Труды МАИ. 2023. № 133
Trudy MAI, 2023, no. 133

Научная статья
УДК 621.396.967
URL: https://trudymai.ru/published.php?ID=177675

СПОСОБ ЗАЩИТНОГО КОДИРОВАНИЯ ДАННЫХ, ПОЛУЧАЕМЫХ ОПТИЧЕСКИМИ СЕНСОРАМИ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

Евгений КонстантиновичГригорьев[1]✉, Александр Михайлович Сергеев[2],
[1,2]Санкт-Петербургский государственный университет аэрокосмического приборостроения (ГУАП), Санкт-Петербург, Россия
[1]ev.grig95@gmail.com✉

Аннотация. В работе обсуждается актуальность задачи обеспечения конфиденциальности визуальной информации, получаемой оптическими сенсорами беспилотных авиационных систем (БАС). Делается вывод о том, что основным фактором, препятствующим во внедрении алгоритмов защиты данных, получаемых оптическими сенсорами гражданских БАС является их вычислительная сложность, в связи с этим целесообразным является поиск и внедрение математически простых способов защиты. Предлагается использование матричного маскирования, как альтернативы криптографическим методам для решения обсуждаемой задачи. Рассматривается и анализируется специфика маскирования полноцветных изображений и кадров видеопотока, получаемых полезной нагрузкой БАС. Результаты анализа показывают, что полноцветные изображения в результате маскирования приводятся к шумоподобному виду с полным разрушением контуров

исходного изображения, делая невозможными любые визуально-аналитические действия, в случае равенства размеров изображения и размеров матрицы-ключа. Выявлено, что маскирование полноцветных изображений имеет свою специфику в отличие от маскирования полутоновых изображений, обеспечивается лучшее перемешивание пикселов, и как следствие лучшее разрушение контуров исходного изображения, в сравнении с маскированием полутоновых изображений, тем самым, становится возможным маскирование матрицами малых размеров.

Ключевые слова: беспилотные авиационные системы, маскирование визуальной информации, квазиортогональные матрицы, обеспечение конфиденциальности

Финансирование: Работа выполнена при финансовой поддержке Министерства науки и высшего образования Российской Федерации, соглашение № FSRF-2023-0003, "Фундаментальные основы построения помехозащищенных систем космической и спутниковой связи, относительной навигации, технического зрения и аэрокосмического мониторинга".

Для цитирования: Григорьев Е.К., Сергев А.М. Способ защитного кодирования данных, получаемых оптическими сенсорами беспилотных авиационных систем // Труды МАИ. 2023. № 133. URL: https://trudymai.ru/published.php?ID=177675

Original article

METHOD FOR SECURITY CODING OF DATA RECEIVED BY OPTICAL SENSORS OF UNMANNED AIRCRAFT SYSTEMS

Evgeniy K. Grigoriev[1]✉, Alexander M. Sergeev[2]

[1,2]Saint-Petersburg State University of Aerospace Instrumentation,

Saint Petersburg, Russia
[1]ev.grig95@gmail.com✉

Abstract. At the current time, unmanned aerial systems (UAS) are widely used in solving problems of real-time monitoring, ecological exploration, inspection of protected areas, as well as in the creation of various media content. One of the main channels for obtaining information is the optical channel.

The article discusses the relevance of the problem of the confidentiality ensuring of visual information received by optical sensors of (UAS). The inference is being made that the main factor hindering the implementation of algorithms data protection received by the civil UAS optical sensors is their computational complexity. In this respect, to searching for and implementing mathematically simple protection techniques seems to be expedient. The authors propose employing matrix masking as an alternative as an alternative to the cryptographic methods for the discussed problem solution. Masking specifics of the full-color images and video stream frames received by the UAS payload are being considered and analyzed. The results of the analysis reveal that masking results in color images reduction to a noise-like form with complete destruction of the contours of the original image, making any visual analytical analysis impossible in the case of equal image sizes and key-matrix sizes. The authors revealed that the full-color images masking has its own specifics in contrast to the halftone images masking, and, as a consequence, ensure better pixels mixing and better contours destruction of the initial image compared to the halftone images masking. Masking with the small-size key matrices thereby becomes possible.

Keywords: unmanned aircraft systems, masking visual information, quasi-orthogonal matrices, ensuring confidentiality

Funding: the paper was prepared with the financial support of the Ministry of Science and Higher Education of the Russian Federation, grant agreement No. FSRF-2023-0003, “Fundamental principles of building of noise-immune systems for space and satellite communications, relative navigation, technical vision and aerospace monitoring”.

For citation: Grigoriev E.K., Sergeev A.M. Method for security coding of data received by optical sensors of unmanned aircraft systems. *Trudy MAI*, 2023, no. 133. URL: https://trudymai.ru/published.php?ID=177675

Введение

Задача обеспечения информационной безопасности данных, получаемых при помощи беспилотных авиационных систем (БАС), сегодня остается актуальной, что подтверждает анализ как отечественных, так и зарубежных работ по данной тематике [1-6].

Одним из основных каналов получения информации является оптический канал. По данным аналитического центра Drone Industry Insight [7], основанным на опросе около 900 компаний, предоставляющих услуги в сфере БАС по всему миру, в 2022 году наиболее востребованные сферы применения БАС в порядке убывания, следующие: фото и видеосъёмка; картографирование; мониторинг объектов.

О важности сегмента рынка БАС гражданского назначения можно судить по данным ассоциации работодателей и предприятий индустрии беспилотных авиационных систем "АЭРОНЕКСТ" [8]. Так, согласно рисунку 1, в РФ в 2022 году

выручка компаний рынка гражданских БАС превысила долю специализированных. При этом значительную долю рынка занимают коммерческие услуги.

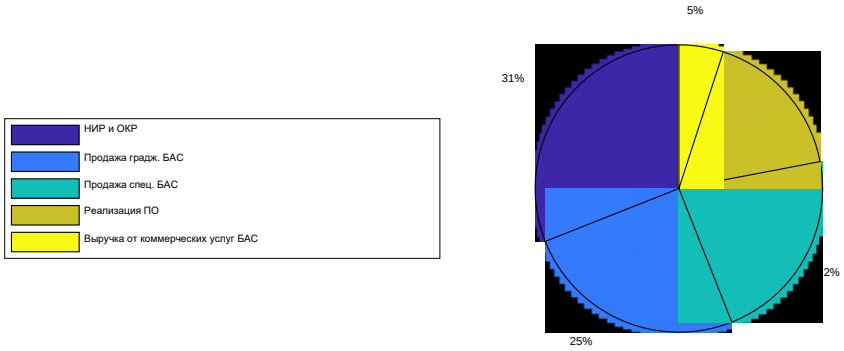


Рисунок 1 - Распределение выручки компаний рынка БАС в РФ, по данным [8]

В таблице 1 на основе открытых данных DRONE Industry Insight [9] представлен рейтинг производителей гражданских БАС по состоянию на 2022 год.

При составлении рейтинга учитывались следующие показатели:

– размер компании,

– развитие компании,

– доли рынка,

– показатели продаж,

– активность в социальных сетях,

– внимание общественности,

– количество и объем финансирования,

– предполагаемый доход и степень активности в Интернете.

Таблица 1. Рейтинг ведущих производителей БАС

Производитель	Страна	Рейтинг, %
DJI	КНР	100

Parrot	Франция	22
Skydio	США	18

Анализ открытых данных и технической документации [10-12] показывает, что защитное кодирование данных от сенсоров оптического информационного канала осуществляется только в коммерческом сегменте БАС с использованием криптографического алгоритма AES с длинами ключа 128 или 256 бит.

Гражданские БАС, доступные широкому кругу пользователей и использующие незащищенное соединение, например, канал wi-fi для связи «летательный аппарат»– «пульт управления», подвержены атакам, приводящим к потере или несанкционированному использованию конфиденциальной визуальной информации их владельцев [13, 14].

Основным фактором, сдерживающим внедрение защитного кодирования передаваемых визуальных данных в потребительском сегменте БАС, является вычислительная ресурсоемкость, и, как следствие, длительное время кодирования/декодирования.

Исходя из вышесказанного вытекает цель работы – показать простой способ защиты визуальных данных, передаваемых по открытому каналу, при использовании БАС гражданского назначения.

Маскирование информации как альтернатива шифрации

В качестве альтернативы криптографическим методам защиты информации в научной литературе [15-20] прослеживается использование матричных методов защитного кодирования – маскирования информации, получаемой по оптическому

[15-18], радиолокационному [19] и звуковому каналам [20]. Методы основаны на применении ортогональных и квазиортогональных матриц и используются в предположении небольшого периода актуальности передаваемой в открытом канале информации.

Использование подобного метода, при учете ограниченных вычислительных ресурсов гражданских БАС имеет следующие преимущества:

– использование простого математического аппарата – матричное умножение, и, как следствие, обеспечение симметричности преобразования с высокой скоростью маскирования/демаскирования визуальной информации, получаемой с полезной нагрузки;

– матрица-ключ для операции маскирования/демаскирования не передается по каналу связи. Достаточно передать только порядковый номер матрицы для выбора из базы данных на приемной стороне;

– использование ортогональных матриц исключает искажения преобразований за счет аппаратных и транспортированных погрешностей. Инструментальные погрешности существуют при использовании матрицы-ключа с вещественными коэффициентами, но отсутствуют при использовании целочисленных матриц.

Отметим, что в рассматриваемых источниках по маскированию визуальной информации [15-18] изображения или кадры видеопотока рассматриваются в оттенках серого, а также при малом размере матрицы-ключа (в сравнении с исходным изображением, или кадром видеопотока) в результирующем – маскированном изображении наблюдаются контуры, позволяющие при визуальном анализе распознать исходное – немаскированное изображение [17]. Следует оговорить, что

проблема наличия контуров на кодированном изображении при малом размере ключа, характерна также и для криптографических алгоритмов, при шифровании изображений с малым размером ключа [21].

Поскольку полезная нагрузка БАС потребительского сегмента предоставляет полноцветное изображение или видеопоток, то целесообразно, учитывая перечисленные достоинства матричного маскирования, оценить возможность использования метода при кодировании полноцветных изображений/кадров видеопотока, получаемых с полезной нагрузки БАС.

Маскирование полноцветных изображений

Процедуру маскирования для изображений или кадров видеопотока (в дальнейшем для простоты изложения будем говорить об изображениях) в оттенках серого обобщенно можно описать как:

При преобразовании на передающей стороне осуществляется следующее преобразование:

$$\mathbf{Y}_n = \mathbf{M}_n \mathbf{X}_n \mathbf{M}_n^T \qquad (1)$$

где $\mathbf{X}_n$ – исходное изображение, $\mathbf{M}_n$ – матрица-ключ, $\mathbf{Y}_n$ – передаваемое по каналу связи защищенное изображение. В случае, если размер матрицы-ключа меньше, чем исходное изображение, то оно делиться на k блоков, длина каждого блока равна размеру матрицы-ключа [19].

Обратное преобразование на приемной стороне выполняется следующим образом:

$$\mathbf{X}_n = \left(\mathbf{M}_n\right)^{-1} \mathbf{Y}_n \left(\mathbf{M}_n^T\right)^{-1} \qquad (2)$$

Использование в качестве матрицы-ключа $\mathbf{M}_n$ структурированных ортогональных матриц, для которых $\mathbf{M}_n^{-1} = \mathbf{M}_n^{\mathrm{T}}$, упрощает обратное преобразование. В случае, если изображение при маскировании делилось на k блоков, обратное преобразование выполняется для каждого блока [17].

Следует отметить, что для упрощения вычислений, изображение (или его фрагмент) на передающей стороне можно умножать на матрицу-ключ только слева или только справа, а на приемной стороне при обратном преобразовании также осуществлять умножение на обратную матрицу только слева или только справа, но именно приведенный выше вариант с двухсторонним умножением дает лучшие результаты, обеспечивая лучше перемешивание пикселов исходного изображения [15].

Для маскирования цветных изображений, указанные процедуры необходимо модифицировать. На рисунках 2 и 3 приведены схемы алгоритмов маскирования и демаскирования цветных изображений.

Следует дать пояснения. На вход алгоритма маскирования поступает исходное изображение цветовой модели RGB, в соответствии с его размером из базы матриц выбирается матрица-ключ. В случае, если в базе есть матрица равная размеру изображения, выбирается она, поскольку на результат маскирования в большей степени влияет порядок маскирующей матрицы [17]. Если такая матрица отсутствует, то выбирается наибольшая по размеру матрица, позволяющая маскировать все фрагменты исходного изображения. Далее из исходного изображения извлекается

красный, зеленый и синий каналы соответственно, каждый из которых умножается на выбранную матрицу согласно (1), в блоках 1.7 – 1.9 осуществляется либо квантование пикселов, если матрица-ключ содержит целочисленные элементы, либо деление на некоторый коэффициент q, в случае, если матрица-ключ содержит вещественные элементы.

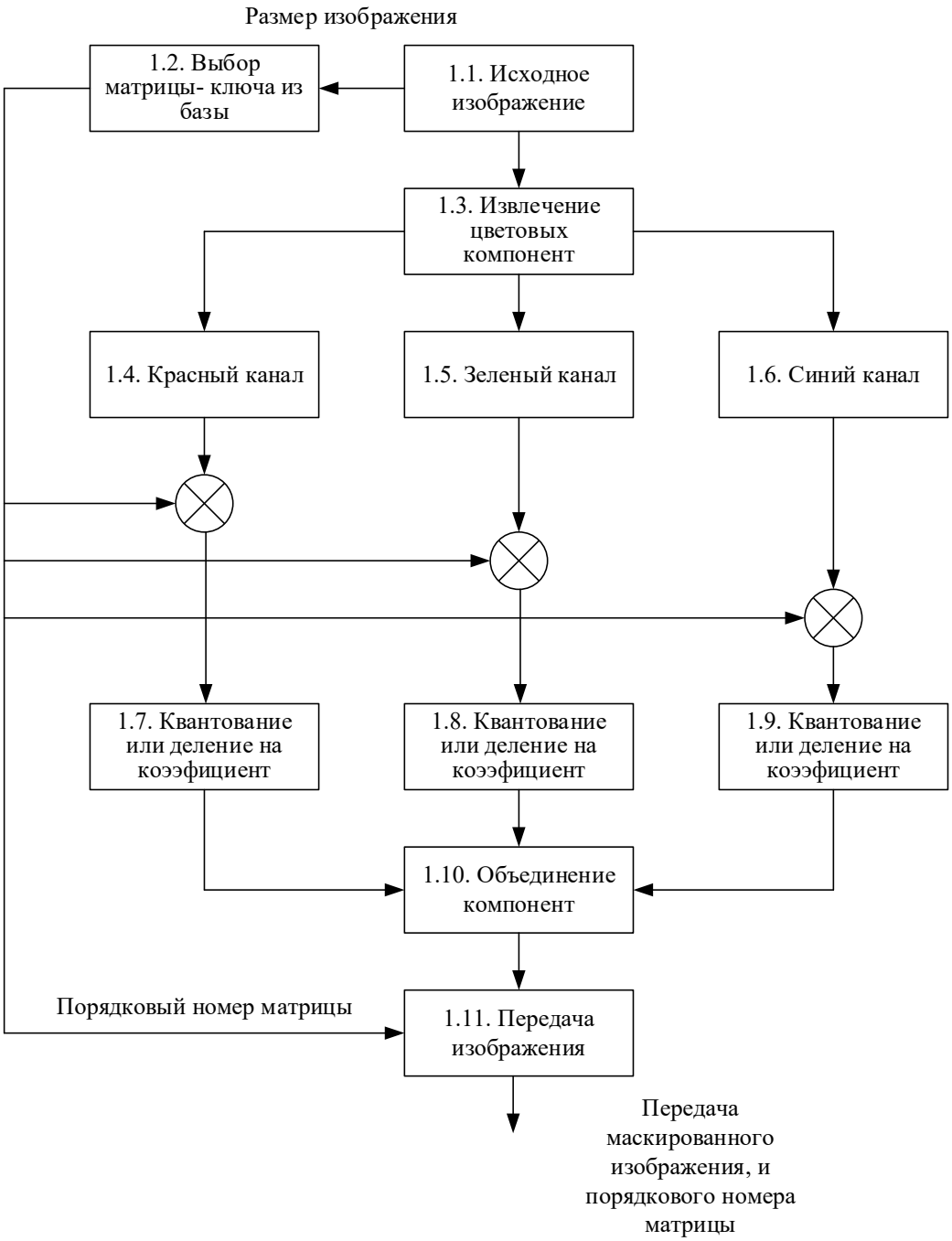


Рисунок 2 - Процедура маскирования RGB изображения

Компоненты маскированного изображения далее объединяются для передачи по каналу связи, как уже упоминалось, достоинством маскирования изображений является то, что нет необходимости передавать матрицу-ключ по каналу связи, достаточно передать само маскированное изображение и порядковый номер в базе матриц.

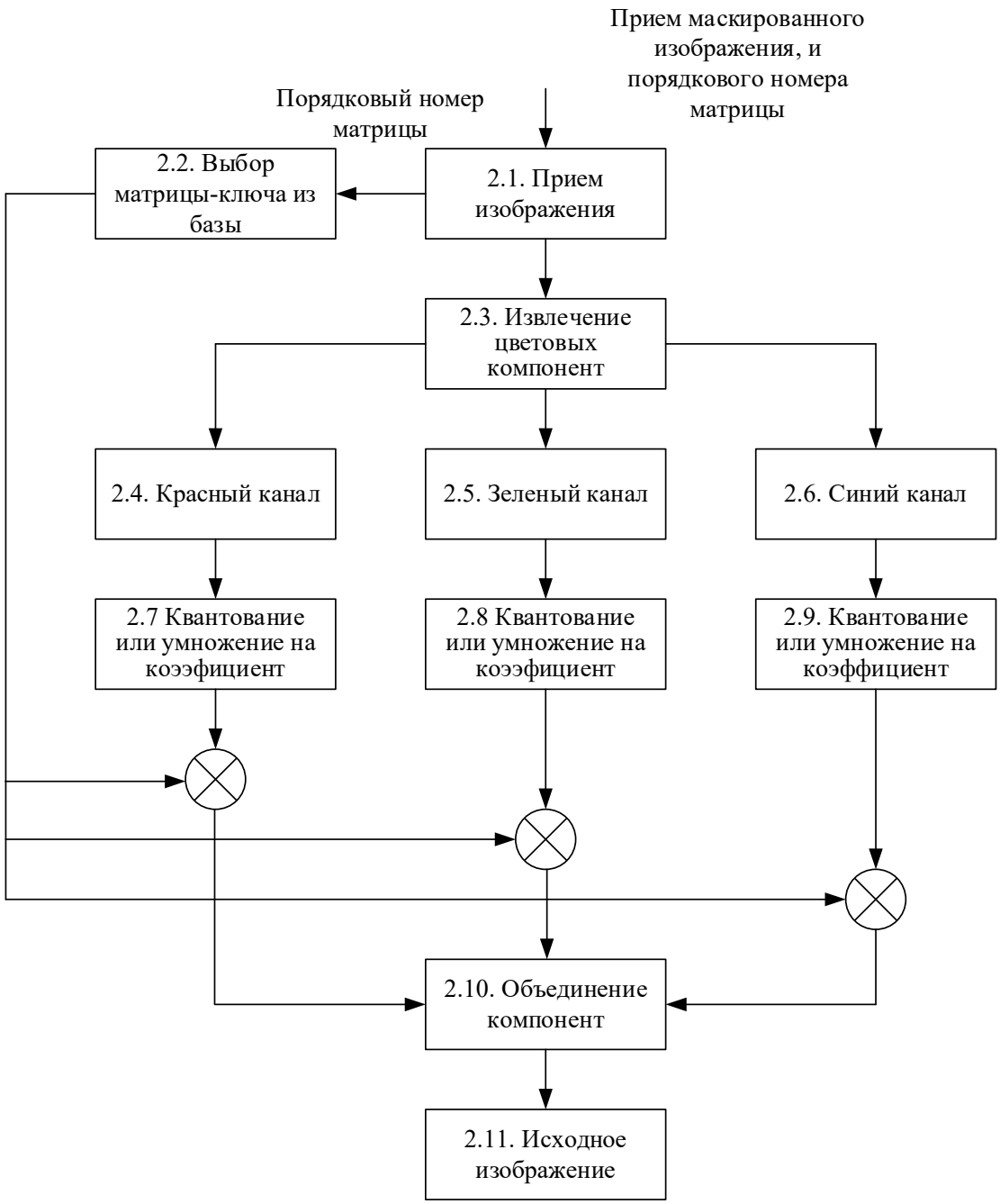


Рисунок 3 - Процедура демаскирования RGB изображения

Процедура демаскирования осуществляется симметрично процедуре маскирования – умножение на матрицу осуществляется согласно (2). Подробнее квантование, умножение и деление на коэффициент блоков 1.7-1.9 и 2.7-2.9 рассмотрено в работе [22].

Описание эксперимента и выбор изображений

Изображения, получаемые полезной нагрузкой, могут быть представлены следующими типами:

– вертикальные изображения, т.е. съемка в надир;

– перспективные изображения, съемка под углом – не в надире;

– развлекательные изображения.

Изображения первого и второго типа могут быть получены как гражданскими, так и коммерческими БАС. При наличии точных данных геопозиционирования изображения первого типа пригодны для решения задач картографирования, что более актуально для коммерческих БАС.

При отсутствии данных геопозиционирования – изображения первого и второго типа пригодны для решения задач оперативного мониторинга и реагирования, а изображения третьего типа представляют собой произвольные фотографии развлекательного содержания.

Изображения первого типа в силу специфики съемки будут иметь большое количество ярко-выраженных контуров. Изображения второго типа будут иметь малое количество ярко-выраженных контуров.

Для дальнейших экспериментов были выбраны 4 изображения – стандартное тестовое изображение Lena [23], а также изображения, относящиеся к каждому из вышеприведенных типов.

Все изображения представлены в формате jpg. Размер каждого изображения для эксперимента приведен к 512x512 пикселов.

а) Тестовое изображение Lena

б) Перспективное изображение

в) Вертикальное изображение

г) Развлекательное изображение

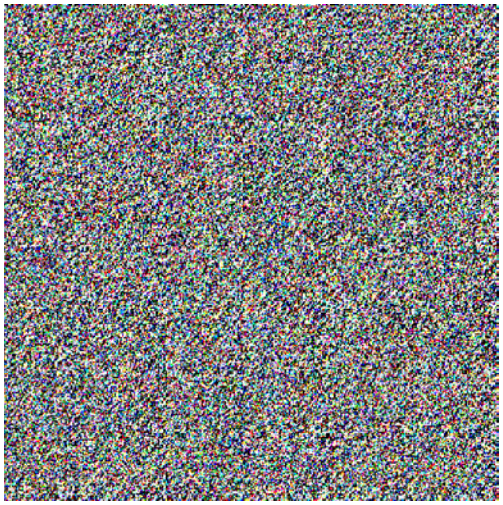
Рисунок 4 - Изображения для экспериментов

В первой части эксперимента, каждое изображение будет маскировано матрицей Адамара размером равным размерам изображения.

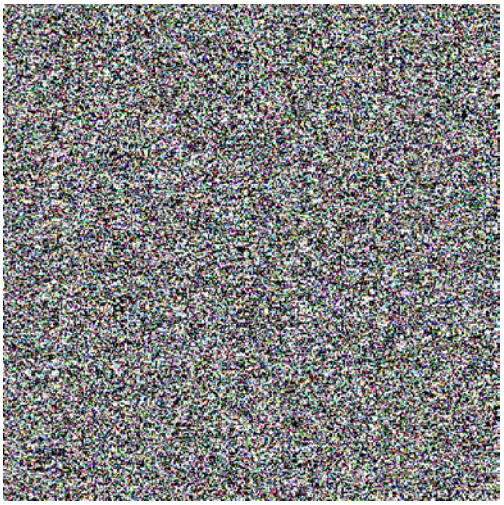
Во второй части эксперимента, каждое изображение будет маскировано матрицей Адамара размером 4x4 и 8x8, что в системе MATLAB соответствует размерам ключа 64 и 256 бит соответственно. Дополнительно каждое изображение будет сопоставлено с маскированным полутоновым изображением с одинаковым размером ключа.

Результаты моделирования

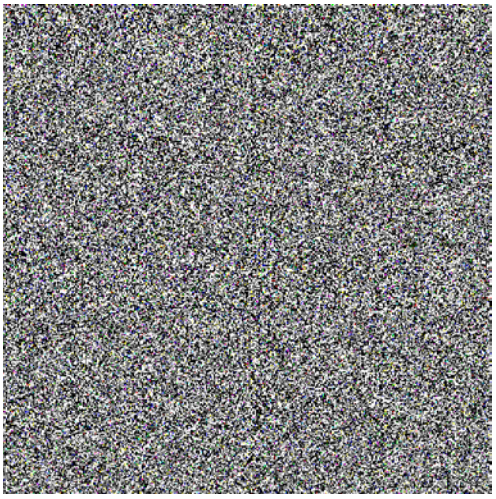
На рисунке 5 представлены результаты маскирования полноцветных изображений, представленных на рисунке 4.

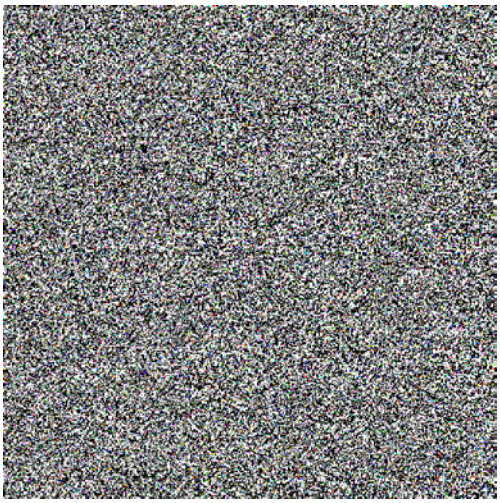


а) Тестовое изображение Lena



б) Перспективное изображение





в) Вертикальное изображение *г*) Развлекательное изображение

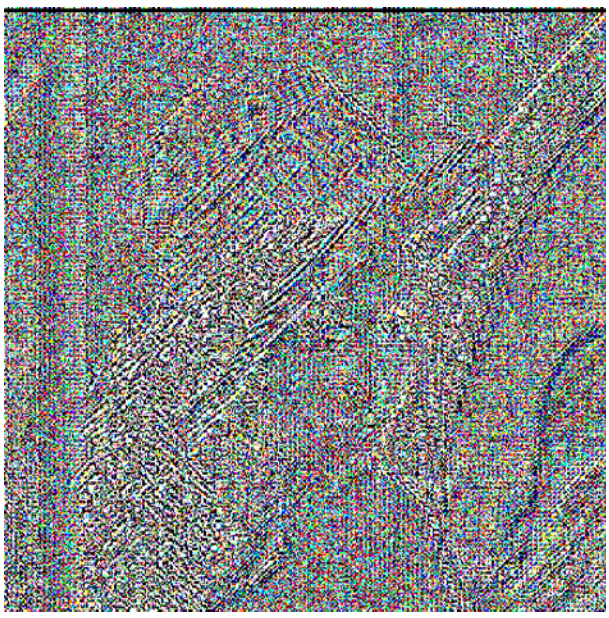
Рисунок 5 - Результаты маскирования матрицей размером, совпадающим с исходным изображением

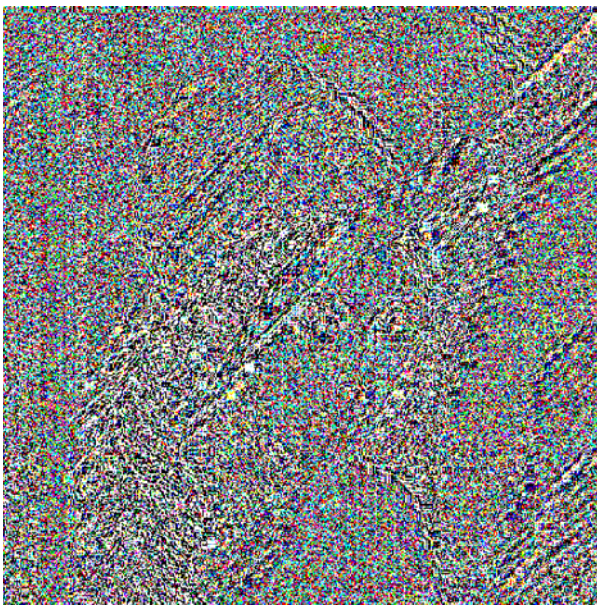
Как видно из рисунка 5, предлагаемый метод обеспечивает разрушение взаимосвязей исходного полноцветного изображения и приводит его к шумоподобному виду.

Результат качественно воспроизводим как для представленных изображений, так и при проведении масштабного эксперимента с изображениями из открытых источников, например базой аэрофотоснимков [24].

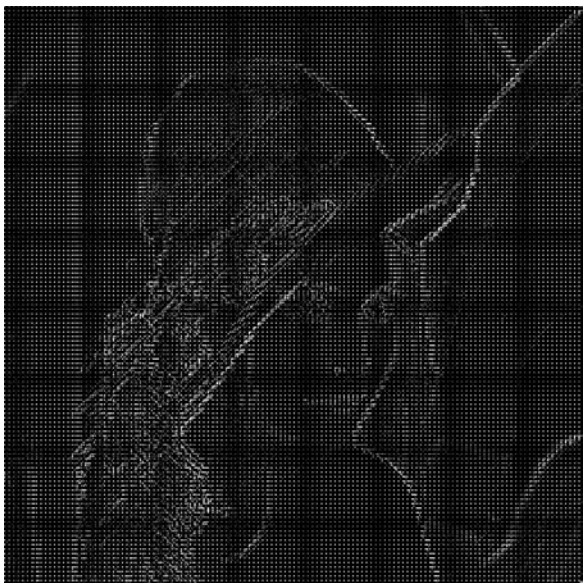
На рисунках 6-9 представлены результаты, проведенные по второй части эксперимента. На каждом из них *а* и *б* представляют собой результаты маскирования полноцветного изображения матрицей Адамара размером 4x4 и 8x8 соответственно.

На рисунках 6-9 *в* и *г* представлены результаты маскирования аналогичного, но полутонового изображения матрицами соответствующих размеров.

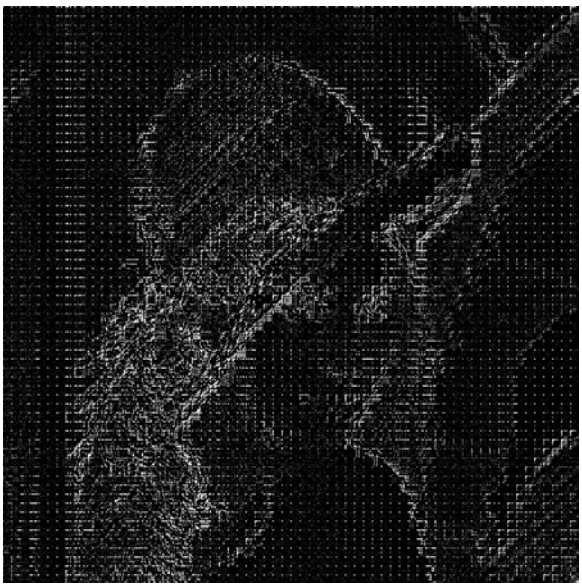




а) Полноцветное, матрица 4x4 *б*) Полноцветное, матрица 8x8



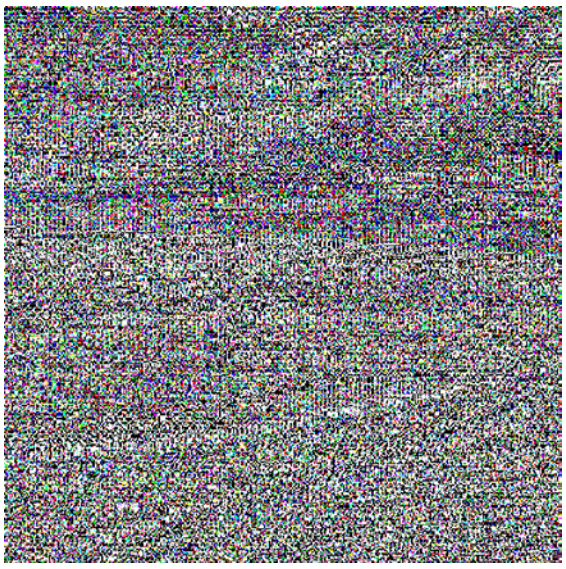
в) Полутоновое, матрица 4x4



г) Полутоновое, матрица 8x8

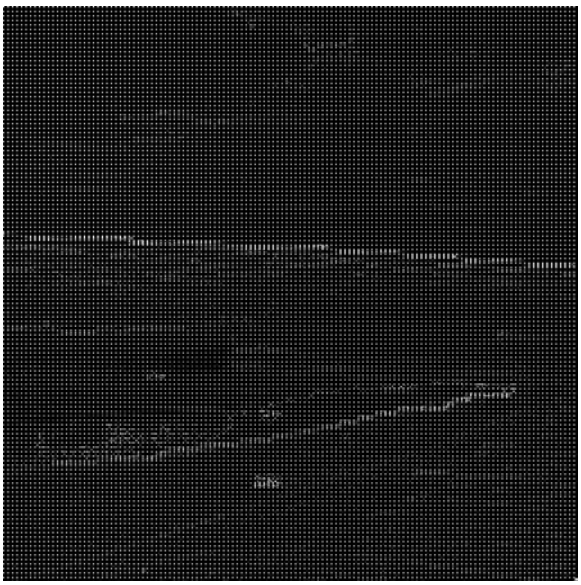
Рисунок 6 - Результаты маскирования тестового изображения «*а*» рисунка 4

Приведенные результаты демонстрируют обеспечение значительно лучшего снижения качества визуального восприятия маскированного изображения при перемешивании пикселов исходного изображения по каждому из трех цветовых каналов.



а) Полноцветное, матрица 4x4

б) Полноцветное, матрица 8x8

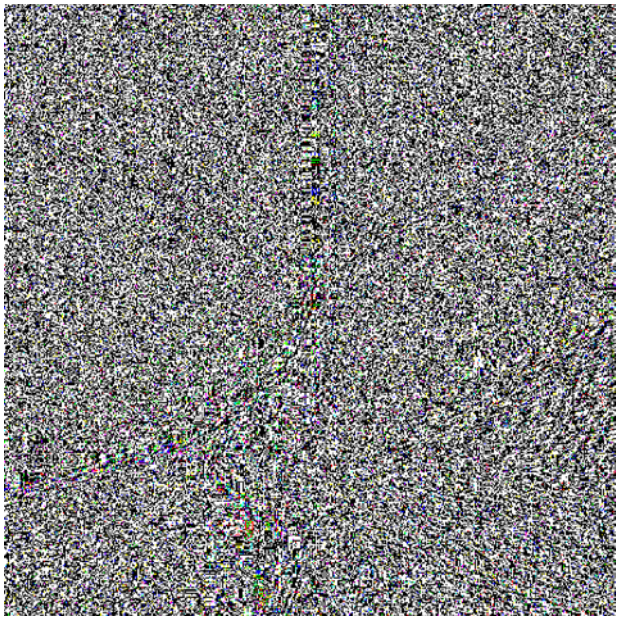


в) Полутоновое, матрица 4х4

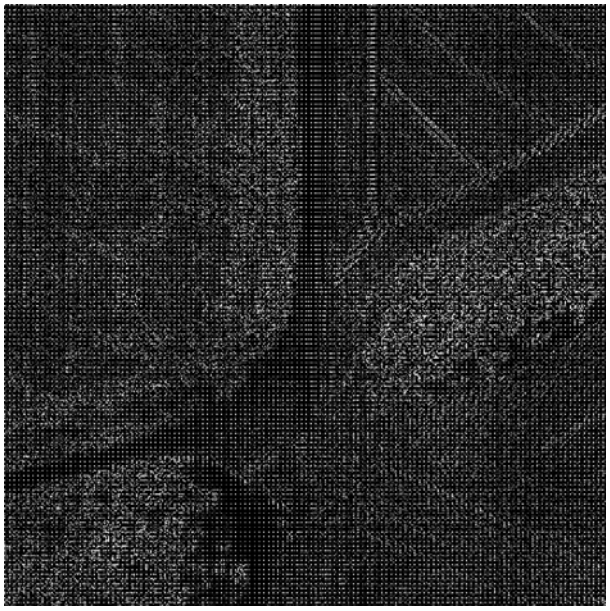
г) Полутоновое, матрица 8х8

Рисунок 7 - Результаты маскирования тестового изображения «*б*» рисунка 4

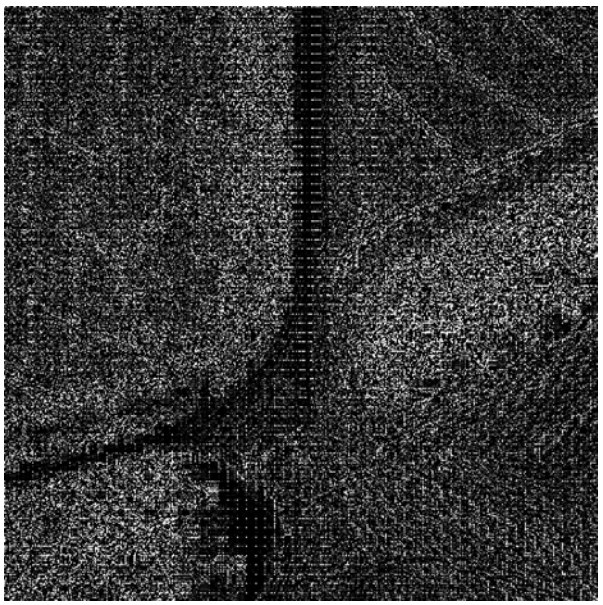
а) Полноцветное, матрица 4х4



б) Полноцветное, матрица 8х8

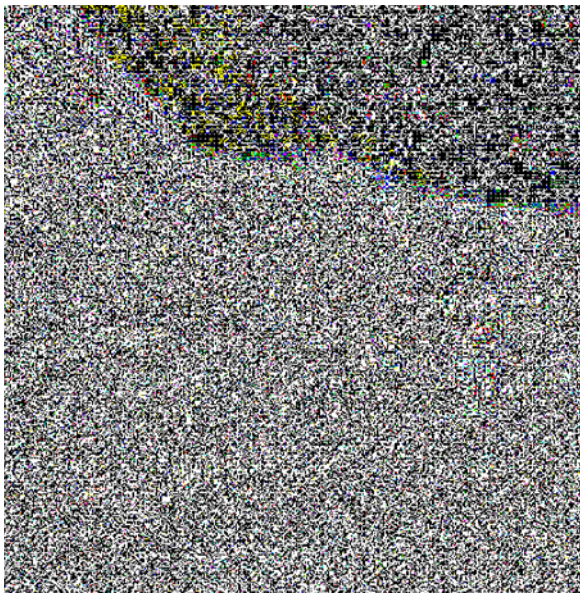


в) Полутоновое, матрица 4x4



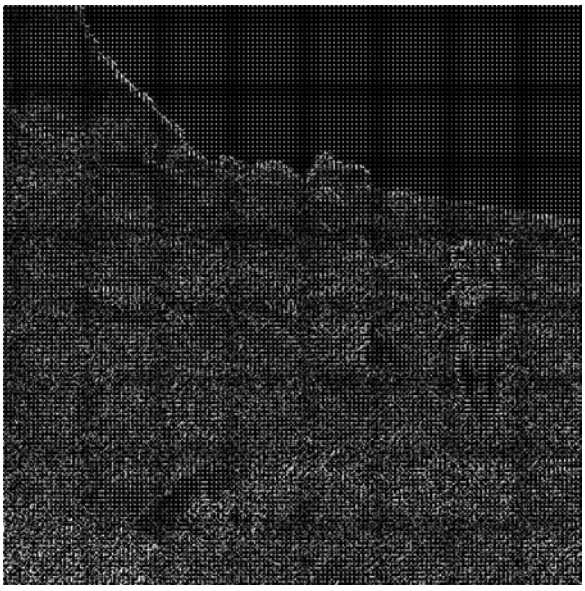
г) Полутоновое, матрица 8x8

Рисунок 8 - Результаты маскирования тестового изображения «*в*» рисунка 4

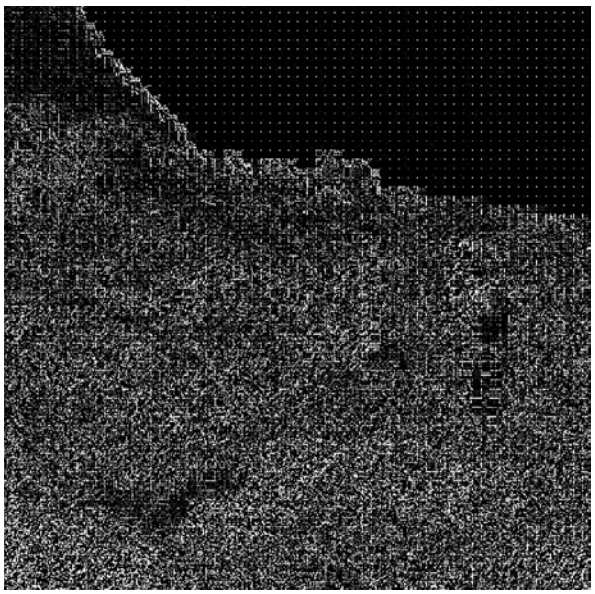


а) Полноцветное, матрица 4x4

б) Полноцветное, матрица 8x8



в) Полутоновое, матрица 4х4



г) Полутоновое, матрица 8х8

Рисунок 9 - Результаты маскирования тестового изображения «*г*» рисунка 4

Тем не менее, большие и ярко выраженные контуры, например, границы «земля»-«небо» для перспективных изображений или «земля»-«вода» для вертикальных изображений требуют увеличения размеров матрицы маскирования. Данное явление не является недостатком рассматриваемого метода, поскольку разнообразие малоуровневых квазиортогональных матриц, в том числе больших размеров, в последнее время существенно выросло [25-28].

Следует также отметить, что для изображений или видеопотока с малым временем актуальности, например, при получении оперативной информации с БАС, наличие контуров на маскированном изображении не имеет значения. В целом, процедура матричного маскирования хорошо подходит для применения в виду специфики получаемых кадров – с большим количеством мелких деталей.

Заключение

В работе предложен математически простой способ защитного кодирования - маскирования полноцветных изображений/кадров видеопотока, получаемых полезной нагрузкой БАС, который может применяться для обеспечения конфиденциальности информации с малым временем актуальности.

По описанной в работе процедуре маскирования возможно приведение полноцветных изображений к шумоподобному виду с полным разрушением контуров исходного изображения, делая невозможными любые визуально-аналитические действия.

Маскирование полноцветных изображений имеет свою специфику в отличие от маскирования полутоновых изображений. Маскирование каждого канала полноцветного изображения дает лучшее перемешивание пикселов, обеспечивая лучшее разрушение контуров исходного изображения, в сравнении с маскированием полутоновых изображений, и, как следствие, становится возможным маскирование матрицами даже малых размеров.

Использование матриц-ключей малых размеров обеспечивает пропорциональное снижение вычислительных затрат процедуры маскирования.

Список источников

1. Авдонин И.А., Беляев С.С., Будько М.Б. и др. Организация защищенного канала передачи данных между беспилотным летательным аппаратом и наземной станцией управления на основе одноразовых блокнотов // Информатизация и связь. 2018. № 5. С. 78-84.

2. Жилин С.В., Архипенко В.В., Басан Е.С. Повышение надёжности оптических каналов передачи данных между БПЛА // Информатизация и связь. 2022. № 2. С. 25-29. DOI: 10.34219/2078-8320-2022-13-2-25-29

3. Аметинский М.В. Анализ потенциальных угроз системы управления беспилотных летательных аппаратов средних и тяжелых классов // Труды МАИ. 2017. № 94. URL: https://trudymai.ru/published.php?ID=81066

4. Alawida M., Teh J.S., Alshoura W.H. A New Image Encryption Algorithm Based on DNA State Machine for UAV Data Encryption // Drones, 2023, vol. 7 (38). DOI: 10.3390/drones7010038

5. Sun X., et al. Physical Layer Security in UAV Systems: Challenges and Opportunities // IEEE Wireless Communications, 2019, vol. 26 (5), pp. 40-47. DOI: 10.1109/MWC.001.1900028

6. Титов А.Г., Неретин Е.С., Дудкин С.О., Брусникин П.М. Разработка архитектуры бортового сервера данных для применения в составе комплекса радиоэлектронного оборудования с применением концепции интегрированной модульной авионики // Труды МАИ. 2019. № 105. URL: https://trudymai.ru/published.php?ID=104257

7. Drone Industry Barometer 2022 White Paper. URL: https://droneii.com/project/drone-industry-barometer

8. Итоги 2022 года для рынка беспилотной авиации. URL: https://aeronext.aero/press_room/analytics/292234

9. Drone Manufacturers Ranking 2022. URL: https://droneii.com/product/drone-manufacturers-ranking#download

10. Scydio. Security Trust Center. URL: https://www.skydio.com/security-trust-center

11. Parrot. Cybersecurity. URL: https://www.parrot.com/en/drones/anafi-ai/technical-documentation/cybersecurity

12. DJI Security White Paper. URL: https://security.dji.com/data/resources/

13. Сенцов А.А., Поляков В.Б., Иванов С.А., Помозова Т.Г. Метод перехвата малоразмерных и малозаметных беспилотных летательных аппаратов // Труды МАИ. 2023. № 129. URL: https://trudymai.ru/published.php?ID=173033. DOI: 10.34759/trd-2023-129-21

14. Hooper M. et al. Securing commercial WiFi-based UAVs from common security attacks // IEEE Military Communications Conference, 2016, pp. 1213-1218. DOI: 10.1109/MILCOM.2016.7795496

15. Востриков А.А., Сергеев М.Б., Литвинов М.Ю. Маскирование цифровой визуальной информации: термин и основные определения // Информационно-управляющие системы. 2015. № 5 (78). С. 116-123. DOI: 10.15217/issn1684-8853.2015.5.116

16. Востриков А.А., Мишура О.В., Сергеев А.М., Чернышев С.А. О выборе матриц для процедур маскирования и демаскирования изображений // Фундаментальные исследования. 2015. № 2 (ч. 24). С. 5335–5339.

17. Сергеев А.М. Структурированные по Уолшу двухуровневые и модульно двухуровневые квазиортогональные матрицы для маскирования изображений // Известия высших учебных заведений. Приборостроение. 2023. Т. 66. № 5. С. 399-408. DOI: 10.17586/0021-3454-2023-66-5-399-408

18. Балонин Ю.Н., Востриков А.А., Сергеев М.Б. О прикладных аспектах применения М-матриц // Информационно-управляющие системы. 2012. № 1 (56). С. 92-93.

19. Tokarevskiy I.V., Sentsov A.A., Sergeev M.B. Features of Matrix Masking of Digital Radar Images // 2022 Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF), 2022, pp. 488-491. DOI: 10.1109/WECONF55058.2022.9803393

20. Григорьев Е.К., Сергеев А.М. Оценка качества матричного маскирования цифровых звуковых данных // Труды учебных заведений связи. 2023. Т. 9. № 3. С. 6-13. DOI: 10.31854/1813-324X-2023-9-3-6-13

21. Ерош И.Л., Сергеев А.М., Филатов Г.П. О защите цифровых изображений при передаче по каналам связи // Информационно-управляющие системы. 2007. № 5 (30). С. 20-22.

22. Чернышев С.А. Разработка и исследование метода матричного маскирования видеоинформации в глобально распределенных системах: автореф. дис. ... канд. техн. наук. Санкт Петербург, 2017. – 120 с.

23. The Lenna Story. URL: http://lenna.org/

24. Aerial images (512x512). URL: https://universe.roboflow.com/alex-shamota-hsa0p/aerial-images-512-512-2

25. Балонин Н.А., Балонин Ю.Н., Востриков А.А., Сергеев М.Б. Вычисление матриц Мерсенна-Уолша // Вестник компьютерных и информационных технологий. 2014. № 11 (125). С. 51-56.

26. Балонин Н.А., Сергеев М.Б. Максимум детерминанта бициклических матриц с каймой // Информационно-управляющие системы. 2023. № 3 (124). С. 2-14. DOI: 10.31799/1684-8853-2023-3-2-15

27. Балонин Н.А., Сергеев М.Б. Критские матрицы Одина и Тени, сопровождающие простые числа и их степени // Информационно-управляющие системы. 2022. № 1 (116). С. 2-7. DOI: 10.31799/1684-8853-2022-1-2-7

28. Балонин Н.А., Сергеев М.Б., Суздаль В.С. Динамические генераторы квазиортогональных матриц семейства Адамара // Труды СПИИРАН. 2017. № 5 (54). С. 224-243. DOI: 10.15622/sp.54.10

References

1. Avdonin I.A., Belyaev S.S., Bud'ko M.B. et al. *Informatizatsiya i svyaz'*, 2018, no. 5, pp. 78-84.

2. Zhilin S.V., Arkhipenko V.V., Basan E.S. *Informatizatsiya i svyaz'*, 2022, no. 2, pp. 25-29. DOI: 10.34219/2078-8320-2022-13-2-25-29

3. Ametinskii M.V. *Trudy MAI*, 2017, no. 94. URL: https://trudymai.ru/eng/published.php?ID=81066

4. Alawida M., Teh J.S., Alshoura W.H. A New Image Encryption Algorithm Based on DNA State Machine for UAV Data Encryption, *Drones*, 2023, vol. 7 (38). DOI: 10.3390/drones7010038

5. Sun X., et al. Physical Layer Security in UAV Systems: Challenges and Opportunities, *IEEE Wireless Communications*, 2019, vol. 26 (5), pp. 40-47. DOI: 10.1109/MWC.001.1900028

6. Titov A.G., Neretin E.S., Dudkin S.O., Brusnikin P.M. *Trudy MAI*, 2019, no. 105. URL: https://trudymai.ru/eng/published.php?ID=104257

7. *Drone Industry Barometer 2022 White Paper*. URL: https://droneii.com/project/drone-industry-barometer

8. *Itogi 2022 goda dlya rynka bespilotnoi aviatsii*. URL: https://aeronext.aero/press_room/analytics/292234

9. *Drone Manufacturers Ranking 2022*. URL: https://droneii.com/product/drone-manufacturers-ranking#download

10. *Scydio. Security Trust Center*. URL: https://www.skydio.com/security-trust-center

11. *Parrot. Cybersecurity*. URL: https://www.parrot.com/en/drones/anafi-ai/technical-documentation/cybersecurity

12. *DJI Security White Paper*. URL: https://security.dji.com/data/resources/

13. Sentsov A.A., Polyakov V.B., Ivanov S.A., Pomozova T.G. *Trudy MAI*, 2023, no. 129. URL: https://trudymai.ru/eng/published.php?ID=173033. DOI: 10.34759/trd-2023-129-21

14. Hooper M. et al. Securing commercial WiFi-based UAVs from common security attacks, *IEEE Military Communications Conference*, 2016, pp. 1213-1218. DOI: 10.1109/MILCOM.2016.7795496

15. Vostrikov A.A., Sergeev M.B., Litvinov M.Yu. *Informatsionno-upravlyayushchie sistemy*, 2015, no. 5 (78), pp. 116-123. DOI: 10.15217/issn1684-8853.2015.5.116

16. Vostrikov A.A., Mishura O.V., Sergeev A.M., Chernyshev S.A. *Fundamental'nye issledovaniya*, 2015, no. 2 (ch. 24), pp. 5335–5339.

17. Sergeev A.M. *Izvestiya vysshikh uchebnykh zavedenii. Priborostroenie*, 2023, vol. 66, no. 5, pp. 399-408. DOI: 10.17586/0021-3454-2023-66-5-399-408

18. Balonin Yu.N., Vostrikov A.A., Sergeev M.B. *Informatsionno-upravlyayushchie sistemy*, 2012, no. 1 (56), pp. 92-93.

19. Tokarevskiy I.V., Sentsov A.A., Sergeev M.B. Features of Matrix Masking of Digital Radar Images, *2022 Wave Electronics and Its Application in Information and Telecommunication Systems (WECONF)*, 2022, pp. 488-491. DOI: 10.1109/WECONF55058.2022.9803393

20. Grigor'ev E.K., Sergeev A.M. *Trudy uchebnykh zavedenii svyazi*, 2023, vol. 9, no. 3, pp. 6-13. DOI: 10.31854/1813-324X-2023-9-3-6-13

21. Erosh I.L., Sergeev A.M., Filatov G.P. *Informatsionno-upravlyayushchie sistemy*, 2007, no. 5 (30), pp. 20-22.

22. Chernyshev S.A. *Razrabotka i issledovanie metoda matrichnogo maskirovaniya videoinformatsii v global'no raspredelennykh sistemakh* (Development and research of a method for matrix masking of video information in globally distributed systems), Ph. D. thesis, Saint-Petersburg, SUAI, 2017, 120 p.

23. *The Lenna Story*. URL: http://lenna.org/

24. *Aerial images (512x512)*. URL: https://universe.roboflow.com/alex-shamota-hsa0p/aerial-images-512-512-2

25. Balonin N.A., Balonin Yu.N., Vostrikov A.A., Sergeev M.B. *Vestnik komp'yuternykh i informatsionnykh tekhnologii*, 2014, no. 11 (125), pp. 51-56.

26. Balonin N.A., Sergeev M.B. *Informatsionno-upravlyayushchie sistemy*, 2023, no. 3 (124), pp. 2-14. DOI: 10.31799/1684-8853-2023-3-2-15

27. Balonin N.A., Sergeev M.B. *Informatsionno-upravlyayushchie sistemy*, 2022, no. 1 (116), pp. 2-7. DOI: 10.31799/1684-8853-2022-1-2-7

28. Balonin N.A., Sergeev M.B., Suzdal' V.S. *Trudy SPIIRAN*, 2017, no. 5 (54), pp. 224-243. DOI: 10.15622/sp.54.10

Статья поступила в редакцию 23.10.2023
Одобрена после рецензирования 28.10.2023
Принята к публикации 25.12.2023
The article was submitted on 23.10.2023; approved after reviewing on 28.10.2023; accepted for publication on 25.12.2023