ҚАЗАҚСТАН РЕСПУБЛИКАСЫ ҒЫЛЫМ ЖӘНЕ ЖОҒАРЫ БІЛІМ МИНИСТРЛІГІ

«Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ» КЕАҚ

Студенттер мен жас ғалымдардың
«ǴYLYM JÁNE BILIM - 2024»
XIX Халықаралық ғылыми конференциясының
БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ
XIX Международной научной конференции
студентов и молодых ученых
«ǴYLYM JÁNE BILIM - 2024»

PROCEEDINGS
of the XIX International Scientific Conference
for students and young scholars
«ǴYLYM JÁNE BILIM - 2024»

2024
Астана

УДК 001
ББК 72
G99

«ǴYLYM JÁNE BILIM – 2024» студенттер мен жас ғалымдардың XIX Халықаралық ғылыми конференциясы = XIX Международная научная конференция студентов и молодых ученых «ǴYLYM JÁNE BILIM – 2024» = The XIX International Scientific Conference for students and young scholars «ǴYLYM JÁNE BILIM – 2024». – Астана: – 7478 б. - қазақша, орысша, ағылшынша.

ISBN 978-601-7697-07-5

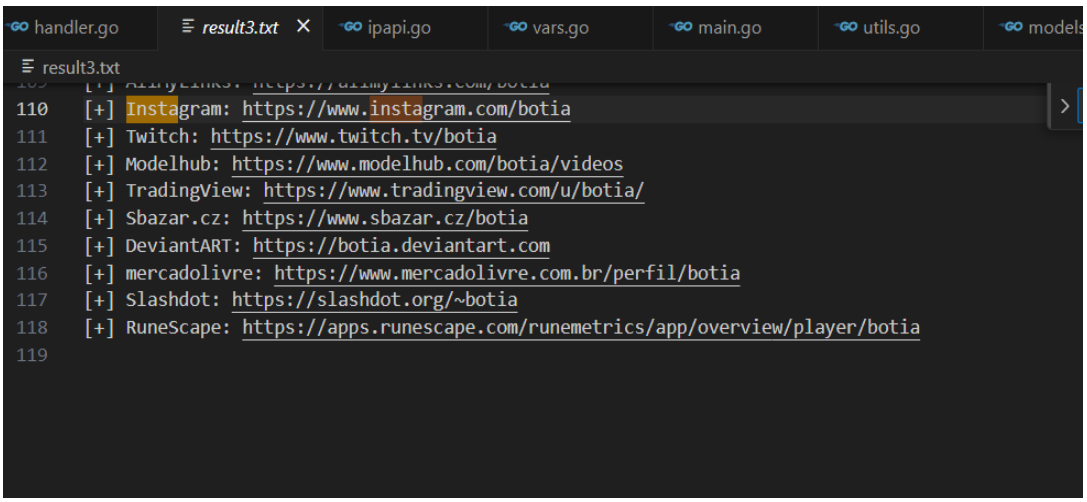
Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов имолодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001
ББК 72
G99

ISBN 978-601-7697-07-5



1-рисунок. Результат работы инструмента в файле txt при вводных данных "botia"

В заключение можно сказать, что разработка инструмента OSINT для автоматического сбора информации из общедоступных источников представляет значимый шаг в области кибербезопасности и разведывательного анализа. Этот инструмент обладает способностью эффективно извлекать и анализировать различные виды данных из разнообразных онлайн-ресурсов, что позволяет специалистам получать ценные сведения для выявления угроз, оценки рисков и принятия обоснованных решений.

Автоматизация процесса сбора информации снижает временные и человеческие затраты, делая его более эффективным и масштабируемым. Разработанный инструмент способствует улучшению работы специалистов по кибербезопасности, аналитиков и расследователей, обеспечивая им возможность оперативного доступа к обширной базе данных для выявления угроз и решения сложных задач.

Таким образом, разработка инструмента OSINT для автоматического сбора информации из общедоступных источников имеет большой потенциал в области кибербезопасности и разведывательного анализа, и его использование может значительно усилить возможности специалистов по защите информации и обеспечить более надежную защиту цифровых активов.

Список использованных источников

1. Open Source Intelligence (OSINT): retour aux sources - Olivier Le Deuff, RayyaRoumanos

2. A multilanguage platform for Open Source Intelligence - N. Baldini, F. Neri, Massimo Pettoni

3. Design Science Research towards Privacy by Design in Maritime Surveillance ICT Systems - Rajamäki 2019 ISIJ

4. What is Open-Source Intelligence and How it Can Prevent Frauds -Chalicheemala,2022

Surveillance and falsification implications for open source intelligence investigationsBayer, Akhgar – 2015Commun. ACM

ОБЗОР МЕТОДОВ ОБНАРУЖЕНИЯ СТЕГАНОГРАФИИ В МУЛЬТИМЕДИЙНЫХ ФАЙЛАХ

Асанов Әділбек Жанболатұлы
asanovadilbek66@gmail.com
Магистрант ЕНУ имени Л.Н. Гумилева, факультета информационных технологий, кафедра информационной безопасности, специальности «Системы информационной безопасности», Астана, Казахстан.

Научный руководитель - PhD доктор, доцент кафедры «Информационная безопасность» – Ахметова Жанар Жумановна.

В современном цифровом мире, где большая часть информации передается и хранится в электронном виде, вопросы конфиденциальности и безопасности данных приобретают особую актуальность. Стеганография, искусство скрытой передачи информации путем внедрения ее в незаметные носители, такие как изображения, аудио или видео файлы, является одним из методов защиты информации. Однако так же, как и для целей защиты, стеганография может использоваться и для маскировки вредоносных действий, что делает задачу обнаружения скрытой информации крайне важной для поддержания информационной безопасности.

Целью данной статьи является всесторонний обзор существующих методов обнаружения стеганографических вставок в мультимедийных файлах. Мы стремимся проанализировать и сравнить различные подходы, оценить их эффективность, преимущества и ограничения. Особое внимание уделяется не только техническим аспектам методов, но и их практическому применению, что позволит читателю получить представление о текущем состоянии исследований в данной области и ориентиры для будущих разработок.

Важность данной работы обусловлена не только академическим интересом к стеганографии как к дисциплине, но и практической необходимостью обеспечения информационной безопасности в условиях постоянно растущего объема цифрового контента и усовершенствования методов скрытой передачи данных. Понимание современных методов обнаружения позволит разработать более эффективные стратегии защиты информации и предотвратить потенциальные угрозы.

Теоретический обзор.

Стеганография — это дисциплина, занимающаяся изучением методов скрытой передачи информации. Этимологически термин происходит от греческих слов "στεγανός" (стеганос), что означает "скрытый", и "γραφία" (графия), означающее "письмо". Искусство стеганографии восходит к древним временам, когда для передачи секретных сообщений использовались различные ухищрения, начиная от невидимых чернил и заканчивая микротекстами.

В эпоху цифровых технологий стеганография обрела новые измерения, благодаря возможностям цифровой обработки данных. Мультимедийные файлы, такие как изображения, аудио и видеозаписи, из-за своей высокой информационной емкости и сложности, стали идеальными носителями для скрытой передачи информации. Основным принципом стеганографии в цифровой среде является внедрение информации таким образом, чтобы не вызвать подозрений и изменений, заметных для человеческого восприятия или стандартных методов анализа.

Методы стеганографии в мультимедийных файлах.

Основные методы включают, но не ограничиваются:

Метод наименее значимого бита (LSB), который заключается в изменении наименее значимых битов пикселей изображения или сэмплов аудиофайла для внедрения информации.

Трансформационные методы, использующие преобразования, такие как дискретное косинусное преобразование (ДКП) или вейвлет-преобразование, для внедрения информации в коэффициенты, полученные в результате этих преобразований.

Маскировка и интеграция, которые включают в себя техники, изменяющие существующие элементы медиафайлов для внедрения информации, например, через адаптацию шума или модификацию контуров объектов на изображении.

Обнаружение стеганографии

С увеличением использования стеганографии возникла потребность в разработке методов для ее обнаружения и анализа. Обнаружение стеганографии — это процесс идентификации файлов, которые могут содержать скрытую информацию. Этот процесс может включать анализ аномалий в статистических характеристиках медиафайлов, использование

специализированного программного обеспечения и применение алгоритмов машинного обучения для распознавания нехарактерных паттернов.

Важность теоретического обзора стеганографии и методов ее обнаружения не может быть переоценена. Понимание основ этих методов является ключевым для разработки эффективных средств обнаружения стеганографических сообщений и, как следствие, для укрепления общей информационной безопасности.

Методы обнаружения стеганографии.

Обнаружение стеганографически скрытой информации в мультимедийных файлах представляет собой значительный вызов для специалистов в области информационной безопасности. В этой главе рассматриваются основные методы и подходы, используемые для выявления стеганографии, каждый из которых имеет свои уникальные характеристики и области применения.

Статистические методы

Одним из наиболее распространенных подходов к обнаружению стеганографии является использование статистических методов. Эти методы анализируют статистические показатели мультимедийного файла, такие как гистограммы распределения цветов в изображениях или амплитудные характеристики в аудиофайлах. Изменения в этих статистических показателях могут указывать на потенциальное наличие стеганографически внедренной информации. Например, метод анализа наименее значимых битов (LSB) может выявлять необычные паттерны в распределении последних битов пикселей изображения, что является признаком стеганографического вмешательства.

Методы на основе машинного обучения

С развитием технологий машинного обучения и искусственного интеллекта появилась возможность создания более продвинутых систем обнаружения стеганографии. Модели машинного обучения, особенно сверточные нейронные сети (CNN), обучаются распознавать сложные паттерны и аномалии, которые могут указывать на наличие скрытой информации в изображениях или аудиофайлах. Эти методы могут адаптироваться к различным типам стеганографии, обеспечивая высокую точность обнаружения при минимальном количестве ложных срабатываний.

Специализированные инструменты и программное обеспечение

На рынке доступно множество специализированных инструментов для обнаружения стеганографии, разработанных для анализа мультимедийных файлов на предмет скрытых сообщений. Эти инструменты используют разнообразные методики, от статистического анализа до сложных алгоритмов машинного обучения, для выявления признаков стеганографической активности. Примеры таких инструментов включают StegExpose для изображений и Audiostego для аудиофайлов, каждый из которых предлагает уникальные функции для анализа соответствующих медиаформатов.

Анализ сложности и ограничений

Важно отметить, что каждый метод обнаружения имеет свои ограничения и области применения. Статистические методы могут быть неэффективны против высокоадаптивных стеганографических алгоритмов, которые специально разработаны для минимизации статистических аномалий. Методы на основе машинного обучения требуют больших объемов обучающих данных и могут быть подвержены переобучению. Специализированные инструменты, в свою очередь, могут не обеспечивать достаточную гибкость для адаптации к новым или нестандартным методам стеганографии. Таким образом, выбор метода или инструмента для конкретной задачи обнаружения должен учитывать как потенциальные преимущества, так и ограничения.

Анализ и сравнение методов обнаружения стеганографии.

Эффективность методов обнаружения стеганографии в мультимедийных файлах является критически важной для обеспечения информационной безопасности. В этой главе проводится анализ и сравнение основных подходов к обнаружению стеганографии,

рассмотренных в предыдущей главе, с акцентом на их преимущества, ограничения и потенциальные области применения.

Сравнительный анализ

Каждый метод обнаружения имеет свои уникальные характеристики, которые определяют его пригодность для конкретных задач и условий. Статистические методы, например, могут быть особенно эффективны для обнаружения простых форм стеганографии, но могут не справиться с более сложными техниками, которые минимизируют статистические аномалии. С другой стороны, методы на основе машинного обучения могут адаптироваться к различным видам стеганографии, но требуют значительных объёмов обучающих данных и могут быть подвержены переобучению.

Эффективность и ограничения

Важным аспектом анализа является оценка эффективности методов в различных сценариях использования, включая разные форматы и типы мультимедийных файлов. Кроме того, необходимо учитывать ограничения каждого метода, включая возможность ложных срабатываний, чувствительность к изменениям в медиафайлах и требования к вычислительным ресурсам.

Практическое применение

Оценка практического применения методов обнаружения стеганографии включает в себя анализ их удобства использования, доступности инструментов и программного обеспечения, а также возможности интеграции в существующие системы информационной безопасности. Например, специализированные инструменты могут быть более подходящими для непрофессионалов, тогда как гибридные и интеллектуальные системы могут требовать специализированных знаний и ресурсов для эффективного использования.

Будущие направления

В заключении главы стоит рассмотреть будущие направления развития методов обнаружения стеганографии, включая потенциальное применение новых технологий, таких как глубокое обучение и квантовые вычисления. Анализ текущих тенденций исследований может выявить области, в которых ожидаются значительные прорывы, а также потенциальные вызовы, с которыми столкнутся разработчики и исследователи в области обнаружения стеганографии.

Перспективы развития методов обнаружения стеганографии.

В условиях постоянно растущего объема цифрового контента и усовершенствования методов скрытой передачи информации, развитие эффективных методов обнаружения стеганографии становится ключевым аспектом обеспечения информационной безопасности. В этой главе рассматриваются текущие тенденции и будущие направления в развитии технологий стеганализа, а также их потенциальное влияние на сферу защиты данных.

Текущие тенденции

На сегодняшний день наблюдается значительный рост интереса к применению искусственного интеллекта и машинного обучения в области обнаружения стеганографии. Алгоритмы глубокого обучения, способные анализировать и обрабатывать большие объемы данных, показывают обнадеживающие результаты в выявлении сложных стеганографических вмешательств. Кроме того, разработка гибридных систем, сочетающих различные методы и подходы, открывает новые возможности для повышения точности и эффективности обнаружения.

Будущие направления

Одним из наиболее перспективных направлений является разработка адаптивных систем обнаружения, способных самостоятельно обучаться и совершенствоваться на основе анализа новых данных и угроз. Такие системы могут не только повышать свою эффективность со временем, но и адаптироваться к специфическим условиям и требованиям конкретных пользователей или организаций.

Влияние на информационную безопасность

Усовершенствование методов обнаружения стеганографии будет иметь значительное влияние на общую картину информационной безопасности, позволяя более эффективно противостоять угрозам, связанным с несанкционированным распространением конфиденциальной информации. Повышение уровня защиты от стеганографических атак также способствует укреплению доверия к цифровым коммуникациям и транзакциям, что крайне важно для развития цифровой экономики.

Вызовы и ограничения

Несмотря на значительный потенциал, развитие методов обнаружения стеганографии сталкивается с рядом вызовов. В частности, необходимо учитывать риск ложных срабатываний, которые могут привести к ненужным затратам ресурсов или нарушению приватности пользователей. Кроме того, постоянное совершенствование стеганографических методов требует непрерывного обновления и адаптации систем обнаружения.

Заключение

Развитие методов обнаружения стеганографии представляет собой динамичную и многообещающую область исследований, имеющую критическое значение для обеспечения безопасности в цифровом мире. Постоянный прогресс в этой сфере позволит не только эффективно противостоять существующим угрозам, но и адаптироваться к будущим вызовам в области информационной безопасности.

Заключение и рекомендации.

В рамках данной статьи был проведён всесторонний обзор существующих методов обнаружения стеганографии в мультимедийных файлах, охватывающий широкий спектр подходов, от статистического анализа до продвинутых алгоритмов на основе машинного обучения. Исследование подчеркнуло важность развития и совершенствования методов стеганализа для обеспечения информационной безопасности в условиях постоянно растущего объёма цифрового контента.

Основные выводы

1. Многообразие методов: Существует широкий арсенал инструментов для обнаружения стеганографии, каждый из которых имеет свои преимущества и ограничения в зависимости от контекста их применения.

2. Важность адаптивности: С учётом постоянного развития стеганографических методов, важно, чтобы системы обнаружения могли адаптироваться и обновляться для эффективного реагирования на новые угрозы.

3. Роль машинного обучения: Алгоритмы машинного обучения и искусственного интеллекта играют ключевую роль в разработке более эффективных и надёжных методов стеганализа.

4. Интеграция и сотрудничество: Эффективное обнаружение стеганографии требует интеграции различных методов и технологий, а также сотрудничества между специалистами в области информационной безопасности, исследователями и разработчиками.

Рекомендации:

1. Продолжение исследований: Необходимы дальнейшие исследования для разработки новых и усовершенствования существующих методов обнаружения стеганографии, особенно в свете развития новых технологий и алгоритмов.

2. Разработка стандартов: важно разработать и внедрить стандарты оценки эффективности методов стеганализа, что позволит организациям и специалистам в области безопасности лучше ориентироваться в выборе подходящих инструментов.

3. Образование и подготовка: Усиление внимания к обучению и подготовке специалистов в области обнаружения стеганографии поможет повысить общий уровень защищённости информационных систем.

4. Сотрудничество между секторами: Поощрение сотрудничества между частным, государственным и академическим секторами способствует обмену знаниями и разработке инновационных решений в области обнаружения стеганографии.

Заключительные мысли

В эпоху цифровизации обнаружение стеганографии остаётся критически важной задачей для защиты конфиденциальной информации и предотвращения несанкционированного доступа к данным. Прогресс в разработке и применении методов стеганализа не только укрепит информационную безопасность, но и способствует развитию более безопасного и надёжного цифрового пространства.

Список использованных источников

1. Фридрих, Й. "Steganography in Digital Media: Principles, Algorithms, and Applications". – Кембридж: Издательство Кембриджского университета, 2009, 364 с.

2. Кокс, И. Дж., Миллер, М. Л., Блум, Дж. А., Фридрих, Й., Калкер, Т. "Digital Watermarking and Steganography". – Берлингтон: Морган Кауфманн, 2007, 624 с.

3. Провос, Н., Ханиман, П. "Hide and Seek: An Introduction to Steganography" // IEEE Журнал о безопасности и конфиденциальности, Т. 1, №3, 2003, С. 32-44.

4. Кер, А. Д. "A Review of Steganalysis Techniques: From Image to Audio" // Журнал математического изображения и зрения, Т. 26, №1, 2007, С. 83-102.

5. Бёме, Р., Кирхнер, М. "Counter-Forensics: Attacking Image Forensics" // В книге "Digital Image Forensics". Нью-Йорк, Нью-Йорк: Спрингер, 2015, С. 327-366.

ЖЕЛІДЕГІ ИНЦИДИЕНТТЕРДІ АНЫҚТАУ ЖӘНЕ АҚПАРАТТЫҚ ЖҮЙЕЛЕРДЕГІ БАҚЫЛАУДЫҢ ТИІМДІ АЛГОРИТМДЕРІНЕ ШОЛУ

Асатай Мардан Кунанбайұлы
mardan.asatay@mail.ru
Л.Н.Гумилев атындағы ЕҰУ Ақпараттық технологиялар факультетінің Ақпараттық қауіпсіздік кафедрасы магистранты , Астана, Қазақстан
Ғылыми жетекші – Ташенова Ж.М.

Аннотация: Бақылау жүйелері өзгерістерге жедел жауап беруге, ауытқуларды анықтауға және жүйенің жұмысын жақсартуға мүмкіндік беретін деректерді үнемі бақылау мен талдауға мүмкіндік береді. Бақылау жүйелерінің маңызды құрамдас бөліктері сенсорлар, деректер жинаушылар, талдау алгоритмдері және есептер болып табылады. Бұл мақалада SIEM технологиясының маңызды аспектілері, киберқауіпсіздіктегі және оның құрамдас бөліктеріндегі рөлдер қарастырылады, қазіргі ақпараттық технологиялар әлеміндегі SIEM жүйесінің негізгі рөлі талқыланады, сонымен қатар Siem жүйесінің негізгі компоненттері, соның ішінде деректерді жинау, корреляция жүйелері, бақылау тақталары мен есептер қарастырылады. SIEM жүйелері қауіпсіздік стратегиясының бөлігі болып табылады және ұйымдарға цифрлық ортадағы қауіптерге тиімді қарсы тұруға мүмкіндік береді.

Кілт сөздер: ақпараттық қауіпсіздік, SIEM, IBM, QRadar, желілік қауіпсіздік.

Кіріспе: Қазіргі киберқылмыскерлер компаниялардың қорғаныс жүйелеріне шабуыл жасағанда барған сайын жетілдірілген әдістерді қолданады. Оларға қарсы тұру үшін ақпараттық қауіпсіздік департаменттері күніне көптеген оқиғаларды талдауға және түсіндіруге мәжбүр. IBM желілік қауіпсіздік қатерлерінен қорғау үшін IBM QRadar Security Intelligence Platform шешімін ұсынады, ол қауіпсіздік туралы ақпаратты және оқиғаларды басқаруды (SIEM) және журналдарды біріктіру, қалыптан тыс жағдайларды анықтау, оқиғаларды талдау, оларға жауап беру, параметрлерді басқару және осалдықтарды жою үшін бірыңғай архитектураны ұсынады.

QRadar Security Intelligence Platform бірыңғай архитектурасы журналдарды, желілік ағындарды, пакеттерді, осалдықтарды, сондай-ақ пайдаланушылар мен ресурстар туралы деректерді талдауға мүмкіндік береді. Sense Analytics-ті қолдану нақты уақыттағы ең үлкен қауіптерді, шабуылдарды және осалдықтарды анықтау үшін корреляциялық талдау жүргізуге мүмкіндік береді. Бұл бөлімдерге үлкен деректер ағынынан ең маңызды оқиғаларға басымдық беруге және бөлуге мүмкіндік береді. Шешім оқиғаларға автоматты түрде жауап береді және