ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ

ҚАЙЫРЫМДЫЛЫҚ ҚОРЫ HALYK CHARITY FOUNDATION

«ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ» РҚБ
«ХАЛЫҚ» ЖҚ

ХАБАРЛАРЫ

ИЗВЕСТИЯ

РОО «НАЦИОНАЛЬНОЙ
АКАДЕМИИ НАУК РЕСПУБЛИКИ
КАЗАХСТАН»
ЧФ «Халық»

NEWS

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
«Halyk» Private Foundation

SERIES
PHYSICS AND INFORMATION TECHNOLOGY

1 (349)

JANUARY – MARCH 2024

PUBLISHED SINCE JANUARY 1963
PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

ЧФ «ХАЛЫҚ»

В 2016 году для развития и улучшения качества жизни казахстанцев был создан частный Благотворительный фонд «Халык». За годы своей деятельности на реализацию благотворительных проектов в областях образования и науки, социальной защиты, культуры, здравоохранения и спорта, Фонд выделил более 45 миллиардов тенге.

Особое внимание Благотворительный фонд «Халык» уделяет образовательным программам, считая это направление одним из ключевых в своей деятельности. Оказывая поддержку отечественному образованию, Фонд вносит свой посильный вклад в развитие качественного образования в Казахстане. Тем самым способствуя росту числа людей, способных менять жизнь в стране к лучшему – профессионалов в различных сферах, потенциальных лидеров и «великих умов». Одной из значимых инициатив фонда «Халык» в образовательной сфере стал проект Ozgeris powered by Halyk Fund – первый в стране бизнес-инкубатор для учащихся 9-11 классов, который помогает развивать необходимые в современном мире предпринимательские навыки. Так, на содействие малому бизнесу школьников было выделено более 200 грантов. Для поддержки талантливых и мотивированных детей Фонд неоднократно выделял гранты на обучение в Международной школе «Мирас» и в Astana IT University, а также помог казахстанским школьникам принять участие в престижном конкурсе «USTEM Robotics» в США. Авторские работы в рамках проекта «Тәлімгер», которому Фонд оказал поддержку, легли в основу учебной программы, учебников и учебно-методических книг по предмету «Основы предпринимательства и бизнеса», преподаваемого в 10-11 классах казахстанских школ и колледжей.

Помимо помощи школьникам, учащимся колледжей и студентам Фонд считает важным внести свой вклад в повышение квалификации педагогов, совершенствование их знаний и навыков, поскольку именно они являются проводниками знаний будущих поколений казахстанцев. При поддержке Фонда «Халык» в южной столице был организован ежегодный городской конкурс педагогов «Almaty Digital Ustaz.

Важной инициативой стал реализуемый проект по обучению основам финансовой грамотности преподавателей из восьми областей Казахстана, что должно оказать существенное влияние на воспитание финансовой грамотности и предпринимательского мышления у нового поколения граждан страны.

Необходимую помощь Фонд «Халык» оказывает и тем, кто особенно остро в ней нуждается. В рамках социальной защиты населения активно проводится работа по поддержке детей, оставшихся без родителей, детей и взрослых из социально уязвимых слоев населения, людей с ограниченными возможностями, а также обеспечению нуждающихся социальным жильем, строительству социально важных объектов, таких как детские сады, детские площадки и физкультурно-оздоровительные комплексы.

В копилку добрых дел Фонда «Халык» можно добавить оказание помощи детскому спорту, куда относится поддержка в развитии детского футбола и карате в нашей стране. Жизненно важную помощь Благотворительный фонд «Халык» оказал нашим соотечественникам во время недавней пандемии COVID-19. Тогда, в разгар тяжелой борьбы с коронавирусной инфекцией Фонд выделил свыше 11 миллиардов тенге на приобретение необходимого медицинского оборудования и дорогостоящих медицинских препаратов, автомобилей скорой медицинской помощи и средств защиты, адресную материальную помощь социально уязвимым слоям населения и денежные выплаты медицинским работникам.

В 2023 году наряду с другими проектами, нацеленными на повышение благосостояния казахстанских граждан Фонд решил уделить особое внимание науке, поскольку она является частью общественной культуры, а уровень ее развития определяет уровень развития государства.

Поддержка Фондом выпуска журналов Национальной Академии наук Республики Казахстан, которые входят в международные фонды Scopus и Wos и в которых публикуются статьи отечественных ученых, докторантов и магистрантов, а также научных сотрудников высших учебных заведений и научно-исследовательских институтов нашей страны является не менее значимым вкладом Фонда в развитие казахстанского общества.

С уважением,
Благотворительный Фонд «Халык»!

«ҚР ҰҒА Хабарлары. Физика және информатика сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика және ақпараттық коммуникациялық технологиялар сериясы.*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

«Известия НАН РК. Серия физика и информатики».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика и информационные коммуникационные технологии.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

News of the National Academy of Sciences of the Republic of Kazakhstan.
Series of physics and informatics.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)
Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *series physics and information technology.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

NEWS OF THE NATIONAL ACADEMY OF SCIENCESOF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 1. Namber 349 (2024). 75–98
https://doi.org/10.32014/2024.2518-1726.243

МРНТИ 81.96.00

© D.Gabdullaev*, I. Zhanseri, A. Aidarbekova, Sh. Mussiraliyeva, 2024
Al-Farabi Kazakh National University, specialty «Information Security Systems», Kazakhstan, Almaty.
E-mail: *zhaqashbaeva@gmail.com*

IMAGE STEGO ANALYSIS BASED ON DEEP LEARNING METHODS

Gabdullaev Dauren — Ph.D. doctoral student of the Department of Information Systems, Al-Farabi Kazakh National University, 050040, Almaty, Al-Farabi Avenue, 71
E-mail: *kazdau@gmail.com; https://orcid.org/0000-0002-2722-0623;*
Zhanseri Ikram — Ph.D. doctoral student of the Department of Information Systems, Al-Farabi Kazakh National University, 050040, Almaty, Al-Farabi Avenue, 71
E-mail: *zhanserikz@gmail.com; https://orcid.org/0009-0001-8059-6590;*
Aidarbekova Aygerim — Ph.D. doctoral student of the Department of Information Systems, Al-Farabi Kazakh National University, 050040, Almaty, Al-Farabi Avenue, 71
E-mail: *zhaqashbaeva@gmail.com*; *https://orcid.org/0009-0004-4745-9879;*
Mussiraliyeva Shynar — Candidate of Physical and Mathematical Sciences, Head of the Department Information Systems of Al-Farabi Kazakh National University, 050040, Almaty, 71 Al-Farabi Avenue
E-mail: *mussiraliyevash@gmail.com*; *http://orcid.org/0000-0001-5794-3649.*

Abstract. Steganography is a complex method of covert transmission of information that involves embedding data or messages in various media formats, including images, audio files and text documents. The main goal of this method is to mask the presence of transmitted data so that its presence remains invisible to an uninformed observer. In contrast to cryptography, which focuses on encrypting information to protect its content, steganography aims to hide the fact that the message itself is being transmitted, thereby providing an additional level of privacy. The use of deep learning methods in the field of detection of steganographic interventions opens up new prospects in the field of information security. Deep learning, due to its ability to analyze and interpret complex and multidimensional data, appears to be an extremely promising tool for identifying hidden messages, even if they are implemented using high-level steganographic techniques. This research involves using deep learning to analyze and detect steganographically modified images. The purpose of the study is not simply to identify the presence of steganographic elements, but also to comprehensively evaluate the effectiveness of various deep learning models in the context of the task. The results of the study are expected to provide significant contributions to the development of steganography

detection methods and improve the overall effectiveness of existing information security systems.

Keywords: steganography, deep learning, steganalysis, information security, LSB

© Д.Г. Габдуллаев*, И. Жансері, А.Б. Айдарбекова, Ш.Ж. Мусиралиева, 2024
Әл-Фараби атындағы Қазақ ұлттық университеті, Қазақстан, Алматы.
E-mail: *zhaqashbaeva@gmail.com*

ТЕРЕҢ ОҚЫТУ ӘДІСТЕРІНІҢ НЕГІЗІНДЕ СУРЕТТЕРГЕ СТЕГОТАЛДАУ ЖАСАУ

Габдуллаев Даурен — Әл-Фараби атындағы Қазақ ұлттық университеті «Ақпараттық жүйелер» кафедрасының Ph.D. докторанты, 050040, Алматы, Әл-Фараби даңғылы, 71
E-mail: *kazdau@gmail.com; https://orcid.org/0000-0002-2722-0623;*
Жансері Икрам — Әл-Фараби атындағы Қазақ ұлттық университеті «Ақпараттық жүйелер» кафедрасының Ph.D. докторанты, 050040, Алматы, Әл-Фараби даңғылы, 71
E-mail: *zhanserikz@gmail.com; https://orcid.org/0009-0001-8059-6590;*
Айдарбекова Айгерим — Әл-Фараби атындағы Қазақ ұлттық университеті «Ақпараттық жүйелер» кафедрасының Ph.D. докторанты, 050040, Алматы, Әл-Фараби даңғылы, 71
E-mail: *zhaqashbaeva@gmail.com*; *https://orcid.org/0009-0004-4745-9879;*
Мусиралиева Шынар — физика-математика ғылымдарының кандидаты, «Ақпараттық жүйелер» кафедрасының меңгерушісі, Әл-Фараби атындағы Қазақ ұлттық университеті, 050040, Алматы, Әл-Фараби даңғылы, 71
E-mail: *mussiraliyevash@gmail.com*; *http://orcid.org/0000-0001-5794-3649.*

Аннотация. Стеганография – ақпаратты жасырын берудің күрделі әдісі, ол деректерді немесе хабарламаларды әртүрлі медиапішімдерге, соның ішінде суреттерді, аудиофайлдарды және мәтіндік құжаттарды енгізуді қамтиды. Бұл әдістің негізгі мақсаты хабарсыз бақылаушыға көрінбейтін етіп жіберілетін деректердің болуын бүркемелеу болып табылады. Мазмұнын қорғау үшін ақпаратты шифрлауға бағытталған криптографиядан айырмашылығы, стеганография хабарламаның өзі жіберіліп жатқанын жасыруды мақсат етеді, осылайша құпиялылықтың қосымша деңгейін қамтамасыз етеді. Стеганографиялық араласуларды анықтау саласында терең оқыту әдістерін қолдану ақпараттық қауіпсіздік саласында жаңа перспективалар ашады. Күрделі және көпөлшемді деректерді талдау және интерпретациялау қабілетіне байланысты терең оқыту, тіпті жоғары деңгейлі стеганографиялық әдістерді қолдану арқылы жүзеге асырылса да, жасырын хабарламаларды анықтаудың өте перспективалы құралы болып көрінеді. Бұл зерттеу стеганографиялық түрлендірілген кескіндерді талдау және анықтау үшін терең оқытуды пайдалануды қамтиды. Зерттеудің мақсаты стеганографиялық элементтердің бар-жоғын анықтау ғана емес, сонымен қатар осы тапсырма контекстінде терең оқытудың әртүрлі үлгілерінің тиімділігін жан-жақты бағалау болып

табылады. Зерттеу нәтижелері стеганографияны анықтау әдістерін дамытуға елеулі үлес қосады және қолданыстағы ақпараттық қауіпсіздік жүйелерінің жалпы тиімділігін арттырады деп күтілуде.

Түйін сөздер: стеганография, терең оқыту, стегоанализ, ақпараттық қауіпсіздік, LSB

© Д.Г. Габдуллаев*, И. Жансери, А.Б. Айдарбекова, Ш.Ж. Мусиралиева, 2024
Казахский национальный университет имени аль-Фараби,
Алматы, Казахстан.
E-mail: *zhaqashbaeva@gmail.com*

СТЕГОАНАЛИЗ ИЗОБРАЖЕНИЙ НА ОСНОВЕ МЕТОДОВ ГЛУБОКОГО ОБУЧЕНИЯ

Габдуллаев Даурен — PhD докторант кафедры «Информационные системы» Казахского национального университета имени Аль-Фараби, 050040, Алматы, проспект Аль-Фараби, 71, Алматы, Казахстан
E-mail: *kazdau@gmail.com; https://orcid.org/0000-0002-2722-0623;*
Жансери Икрам — PhD докторант кафедры «Информационные системы» Казахского национального университета имени Аль-Фараби, 050040, Алматы, проспект Аль-Фараби, 71, Алматы, Казахстан
E-mail: *zhanserikz@gmail.com; https://orcid.org/0009-0001-8059-6590;*
Айдарбекова Айгерим — PhD докторант кафедры «Информационные системы» Казахского национального университета имени Аль-Фараби, 050040, Алматы, проспект Аль-Фараби, 71, Алматы, Казахстан
E-mail: *zhaqashbaeva@gmail.com*; *https://orcid.org/0009-0004-4745-9879;*
Мусиралиева Шынар — кандидат физико-математических наук, заведующая кафедрой «Информационные системы» Казахского национального университета им. Аль-Фараби, 050040, Алматы, проспект Аль-Фараби, 71, Алматы, Казахстан
E-mail: *mussiraliyevash@gmail.com*; *http://orcid.org/0000-0001-5794-3649.*

Аннотация. Стеганография представляет собой сложный метод скрытой передачи информации, заключающийся во внедрении данных или сообщений в различные медиаформаты, включая изображения, аудиофайлы и текстовые документы. Основная цель данного метода – маскировка наличия передаваемых данных таким образом, чтобы их присутствие оставалось незаметным для неосведомленного наблюдателя. В контрасте с криптографией, которая акцентируется на шифровании информации для защиты её содержания, стеганография направлена на скрытие факта передачи самого сообщения, тем самым обеспечивая дополнительный уровень конфиденциальности. Применение методов глубокого обучения в области обнаружения стеганографических вмешательств открывает новые перспективы в сфере информационной безопасности. Глубокое обучение, благодаря своей способности анализировать и интерпретировать сложные и многомерные данные, представляется исключительно перспективным

инструментом для идентификации скрытых сообщений, даже если они внедрены с применением высокоуровневых стеганографических методик. В рамках данного исследования предполагается использование глубокого обучения для анализа и обнаружения стеганографически модифицированных изображений. Цель исследования – не просто выявление наличия стеганографических элементов, но и всесторонняя оценка эффективности различных моделей глубокого обучения в контексте задачи. Ожидается, что результаты исследования внесут значимый вклад в развитие методов обнаружения стеганографии и повысят общую эффективность существующих систем информационной безопасности.

Ключевые слова: стеганография, глубокое обучение, стегоанализ, информационная безопасность, LSB

Введение

С быстрым развитием мультимедийных информационных технологий, таких как изображения, аудио и видео, технология стеганографии и способы её применения также сделали большой прогресс в последние десятилетия. Среди них, стеганография JPEG с адаптацией к контенту (изображение), которая скрывает секретные сообщения в квантованных коэффициентах DCT (Дискретное Косинусное Преобразование), в настоящее время является самой популярной и практичной, так как изображения в формате 'jpg' наиболее часто используются в нашей жизни. Алгоритмы стеганографии, использующие DCT и другие методы для встраивания информации, стали основой современной стеганографии. Среди них особо выделяются S-UNIWARD, J-UNIWARD, UERD и J-MIPOD, каждый из которых применяет уникальные стратегии для минимизации возможности обнаружения внедренной информации. J-UNIWARD, основан на использовании DCT для минимизации визуальных искажений, происходящих в процессе встраивания. Данный метод обеспечивает встраивание, изменяя DCT коэффициенты в соответствии с функцией стоимости. UERD, представляет собой еще одну инновационную методику, в которой применяется адаптивный механизм управления ошибками для оптимизации процесса встраивания. Данный метод призван минимизировать аномалии, которые могут возникнуть в статистике изображений, и тем самым затрудняет обнаружение стеганографии с использованием статистического анализа. С другой стороны, J-MIPOD, использует другой подход, акцентируя внимание на статистической неравномерности. Данный алгоритм стеганографии стремится минимизировать общее количество изменений пикселей, создавая изменения, которые наиболее естественно соответствуют статистическим характеристикам оригинального изображения. Используя данный метод, изображения сохраняют свои естественные свойства, делая внедренную информацию менее обнаружимой для стеганоаналитических методов. Более того, нужно отметить, что вышеперечисленные алгоритмы стеганографии были разработаны для обеспечения оптимального баланса

между невидимостью встраивания и емкостью, т. е. количеством информации, которое можно встроить без обнаружения.

Датасеты по стеганографии

Эффективность стратегий тренировки моделей в значительной степени зависит от качества и объема используемых для обучения датасетов. За последние несколько лет было создано немало важных датасетов, такие как ALASKA, BOSS, RAISE, Dresden, StegoAppDB и IStego100k, которые играют критически важную роль, предоставляя необходимые данные для обучения и верификации стеганоаналитических методов. IStego100k (Yang и др., 2019) включает в себя 208,104 картинок, где размер каждого изображения 1024x1024 пикселей. В этом датасете исследователи разделили датасет на 200000 тренировочных и 8104 тестовых данных. На картинки применяли популярные алгоритмы стеганографии как J-uniward и Uerd. BOSS (BreakOurSteganographySystem), является одним из самых известных датасетов в этой области. Он содержит около 10 000 изображений в оттенках серого, созданных с использованием различных цифровых камер. Датасет разработан для проведения соревнований по стеганографии и стеганоанализу, предоставляя исследователям обширную коллекцию изображений для разработки и тестирования новых методик обнаружения. ALASKA (A Le arnedSteganalysisAssessmentKernelforAachen) включает в себя подборку изображений, специально собранных для соревнований по стегоанализу. Его разработка была направлена на создание стандартизированного бенчмарка для оценки прогресса в области стегоанализа (Cancelli и др., 2020). Последний, но немаловажный датасет StegoAppDB, коллекция приложений и их стеганографических компонентов. Данный датасет уникален тем, что он сфокусирован на мобильных приложениях и предоставляет данные, необходимые для исследования методов маскировки и обнаружения в мобильных коммуникациях.

Методы обнаружения стеганографии можно разделить на две части: классические и современные.

Современные методы стегоанализа

Несмотря на успехи, классические методы обнаружения стеганографии столкнулись с проблемами при генерализации к более сложным методам стеганографии и высокой степени сжатия данных, что потребовало разработки новых, более эффективных подходов, основанных на нейронных сетях и глубоком обучении.

Современные методы в основном включают в себя глубокое обучение. Первые шаги в использовании нейронных сетей в стегоанализе было предложено (Qian и др., 2015). Метрики предложенной модели высчитывались на трех современных стеганографических алгоритмах, работающих в пространственной области: HUGO, WOW и S-UNIWARD. По сравнению с пространственной моделью SRM (SpatialRichModel), их модель достигает сопоставимой производительности на базе данных BOSS. Далее в (Xu и др.,

2017) проведено эмпирическое исследование, направленное на применение сверточных нейронных сетей (CNN) для обнаружения метода стеганографии J-UNIWARD в изображениях формата JPEG. Автор составил 20-слойную сеть подстроив под задачу стеганографии и превзошел более сложные нейронки. В статье (Xu и др., 2016) авторы используют абсолютные значения элементов в признаковых картах, сгенерированных первым сверточным слоем, чтобы облегчить и улучшить статистическое моделирование в последующих слоях. Для того, чтобы модель не переобучалась они ограничивают диапазон значений данных с насыщенными областями гиперболического тангенса (TanH) на ранних этапах сети и уменьшают количество фичмоделя с помощью сверток 1x1 на более глубоких уровнях (Xu и др., 2016). В статье (Ruiz и др., 2020) авторы рассматривают последние результаты, полученные сообществом, работающим в области искусственного интеллекта, и связанные с поведением нейронных сетей глубокого обучения при увеличении размера модели или размера базы данных. Затем предлагается экспериментальная настройка с целью оценить поведение средней сверточной нейронной сети (LC-Net) стегоанализатора при масштабировании размера базы данных. По результатам средняя сеть не теряет своей производительности при увеличении размера базы данных, даже если база данных разнообразна. Более того, ее производительность увеличивается при увеличении размера базы данных. Наконец, наблюдается, что степень ошибки также применима в области стегоанализа. Таким образом, оценивается, какова была бы точность сети, если бы база данных состояла из 20 миллионов изображений. В работе (Wu и др., 2019) представлена новая модель, названная CoverImageSuppressionNetwork (CIS-Net), которая улучшает производительность пространственного стегоанализа изображений, подавляя информацию о натуральных основах в процессе обучения модели. В работе предложены два новых слоя: Single-value Truncation Layer (STL) и Sub-linear Pooling Layer (SPL). STL обрезает входные значения до одного и того же порога, когда они выходят за заданный интервал. Теоретически было доказано, что STL может уменьшить дисперсию карты признаков входных данных, не ухудшая полезной информации. SPL использует под-линейную степенную функцию для подавления больших значений, внесенных информацией о натуральных основах, и агрегирует слабые встроенные сигналы с помощью среднего пулинга. Далее была предложена улучшенная архитектура авторами (Zhang и др., 2020). Вначале, они используют сверточные матрицы размером 3x3 вместо традиционных 5x5 и оптимизируют их в предварительном слое. Меньшие сверточные ядра применяются для снижения числа параметров и моделирования признаков в небольших локальных областях. После они используют раздельные свертки для использования канальной корреляции остатков, сжатия содержания изображения и увеличения отношения сигнал-шум (между сигналом с прячущей информацией и сигналом изображения). Далее, применяется пространственное пирамидальное пулинг (SPP) для агрегации локальных признаков и улучшения возможностей представления

признаков с помощью многоуровневого пулинга. В конце, для дополнительного улучшения производительности сети используется аугментация данных. Данную работу улучшили другие авторы (Yu и др., 2020), предложив новый метод аугментации данных, названный "BitMix," предназначенный для стегоанализа пространственных изображений. BitMix работает путем обмена случайных участков/патчей между оригинальным изображением и его стеганографической версией, а также создает адаптивные метки, которые указывают на отношение количества измененных пикселей в обменном патче к количеству пикселей в исходной паре, которая состоит из оригинального и стеганографического изображений. Более того, чтобы повысить точность обнаружения и обобщения стегоанализа в статье (Tan и др., 2020) предлагается SteganalysisContrastiveFramework (SCF) на основе контрастного обучения. SCF улучшает представление признаков в стегоанализа, максимизируя расстояние между признаками выборок разных категорий и минимизируя расстояние между признаками выборок одной и той же категории. Для уменьшения вычислительной сложности контрастной потери в надзорном обучении, была разработана новая SteganalysisContrastiveLoss (StegCL) на основе эквивалентности и транзитивности сходства. StegCL устраняет избыточные вычисления в существующей контрастной потере. Экспериментальные результаты показывают, что SCF улучшает обобщение и точность обнаружения существующих DNN-моделей стеганализа, и максимальное улучшение составляет 2 % и 3 % соответственно. Без уменьшения точности обнаружения время обучения с использованием StegCL составляет всего 10 % от времени обучения с использованием контрастной потери в надзорном обучении. В статье (Yang и др., 2019), в отличие от традиционных подходов, предлагаемая модель сначала извлекает остаточный шум с использованием обученных денойзинговых ядер для увеличения отношения сигнал-шум. После предварительной обработки разреженные остаточные шумы подаются на вход новой многоконтекстной сверточной нейронной сети (M-CNET), которая использует различные размеры контекста для изучения разреженного и малоамплитудного представления остаточных шумов. Производительность модели дополнительно улучшается за счет включения модуля self-attention для фокусировки на областях, подверженных стегоаналитическим внедрениям. В статье (Ren и др., 2021) авторы предлагают методику CALPA-NET, основанную на поиске архитектуры глубокой сети с прореживанием каналов, чтобы уменьшить структуру сетей существующих стегоанализаторов на основе глубокого обучения, которые часто являются переусложненными и избыточными по параметрам. Авторы обращают внимание на широкую пирамидальную структуру существующих стегоанализаторов на основе глубокого обучения и считают, что она может противоречить принципам разнообразия моделей. Поэтому предложенный ими подход CALPA-NET нацелен на адаптивное прореживание сверточных слоев в соответствии с гибридным критерием, объединяющим две схемы

прореживания сетей. В результате прореживания структура сети становится более компактной и напоминает узкий бутылочный силуэт. Обширные эксперименты были проведены на нескольких наборах данных, включая BOSSBase+BOWS2, более разнообразный ALASKA и крупномасштабное подмножество, извлеченное из ImageNet CLS-LOC. Результаты показали, что структура модели, сгенерированной методикой CALPA-NET, способна достичь сравнимой производительности с использованием менее чем двух процентов параметров и приблизительно трети операций с плавающей запятой (FLOPs) по сравнению с исходной структурой стегоаналитической модели. Новая модель также обладает улучшенной адаптивностью, переносимостью и масштабируемостью.

Кроме сверточных сетей, для стегоанализа широко применяются и рекуррентные нейронные сети (RNN) и в основном с текстовыми данными. В статье (Singh и др., 2021) авторы обращают внимание на то, что условное вероятностное распределение каждого слова в автоматически сгенерированных стеганографических текстах искажается после встраивания скрытой информации. Для извлечения этих различий в распределении признаков используются рекуррентные нейронные сети. Затем полученные признаки классифицируются на основе текстов как признаки нормального текста и стеганографического текста. Анализ текста обсуждалась и в (Wu и др., 2021) но, уже в парадигме графовых нейронных сетей. Путем обучения графовой сверточной нейронной сети (GNN) для извлечения признаков, каждый узел графа может собирать контекстную информацию для обновления собственного представления, что позволяет эффективно решить проблему ограниченного представления многозначных слов. В то же время в методе используется глобально общая матрица для регистрации корреляционной силы между словами, так что каждый текст может эффективно использовать глобальную информацию для улучшения собственного представления. GNN также использовали (Liu и др., 2023). В статье представлен метод стегоанализа JPEG-изображений, который включает в себя два ключевых модуля: модуль обучения с учетом графовых данных и модуль улучшения признаков. Главной целью данного метода является повышение производительности стегоанализа и уменьшение потери признаков при использовании сверточных нейронных сетей. Модуль обучения с учетом графовых данных разработан с целью избежать потери глобальных признаков, которая может возникнуть из-за локального обучения признаков сверточной нейронной сети и зависимости от увеличения глубины сети для расширения воспринимаемой области. Данный метод добавляет улучшение в способности сети извлекать дискриминирующие признаки путем использования информации о графах для более глобального восприятия данных.

Последние годы набирают обороты и генеративные модели. В статье (Corley и др., 2019) предлагается DeepDigitalSteganographyPurifier (DDSP), генеративно-состязательная сеть (GAN), которая оптимизирована для

очищения от стеганографического содержания, не ухудшая при этом восприятия качества оригинального изображения. По результатам, их модель способна обеспечивать высокую степень уничтожения стеганографического содержания при сохранении высокого визуального качества в сравнении с другими современными методами фильтрации. Авторы (Zhang и др., 2022) отмечают, что несмотря на большое количество разных баз данных по стеганографии, все равно есть проблема нехватки данных. Для того, чтобы решить эту проблему они предложили новую нейронную сеть на базе GAN, что помогло улучшить результаты их исследования на базе картинок S-UNIWARD.

Материалы и основные методы

В целях демонстрации основополагающих принципов стеганографии, можно рассмотреть метод, известный как LeastSignificantBits (LSB), который представляет собой один из наиболее элементарных подходов к маскировке информации в цифровых изображениях. Сущность данного подхода заключается во внедрении информации в наименее значимые биты пикселей, что позволяет сохранить визуальную целостность изображения при одновременном скрытии данных. В структуре цветного изображения, где каждый пиксель кодируется определенным числом битов для отображения цветовых каналов - красного (RED), зеленого (GREEN) и синего (BLUE), наиболее значимые биты несут ключевую информацию о цветовых характеристиках пикселя. В контексте LSB, менее значимые биты, часто оставаясь вне поля зрения при стандартном визуальном анализе, предоставляют идеальную среду для встраивания дополнительных данных.

Применение метода LSB в стеганографии обеспечивает возможность интеграции скрытых сообщений в изображения с минимальным влиянием на их визуальное восприятие. Следует отметить, что при маскировке значительного объема информации, когда большое количество битов в каждом пикселе задействовано для внедрения данных, возникают риски ухудшения качества изображения. Подобные изменения могут облегчить задачу обнаружения стеганографических вмешательств, особенно при применении продвинутых методов цифрового анализа и глубокого обучения.

В контексте дискуссии о методе LSB стеганографии, его роль можно охарактеризовать как балансирующую между необходимостью эффективного сокрытия информации и сохранения исходного качества изображения. Применение LSB представляет значительный интерес в рамках исследований в областях кибербезопасности и стеганографии, особенно в контексте поиска оптимальных способов сокрытия данных. Особое внимание в данном процессе уделяется балансу между количеством внедряемой информации и её влиянием на визуальное качество изображения. Подход, основанный на тщательном управлении этим балансом, является ключевым для обеспечения эффективности стеганографических методов, с одновременным минимизированием рисков обнаружения скрытой информации средствами современного анализа данных.

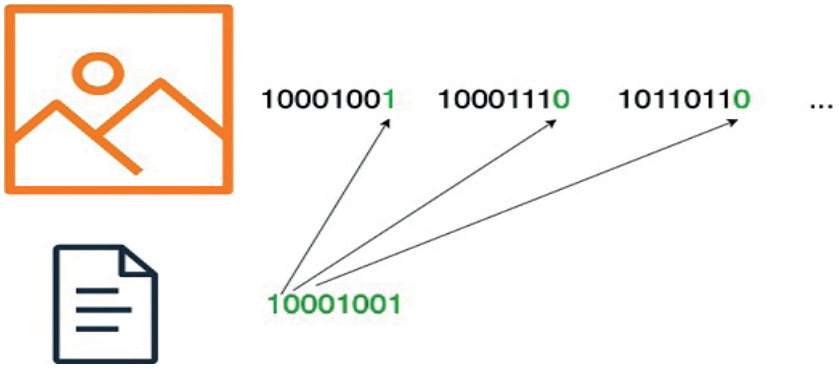


Рисунок 1 - Замена битов картинки на биты входящего сообщения путем LSB

В рамках представленного исследования предполагается использование данных, полученных в результате применения передовых алгоритмов стеганографии, включая JMiPOD, UERD и JUNIWARD. Целью является обучение нейронной сети, способной проводить глубокий анализ информации на предмет выявления встроенных скрытых данных. Процесс обучения будет направлен на достижение способности нейронной сети к высокоточной классификации данных в соответствии с определенными категориями.

Эффективность работы глубоких нейронных сетей

	RichModels + EnsembleClassifiers	FNN	CNN	Dataset
Avg_Error	24.67 %	7.4 %	8.66 %	BossBase
Avg_Error	48.29 %	5.89 %	5.16 %	LIRMM

Таблица 1 - Сравнение метрик классических методов и нейронных сетей (Pibre и др., 2016)

Как упоминалось выше, глубокие нейронные сети доказали свою устойчивость в задачах стегоанализа в сравнении с классическими методами. Авторы (Pibre и др., 2016) провели множество экспериментов для определения оптимальной "формы" CNN. Эксперименты проводились в условиях "прозрачного" сценария для сравнения CNN и FNN с RM и ансамблевыми классификаторами. Результаты показали снижение ошибки классификации более чем на 16 % с использованием CNN или FNN (см. Таблицу 1). Более того, результаты демонстрируют естественную устойчивость CNN и FNN к проблеме несоответствия.

Кроме этого, в статье (Xie и др., 2019) было подтверждено (см. Таблицу 2), что предложенная 20-слойная сверточная нейронная сеть SRNeT превосходит лучший метод, основанный на характеристиках, а именно SCA-GFR на датасете сгенерированных путем использования J-Uniward и UERD.

Алгоритм	SCF-GFR (errorrate)	SRNeT (errorrate)	Dataset
J-UNI-75	0.0792	0.0670	BossBase
UERD-75	0.0377	0.0188	BossBase
J-UNI-95	0.2617	0.1762	BossBase
UERD-95	0.1662	0.0877	BossBase

Таблица 2 - Сравнение метрик классического метода и нейронной сети (Xie и др., 2019)

Dataset

Процесс скрытия информации в формате JPEG состоит из нескольких этапов (см. Рисунок 1).

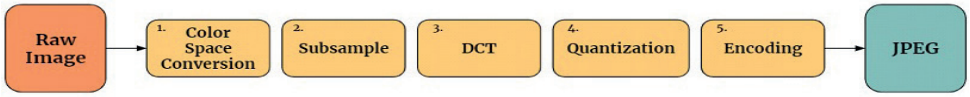


Рисунок 2 - Конвертация изображения в формат JPEG. Во время конвертации применяется стеганография

● В начале процесса (см. Рисунок 2) имеются необработанные данные, представляющие изображение в формате RAW. Данный формат обеспечивает максимальную сохранность деталей и цветов, не подвергаясь сжатию. В стеганографии выбор участка для скрытого внедрения информации в данном контексте часто определяется анализом статистики цветов и текстур изображения.

● Следующим этапом является преобразование необработанных данных в выбранное цветовое пространство, такое как RGB или YCbCr. Данное преобразование позволяет более эффективно работать с цветовой информацией изображения.

● На этапе субдискретизации происходит уменьшение разрешения цветовой информации для каждого канала. В стеганографии эта стадия может быть использована для выбора определенных компонентов изображения, где будет внедряться скрытая информация.

● После субдискретизации применяется DCT, преобразовывая блоки изображения в частотное пространство. Важно отметить, что выбор блоков для DCT может также определяться стеганографическими целями, например, выбор блоков с высокой чувствительностью к изменениям.

● Коэффициенты DCT подвергаются процессу квантования, где значения делятся на предопределенные квантованные уровни. В стеганографии этот этап предоставляет возможность встраивания информации, изменяя значения квантованных коэффициентов.

● Завершающей стадией является кодирование, включающее в себя применение методов сжатия данных, таких как кодирование Хаффмана. В контексте стеганографии этот этап может быть также использован для дополнительного сокрытия информации.

Для тренировки моделей были использованы данные ALASKA2. Набор данных ALASKA2 состоит из 75 000 изображений, полученных с использованием более чем 40 различных камер. В этот перечень входят устройства разного класса - от смартфонов и планшетов до недорогих камер и высококачественных полнокадровых цифровых зеркальных камер (DSLR). Обработка изображений в данном наборе данных выполнена реалистично и отличается высокой степенью гетерогенности.

Объем данных

Данный набор данных включает большое количество неизмененных изображений, именуемых как "Cover", а также соответствующие примеры, в которых информация была скрыта с использованием одного из трех алгоритмов стеганографии: JMiPOD, JUNIWARD, UERD.

Следует отметить, что для придания большей реалистичности длина скрытых сообщений (payload) не предоставляется. Единственной доступной информацией о наборе является:

- Каждый алгоритм встраивания используется с одинаковой вероятностью.
- Полезная нагрузка (длина сообщения) регулируется таким образом, чтобы "сложность" была примерно одинаковой независимо от содержания изображения. Изображения с плавным содержанием используются для скрытия более коротких сообщений, в то время как изображения с высокой текстурностью используются для скрытия большего количества секретных бит. Полезная нагрузка регулируется одинаково для тестовых и обучающих наборов.
- Средняя длина сообщения составляет 0.4 бита на каждый ненулевой коэффициент AC DCT.
- Все изображения сжаты с использованием одного из трех следующих факторов качества JPEG: 95, 90 или 75.
- Размер всех картинок 512x512

Файлы

Cover/Обложка - содержит 75 тыс. неизмененных изображений, предназначенных для использования в обучении.

JMiPOD - содержит 75 тыс. примеров применения алгоритма JMiPOD к изображениям обложки.

JUNIWARD - содержит 75 тыс. примеров применения алгоритма JUNIWARD к изображениям обложки.

UERD - содержит 75 тыс. примеров применения алгоритма UERD к изображениям обложки.

file	method	quality	num_bits
00001.jpg	Cover	90	0
00001.jpg	JUNIWARD	90	5883
00001.jpg	JMiPOD	90	15488
00001.jpg	UERD	90	7968
00002.jpg	Cover	95	0
00002.jpg	JUNIWARD	95	35186
00002.jpg	JMiPOD	95	9918
00002.jpg	UERD	95	33722
00003.jpg	Cover	90	0
00003.jpg	JUNIWARD	90	1042
00003.jpg	JMiPOD	90	2845
00003.jpg	UERD	90	1069

Таблица 3 - Количество битов, встроенных в каждое изображение

Визуализация

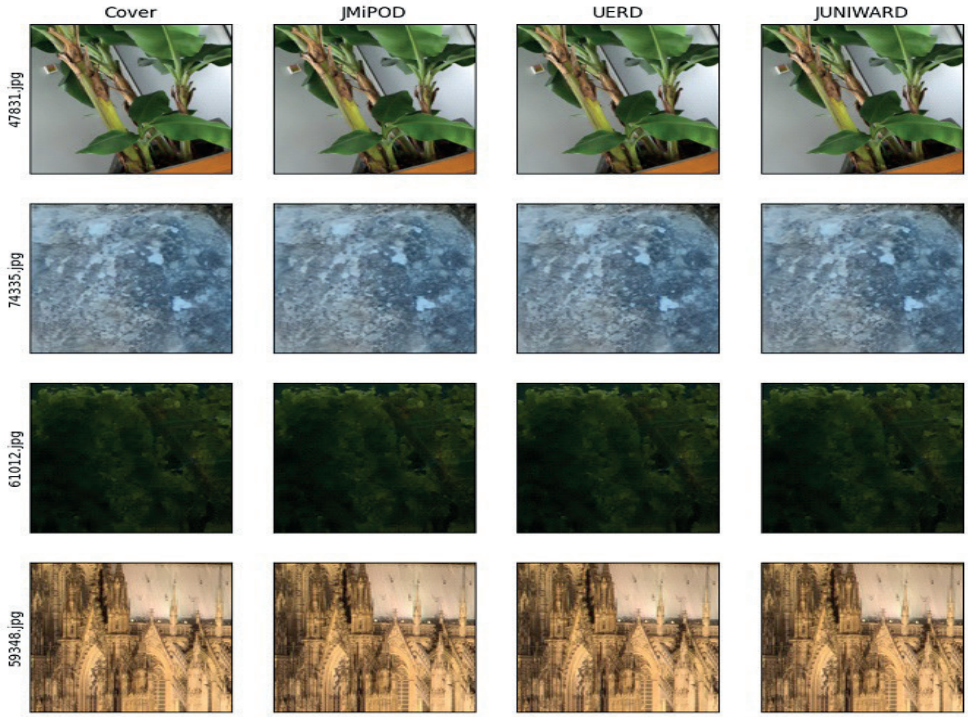


Рисунок 3 - Примеры из датасета

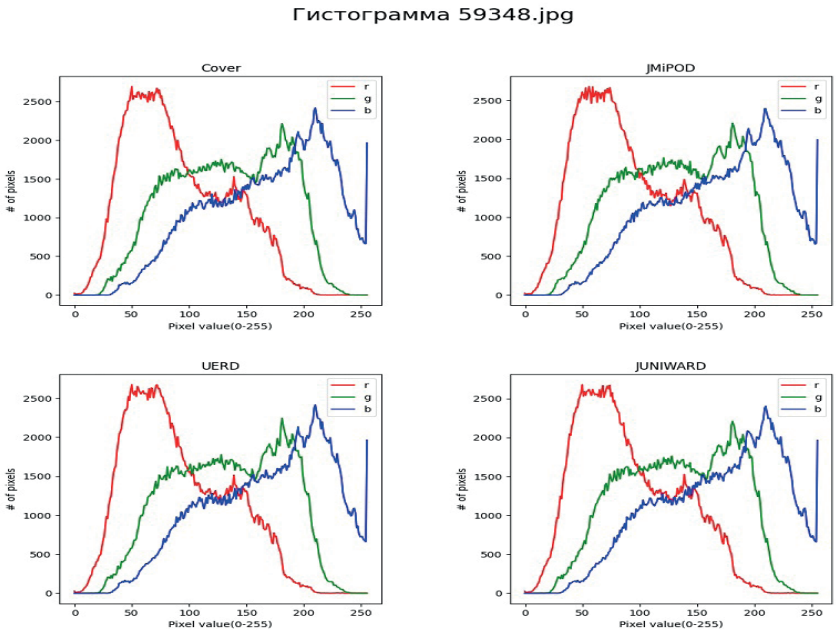


Рисунок 4 - Гистограмма пикселей для каждого канала

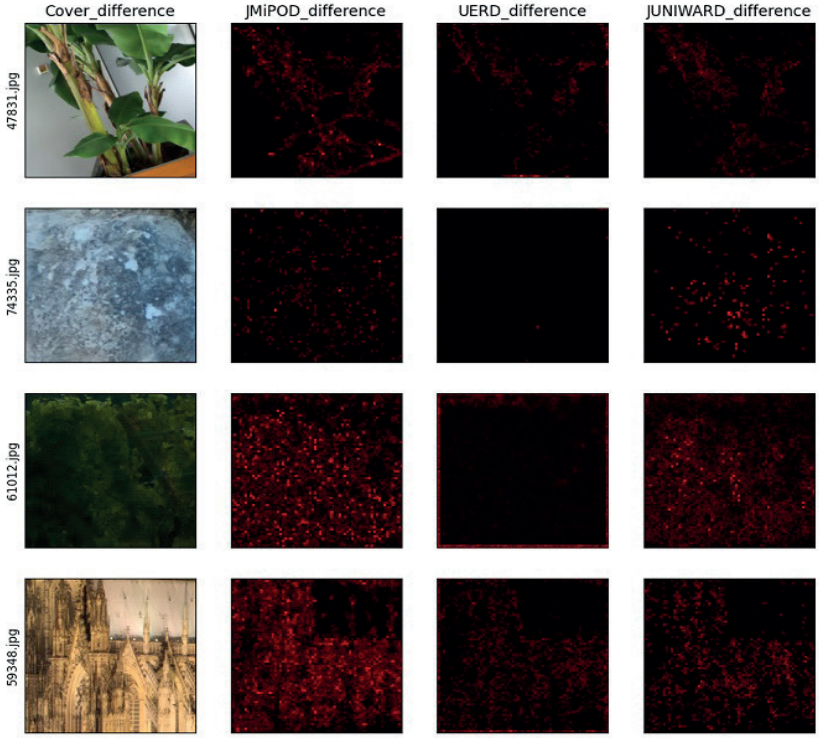


Рисунок 5 - Разница между оригинальной и Jmipod, UERD, Juniward соответственно. Канал R

Методология

В рамках исследования по обнаружению стеганографии применялась модель EfficientNet (Tan и др., 2019), которая представляет собой инновационное решение в области сверточных нейронных сетей (CNN). Основным преимуществом данной модели является ее способность к масштабированию всех трех измерений — глубины, ширины и разрешения — с использованием простого, но эффективного комплексного коэффициента. Данный подход демонстрирует значительное улучшение точности и эффективности по сравнению с предыдущими моделями сверточных нейронных сетей. Например, модель EfficientNet-B7 (см. Рисунок 6) достигла лидирующей точности в 84.3 % по показателю top-1 на ImageNet, при этом она в 8.4 раза меньше и в 6.1 раза быстрее лучшей существующей сверточной сети в инференции. Кроме того, EfficientNets показали отличные результаты в переносимости обучения, достигая лучшей точности на CIFAR-100 (91.7 %), Flowers (98.8 %) и других наборах данных.

Архитектура EfficientNet, построена на новом методе масштабирования, который использует композитный коэффициент для равномерного масштабирования ширины, глубины и разрешения сети. Масштабирование основано на наборе фиксированных коэффициентов масштабирования, определенных с помощью небольшого поиска по сетке. Базовая архитектура, EfficientNet-B0, оптимизирована с помощью поиска архитектуры нейронных сетей (NAS), и метод масштабирования применяется к этой базе для получения других вариантов EfficientNet (B1 до B7).

$$\mathcal{N}(d, w, r) = \bigodot_{i=1\ldots s} \hat{\mathcal{F}}_i^{d\cdot\hat{L}_i}\left(X_{\langle r\cdot\hat{H}_i, r\cdot\hat{W}_i, w\cdot\hat{C}_i\rangle}\right)$$

Формула 1. Общая формула масштабирования EfficientNet

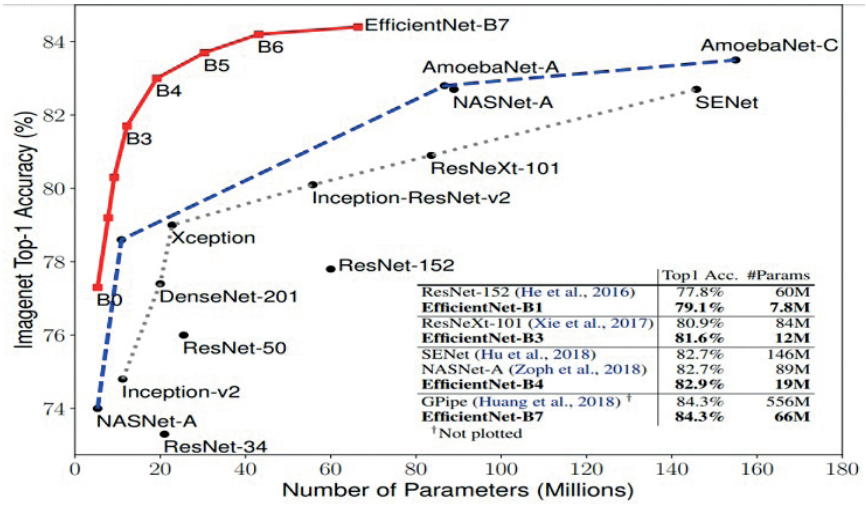
- N нейронная сеть
- $\hat{F}, \hat{H}, \hat{W}, \hat{C}, \hat{L}$ - тип слоя, глубина, ширина, канал и количество слоев
- Глубина: $d = \alpha^{\phi}$
- Ширина: $\omega = \beta^{\phi}$
- Разрешение: $r = \gamma^{\phi}$
- Композитный коэффициент: ϕ
- $\alpha \geq 1, \beta \geq 1, \gamma \geq 1$

Где,

- d, ω, r - представляют глубину, ширину и разрешение сети соответственно.
- α, β, γ - константы, которые определяют, насколько увеличивается глубина, ширина и разрешение сети.
- ϕ - композитный коэффициент, который контролирует, сколько ресурсов доступно для масштабирования модели.

● Каждый вариант EfficientNet (B1 до B7) масштабируется от базовой модели B0 с использованием различных значений композитного коэффициента. Например, EfficientNet-B1 имеет немного больший ϕ, чем B0, что приводит к немного более крупной и точной модели, и так далее до B7. Фактические значения α, β, γ, ϕ определяются через комбинацию теоретических основ и эмпирической настройки, основанные на доступных вычислительных ресурсах и конкретных требованиях производительности для конкретной задачи.

● В данной работе используется последний слой, который модифицируется на 4 выхода, на каждый класс: Cover, UERD, J-miPod, J-Uniward.



	Top1 Acc.	#Params
ResNet-152 (He et al., 2016)	77.8%	60M
EfficientNet-B1	**79.1%**	**7.8M**
ResNeXt-101 (Xie et al., 2017)	80.9%	84M
EfficientNet-B3	**81.6%**	**12M**
SENet (Hu et al., 2018)	82.7%	146M
NASNet-A (Zoph et al., 2018)	82.7%	89M
EfficientNet-B4	**82.9%**	**19M**
GPipe (Huang et al., 2018) †	84.3%	556M
EfficientNet-B7	**84.3%**	**66M**

†Not plotted

Рисунок 6 - Сравнительный график EfficienNet моделей на датасете Imagenet (Tan и др., 2019)

Метрика

Для акцента на надежном обнаружении с минимизацией ложных тревог оценка представленных работ осуществляется на основе взвешенной площади под кривой (AUC). Расчет взвешенной AUC предполагает присвоение весов каждому сегменту кривой рабочих характеристик приемника (ROC) в соответствии с выбранными параметрами:

● Пороги истинно-положительной оценки (TPR, см. Формулу 2): [0.0,0.4,1.0]

● Веса: [2,1]

Формула 2. Формула TPR $$TPR = \frac{TP}{TP + FN}$$

Формула 3. Формула FPR $$FPR = \frac{FP}{TP + FP}$$

Иными словами, участок между значениями истинно-положительной оценки 0 и 0.4 учитывается с двойным весом 2X, а участок между 0.4 и 1 — с

одинарным весом 1X. Общая площадь нормализуется суммой весов, таким образом, итоговая взвешенная AUC находится в пределах от 0 до 1.

Разделение датасета

GroupKFold — метод кросс-валидации, используемый для разделения данных на подмножества (folds). В данном методе одна и та же группа не появляется в обучающем и тестовом наборах одного и того же fold. В контексте изображений это предотвращает утечку данных и обеспечивает, что модель не будет тестироваться на данных, на которых она обучалась. Датасет разделяется на пять частей, где каждый fold представляет собой уникальное подмножество данных. В этом случае один fold используется для тестирования, а оставшиеся четыре — для обучения и валидации модели. В процессе кросс-валидации модель обучается на трех из пяти folds, в то время как четвертый fold используется для валидации, а пятый для теста. Процесс повторяется таким образом, чтобы каждый fold однажды использовался в качестве валидационного набора. В итоге, данный метод поможет сделать необходимый ансамбль натренированных моделей.

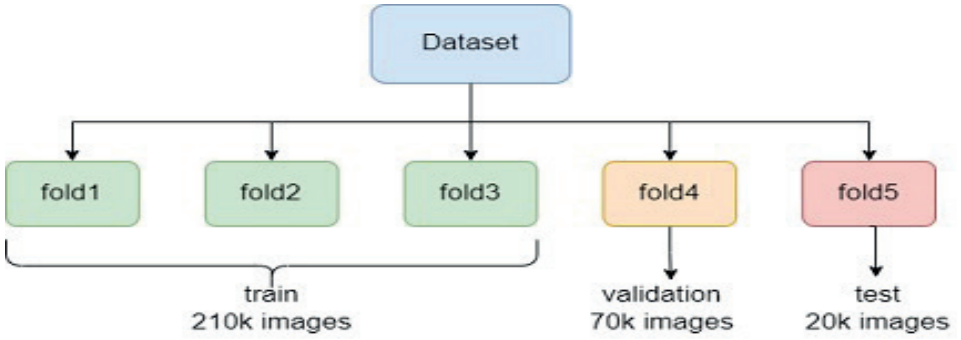


Рисунок 7 - Разделение данных для экспериментов. Test фиксированный, тогда как остальные fold-ы меняются для валидации.

Гиперпараметры

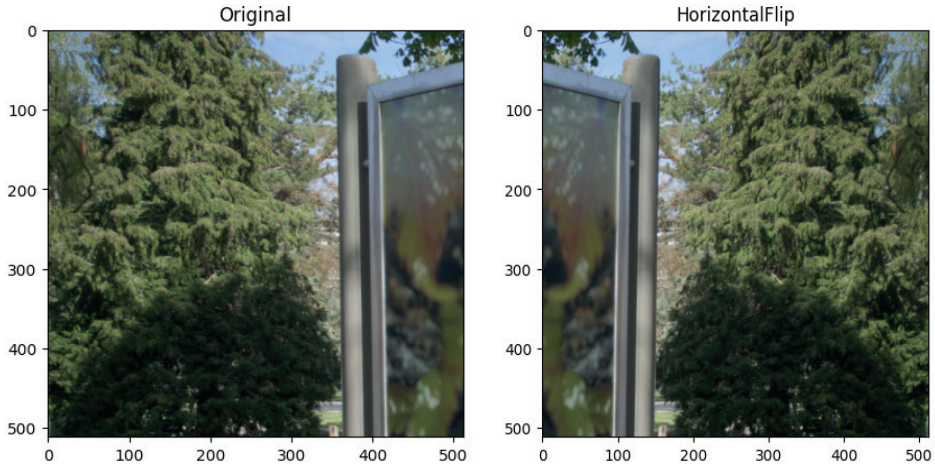
- AdamW, модификация стандартного оптимизатора Adam, включает корректировку весов (WeightDecay). Основное отличие AdamW от классического Adam заключается в прямом применении регуляризации весов к градиентам, что способствует более точной и стабильной оптимизации в сложных нейросетях. Благодаря этому методу достигается улучшение в коррекции весов, снижая вероятность переобучения и повышая общую производительность модели.
- Метод ReduceLROnPlateau с параметрами начального значения lr=0.001, patience=3 и factor=0.5 обеспечивает адаптивное уменьшение скорости обучения (learningrate, lr) при достижении плато в процессе обучения. Значение patience, равное 3, определяет количество эпох без улучшения модели для активации снижения скорости обучения, при этом фактор factor,

равный 0.5, указывает на уменьшение скорости обучения в два раза при каждом снижении.

- Функция потерь CrossEntropyLoss с интеграцией техники LabelSmoothing на уровне 0.05. Применение "LabelSmoothing" с параметром 0.05 позволяет размывать метки классов, снижая уверенность модели в точности принадлежности каждого образца к определённому классу. Такая стратегия улучшает обобщающую способность модели, предотвращая её чрезмерную уверенность в предсказаниях и улучшая работу с несбалансированными или зашумлёнными данными.

Аугментации

В целях обогащения и расширения набора данных применялись техники аугментации. Особое внимание в задачах стегоанализа уделяется сохранению качества изображения, что делает использование легких аугментаций предпочтительным. Среди таких методов выделяются VerticalFlip, HorizontalFlip и Rotate. Каждый из этих подходов обеспечивает вариативность данных без значительного влияния на исходное качество изображений. В то же время, наиболее нестандартной аугментацией является Cutout, которая добавляет дополнительный уровень сложности, удаляя части изображения для создания новых уникальных образцов. Данная техника, хотя и более агрессивная, также способствует увеличению обобщающей способности модели, тренируя её работать с частично неполными или измененными данными.



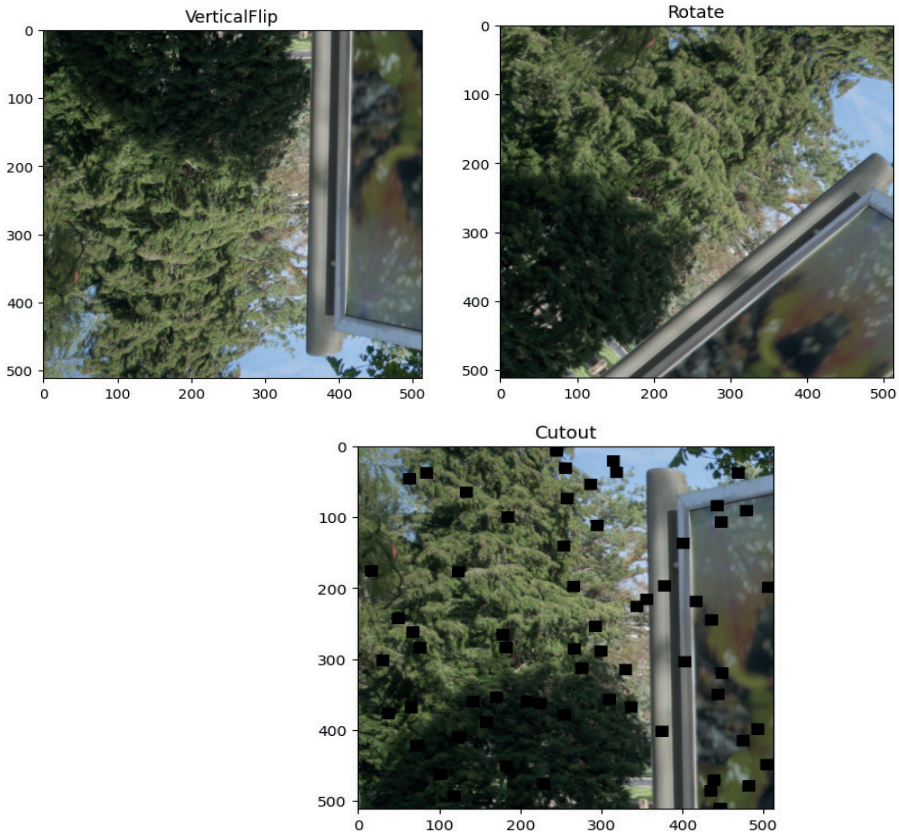


Рисунок 8 - Использованные аугментации

Результаты EfficientNetB4

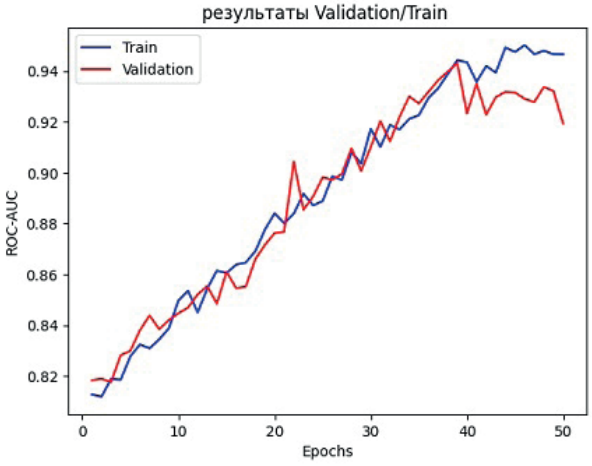


Рисунок 9 - График тренировки EfficientNetB4 с использованием аугментаций (см. Из. 8) и техники LabelSmoothing

ModelType	validation	test
EfficientnetB4	0.929	0.923
EfficientnetB4+Cutout	0.929	0.924
EfficientnetB4+Cutout+LabelSmoothing	0.931	0.926

Таблица 2- Экспериментальные результаты. ROC-AUC

Базовая модель без модификаций достигла на валидационном наборе данных 0.929 и на тестовом наборе данных 0.923. Модель с аугментацией 'cutout' не показала улучшения точности на валидационном наборе данных, но незначительно улучшила точность на тестовом наборе до 0.924. Добавление 'cutout' и 'LabelSmoothing' улучшило метрику как на валидационном наборе 0.931, так и на тестовом наборе 0.926.

EfficientNetB3

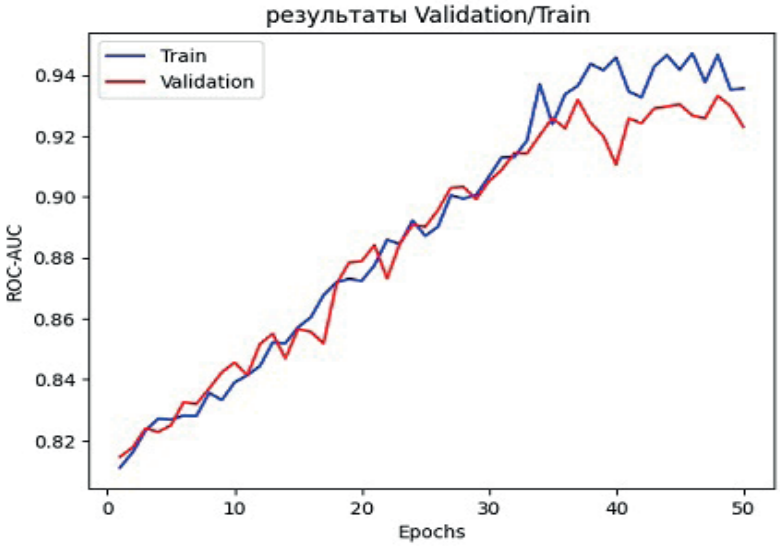


Рисунок 10 - График тренировки EfficientNetB3 с использованием аугментаций (см. Из. 8) и техники LabelSmoothing

ModelType	validation	test
EfficientnetB3	0.927	0.923
EfficientnetB3+Cutout	0.927	0.925
EfficientnetB3+Cutout+LabelSmoothing	0.929	0.925

Таблица 3 - Экспериментальные результаты. ROC-AUC

Базовая модель имела точность на валидационном наборе 0.927 и на тестовом наборе 0.923. С аугментацией 'cutout' точность на валидационном

наборе осталась прежней, но точность на тестовом наборе незначительно увеличилась до 0.925. Модель с 'cutout' и 'LabelSmoothing' показала небольшое увеличение точности на валидационном наборе до 0.929 и сохранила точность на тестовом наборе на уровне 0.925.

Ансамбль

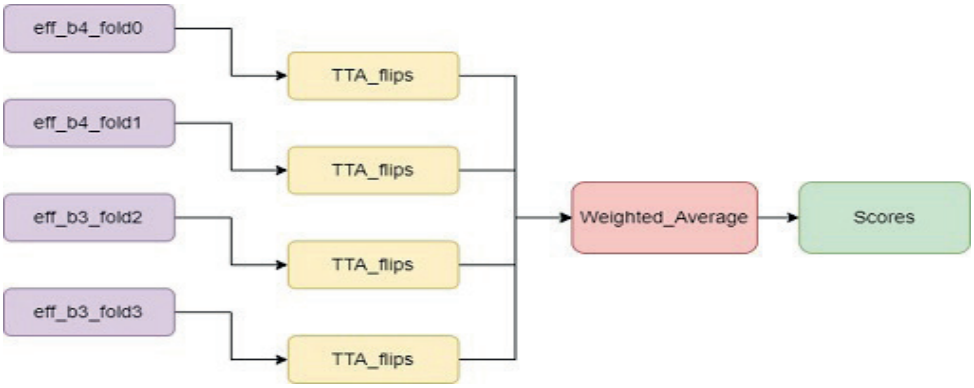


Рисунок 11 - Ансамбль моделей на различных фолдах

ModelType	validation	test
Ensemble	0.930	0.928

Таблица 4 - Результаты ансамбля моделей. ROC-AUC

Модель ансамбля (см. Из. 11), которая включает в себя 4 модели на разных фолдах и дальше используется метод “аугментация во время теста” (TestTimeAugmentation) достигла наивысшей точности на тестовом наборе 0.928 (см. Таб. 4), превзойдя все индивидуальные модели. Более того, для усреднения использовались взвешенные коэффициенты 0.28, 0.24, 0.24, 0.24 соответственно для фолдов 0,1,2,3.

Анализ результатов

Использование аугментации 'cutout' способствует незначительному улучшению точности на тестовом наборе для моделей EfficientNetB4 и B3. Добавление 'LabelSmoothing' оказывается более полезным при сочетании с 'cutout', улучшая точность как на валидационном, так и на тестовом наборах для модели EfficientNetB4. Ансамблевый подход оказывается наиболее эффективной стратегией для повышения точности в данном конкретном случае. Одним важным недостатком ансамблевых моделей является скорость. Однако, используя различные оптимизационные методы можно решить эту проблему при необходимости.

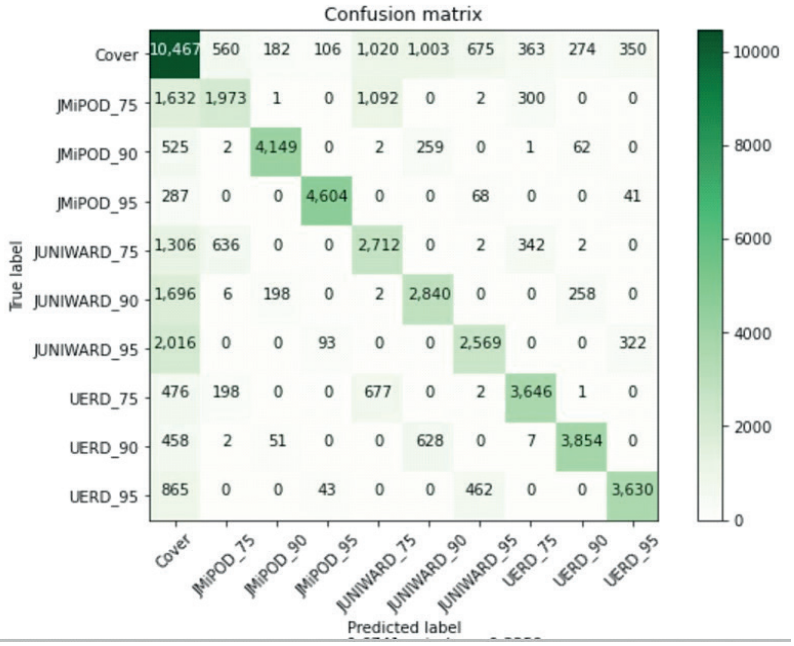


Рисунок 12 - Матрица ошибок для каждого типа алгоритма с соответствующим качеством

Вертикальная ось (см. Рисунок 12) отображает фактические классы, а горизонтальная ось — предсказанные метки. Метки, являются названиями стеганографических методов с различными уровнями встраивания 75, 90, 95. Например: изображения категории "Cover" были правильно идентифицированы 10,467 раз, изображения, на самом деле являющиеся Cover, были неверно идентифицированы как JMiPOD_75 560 раз. Как видно, модель очень хорошо справляется с правильной идентификацией категории Cover и различных стеганографических методов, особенно при уровне встраивания 95, как видно по JMiPOD_95, JUNIWARD_95 и UERD_95. Однако, модель испытывает больше трудностей с различением между JMiPOD_75 и JUNIWARD_75, а также между JMiPOD_90 и JUNIWARD_90, учитывая более высокие числа вне диагонали между этими категориями, что указывает на то, что признаки, используемые моделью для различения между этими категориями при этих конкретных уровнях встраивания, не настолько дискриминативны. Модель имеет тенденцию к лучшей производительности при более высоких уровнях встраивания, что предполагает более легкое обнаружение стеганографии с большим объемом данных. Более низкие уровни встраивания, представляют большую сложность для модели, что приводит к большему количеству ошибочных классификаций.

Заключение

В данной работе было разработано комплексное решение на базе глубоких нейронных сетей для классификации стеганографических картин на данных

из 3 современных и устойчивых алгоритмов. Результаты показывают, что ансамбль нескольких моделей, натренированных и протестированных различными техниками как уникальные аугментаций, кросс валидация и аугментация во время тестирования улучшает качество обнаружения. Для будущих исследований, предлагается рассмотреть увеличение базы и оптимизация моделей для быстрой обработки данных.

Более того, по мере развития технологий виртуальной и дополненной реальности VR и AR, возникает потенциал для встраивания стеганографических сообщений в 3D контент, используемый в этих средах. Соответственно, методы стегоанализа должны будут учитывать особенности обработки данных в VR и AR. Таким образом, целью 3D стегоанализа является выявление тонких незаметных изменений в графических объектах, создаваемых с помощью цифрового водяного знака или стеганографии. Наборы статистических представлений 3D признаков, извлекаемых как из исходных, так и из модифицированных 3D сеточных объектов, используются в качестве входных данных для классификаторов машинного обучения для определения наличия скрытой информации в данном графическом объекте. Несмотря на то, что методы глубокого обучения показали перспективные результаты в стегоанализе 2D изображений, два вопроса остаются потенциально сложными: обеспечивают ли методы стегоанализа 3D на основе глубокого обучения лучшую производительность? Достаточно ли 3D данных, которые можно использовать для обучения моделей сверточных нейронных сетей в стегоанализе? Еще одним шагом для развития этого исследования будут ответы на вышеперечисленные вопросы.

REFERENCES

Cancelli G., et al. (2020). ALASKA: A Learned Steganalysis Assessment Kernel for Aachen. Proceedings of the IEEE International Conference on Acoustics. — Speech, and Signal Processing.

Corley I., Lwowski J. & Hoffman J. (2019). Destruction of Image Steganography using Generative Adversarial Networks. Booz Allen Hamilton. — San Antonio, Texas.

Liu Q., Yang Z., & Wu H. (2023). JPEG Steganalysis Based on Steganographic Feature Enhancement and Graph Attention Learning

Pibre L., Pasquet J., Ienco D. & Chaumont M. (2016). Deep learning is a good steganalysis tool when embedding key is reused for different images, even if there is a cover source-mismatch. In Media Watermarking, Security, and Forensics, IS&T International Symposium on Electronic Imaging. San Francisco. — California, USA.

Qian Y., Dong J., Wang W. & Tan T. (2015). Deep Learning for Steganalysis via Convolutional Neural Networks. In Proceedings of Media Watermarking, Security, and Forensics 2015, — MWSF'2015, Part of IS&T/SPIE Annual Symposium on Electronic Imaging. — SPIE'2015. — Vol. 9409. — Pp. 94090J–94090J–10). — San Francisco, California, USA.

Ren Y., Liu Y. & Wang L. (2021). Using contrastive learning to improve the performance of steganalysis schemes.

Ruiz H., Chaumont M., Yedroudj M., Amara A.O., Comby F. &Subsol G. (2020). Analysis of the Scalability of a Deep-Learning Network for Steganography — "Into the Wild."

Singh B., Sur A. &Mitra P. (2021). Multi-Contextual Design of Convolutional Neural Network for Steganalysis

Tan M. & Le Q.V. (2019). EfficientNet: Rethinking Model Scaling for Convolutional Neural Networks. Proceedings of the 36th International Conference on Machine Learning (PMLR 97), — Long Beach, California.

Tan S., Wu W., Shao Z., Li Q., Li B. & Huang J. (2020). CALPA-NET: Channel-pruning-assisted Deep Residual Network for Steganalysis of Digital Images.

Wu H., Yi B., Ding, F., Feng G. & Zhang X. (2021). Linguistic SteganalysisWith Graph Neural Networks.

Wu S., Zhong S.H., Liu Y. & Liu M. (2019). CIS-Net: A Novel CNN Model for Spatial Image Steganalysis via Cover Image Suppression.

Xie G., Ren J., Zhao H., Zhao S. & Marshall S. (2019). Evaluation of deep learning and conventional approaches for image steganalysis. Department of Electronic and Electrical Engineering, University of Strathclyde, Glasgow, — UK; School of Computer Science, Guangdong Polytechnic Normal University, Guangzhou, — P.R. China.

Xu G. (2017). Deep Convolutional Neural Network to Detect J-UNIWARD

Xu G., Wu H., Shi Y.Q. (2016). Structural Design of Convolutional Neural Networks for Steganalysis

Yang Z., Wang K., Li J., Huang Y. & Zhang Y.-J. (2019). TS-RNN: — Text Steganalysis Based on Recurrent Neural Networks.

Yang Z., Wang K., Ma S., Huang Y., Kang X. & Zhao X. (2019). — IStego100K: — Large-scale Image Steganalysis Dataset.

Yu I.-J., Ahn W., Nam S.-H., & Lee H.-K. (2020). BitMix: — Data Augmentation for Image Steganalysis.

Zhang H., Song Z., Xing Q., Feng B. & Lin X. (2022). A Generative Learning Steganalysis Network against the Problem of Training-Images-Shortage. Electronics, — 11(20), — 3331. — https://doi.org/10.3390/electronics11203331

Zhang R., Zhu F., Liu J. & Liu G. (2020). Depth-Wise Separable Convolutions and Multi-Level Pooling for an Efficient Spatial CNN-Based Steganalysis. IEEE Transactions on Information Forensics and Security, — 15

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Подписано в печать 28.03.2024.
Формат 60x881/8. Бумага офсетная. Печать–ризограф.
21,0 п.л. Тираж 300. Заказ 1.

РОО «Национальная академия наук РК» 050010,
Алматы, ул. Шевченко, 28, т. 272-13-19