приема видовой информации; $P_{\text{под}}$ – вероятность подавления видовой информации.

Таким образом, результирующее качество изображения определяется эффективностью методов обработки и защиты информации и может оцениваться показателями: СКО, PSNR, $P_{\text{пр}}$.

Рассмотренная типовая модель системы обработки и защиты видовой информации в комплексах БЛА отражает следующие противоречия:

- между увеличением объема видовой информации, необходимой для достоверного принятия решения о характеристиках объекта мониторинга, с одной стороны, и ограниченным временем на ее обработку и передачу, с другой;

- между требуемой скоростью передачи видовой информации, с одной стороны, и пропускной способностью радиолинии в условиях целенаправленных воздействий противника, с другой;
- между необходимостью обеспечения криптозащиты видовой информации, с одной стороны, и «чувствительностью» криптоалгоритмов к ошибкам, возникающим в канале связи с помехами, с другой.

1. Модель системы обработки и защиты видовой информации

Целью статьи является разработка согласованных методов (способов) обработки и защиты видовой информации с целью нахождения баланса между ее качеством и временем обработки, криптозащиты и передачи.

Построим модель системы обработки и защиты видовой информации на основе теоретико-множественного подхода в виде:

$$M = (V_{вх}, V_{цн}, V_{вых}, Y, Y', K_e, f_{по}, f_{сж}, f_{кр}, f_{пк}, f_{пк}^{-1}, f_{кр}^{-1}, f_{сж}^{-1}), \quad (5)$$

где $V_{вх}$, $V_{цн}$, $V_{вых}$, Y, Y', K_e – конечные множества:

входных потоков $v_{вх} \in V_{вх}$;

изображений целевых нагрузок $v_{цн} \in V_{цн}$;

сжатых изображений $v_{вых} \in V_{вых}$;

зашифрованных изображений $y \in Y$;

помехозащищенных изображений $y' \in Y'$;

ключей криптозащиты $\kappa_e \in K_e$;

$f_{по}$ – функция предварительной обработки , $f_{по}: V_{вх} \rightarrow V_{цн}$;

$f_{сж}$ – функция окончательной обработки, $f_{сж}: V_{цн} \rightarrow V$;

$f_{кр}$ – функция криптозащиты, $f_{кр}: V \rightarrow Y$;

$f_{пк}$ – функция помехоустойчивого кодирования, $f_{пк}: Y \rightarrow Y'$;

$f_{пк}^{-1}$ – функция декодирования, $f_{пк}^{-1}: Y' \rightarrow Y$;

$f_{кр}^{-1}$ – функция снятия криптозащиты, $f_{кр}^{-1}: Y \rightarrow V$;

$f_{сж}^{-1}$ – функция декомпрессии, $f_{сж}^{-1}: V \rightarrow V_{вх}$.

Функционально-временная последовательность этапов обработки и защиты видовой информации представлена на рис. 2.

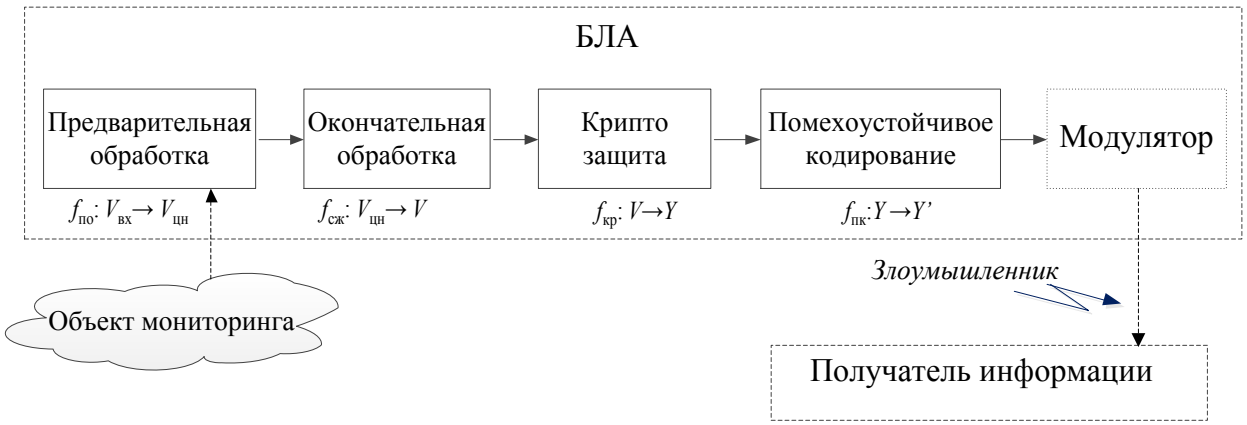

Рис. 2. Функционально-временная последовательность этапов обработки и защиты видовой информации
(Fig. 2. Functional-time sequence of stages of processing and protection of visual information)

В рассмотренной последовательности этапов обработки и защиты видовой информации (рис. 2) принципиально важным является влияние процесса шифрования на ее помехоустойчивость. Независимо от первоначальной степени избыточности информации традиционные методы шифрования устраняют возможность использования

исходной (естественной) избыточности для обеспечения помехоустойчивости, т.е. подсистема криптозащиты «разрушает» связь между структурой файла видовой информации после его сжатия и формированием кадров (пакетов).

В зависимости от требований лица, принимающего решения (ЛПР), которым может являться оператор БЛА или должностное лицо, в интересах которого осуществляется эксплуатация БЛА, заключающихся в повышении достоверности или оперативности прохождения информации, возможна постановка двух соответствующих оптимизационных задач (6) или (7):

$$P_{\text{пр}} \to \max\big|_{\Delta N-\text{const}}; \tag{6}$$

$$\Delta N \to \min\big|_{P_{\text{пр}}-\text{const}}. \tag{7}$$

где ΔN – порог увеличения исходного размера файла информации.

Независимо от вида оптимизационной задачи используются следующие стратегии их решения:

1. Уменьшение объема изображений с целью адаптации к пропускной способности канала связи без снижения их ценностного аспекта. При этом сохраненная естественная избыточность изображений используется для обеспечения помехоустойчивости при передаче по радиоканалам низкого качества.

2. Применение помехоустойчивых методов криптозащиты.

2. Параметрическая обработка видовой информации

При использовании первой стратегии предлагается учитывать следующие условия:

- объекты мониторинга в основном менее динамичны по сравнению со скоростью БЛА (полезной нагрузки);

- для ЛПР требуется не высокое разрешение исходного изображения (видео), а высокая степень детализации объекта (цели) мониторинга и оперативность его получения за время, не превышающее актуальности информации.

Методологическим базисом решения поставленной задачи является применение искусственных нейросетей, перераспределение ресурсов («интеллекта») между подсистемами обработки, расшифрования видовой информации и принятия решения на наземном пункте управления (НПУ) и подсистемами обработки и защиты информации на борту БЛА, а также «перераспределение избыточности» видовой информации путем сохранения естественной избыточности изображений и ее использования для обеспечения помехоустойчивости.

Для решения задачи предлагается применение алгоритмов параметрического метода обработки информации (сегментация изображения, идентификация объектов, параметрическое представление изображений, фрагментация) [9, 10].

Для выделения контуров изображения применяется градиентный метод, основанный на процедурах пространственного дифференцирования посредством использования различных дифференциальных операторов: Робертса, Собеля, Кирша, Превита и др. [9]. Для обнаружения и распознавания цели мониторинга, характеризующейся яркостным контрастом относительно фона и по особенностям внешней формы, другими характеризующими признаками и их совокупностью, определения принадлежности к определенному классу, используется нейронная сеть с обратным распространением ошибки. Основу статистического подхода к задаче классификации образов составляет байесовская теория принятия решений. Результатом успешной идентификации целей будут массивы пикселей, соответствующие их изображениям. Этим массивам присваивается максимальный коэффициент значимости, к оставшимся фрагментам изображения применяется алгоритм объединения пикселей и уменьшения разрешения изображения.

3. Комбинированная криптозащита

Сохранение естественной избыточности изображений расширяет область применяемых методов криптозащиты за счет потенциально возможного применения *непомехоустойчивых шифров*, где под *помехоустойчивостью* понимается влияние искажений в блоке зашифрованного текста на процесс расшифрования последующих блоков.

На выбор типа шифра влияет его свойство распространения искажений. Согласно теореме А.А. Маркова [11], в классе эндоморфных шифров, не изменяющих длины сообщений, не распространяют искажений типа замены знаков шифры перестановки, поточные шифры однозначной замены, а также их композиции.

Рассмотрим вариант криптографической защиты видовой информации путем использования комбинированного шифра. Формирование криптозащищенной информации E определяется следующим образом:

$$E = f(M_{\text{исх}}, K_1, K_2), \tag{8}$$

где $M_{\text{исх}}$ – исходная видовая информация; K_1 – ключ перестановки; K_2 – ключ гаммирования.

Последовательное применение шифров перестановки и гаммирования, в отличие от применяемых в настоящее время блочных шифров [12 - 14], позволяет снизить запас помехоустойчивости системы передачи данных, так как искажение отдельных бит видовой информации не приводит к потере блока (пакета).

Для исследования эффективности комбинированной криптозащиты изображений было разработано программное средство, обеспечивающее шифрование двоичных данных путем последовательного применения алгоритма перестановки блоков и наложения гаммы шифра, интерфейс которого приведен на рис. 3.

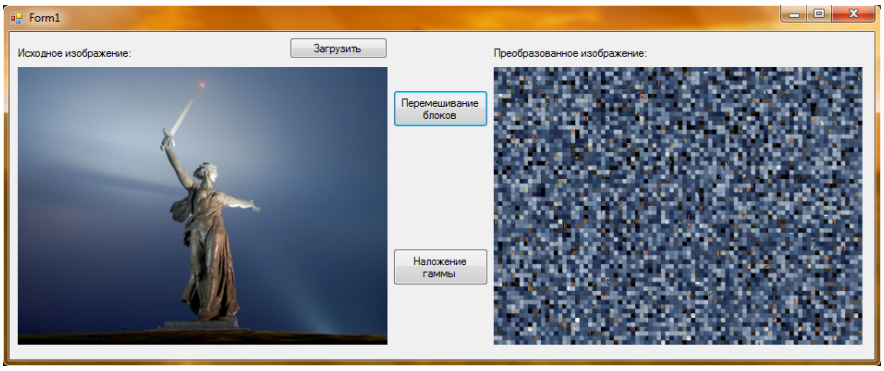

Рис. 3. Интерфейс программного средства комбинированного криптопреобразования
(Fig. 3. The interface of the combined encryption software)

Программное средство предусматривает выполнение следующих этапов:

- загрузка изображения в формате BMP;
- выбор размера блока;
- перестановка блоков;
- выбор из списка неприводимого многочлена, образующего псевдослучайную последовательность (ПСП);
- наложение на изображение ПСП (гаммирование);
- вывод зашифрованного изображения на экран и в файл в виде двоичных данных.

Качество криптозащиты информации определяется визуальным отображением полученного изображения и на основании корреляционного анализа.

Матрица корреляций для зашифрованного тестового изображения имеет следующий вид:

1	-0,0017	-0,0341	0,0421	0,0097	0,0582	-0,0074	0,0172	0,0195	-0,0104	-0,0037	-0,0268
-0,0017	1	0,005	0,0047	0,0207	0,0045	0,0039	0,0017	0,0042	-0,0102	-0,0217	0,0237
-0,0341	0,005	1	-0,0437	0,0886	-0,0475	0,0037	0,0147	-0,0629	0,0289	-0,0766	-0,0322
0,0421	0,0047	-0,0437	1	-0,1151	0,0435	-0,0069	0,0009	0,043	-0,0475	0,0052	-0,0369
0,0097	0,0207	0,0886	-0,1151	1	-0,0192	-0,0029	0,0161	0,0213	0,0625	-0,0081	0,0301
0,0582	-0,0045	-0,0475	0,0435	-0,0192	1	-0,0068	0,0052	0,066	0,0113	0,106	-0,0092
-0,0074	-0,0039	0,0037	-0,0069	-0,002	-0,0068	1	-0,0059	0,0064	0,023	0,008	0,0813
-0,0001	0,0017	0,0147	0,0009	0,0161	0,0052	-0,0059	1	0,0172	-0,004	0,0398	0,0087
0,0195	-0,0042	-0,0629	0,043	0,0213	0,066	0,0064	0,0001	1	-0,0242	0,1446	-0,0448
-0,0104	-0,0102	0,0289	-0,0475	0,0625	0,0113	0,023	-0,004	-0,0242	1	-0,0158	0,1145
-0,0037	-0,0217	-0,0766	0,0052	-0,0081	0,106	0,008	0,0398	0,1446	-0,0158	1	-0,0005
-0,0268	0,0237	-0,0322	-0,0369	0,0301	-0,0092	0,0813	0,0087	-0,0448	0,1145	-0,0005	1

Корреляция каждого блока имеет следующие средние арифметические значения:
0,0093 0,027 0,0247 0,0101 0,0229 0,0151 0,0198 0,0287 0,0095 0,0188 0,0134 0,0187.

Анализ полученных значений показывает повышение сложности задачи поиска коррелирующих блоков и восстановления исходного изображения методом корреляционного анализа. Таким образом, двухуровневая криптозащита видовой информации позволяет обеспечить требуемую криптостойкость при условии применения ПСП ограниченного периода, что является приоритетным фактором при ограничениях на ресурсы, выделяемые на цели защиты информации.

4. Имитационное моделирование синтеза параметров помехоустойчивого кодирования

Зависимость вероятности правильного приема файла $P_{\text{пр}}$ от вероятности ошибки символа сообщения (битовой ошибки) $P_{\text{ош}}$ при исправлении всех ошибок кратности $e_{\text{испр}}$ и меньшей при их биномиальном распределении определяется по формуле Бернулли:

$$P_{\text{пр}} = \left(\sum_{i=1}^{e} C_n^i P_{\text{ош}}^{\ i} (1 - P_{\text{ош}})^{n-i}\right)^{N/n} \quad (9)$$

Исходя из формулы (9) решение оптимизационной задачи (6) возможно путем уменьшения размера блока сообщения n или увеличения количества исправляемых ошибок e.

Для решения оптимизационной задачи (6) и выбора параметров помехоустойчивого кода проведено имитационное моделирование при следующих исходных данных:

$A = (P_{\text{ош}}, N, n, e)$ – вектор изменяемых параметров, где $P_{\text{ош}}=10^{-4}..10^{-2}$ – вероятность битовой ошибки;

N = 0,2..5 Мб – исходный размер файла;

n = 32..1024 бита – размер информационного блока;

$e = 0..n/4$ – количество исправляемых ошибок.

$P_{\text{пр.тр}}$ = 0,999 – требуемая вероятность правильного приема файла.

Алгоритм синтеза параметров помехоустойчивого кодирования предусматривает полный перебор параметров A при следующей длине шагов, определяющих количество итераций внутри цикла: ΔN = 0,2 Мб; $\Delta n = n_{\min} \cdot 2^i$, где $1 \le i \le 5$ – количество шагов цикла; Δe = 1; для $P_{\text{ош}}$ предлагаются дискретные значения: 10^{-4}, $5 \cdot 10^{-3}$, 10^{-3}, 10^{-2}.

Для всех наборов параметров A^*, удовлетворяющих условию $P_{\text{пр}} \ge P_{\text{пр.тр}}$ записываются в массив данных и выводятся на экран. Дополнительно предусмотрена запись всех наборов данных при полном переборе параметров A в соответствии с ограничениями и шагом изменения значений с целью формирования полной статистической совокупности данных.

Блок-схема алгоритма синтеза параметров помехоустойчивого кодирования приведена на рис. 4.

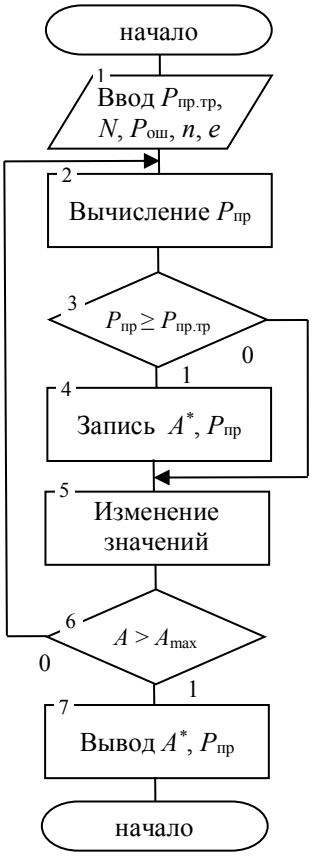

Рис. 4. Блок-схема алгоритма синтеза параметров помехоустойчивого кодирования
(Fig. 4. Block diagram of the algorithm for the synthesis of error-correcting coding parameters)

С целью автоматизации сбора статистических данных на основании предложенного алгоритма разработано программное средство для выбора оптимальных параметров помехоустойчивого кода в среде моделирования C# [15], зарегистрированное в Реестре программ для ЭВМ. На основании использования программного средства получены статистические данные, позволяющие решать оптимизационную задачу (7) для фиксированных значений $P_{пр}$.

В табл. 1 отражены зависимости между параметрами помехоустойчивого кода и увеличением размера N = 200 Кб исходного файла при $P_{ош} = 10^{-4}$ при условии $P_{пр} \geq 0{,}999$.

Таблица 1. Зависимость увеличения размера исходного файла N от размера блока n и исправляемых ошибок e при $P_{ош}=10^{-4}$

	Длина блока сообщения n (бит)					
	32	64	128	256	512	1024
e=0	-	-	-	-	-	-
e=1	-	-	-	-	-	-
e=2	225	225	-	-	-	-
e=3	237,5	237,5	237,5	237,5	237,5	-
e=4	250	250	250	250	250	250

Анализ значений, представленных в табл. 1, показывает, что минимальное увеличение размера исходного файла осуществляется при выборе минимального размера блока, а также видно, а также что увеличение исправляющих способностей кода при заданных условиях более 4 ошибок является нецелесообразным.

Аналогичным способом возможно получение статистических данных и определение оптимальных по заданному критерию параметров помехоустойчивого кодирования при других значениях битовой ошибки в канале связи.

Значения параметров оптимального помехоустойчивого кода для кадра изображения объемом 200 Кб приведены в табл. 2.

Таблица 2. Значения параметров оптимального помехоустойчивого кода для кадра изображения объемом 200 Кб

$P_{ош}$	n	k	e	$P_{пр}$	N^*,кБ
10^{-4}	72	64	2	0,998	225
10^{-3}	80	64	4	0,9994	250
$5{\cdot}10^{-3}$	88	64	6	0,991	275
10^{-2}	96	64	8	0,984	300

Как видно из результатов, представленных в табл. 2, для конкретного значения вероятности битовой ошибки $P_{ош}$ оптимальным по выбранным критериям является помехоустойчивый код с соответствующими параметрами, что может учитываться разработчиками системы обработки и передачи визуальной информации в радиолинии БЛА.

Заключение

При передаче видовой информации по радиолиниям в комплексах БЛА при ухудшении помеховой обстановки, применение систем с обратной связью становится неэффективным. Обеспечение требуемых показателей достоверности, конфиденциальности и оперативности видовой информации становится возможным за счет согласованного применения методов ее обработки, криптозащиты и помехоустойчивого кодирования. Применение помехоустойчивых методов криптозащиты позволяет использовать естественную избыточность видовой информации для устранения ошибок, вызванных помехами в радиолинии, что обеспечивает адаптацию объема видовой информации к пропускной способности радиолинии при требуемой вероятности ее правильного приема в условиях помех.

СПИСОК ЛИТЕРАТУРЫ:

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Госстандарт Российской Федерации, 2006.
2. Ричардсон Я. Мир цифровой обработки. Видеокодирование. H.264 и MPEG-4 – стандарты нового поколения. – М.: Техносфера, 2006. 113 с.
3. Bozinovic N., Konrad J. Scan order and quantization for 3D-DCT coding in Proc. Of SPIE Vis. Comm. And Im. Proc. Vol.5150, 2003. P.1204 – 1215.
4. Сэломон Д. Сжатие данных, изображений и звука. – М.: Техносфера, 2004. 368 с.
5. Anand Deshpande, Prashant Patavardhan, Multi-frame super-resolution for long range captured iris polar image, IET Biometrics, Vol. 6, Issue-2, 2016. P. 108 – 116.
6. McAndrew A. A Computational Introduction to Digital Image Processing, 2nd Edition, Chapman and Hall/CRC Published November 5, 2015. Textbook. 535 p.
7. Иванов Ю.А. Оценка качества потокового видеостандарта H.264 /AVC при передаче в нестабильных каналах связи широкополосных сетей беспроводного доступа 4G // Вестник Чувашского университета, 2010. – № 3. С. 268 – 278.
8. Иванов Ю.А., Лукьянцев С.А. Методика оценки качества декодирования видеостандарта H.264/AVC/SVC в беспроводных сетях // Электротехнические и информационные комплексы и системы. 2009. Т. 5, № 4. С. 35 – 48.
9. Винокуров А.В. Параметрический метод обработки видеоинформации на основе применения нейронных сетей как механизм адаптации размера изображений к пропускной способности канала связи // Журнал промышленные АСУ и контроллеры. 2017. № 6. С. 36 – 39.
10. Винокуров А.В., Махов Д.С. Разработка программно-алгоритмического обеспечения адаптивной обработки видеоинформации на борту беспилотного летательного аппарата // Региональная информатика (РИ-2016): материалы Юбилейной XV Санкт-петербургской международной конференции (26 – 28 октября 2016 г.), СПОИСУ. – СПб. – 2016. – С. 76.

11. Алферов, А.П. Основы криптографии / А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин // учеб. пособие, 2-е изд., испр. и доп. – М.: Гелиос АРВ, 2002. 480 с.
12. Sudha S, Divya. Cryptography in image using blowfish algorithm. Intl. J. Sci. Res. 2015. Vol. 4. P. 1289 – 1291.
13. Ali Y.H., Ressan. Image encryption using block cipher based serpent algorithm. Eng. Technol. J. 2016. Vol. 34. P. 278 – 286.
14. Padate R, Patel A. Image encryption and decryption using AES algorithm. Intl. J. Electron. Commun. Eng. Technol. J. 2015. Vol. 6. P. 23 – 29.
15. Свидетельство о регистрации программы для ЭВМ № 2018619979. Программа выбора оптимальных параметров помехоустойчивого кода, дата государственной регистрации в Реестре программ для ЭВМ 15 августа 2018 г., опубл. 15.08.2018, Бюл. № 8 / А.В. Винокуров, Глазырин Н.А., Задвижкин А.А., Калашников А.В., Фролов А.Д.

REFERENCES:

[1] GOST R 50922-2006. Data protection. Basic terms and definitions. M.: Gosstandart of the Russian Federation, 2006. (in Russian).
[2] Richardson Ja. Mir cifrovoj obrabotki. Videokodirovanie. N.264 i MPEG-4 – standarty novogo pokolenija. M.: Tehnosfera, 2006. 113 p. (in Russian).
[3] Bozinovic N., Konrad J. Scan order and quantization for 3D-DCT coding in Proc. Of SPIE Vis. Comm. And Im. Proc. Vol.5150, 2003. P.1204 – 1215.
[4] Sjelomon D. Szhatie dannyh, izobrazhenij i zvuka. – M.: Tehnosfera, 2004, 368 p. (in Russian).
[5] Anand Deshpande, Prashant Patavardhan, Multi-frame super-resolution for long range captured iris polar image, IET Biometrics, Vol. 6, Issue-2, 2016. P. 108 – 116.
[6] McAndrew A. A Computational Introduction to Digital Image Processing, 2nd Edition, Chapman and Hall/CRC Published November 5, 2015. Textbook. 535 p.
[7] Ivanov Ju.A. Assessment of the quality of streaming video standard H. 264 /AVC when the transfer in the unstable communication channels of broadband wireless access networks for 4G. Vestnik Chuvashskogo universiteta, 2010. № 3. P. 268 – 278.
[8] Ivanov Ju.A., Luk'jancev S.A. H. 264/AVC/SVC video decoding quality assessment methodology in wireless networks. Jelektrotehnicheskie i informacionnye kompleksy i sistemy. 2009. T.5, № 4. P. 35 – 48. (in Russian).
[9] Vinokurov A.V. Parametric method of processing video information based on the use of neural networks as a mechanism for adapting the image size to the bandwidth of the communication channel. Zhurnal promyshlennye ASU i kontrollery. 2017, № 6. P. 36 – 39. (in Russian).
[10] Vinokurov A.V., Mahov D.S. Development of software and algorithmic support for adaptive processing of video information on board an unmanned aerial vehicle. Regional Informatics (RI-2016): materials of the Jubilee XV St. Petersburg International Conference (26-28 October 2016), SPOISU. St. Petersburg. 2016. P. 76. (in Russian).
[11] Alferov, A.P. Basics of cryptography. A.P. Alferov, A.Ju. Zubov, A.S. Kuz'min, A.V. Cheremushkin ucheb. posobie, 2-e izd., ispr. i dop. M., Gelios ARV, 2002. 480 p. (in Russian).
[12] Sudha S, Divya. Cryptography in image using blowfish algorithm. Intl. J. Sci. Res., 2015. Vol. 4. P. 1289 – 1291.
[13] Ali Y.H., Ressan. Image encryption using block cipher based serpent algorithm. Eng. Technol. J. 2016, 34. P. 278 – 286.
[14] Padate R, Patel A. Image encryption and decryption using AES algorithm. Intl. J. Electron. Commun. Eng. Technol. J. 2015, 6. P. 23 – 29.
[15] Certificate of registration of the computer program No. 2018619979, Program for selecting the optimal parameters of the noise-proof code, date of state registration in the Computer Program Register on August 15, 2018, publ. August 15, 2018, Bul. No. 8 A.V. Vinokurov, N.A. Glazyrin, A.A. Zadvizhkin, A.V. Kalashnikov, A.D. Frolov (in Russian).

Поступила в редакцию – 09 сентября 2018 г. Окончательный вариант – 31 января 2019 г.
Received – September 09, 2018. The final version – January 31, 2019.