УДК 004.932.2
DOI 10.17513/snt.40526

ПАРАМЕТРИЧЕСКИЙ МЕТОД СКРЕМБЛИРОВАНИЯ ИЗОБРАЖЕНИЙ НА ОСНОВЕ ПРЕОБРАЗОВАНИЯ АРНОЛЬДА

Земцов А.Н. ORCID ID 0000-0001-6430-3615,
Кузнецов М.А. ORCID ID 0000-0001-5044-1427,
Садек Сажжад, Пшеничный Д.С., Майданников К.А.

ФГБОУ ВО «Волгоградский государственный технический университет», Россия, Волгоград, e-mail: azemtsow@mail.ru

В работе рассматривается проблема защиты материалов фотовидеофиксации в интеллектуальных транспортных сетях, уязвимых к несанкционированному изменению и подделке. Несанкционированное изменение материалов может привести к серьезным последствиям, заключающимся в подрыве доверия к государственным службам, угрозе личной и общественной безопасности. Целью исследования является разработка параметрического метода скремблирования изображений на основе преобразования Арнольда, преодолевающего ограничения классического подхода и повышающего устойчивость систем к криптоанализу. Исследование проводилось в Волгоградском государственном техническом университете в 2024–2025 гг. с использованием математического моделирования преобразования Арнольда и его параметрической модификации. Показано, что введение дополнительных параметров существенно расширяет пространство ключей и устраняет предсказуемость преобразования, обеспечивая эффективное разрушение корреляционных связей между пикселями, что позволяет повысить устойчивость к современным видам атак, включая статистический анализ и атаки грубой силы. Предложенный метод сохраняет обратимость и низкую вычислительную сложность, что позволяет интегрировать его в многоуровневые системы защиты. Параметрическая модификация преобразования Арнольда повышает эффективность защиты графической информации в системах фотовидеофиксации и может быть использована совместно с другими криптографическими средствами для создания комплексных решений в интеллектуальных транспортных сетях.

Ключевые слова: преобразование Арнольда, скремблирование, интеллектуальные транспортные сети, видеонаблюдение, фотовидеофиксация, защита информации

PARAMETRIC IMAGE SCRAMBLING METHOD BASED ON THE ARNOLD TRANSFORM

Zemtsov A.N. ORCID ID 0000-0001-6430-3615,
Kuznetsov M.A. ORCID ID 0000-0001-5044-1427,
Sadek Sazhzhad, Pshenichnyy D.S., Maydannikov K.A.

Volgograd State Technical University, Russia, Volgograd, e-mail: azemtsow@mail.ru

This paper examines the problem of protecting photo and video recording materials in intelligent transport networks, which are vulnerable to unauthorized modification and forgery. Unauthorized modification of materials can have serious consequences, including undermining trust in government services and threatening personal and public safety. The aim of the study is to develop a parametric image scrambling method based on the Arnold transform that overcomes the limitations of the classical approach and increases the system's resistance to cryptanalysis. The study was conducted at Volgograd State Technical University in 2024–2025 using mathematical modeling of the Arnold transform and its parametric modification. It is shown that the introduction of additional parameters significantly expands the key space and eliminates the predictability of the transformation, ensuring effective destruction of correlations between pixels, thereby increasing resistance to modern attacks, including statistical analysis and brute-force attacks. The proposed method maintains reversibility and low computational complexity, allowing for its integration into multi-level security systems. A parametric modification of the Arnold transform increases the efficiency of protecting graphic information in photo and video recording systems and can be used in conjunction with other cryptographic tools to create comprehensive solutions in intelligent transport networks.

Keywords: Arnold transform, scrambling, VANET, video surveillance, photo and video recording, information security

Введение

В современном городе безопасность дорожного движения является одной из приоритетных задач, для обеспечения решения которой интеллектуальные транспортные сети играют ключевую роль [1]. Эти мобильные самоорганизующиеся сети позволяют транспортным средствам в режиме реального времени взаимодействовать друг с другом, а также с элементами дорожной инфраструктуры, что позволяет обеспечить раннее предупреждение аварий, оптимизацию транспортных потоков, повысить безопасность движения в целом [2].

Одним из важнейших компонентов системы управления городским движением являются аппаратно-программные средства фотовидеофиксации нарушений, которые не только контролируют дорожную ситуацию, но и служат источником юридически

значимых доказательств при проведении административного или уголовного расследования [3]. Однако фотоматериалы и видеозаписи остаются крайне уязвимыми, так как злоумышленники могут внести в изображение изменения – затереть номер, исказить временные метки или внедрить дополнительные кадры в результат видеофиксации. С другой стороны, передача материалов фотовидеофиксации нарушений посредством публичных каналов подвергает их риску перехвата и модификации [4].

Подделка материалов фотовидеофиксации нарушений ведет к серьезным последствиям: подрывается доверие граждан к государственным органам, снижается эффективность судебных разбирательств, что в конечном итоге отражается на общей дисциплине дорожного движения [5, 6]. Кроме того, несанкционированный доступ, а также проведение анализа видеопотока может помочь злоумышленнику в раскрытии маршрута, паттернов передвижения, личной информации, что создает риски для личной и общественной безопасности.

Для противодействия этим криминальным явлениям могут применяться криптографические методы, которые обеспечивают конфиденциальность, целостность и подлинность данных. Не только простые криптографические алгоритмы могут быть уязвимы к статистическому анализу зашифрованной информации, но и криптостойкие, такие как AES, могут оставлять определенные статистические следы, которые атакующий может использовать [7, 8]. Перспективным решением этой проблемы в условиях ограниченных ресурсов и необходимости работы в реальном времени является эффективное распределение ключей и использование быстрого потокового шифра, а также гибридных схем шифрования.

Гибридные криптосхемы, сочетающие симметричные и асимметричные алгоритмы, позволяют обеспечить баланс между скоростью обработки больших объемов видео и безопасностью при распределении ключей [2, 5, 9].

Другими важными компонентами, рекомендуемыми к реализации в модуле защиты транспортного средства, а также при доступе к хранилищу материалов фотовидеофиксации нарушений, представляются цифровые подписи, метки времени и хэширование, обеспечивающие аутентификацию и подтверждение целостности каждого видеокадра [10].

Кроме того, необходимо добиться компромисса между уровнем безопасности и производительностью комплексной системы фотовидеофиксации, которые генерируют значительные объемы данных, и их защита требует значительных вычислительных ресурсов. В связи с этим представляется целесообразным использование вычислительно простых криптоалгоритмов, оптимизированных для работы в условиях ограниченных ресурсов, а также методов селективного шифрования, которые защищают только наиболее важные компоненты материалов фотовидеофиксации нарушений (например, ключевые кадры или заголовки видеопотока, государственные регистрационные номера, лица участников и т.д.). Такой подход позволяет достичь необходимого уровня защиты при сохранении приемлемого времени отклика системы и минимальной задержки передачи, которые являются особенно значимыми [11] для обеспечения качества обслуживания пакетов в региональной ведомственной сети.

Таким образом, для обеспечения надежности, производительности и устойчивости хранилища материалов фотовидеофиксации нарушений к атакам криптографическая защита графической информации должна быть многоуровневой и сбалансированной, включающей симметричное и асимметричное шифрование, цифровые подписи, простые криптоалгоритмы и гибридные схемы [12].

Необходимо отметить, что для устройств с ограниченными ресурсами, к которым относятся транспортные средства, подходят простые потоковые криптоалгоритмы для передачи видеотрафика [13]. Устройства интернета вещей (IoT) также ограничены в ресурсах, таких как вычислительная мощность, оперативная память, заряд батареи. Как следствие, при организации сетевого взаимодействия устройств интернета вещей актуальность разработки простых потоковых криптоалгоритмов стоит особенно остро [14–16]. Алгоритмы, оптимизированные для видеопотоков интеллектуальных транспортных сетей и устройств интернета вещей, включают методы генерации ключей через генетические алгоритмы [17] и схема защиты контента с использованием селективного шифрования, обеспечивающие защищенное кодирование без полного дешифрования [18]. В предложенной схеме ключ дешифрования не требуется предоставлять на промежуточных устройствах и в облачном центре обработки данных.

Цель исследования – разработка параметрического метода скремблирования изображений на основе преобразования Арнольда, преодолевающего ограничения классического подхода и повышающего устойчивость систем к криптоанализу.

Материалы и методы исследования

Исследование выполнено на кафедре ЭВМ и систем в Волгоградском государственном техническом университете в 2024–2025 гг. Объектом исследования являлись цифровые изображения, полученные системами фотовидеофиксации нарушений дорожного движения. Методологической основой послужило математическое моделирование преобразования Арнольда и его параметрической модификации. В программной реализации применялись методы линейного отображения дискретных множеств. Для оценки результатов был проведен статистический анализ корреляционных связей между пикселями изображений. Эффективность предложенного метода оценивалась с помощью анализа метрик декорелирующего воздействия преобразования на исходные цифровые изображения.

Результаты исследования и их обсуждение

В 1960-е гг. выдающийся советский математик Владимир Игоревич Арнольд, предложил двумерное отображение с фазовым пространством в виде тора, проиллюстрировав его на примере изображения головы кошки. Двумерное отображение Арнольда представляет собой классическое линейное отображение точек двумерной решетки, определенной на дискретном множестве, и получило популярность для скремблирования [19, 20]. Необходимо отметить, что отображение Арнольда также применяется в качестве одного из этапов в стеганографических алгоритмах для защиты графической информации [21–23].

Каждый элемент множества описывается координатами (x,y), где N – размерность множества и $x, y \in \{0,1,2, ..., N-1\}$.

Отображение Арнольда может быть записано в виде

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N)$$

или в развернутом виде

$$x' = (x + y)\, mod\ N,$$

$$y' = (x + 2y)\, mod\ N.$$

Здесь (x', y') – координаты пикселя после итерации линейного отображения. Отображение является обратимым, так как

$$det \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} = 1 \cdot 2 - 1 \cdot 1 = 1.$$

Результат вычисления преобразования Арнольда показан на рис. 1.

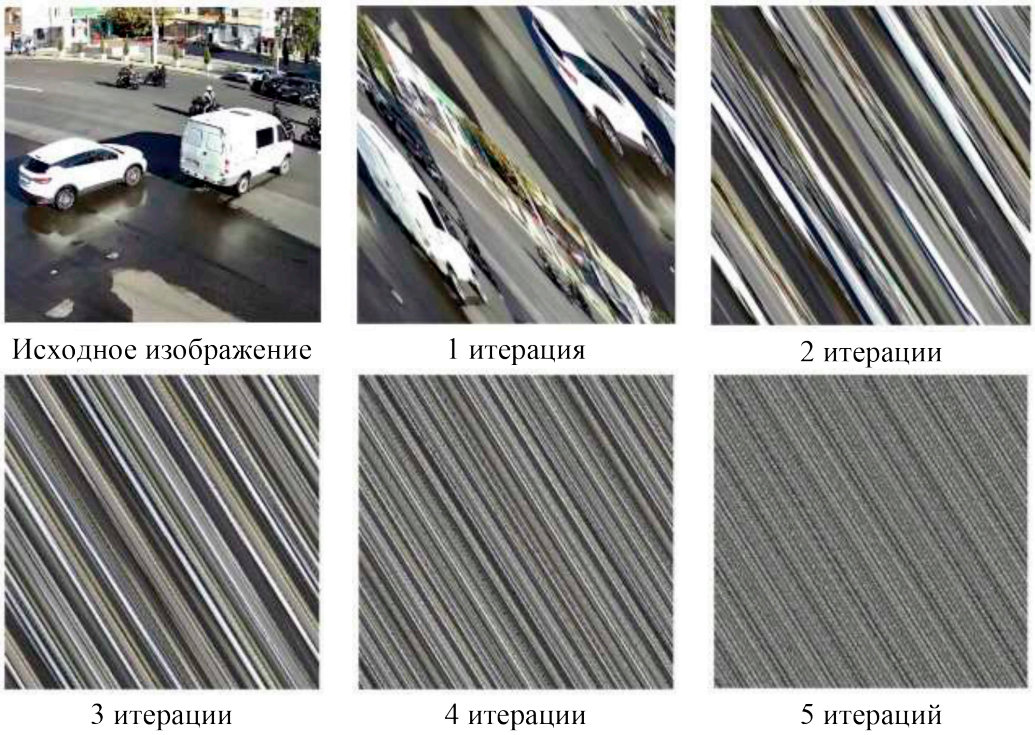

Рис. 1. Результат вычисления преобразования Арнольда
Источник: составлено авторами по результатам данного исследования

Преобразование Арнольда эффективно разрушает пространственные зависимости, но обладает рядом ограничений. В силу фиксированности матрицы отображение имеет предсказуемую структуру и фиксированный период. Если известны габариты изображения, злоумышленник может перебором итераций восстановить исходное изображение. Кроме того, пространство ключей у классического варианта преобразования Арнольда ограничено только числом итераций, что делает его потенциально уязвимым для атак грубой силы.

Для преодоления указанных ограничений предлагается обобщенная форма параметризованного преобразования Арнольда с дополнительными параметрами ϑ_1 и ϑ_2. В этом случае отображение Арнольда будет описываться как

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & \vartheta_1 \\ \vartheta_2 & \vartheta_1\vartheta_2 + 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (mod\ N)$$

или (в развернутом виде) как

$$x' = (x + \vartheta_1 y)\, mod\ N,$$

$$y' = (\vartheta_2 x + (\vartheta_1\vartheta_2 + 1)\, y)\, mod\ N.$$

Здесь $\vartheta_1, \vartheta_2 \in \{1, 2, ..., N-1\}$ – оказывающие значительное влияние на динамику и периодичность преобразования параметры, которые могут выступать частью секретного ключа. Обратимость обобщенного преобразования также сохраняется при условии, что определитель матрицы преобразования равен 1:

$$det \begin{pmatrix} 1 & \vartheta_1 \\ \vartheta_2 & \vartheta_1\vartheta_2 + 1 \end{pmatrix} = 1 \cdot (\vartheta_1\vartheta_2 + 1) - \vartheta_1\vartheta_2 = 1.$$

С целью анализа эффективности предлагаемой методики защиты графической информации проводится исследование влияния параметров преобразования Арнольда на оказываемое декоррелирующее воздействие на исходное изображение. При вычислении преобразования Арнольда осуществляется сравнение результирующего изображения с исходным с целью расчета меры вносимых искажений.

Для вычисления статистически значимой связи между соседними пикселями в полученных после вычисления преобразования Арнольда воспользуемся выборочным коэффициентом корреляции Пирсона для n-выборки $\{(x_1, y_1), ..., (x_n, y_n)\}$:

$$r = \frac{n\sum x_i y_i - \sum x_i \sum y_i}{\sqrt{n\sum x_i^2 - \left(\sum x_i\right)^2}\sqrt{n\sum y_i^2 - \left(\sum y_i\right)^2}}.$$

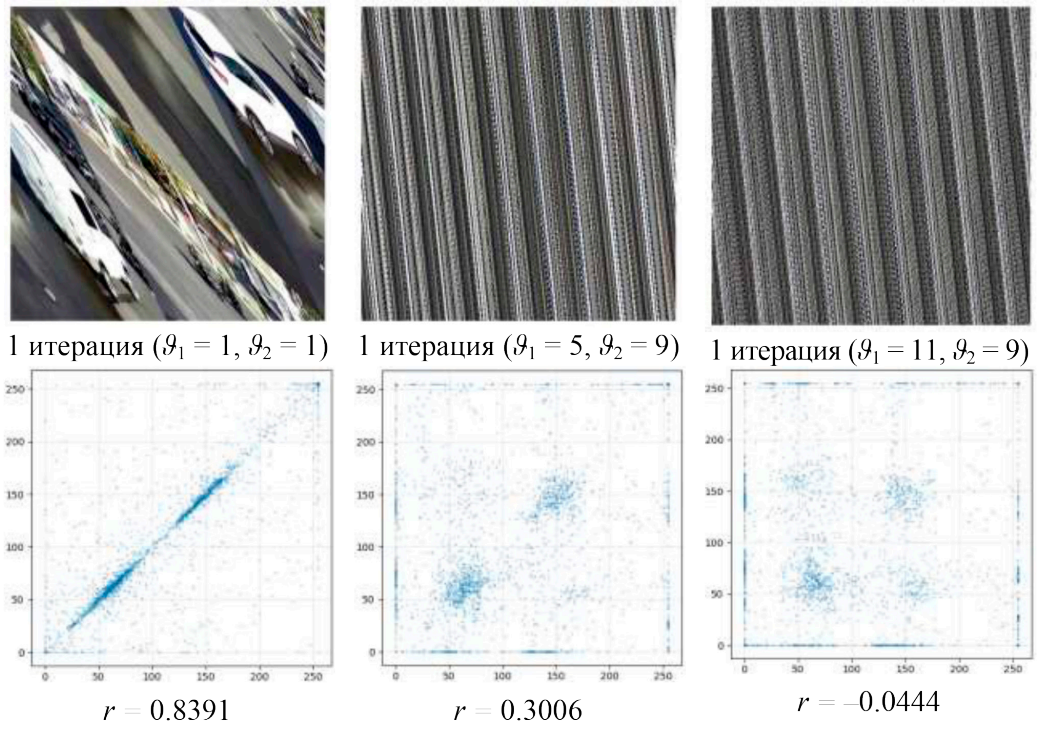

Рис. 2. Корреляция пикселей для различных преобразований
Источник: составлено авторами по результатам данного исследования

Примеры результатов вычисления 1 итерации параметрического преобразования Арнольда с различными ϑ_1 и ϑ_2, а также корреляции между соседними пикселями показаны на рис. 2.

Как видно из рисунка, в результате вычисления 1 итерации оригинального преобразования Арнольда с $\vartheta_1 = 1$ и $\vartheta_2 = 1$ статистически значимая связь между пикселями сохраняется, выборочный коэффициент корреляции Пирсона $r = 0.8391$. Помимо значения метрики зависимость между соседними пикселями также хорошо видна на рисунке. Для других пар параметров (5,9) и (11,9) видно, что связь между пикселями нарушается, и преобразование оказывает значительное декоррелирующее воздействие на исходное изображение, что подтверждается и значениями коэффициента корреляции: $r = 0.3006$ и $r = –0.0444$ соответственно.

Таким образом введение параметров ϑ_1 и ϑ_2 значительно расширяет функциональные возможности преобразования Арнольда и устраняет многие его ограничения. Одним из основных преимуществ является существенное увеличение пространства ключей. В классическом преобразовании Арнольда ключевой параметр фактически один – число итераций. В параметрическом варианте преобразования добавляются параметры, принимающие множество значений. Наблюдается экспоненциальный рост пространства ключей, что делает атаку полного перебора параметров чрезвычайно затруднительной.

Благодаря введению параметров ϑ_1 и ϑ_2 нарушается предсказуемость структуры преобразования и усложняется анализ периодичности. Даже если атакующий знает число итераций, без сведений о значениях параметров ϑ_1 и ϑ_2 восстановление исходного изображения становится чрезвычайно затруднительным.

Параметры преобразования влияют на характер перестановки пикселей, что позволяет адаптировать предложенное преобразование под конкретные требования к скорости, типу скремблирования и устойчивости к статистическому анализу.

В классическом преобразовании период зависит только от размера изображения и может быть заранее вычислен. В предложенном подходе период является функцией не только N, но и параметров ϑ_1 и ϑ_2, что делает его сложно предсказуемым.

Таким образом, предложенное преобразование сохраняет все свойства преобразования Арнольда: остается обратимым, не изменяет значения яркости пикселей и имеет эквивалентную вычислительную сложность.

Заключение

В настоящей работе было проведено исследование, посвященное анализу актуальной проблемы защиты графической информации в интеллектуальных транспортных системах с фотовидеофиксацией нарушений дорожного движения. Учитывая ключевую роль таких данных в обеспечении правопорядка и общественной безопасности, их защита от несанкционированного доступа и подделки является стратегически важной задачей. Показано, что применение традиционных криптографических алгоритмов, несмотря на их высокую криптостойкость и устойчивость к статистическому анализу, сопряжено с существенными ограничениями при использовании в сетях с быстро изменяющейся топологией и в условиях реального времени. Высокая вычислительная сложность делает их малопригодными для внедрения в конечные устройства с ограниченными ресурсами, к которым относятся транспортные средства и элементы дорожной инфраструктуры.

В ходе исследования показано, что преобразование Арнольда может служить эффективным инструментом для скремблирования изображений, но классический вариант преобразования обладает рядом недостатков, позволяющих злоумышленнику восстановить исходное изображение путем перебора итераций. Для преодоления ограничений предложена параметрическая модификация классического преобразования, существенно затрудняющая проведение криптоанализа. Полученные результаты показали, что пространственная корреляция между пикселями статистически незначительна, что подтверждает высокую эффективность декоррелирующего воздействия предлагаемого преобразования.

Список литературы

1. Галенко Л.А., Николаева Р.В. Интеллектуальные транспортные системы – решение транспортных проблем // Техника и технология транспорта. 2017. № 3 (4). С. 12. URL: http://transport-kgasu.ru/files/N4-12ITS317.pdf (дата обращения: 02.08.2025). EDN: ZIDZOT.

2. Gopalakrishnan M., Elangovan U. Secure Data Transmission in VANETs Using Efficient Key-Management Techniques // Intelligent Communication Technologies and Virtual Mobile Networks (ICICV 2019). Cham: Springer. 2019. P. 494–503. DOI: 10.1007/978-3-030-28364-3_50.

3. Майоров В.И., Дымберов А.Д., Молчанов П.В. Правовые проблемы применения специальных технических средств автоматической фотовидеофиксации нарушений правил дорожного движения // Юридическая наука и правоохранительная практика. 2016. № 3 (37). С. 69–77. URL: http://naukatipk.ru/images/2016/3/mayorov_dymberov_molchanov.pdf (дата обращения: 02.08.2025). EDN: XBIBSX.

4. Земцов А.Н., Садек С. Защита графической информации в системе управления городским движением от неправомерного использования // Инженерный вестник Дона. 2023. № 12 (108). С. 207–216. URL: http://www.ivdon.ru/ru/maga-

zine/archive/n12y2023/8887 (дата обращения: 02.08.2025). EDN: OFZAOA.

5. Meddeb N., Meddeb M.A., Ben Ayed M.A. Secure and Efficient Video Transmission in VANET // International Journal of Communication Networks and Information Security. 2021. Vol. 13 (1). DOI: 10.17762/ijcnis.v13i1.4888.

6. Rahim A., Khan Z.S., Muhaya F.T.B., Sher M., Kim T.H. Sensor-Based Framework for Secure Multimedia Communication in VANET // Sensors. 2010. Vol. 10 (11). P. 10146–10166. DOI: 10.3390/s101110146.

7. Alghamdi Y., Munir A. Image Encryption Algorithms: A Survey of Design and Evaluation Metrics // Journal of Cybersecurity and Privacy. 2024. Vol. 4 (1). P. 126–152. DOI: 10.3390/jcp4010007.

8. Hosny K.M., Zaki M.A., Lashin N.A., Fouda M.M., Hamza H.M. Multimedia Security Using Encryption: A Survey // IEEE Access. 11. P. 63027–63056. DOI: 10.1109/ACCESS.2023.3287858.

9. Xu S., Chen X., He Y., Cao Y., Gao S. VMT: Lightweight blockchain-based secure video transmission in VANET // Advances in Information and Communication. Cham: Springer. 2022. P. 244–257. DOI: 10.1007/978-3-031-19208-1_21.

10. Alaya B., Sellami L. Multilayer Video Encoding for QoS Managing of Video Streaming in VANET Environment // ACM Transactions on Multimedia Computing, Communications, and Applications. 2022. Vol. 18 (3). P. 1–19. DOI: 10.1145/3491433.

11. Антоненко А.С. Оценка параметров QoS для бесперебойной работы IPTV // T-Comm: Телекоммуникации и транспорт. 2020. № 14 (10). С. 33–38. DOI: 10.36724/2072-8735-2020-14-10-33-38.

12. Okpok M., Kihei B. Challenges and Opportunities for Multimedia Transmission in Vehicular Ad Hoc Networks: A Comprehensive Review // Electronics. 2023. Vol. 12 (20). P. 4310. DOI: 10.3390/electronics12204310.

13. Shifa A., Asghar M.N., Batool N., Fleury M. Efficient Lightweight Encryption Algorithm for Smart Video Applications // 2018 International Conference on Frontiers of Information Technology (FIT). 2019. DOI: 10.1109/FIT.2018.00032.

14. Nayak M.K., Dash D.K., Swain P.K., Sahu A. Video Encryption Using Optimization Lightweight Algorithm for Secure Internet of Things // ICDAI 2023. 2023. P. 331–341. DOI: 10.1007/978-981-99-3878-0_28.

15. Chun M., Weber S., Tewari H. A Lightweight Encryption Scheme for IoT Devices in the Fog // Proceedings of the Future Technologies Conference (FTC) 2022. 2023. P. 147–161. DOI: 10.1007/978-3-031-18458-1_11.

16. Naz I., Illahi R., Shahzadi N., Ahmad H.G.U. Lightweight Encryption Model for IoT Security and Privacy Protection // Advances. 2024. Vol. 5 (3). P. 84–92. DOI: 10.11648/j.advances.20240503.13.

17. Shah R.A., Asghar M.N., Abdullah S., Fleury M., Gohar N. Effectiveness of Crypto-Transcoding for H.264/AVC and HEVC Video Bit-streams // Multimedia Tools and Applications. 2019. Vol. 15. P. 21455–21484. DOI: 10.1007/s11042-019-7451-5.

18. Khan M., Dagenborg H., Johansen D. Performance Evaluation of Lightweight Stream Ciphers for Real-Time Video Feed Encryption on ARM Processor // Future Internet. 2024. Vol. 16 (8). P. 261. DOI: 10.3390/fi16080261.

19. Бахрушина Г.И., Пархоменко И.С. Скремблирование изображения с помощью преобразования Арнольда и преобразования Фибоначчи // Ученые заметки ТОГУ. 2019. № 10 (4). С. 124–131.; URL: https://togudv.ru/ejournal/pub/articles/2566/ (дата обращения: 02.08.2025). EDN: ZCPAGA.

20. Земцов А.Н., Цыбанов В.Ю. Скремблирование цифровых изображений // Инженерный вестник Дона. 2020. № 6 (66). URL: http://ivdon.ru/ru/magazine/archive/N6y2020/6503 (дата обращения: 02.10.2025). EDN: NXFFOI.

21. Земцов А.Н. Методы цифровой стеганографии для защиты авторских прав: монография. Saarbrucken: LAP Lambert. 2012. 148 с. EDN: JXFEXL. ISBN 9783659105630.

22. Soualmi A. A New Blind Medical Image Watermarking Based on Weber Descriptors and Arnold Chaotic Map // Arabian Journal for Science and Engineering. 2018. Vol. 43 (12). P. 7893–7905. DOI: 10.1007/s13369-018-3246-7.

23. Sehra K., Raut S., Mishra A. Robust and Secure Digital Image Watermarking Technique Using Arnold Transform and Memristive Chaotic Oscillators // IEEE Access. 2021. Vol. 9. P. 72465–72483. DOI: 10.1109/access.2021.3079319.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.