

electronic sources to each other and to protect their own information resources from unauthorized cybernetic influence. The solution of such problems is impossible without building now an overwhelming majority of the world's own systems cyber security, and the development and introduction of new, more effective methods and methods of intelligence information and telecommunication (IT) systems. First of all, this is due to the continuous growth of information that circulates is stored and processed in the information and cyberspace these countries, the need to protect such information from the influence of internal and external cyber threats and interventions, the rapid development of new IT technologies and global computerization. With this in mind, the article discussed the purpose and the main varieties of intelligence information and telecommunication systems. Proposed definition of intelligence in telecommunication systems (IST). Defines the scope of the possible interests of the IST and the method of its conduct, and place of the IST in the overall process of

getting information. An example of the use of wireless technologies during the execution of the tasks of exploration of the IST.

Key words: the information, information and telecommunication systems, investigation of systems of telecommunications.

Бурячок Володимир Леонідович, доктор технічних наук, старший науковий співробітник, завідувач кафедри безпеки інформаційних технологій Державного університету телекомунікацій.

E-mail: BVL-home@ua.fm

Бурячок Владимир Леонидович, доктор технических наук, старший научный сотрудник, заведующий кафедрой безопасности информационных технологий Государственного университета телекоммуникаций.

Buryachok Volodymyr, Dr Eng (Information security), Senior Research Fellow, Head of the Department of Information Technology Security of the State University of Telecommunications.

УДК 621.327:681.5

МЕТОД КОДИРОВАНИЯ ДЛЯ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ВИДЕОИНФОРМАЦИИ АЭРОМОНИТОРИНГА ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Владимир Баранник, Кулица Олег

Проводится исследование условий функционирования видеомониторинга с использованием бортовых комплексов в процессе предупреждения и ликвидации кризисных ситуаций. Выявляются факторы, формирующие угрозы для нарушения свойств доступности и целостности видеoinформации аэромониторинга как категорий информационной безопасности. Это приводит к устареванию получаемой информации, принятию запоздалых и ошибочных решений. Показывается актуальность повышения безопасности видеoinформации аэромониторинга в системе предупреждения и ликвидации кризисных ситуаций. Обосновано, что для решения данной задачи предлагается использовать технологии компрессионного кодирования видеоданных. Проводится обоснование выбора технологии компрессии изображений. Показывается, что для исключения недостатка, связанного с понижением нижней границы дифференциального полиадического пространства необходимо для технологии перфорирования дополнительно учитывать двоичную маску всплесковых элементов верхнего и нижнего уровней. Излагаются основные этапы метода кодирования изображений для повышения доступности видеoinформации, базирующегося на: дифференциальном представлении фрагментов изображений по комбинированной схеме; организации перфорирования массивов дифференциального представления в двумерном полиадическом пространстве с маской; представлении массивов элементов верхнего перфорационного уровня в дифференциальном полиадическом пространстве, что обеспечивает дополнительное сокращение комбинаторной избыточности; одномерное кодирование по блочной схеме. Приводится экспериментальная оценка эффективности разработанного метода с существующими методами в классе контролируемых потерь качества.

Ключевые слова: дифференциальное представление, перфорированное полиадическое пространство, комбинаторная избыточность, двоичная маска.

Введение. Для построения систем своевременного предупреждения, локализации и ликвидации кризисных ситуаций (КС) важное значение имеет использование инфокоммуникационных технологий для мониторинга обстановки [1–3]. В свою очередь для минимизации ущерба от КС и экономии затрат

на организацию мониторинга осуществляется видеoinформационное обеспечение с использованием бортовых средств воздушного наблюдения. Здесь ключевой составляющей является обеспечение требований по доступности видеoinформационного ресурса аэромониторинга [3; 4].

Под доступностью в общем случае понимается возможность доступа к информационному ресурсу в процессе ее обработки, хранения и передачи. В общем случае здесь понимается как возможность непосредственного доступа к информации, так и возможность занятия ресурса в течение некоторого промежутка времени [5; 6]. В дальнейшем интерес будет представлять только первая составляющая.

Доступность информации в информационных системах как категория информационной безопасности это свойство информации, которое состоит в возможности непосредственного доступа к ней со стороны процесса или авторизованного пользователя в соответствии с установленной политикой безопасности в необходимой форме и в требуемые временные сроки [5; 6].

Под требуемыми временными сроками, за которое должен быть обеспечен доступ к видеомониторингу КС, обычно понимается реальное время.

В тоже время видеомониторинговое обеспечение с использованием аэромобильных средств организуется в условиях действия следующих объективных факторов [4]:

- ограниченность массогабаритных и энергетических возможностей воздушных средств видеонаблюдения;
- значительная удаленность от наземных центров приема информации;
- сложный рельеф местности (горные участки и лесные массивы).

Это является причиной возникновения таких проблемных сторон воздушного видеомониторинга как [3; 4]:

- рост задержки на обработку и передачу видеоданных с борта;
- ограниченное время сеанса связи.

В свою очередь это приводит к формированию угроз нарушения свойства доступности информации как категории информационной безопасности, а именно существуют угрозы следующего характера:

- превышение требуемой задержки доступа к информации;
- получение информации в форме, несоответствующей требуемому виду представления;
- получению не полной информации.

Значит, в процессе видеомониторинга существует угроза нарушения категории доступности видеомониторинга АМКС, вызванная условиями ее

дистанционного формирования, обработки и передачи с использованием существующих беспроводных инфокоммуникационных технологий.

Другой составляющей категории безопасности видеомониторинга является ее целостность.

Для такого информационного ресурса как видеомониторинг аэромониторинга с использованием дистанционных бортовых средств в процессе предупреждения и ликвидации КС возможна следующая конкретизация определения целостности как категории информационной безопасности.

В узком смысле под целостностью видеомониторинга аэромониторинга понимается состояние, в котором видеомониторинговая информация полностью соответствует видеомониторинговой информации, регистрируемой бортовыми средствами наблюдения на передающей стороне.

В широком смысле целостность видеомониторинга аэромониторинга в процессе контроля кризисных объектов – это состояние, в котором видовые изображения, получаемые на приемной стороне, сохраняют информационное содержание, обеспечивающее необходимый комплекс решения задач идентификации и распознавания объектов мониторинга.

Отсюда целостность видеомониторинговой информации аэромониторинга будет формироваться на основе двух базовых составляющих, а именно: качество видеомониторинговой информации; достоверность видеомониторинговой информации.

Обеспечение целостности информации для систем видеомониторинга имеет свои особенности, а именно [4]:

1) растет важность видеомониторинговой информации, повышается ее ценность, что вызвано необходимостью принятием оперативных решений в кризисных ситуациях;

2) аэромониторинг характеризуется формированием видовых изображений насыщенных объектами различной детальности. Это выдвигает повышенные требования относительно обеспечения разрешающей способности снимков;

3) для обеспечения требуемого качества и достоверности информации в процессе решения задач по анализу объектов контроля требуется формировать видовые изображения, имеющие значительные объемы, достигающие порядка 100 Мбит. Это диктуется необходимостью обеспечения требований по характерной детальности объектов мониторинга.

На практике повышение оперативности доставки информации достигается путем сокращения размеров изображений или использованием каналов связи с большей интенсивностью помех. Но в тоже время такие подходы связаны с потерей качества и достоверности видеоинформации. Следовательно, создается угроза нарушению категории целостности видеоинформации. Угрозами целостности информации представляют угрозы, которые относятся к несанкционированной модификации информации.

Угрозы целостности видеоинформации аэромониторинга, приводят к нарушению функционирования системы предупреждения и ликвидации КС, и обусловлены:

- несоответствием требуемой степени характерной детальности, т.е. несоответствие требуемой разрешающей способности;

- потерей части видеоданных в результате ограниченного сеанса связи;

- искажением семантического содержания изображений в результате внесения как активных, так и пассивных искажения.

В результате процесс информационного обеспечения системы контроля кризисных ситуаций на основе средств воздушного видеонаблюдения характеризуется наличием **противоречия**, что ведет к появлению угроз относительно нарушения информационной безопасности по категориям доступности и целостности видеоинформационных ресурсов. Поэтому повышение безопасности видеоинформации аэромониторинга в системе предупреждения и ликвидации кризисных ситуаций является **актуальной научно-прикладной задачей**.

В настоящее время сделано значительное развитие в области теории и практики обеспечения таких категорий информационной безопасности как доступность, целостность и конфиденциальность [5; 6]. Требуется принимать во внимание сторону базовых категорий информационной безопасности, обусловленную особенностями формирования, обработки, передачи, восприятия и влияния на пользователей видеоинформационных ресурсов. Здесь следует учитывать такие характеристики как оперативность и своевременность доставки, качество и достоверность видовых изображений. В связи с чем, вариантом обеспечения данного аспекта информационной безопасности является направление, основанное на использовании технологий компрессионного кодирования изображений.

Анализ технологий компрессионного кодирования видеоданных. Современные технологии компрессии изображений строятся на основе комплексного принципа, что создает возможность для устранения нескольких классов избыточности (психовизуальная, статистическая и структурная) [7; 8]. Однако в процессе использования технологий компрессии для решения сформулированной задачи проявляется **противоречие**, имеющее следующие аспекты.

Первый аспект. С одной стороны методы с внесением искажений (методы на платформах JPEG, JPEG2000) приводят к снижению разрешающей способности, а следовательно, нарушается условие обеспечения характерной детальности объектов мониторинга [7–9]. Это приводит к нарушению целостности. С другой стороны использование методов без потери целостности (словарные методы семейства LZ, методы статистического кодирования, комплексные методы платформ GIF, TIFF) связано с низкими степенями сжатия, и как следствие с ростом времени доставки данных. Откуда нарушается категория доступности информации.

Второй аспект. С одной стороны использования методов сжатия, требующих низкой сложности вычисления (методы поэлементного унитарного кодирования, методы структурного кодирования на основе выявления длин серий и методов, основанных на кодах Хаффмана) обеспечивает снижение задержки на обработку [8; 9]. С другой стороны такие методы не обеспечивают требуемого уровня сжатия, что увеличивает время передачи, а значит, приводит к нарушению доступности видеоинформации.

В связи с чем, для разрешения противоречия предлагается развивать класс методов, обладающих такими свойствами как сжатие с контролируемыми потерями качества реконструируемых изображений и реализации процесса сжатия с ограниченной сложностью. Это позволит сохранить требуемую целостность видеоинформации и повысить доступность к ней с использованием информационно-телекоммуникационных технологий аэромобильного мониторинга.

Поэтому **цель исследований** состоит в разработке метода компрессионного кодирования изображений с контролируемыми искажениями и ограниченной сложностью реализации для повышения безопасности видеоинформации аэромобильного мониторинга.

Разработка метода кодирования. Предлагается повысить доступность на основе методов сжатия, использующих ортогональные преобразования, за счет:

1) осуществления дополнительного выявления в трансформированных изображениях структурных закономерностей;

2) реализации процесса кодирования с использованием блочной схемы. Это позволит сохранить требуемую целостность видеoinформации и повысить доступность к ней с использованием информационно-телекоммуникационных технологий аэромобильного мониторинга.

Для обеспечения требований относительно оперативности обработки на борту воздушных средств необходимо сократить количество операций умножения, приходящихся на один обрабатываемый элемент. Для чего в качестве базовых технологий предлагается использовать трансформацию изображений на основе ортогональных преобразований и перевод обрабатываемых данных в дифференциальное пространство используя два подхода.

В результате чего метод сжатия предлагается строить с учетом следующих стратегий обработки [8; 9]:

1. Учитывать базовые технологии преобразования видеоданных в системе сжатия изображений с предварительным дифференцированием.

В процессе разработки метода сжатия требуется учитывать следующие:

— осуществляется предварительное дифференцирование изображений по комбинированной схеме с учетом выбора порога S' минимального количества избыточности;

— для выделения двухградационности динамических диапазонов массивов дифференциального представления проводится их перфорирование с учетом двоичной маски;

— сокращение комбинаторной избыточности в массивах дифференциального представления организуется на базе одномерного кодирования в двумерном полиадическом пространстве по блочной схеме.

2. Обеспечивать исключение неконтролируемых потерь видеoinформации.

3. Осуществлять сокращение структурной, статистической избыточности, на основе выявления таких закономерностей как: корреляции между соседними элементами фрагмента изображения; когерентности элементов в столбцах фрагментов изображения, для которых выполняется одномерное ортогональное преобразование;

ограниченного количества резких перепадов для фрагментов изображений; ограниченного значения и неравномерности динамических диапазонов перепадов между соседними элементами изображения; ограниченного количества перепадов имеющих высокие динамические диапазоны.

4. Исключить дополнительные затраты служебной информации, которые не предусмотрены процессом сокращения избыточности.

Для реализации данных стратегий метод сжатия **предлагается** строить на основе следующих технологий (рис. 1).



Рис. 1. Структурная схема метода (процесса) компрессии дифференцированных изображений

Первый механизм технологии компрессии связан с процессом дифференцирования фрагментов изображений по комбинированной схеме. Для этого выполняются следующие этапы:

1. Поводится дифференцирование фрагмента изображения. Формируется массив H' дифференциального представления первого типа.

2. Формируются динамические диапазоны d'_{kl} массива ДП.

3. Оценивается количества Q'_2 информации, содержащееся в одном массиве дифференциального представления:

$$Q'_2 = \sum_{k=1}^n \sum_{l=1}^n \log_2 (\min \{ \max_{1 \leq l \leq n} (h'_{kl}); \max_{1 \leq k \leq n} (h'_{kl}) \} + 1)$$

4. Определяется порог S_{\min} минимального количества комбинаторной избыточности

$$S_{\min} = 100 \left(\frac{n^2 b}{Q_2} - 1 \right) \%,$$

где b – количество разрядов на представление одного элемента массива ДП без выявления ограничений на динамические диапазоны.

5. Осуществляется выбор направления дифференцирования. Для чего проверяется следующее условие:

$$S_{\min} = 100 \left(n^2 b / \left(\sum_{k=1}^n \sum_{l=1}^n \log_2 \left(\min_{1 \leq l \leq n} \{ \max_{1 \leq k \leq n} (h'_{kl}) \} + 1 \right) \right) - 1 \right) \% \geq S',$$

где S' – заданное количество относительной избыточности.

Если неравенство выполняется, т.е. $S_{\min} \geq S'$, то минимальное количество потенциально устранимой избыточности считается допустимым, дифференцирование осуществляется по первому направлению. Наоборот, если $S_{\min} < S'$, то для дополнительного сокращения избыточности проводится предварительное одномерное ортогональное преобразование, т.е. выбирается второе направление дифференцирования.

6. Данный этап выполняется, для случая когда $S_{\min} < S'$. Он заключается проведение одномерного ортогонального преобразования.

7. После выполнения ортогонального преобразование осуществляется получение массивов дифференциального представления второго типа.

Второй механизм технологии компактного представления сводится к организации перфорирования массивов дифференциального представления в двумерном полиадическом пространстве с маской. Он включает в себя следующие этапы:

1. На основе значений динамических диапазонов d'_{kl} массива ДП осуществляется вычисление порога перфорирования. Для этого используется следующее выражение:

$$K(h')_{\text{нор}} = \left(\sum_{k=1}^n \sum_{l=1}^n d'_{kl} \right) / n^2.$$

2. Организуется перфорирование массива ДП [8].

3. Выполняется технология маскирования элементов массива дифференциального представления. Для этого используется маркер, заданный следующей системой:

$$p_{kl} = \begin{cases} 0, \rightarrow d_{kl} \notin K(h')_{\text{нор}} \vee h'_{kl} \geq K(h')_{\text{нор}}; \\ 1, \rightarrow d_{kl} > K(h')_{\text{нор}} \ \& \ h'_{kl} < K(h')_{\text{нор}}, \end{cases}$$

где p_{kl} – элемент маски $P^{(2)}$ на позиции $(k; l)$.

4. Элементы массивов нижнего $h_{kl}^{(1)}$ и верхнего $h_{kl}^{(2)}$ перфорирующего уровня могут находиться на разных позициях в массиве ДП. Поэтому на очередном этапе обработки необходимо из отобранных элементов сформировать наиболее полные массивы для упрощения процесса кодирования. Построение подмассивов нижнего и верхнего уровней перфорации предлагается проводить с учетом того, что: массивы заполняются в направлении строк, т.к. это соответствует направлению кодирования; в случае заполнения неполной строки элементом из другой строки, имеющего больший диапазон необходимо пересчитать диапазоны для элементов всей строки. В результате формируются две составляющие массива дифференциального представления, $H^{(0)}$ и $H^{(1)}$.

5. Осуществляется пересчет динамических диапазонов $d_{kl}^{(0)}$ элементов массива нижнего перфорационного уровня с учетом маскирования. Выполняется следующая система:

$$d_{kl}^{(0)} = \begin{cases} d'_{kl}, & \rightarrow p_{kl} = 0; \\ K(h')_{\text{нор}}, & \rightarrow p_{kl} = 1. \end{cases}$$

6. Проводится обработка массива верхнего перфорационного уровня [9].

7. Проводится сборка составляющих перфорационных уровней в единый массив. В результате чего строится композиционное представление перфорационного массива дифференциального представления в двумерном полиадическом пространстве. Композиция заключается в расстановки элементов массивов $H^{(0)}$, $\bar{H}^{(1)}$ на исходные позиции в массиве H дифференциального представления. Для этого используется информация о динамических диапазонах d'_{kl} массива ДП. Результатом сборки является композиционный массив H'' , $H'' = \{h''_{k,l}\}$. С другой стороны данный массив представляет собой композиционное перфорированное число в двумерном полиадическом пространстве.

Третий механизм процесса сжатия осуществляет технологию одномерного кодирования по блочной схеме. Для этого требуется вычислить код для композиционных перфорированных с маской чисел в двумерном полиадическом пространстве.

Описание перфорированных с маской композиционных чисел в полиадическом пространстве задается следующей системой:

$$h''_{k,l} = \begin{cases} h_{kl}^{(0)}; d_{kl}^{(0)} = d_{kl}, & \rightarrow d'_{kl} \leq K(h')_{\text{пор}}; \\ h_{kl}^{(0)}; d_{kl}^{(0)} = K(h')_{\text{пор}}, & \rightarrow \\ & d'_{kl} > K(h')_{\text{пор}} \text{ \& } h'_{k,l} < K(h')_{\text{пор}}; \\ \bar{h}_{kl}^{(1)}; d_{kl}^{(1)} = s_{kl} = d_{kl}^{(1)} - \mu, & \rightarrow d'_{kl} > K(h')_{\text{пор}}. \end{cases}$$

Здесь $h''_{k,l}$ – $(k; l)$ -й элемент перфорированного с маской композиционного числа в двумерном полиадическом пространстве.

Особенность обработки в перфорированном с маской полиадическом пространстве заключается в том, что формирование кода-номера осуществляется одновременно для элементов двух перфорированных уровней с учетом наложения маски и дифференциального преобразования составляющей верхнего динамического уровня. Соответственно динамические диапазоны элементов $h''_{k,l}$ будут иметь три типа коррекций относительно системы оснований двумерного полиадического пространства.

В тоже время при обработке областей реалистических изображений заранее неизвестно их структурное содержание. Значит, для разных фрагментов изображений будут различные значения кодов-номеров. Поэтому для композиционных массивов в зависимости от их содержания соответствуют различные значения кодов-номеров.

С другой стороны для фиксированной длины КПМ числа могут возникнуть несоответствия между длиной его кодового слова и структурными особенностями композиционного перфорированного числа. Такое несоответствие может привести к следующим последствиям [8; 9]: к уменьшению коэффициента сжатия в случае формирования кодов для отдельных столбцов композиционного массива; к потере информации из-за нехватки длины кодового слова для представления значения кода-номера, полученного сразу для всего композиционного массива. Следовательно, в результате такой обработки снижается значение коэффициента сжатия или теряется часть информации.

Поэтому для учета: с одной стороны нестационарности содержания массивов дифференциального представления; с другой стороны для исключения дополнительных затрат служебных данных на маркировку кодовых комбинаций – предлагается осуществлять формирование неравномерных кодовых комбинаций для композиционных перфорированных с маской чисел (КПМЧ), имеющих равномерную длину.

В этом случае КПМ числами будут столбцы массива H'' , а длина неравномерных кодовых

комбинаций будет определяться на основе накопленного произведения оснований элементов КПМ числа. Отсюда значение кода-номера $N^{(l)}$ и длина $C^{(l)}$ кодовой комбинации будут формироваться для отдельных столбцов, и определяться по технологии представленной на рис. 2.

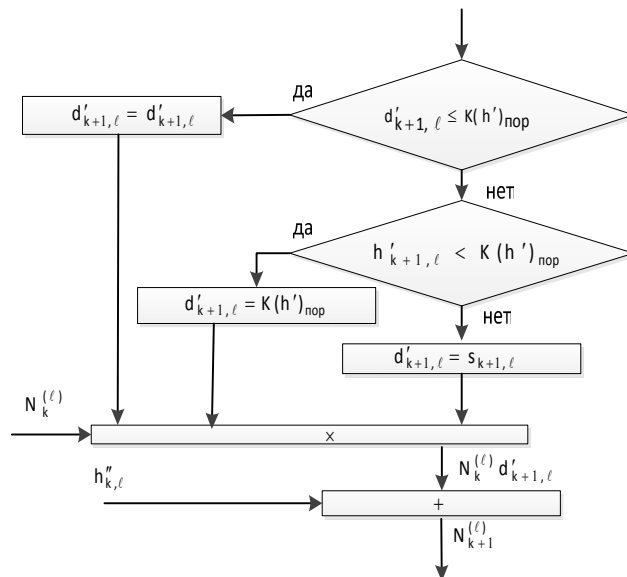


Рис. 2. Схема реализации формирования кода-номера $N_{k+1}^{(l)}$

Значение кода-номера для l -го столбца будет равна величине $N^{(l)}$, а величина накопленного произведения $V^{(l)}$. Отсюда длину $C^{(l)}$ кодовой комбинации, содержащей значение кода-номера $N^{(l)}$ предлагается определять на основе соотношения (рис. 3) $C^{(l)} = [\log_2 V^{(l)}] + 1$ (бит).

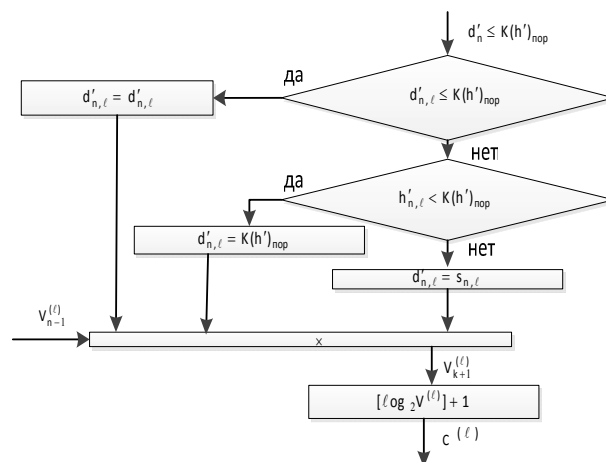


Рис. 3. Схема реализации технологии формирования кодограммы

Данное выражение позволяет определить длину кодового слова под код-номер КПМ числа на основе значений оснований его элементов без использования дополнительной служебной информации.

Сравнительная оценка по задержке на передачу сжатых видовых изображений для разработанного метода (ККПМ) и методов компрессии с контролируемыми потерями качества (JPEG, JPEG2000, комбинированный метод сжатия КМС) рассматривается на рис. 4. Исследование результатов на рис. 4 позволяет заключить, что снижение задержки на передачу видовых изображений с бортовых комплексов в случае сжатия на основе созданного метода по сравнению с известными методами достигает 35%.

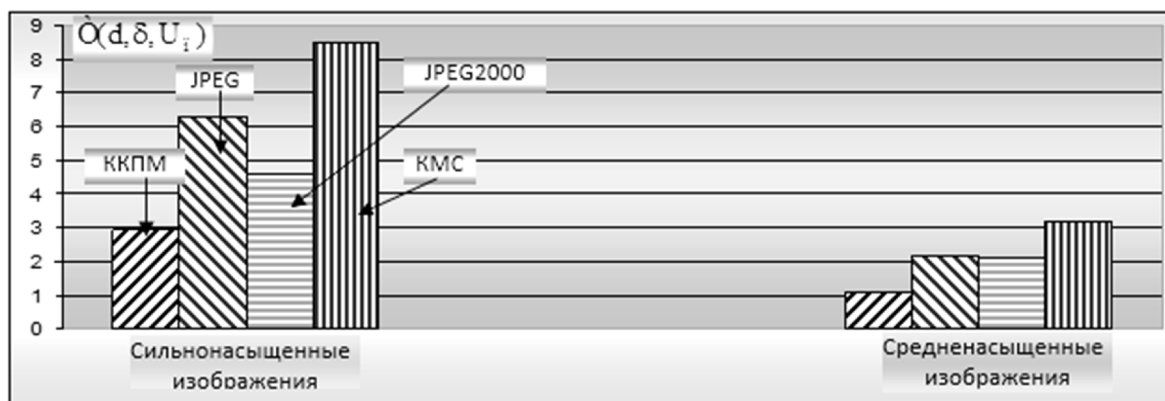


Рис. 4. Диаграммы зависимости времени передачи от класса обрабатываемых изображений для объемом 11 Мбит и скорости передачи 512 Кбит/с

Таким образом, разработан метод сжатия дифференцированных изображений на основе организации перфорирования массивов дифференциального представления в двумерном полиадическом пространстве с маской с последующим одномерным кодированием по блочной схеме.

Выводы:

1. Разработан метод компрессионного кодирования дифференцированных изображений для повышения безопасности видеoinформации. Метод базируется на следующих технологических решениях:

- дифференцировании фрагментов изображений по комбинированной схеме;
- организации перфорирования массивов дифференциального представления в двумерном полиадическом пространстве с маской;
- одномерное кодирование по блочной схеме для формирования кода композиционным перфорированным с маской числам в двумерном полиадическом пространстве.

2. Обеспечивается выполнение следующих стратегий обработки: предварительное преобразование видеоданных в системе сжатия изображений с предварительным дифференцированием; исключение неконтролируемых потерь видеoinформации; сокращение структурной, статистической избыточности; исключение дополнительных затрат служебной информации.

Сравнительное анализ затрат количества операций позволяет заключить, что для разработанного метода: количество операций умножения сокращается на 16% для $n = 8$ и на 25% для $n = 16$; количество операций типа сложения/вычитания снижается на 50%; – удельное количество операций умножения целочисленного типа относительно вещественного для разработанного метода составляет 33% в то время как для технологий JPEG такое количество достигает 100%.

Научная новизна состоит в том, что получил дальнейшее развитие метод сжатия изображений с контролируемой потерей их качества на основе предварительного дифференцирования. Отличительные характеристики относительно других методов заключаются в том, что формируются одномерные коды по блочной схеме в двумерном перфорированном полиадическом пространстве с маскированием, образованном для комбинированного дифференциального представления изображений. Это позволяет повысить доступность видеoinформации при заданных условиях относительно ее целостности.

Практическое значение полученных результатов исследований состоит в том, что:

1. На основе программной реализации созданного метода кодирования для повышения безопасности видеoinформации путем компрессии изображений по сравнению с использованием известных методов обеспечивается уменьшение на 35% задержки на передачу видовых изображений с заданным уровнем ее целостности.

2. Реализация процессов сжатия изображений на бортовых комплексах на основе разработанного метода позволяет повысить доступность видеoinформации относительно использования существующих методов с контролируемой потерей качества в среднем в 1,35 раза для сильнонасыщенных и в среднем в 1,8 раза для слабонасыщенных изображений.

ЛІТЕРАТУРА

- [1]. Лабутина И. А. Дешифрование аэрокосмических снимков : Учебное пособие / И. А. Лабутина. – М. : Аспект-Пресс, 2004. – 184 с.
- [2]. Кашкин В.Б. Цифровая обработка аэрокосмических изображений: Конспект лекций / В.Б. Кашкин. – Красноярск: ИПК СФУ, 2008. – 121 с.
- [3]. Баранник В. В. Методологический анализ системы аэрокосмического видеомониторинга чрезвычайных ситуаций / В. В. Баранник, А. В. Яковенко, А. Ю. Школьник // Сучасна спеціальна техніка. – 2011. – № 4 (27). – С. 12 – 22.
- [4]. Кулиса О. С. Обоснование требований относительно целостности видеoinформации воздушного мониторинга чрезвычайных ситуаций / О. С. Кулиса // Сучасна спеціальна техніка. – № 4. – 2012. – С. 12 – 22.
- [5]. Юдин О. К. Захист інформації в мережах передачі даних: підручник / Г. Ф. Конахович, О. Г. Корченко, О. К. Юдин. – К. : Видавництво ТОВ НВП «ІНТЕРСЕРВІС», 2009. – 714с.
- [6]. Юдин О. К. Інформаційна безпека. Нормативно-правове забезпечення : підручник / О. К. Юдин. – К. : НАУ, 2011. – 640с.
- [7]. Гонсалес Р. Цифровая обработка изображений / Р. Гонсалес, Р. Вудс. – М. : Техносфера, 2005. – 1073 с.
- [8]. Сэломон Д. Сжатие данных, изображений и звука / Д. Сэломон. – М. : Техносфера, 2004. – 368 с.
- [9]. Barannik V. Image Encoding Design Based On 2-D Combinatory Transformation / V. Barannik., V. Hahanov // International Symposium ["IEEE East-West Design & Test"], (Yerevan, Armenia, September 7 – 10, 2007) / Yerevan: 2007. – P. 124 – 127.
- [10]. Баранник В. В. Технология перфорированного описания массивов дифференциального представления в системах доставки сжатых изображений / В. В. Баранник, О. С. Кулиса // Сучасна спеціальна техніка. – № 2. – 2013. – С. 8 – 17.
- [7]. Gonzalez R., Woods R. Digital Image Processing., M. : Technosphere, 2005, 1073 p.
- [8]. Salomon D. Data compression, image, and audio, M. : Technosphere, 2004, 368 p.
- [9]. Barannik V., Hahanov V. Image Encoding Design Based On 2-D Combinatory Transformation // International Symposium ["IEEE East-West Design & Test"], (Yerevan, Armenia, September 7-10, 2007) / Yerevan: 2007, P. 124-127.
- [10]. Barannik V. V., Kulitsa O. S. Technology perforated writing arrays differential representation in the systems of delivery of compressed images // Suchasna spetsialna tehnika, № 2, 2013, P. 8-17.

МЕТОД КОДУВАННЯ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ ВІДЕОІНФОРМАЦІЇ АЕРОМОНІТОРІНГА НАДЗВИЧАЙНИХ СИТУАЦІЙ

Проводяться дослідження умов функціонування відеомоніторингу з використанням бортових комплексів у процесі попередження та ліквідації кризових ситуацій. Виявляються фактори, що формують загрози для порушення властивостей доступності та цілісності відеоінформації аеромоніторингу як категорій інформаційної безпеки. Це призводить до застарівання одержуваної інформації, прийняттю запізнених і помилкових рішень. Показується актуальність підвищення безпеки відеоінформації аеромоніторингу у системі попередження та ліквідації кризових ситуацій. Обґрунтовано, що для вирішення даного завдання пропонується використовувати технології компресійного кодування відеоданих. Проводиться обґрунтування вибору технології компресії зображень. Показується що для виключення нестачі, пов'язаного з пониженням нижньої межі диференціального поліадичного простору, необхідно для технології перфорування додатково враховувати двійкову маску всплескових елементів верхнього і нижнього рівнів. Викладаються основні етапи методу кодування зображень для підвищення доступності відеоінформації, що базується на: диференціальному поданні фрагментів зображень за комбінованою схемою; організації перфорування масивів диференціального представлення в двовимірному поліадичному просторі з маскою; поданні масивів елементів верхнього перфорацийного рівня в диференціальному поліадичному просторі, що забезпечує додаткове скорочення комбінаторної надмірності; одномірне кодування за блочною схемою. Наводиться експериментальна оцінка ефективності розробленого методу з існуючими методами в класі контрольованих втрат якості.

Ключові слова: диференціальне представлення, перфорування поліадичного простору, комбінаторна надмірність, двійкова маска.

REFERENCES

- [1]. Labutina I. A. Decryption space images : Textbook. – Moscow : Aspect Press, 2004, 184 p.
- [2]. Kashkin V. B. Digital processing of space images : Lectures, Atlanta : IPK SFU, 2008, 121.
- [3]. Barannik V. V., Yakovenko A. V., Shkolnik A. J. Methodological analysis of the aerospace video monitoring of emergencies // Suchasna spetsialna tehnika, 2011, № 4 (27), P. 12-22.
- [4]. Kulitsa O. S. Requirements rationale regarding the integrity of the video air disaster monitoring // Suchasna spetsialna tehnika, № 4, 2012, P. 12-22.
- [5]. Konahovich G. F., Korchenko O. G., Yudin O. K. Information security in data networks: a tutorial. – K. : Vydavnytstvo TOV NVP "INTERSERVIS", 2009, 714 p.
- [6]. Yudin O. K. Information Security. Regulatory support: a textbook, K. : UNAM, 2011, 640 p.

METHOD FOR ENCODING VIDEO INFORMATION SAFETY IMPROVEMENT AEROMONITORING EMERGENCY

A study of the conditions of operation using on-board video monitoring systems in the process of prevention and crisis management. Identifies the factors shaping the threat to disrupt the properties of availability and integrity of video aeromonitoring as categories of information security. This leads to the obsolescence of the information obtained, and the belated adoption of wrong decisions. Shows the actual increase security video aeromonitoring in the prevention and management of crisis situations. It is proved that the solution of this problem are encouraged to use compression for the video encoding technology. We justify the choice of image compression technology. It is shown that to avoid the disadvantages associated with a decrease in the lower limit of the differential Polyadic space required for perforating technology further consider the binary mask wavelet elements of the upper and lower levels. The principal stages of image coding method to improve the accessibility of video, which is based on: a differential representation of the images by a combined scheme, the organization perforation arrays in a two-dimensional representation of the differential Polyadic space, mask presentation of arrays of elements of the upper level of the perforation in the differential Polyadic space that provides an

additional reduction of the combinatorial redundancy, one-dimensional coding block diagram. We present experimental evaluation of the effectiveness of the developed method with existing methods in the class of controlled loss of quality.

Keywords: differential representation, perforated polyadic space, combinatorial redundancy, the binary mask.

Бараннік Володимир Вікторович, доктор технічних наук, професор, начальник кафедри, Харківський університет Повітряних Сил імені Івана Кожедуба.

E-mail: Barannik_V_V@mail.ru

Баранник Владимир Викторович, доктор технических наук, профессор, начальник кафедры, Харьковский университет Воздушных Сил имени Ивана Кожедуба.

Barannik Vladimir, Doctor of Science (eng.), Professor, chief of chair, Kharkov University of Aircraft of the name of Ivan Kozhedub.

Куліца Олег Сергійович, ад'юнкт, Академія пожежної безпеки імені Героїв Чорнобиля, м. Черкаси.

E-mail: Barannik_V_V@mail.ru

Кулиця Олег Сергеевич, ад'юнкт, Академія пожежної безпеки імені Героїв Чорнобиля, г. Черкаси.

Kulitsa Oleg, associate, Academy of Fire Safety named Heroes of Chernobyl, Cherkasy.

УДК 621.391.7

АЛГОРИТМ ШИФРУВАННЯ ІНФОРМАЦІЇ НА ОСНОВІ ДВОХ ХАОТИЧНИХ ДИНАМІЧНИХ СИСТЕМ ДЛЯ ЗАХИЩЕНИХ СИСТЕМ ЗВ'ЯЗКУ

Григорій Косован, Микола Кушнір, Леонід Політанський

На сучасному етапі розвиток інформаційних технологій, засобів телекомунікацій та комп'ютерної техніки широко постає проблема захисту конфіденційної інформації від несанкціонованого доступу при її передаванні чи зберіганні. Щоб вирішити дану проблему часто звертаються до криптографічних методів захисту інформації. Крім методів шифрування, що базуються на алгебраїчних поняттях, проводяться розроблення алгоритмів на основі детермінованого хаосу. В даній роботі представлено алгоритм шифрування текстової інформації, що базується на використанні двох динамічних систем, системи Реслера та кубічного відображення. Система Реслера використовується для генерації початкових умов, що використовується кубічним відображенням при шифруванні кожного окремого символу текстового повідомлення. В результаті роботи даного алгоритму символи вхідного повідомлення в результаті шифрування замінюються на цілі числа. В роботі також було проведено моделювання роботи динамічних систем в середовищі Matlab та приведено приклад роботи програми написаної на мові Delphi 7. В роботі також дано оцінку захищеності запропонованого алгоритму. Алгоритм володіє великою кількістю ключів шифрування, що робить процес їх підбору дуже складним. Використання двох динамічних систем ускладнює можливість статистичної атаки.

Ключові слова: криптографія, шифрування, дешифрування, динамічна система, хаос, алгоритм, оцінювання рівня захищеності.

Вступ. Розвиток інформаційних технологій та засобів телекомунікацій в значній мірі визначається закономірностями передавання даних по каналах цифрових систем зв'язку. Крім методів шифрування, що базуються на алгебраїчних

поняттях, проводяться розроблення алгоритмів на основі детермінованого хаосу [1-4]. Відомі програмні реалізації схем шифрування, що ґрунтуються на логістичному відображенні Арвінда, а також схеми генерації багаторазових ключів на