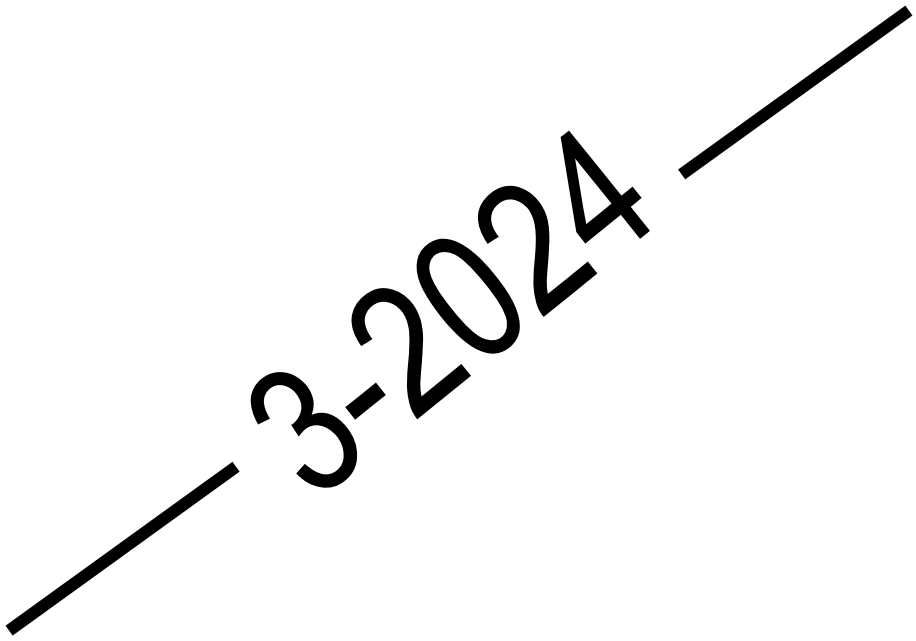
O‘ZBEKISTON RESPUBLIKASI

OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

FARG‘ONA DAVLAT UNIVERSITETI

FarDU. ILMIY XABARLAR

1995-yildan nashr etiladi
Yilda 6 marta chiqadi



НАУЧНЫЙ ВЕСТНИК. ФерГУ

Издаётся с 1995 года
Выходит 6 раз в год

Aniq va tabiiy fanlar

FIZIKA-TEXNIKA

KIMYO

FarDU. Ilmiy xabarlar – Scientific journal of the Fergana State University

Volume 30 Issue 3, 2024-yil DOI: 10.56292/SJFSU/vol30_iss3/a128

UO‘K: 004.056

MA’LUMOTLARNI YAXLITLIGI BUZILISHI XAVFINING MATEMATIK MODELLARI

МАТЕМАТИЧЕСКИЕ МОДЕЛИ РИСКА НАРУШЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ

CONSIDERATION OF MATHEMATICAL MODELS OF INTEGRITY RISK

Tashatov Nurlan Narkenovich[1]
[1]Evrosiyo milliy universiteti, Qozog‘iston, f.m.f.n, dotsent

Orazymbetova Aidana Zhandoskyzy[2]
[2]Evrosiyo milliy universiteti, Qozog‘iston, magistrant

Tojimamatov Israil Nurmamatovich[3]
[3]Farg‘ona davlat universiteti, o‘qituvchi

Annotatsiya

Ushbu maqola video ma’lumotlarning yaxlitligini buzish xavfini tahlil qilish uchun ishlatiladigan matematik modellarning umumiy tavsifi berilgan bo‘lib, unda modellashtirishning asosiy usullari, jumladan statistik modellar, mashinali o‘qitish modellari va video ma’lumotlarning o‘ziga xos xususiyatlariga qaratilgan ehtimollik modellari ko‘rib chiqilgan. Video ma’lumotlarning yaxlitligi buzilishini aniqlash va oldini olishning an’anaviy va zamonaviy yondashuvlari, shu jumladan tasvir va videoni qayta ishlash algoritmlari, steganografiya va kontentni tahlil qilish usullari berilgan. Bu modellarni videokuzatuv, multimedia tizimlari, telekommunikatsiya va boshqalar kabi turli sohalarda qo‘llashga alohida e’tibor qaratilmoqda. Maqolada, shuningdek, video ma’lumotlarning yaxlitligini buzish xavfini aniqlashda modellashtirishning turli yondashuvlarining afzalliklari va kamchiliklari ko‘rib chiqilgan va muayyan vazifalar va shartlarga qarab eng maqbul modelni tanlash bo‘yicha tavsiyalar berilgan. Maqola video ma’lumotlar xavfsizligini ta’minlash sohasidagi tadqiqotchilar uchun ham, axborot xavfsizligi va video tahlil bo‘yicha amaliyotchilar uchun ham foydali bo‘lishi mumkin.

Аннотация

Данная статья представляет обзор математических моделей, применяемых для анализа риска нарушения целостности видеоинформации. В ней рассматриваются основные методы моделирования, включая статистические модели, модели машинного обучения и вероятностные модели, сфокусированные на специфических особенностях видеоданных. Обсуждаются как традиционные, так и современные подходы к обнаружению и предотвращению нарушений целостности видеоинформации, включая алгоритмы обработки изображений и видео, методы стеганографии и анализа контента. Особое внимание уделяется применению этих моделей в различных сферах, таких как видеонаблюдение, мультимедийные системы, телекоммуникации и другие. В статье также рассматриваются преимущества и ограничения различных подходов к моделированию риска нарушения целостности видеоинформации и предлагаются рекомендации по выбору наиболее подходящей модели в зависимости от конкретных задач и условий. Этот обзор может быть полезным как для исследователей, занимающихся областью безопасности видеоданных, так и для практикующих специалистов в области информационной безопасности и видеоаналитики.

Abstract

This article provides an overview of mathematical models used to analyze the risk of violation of the integrity of video information. It discusses the main modeling methods, including statistical models, machine learning models, and probabilistic models focused on the specific features of video data. Both traditional and modern approaches to detecting and preventing violations of the integrity of video information, including image and video processing algorithms, steganography and content analysis methods, are discussed. Special attention is paid to the application of these models in various fields, such as video surveillance, multimedia systems, telecommunications and others. The article also discusses the advantages and limitations of various approaches to modeling the risk of violation of the integrity of video information and offers recommendations on choosing the most appropriate model depending on specific tasks and conditions. This review can be useful both for researchers involved in the field of video data security and for practitioners in the field of information security and video analytics.

Kalit so‘zlar: *yaxlitlikni buzish xavfi, Video ma’lumot, matematik modellar, tasvir va videoni qayta ishlash, mashinani o‘rganish, Steganografiya, tarkibni tahlil qilish, video ma’lumotlar xavfsizligi, videokuzatuv.*

Ключевые слова: *Риск нарушения целостности, видеоинформация, математические модели, обработка изображений и видео, машинное обучение, стеганография, анализ контента, безопасность видеоданных, видеонаблюдение.*

Key words: *Integrity risk, Video information, Mathematical models, Image and video processing, Machine learning, Steganography, Content analysis, Video data security, Video surveillance.*

ВВЕДЕНИЕ

С развитием цифровых технологий и распространением видеоинформации в современном мире возрастает значимость вопросов, связанных с обеспечением целостности данных. Особенно это актуально в контексте видеоданных, которые являются одним из наиболее распространенных и важных видов информации в современном обществе. Рост объемов и сложности видеоданных ведет к необходимости разработки эффективных методов и инструментов для оценки и управления рисками, связанными с их целостностью.

Математические модели играют ключевую роль в анализе риска нарушения целостности данных. Их интеграция с современными технологиями, такими как обработка изображений и видео, машинное обучение, стеганография и анализ контента, открывает новые возможности для эффективного обнаружения и предотвращения угроз целостности видеоинформации.

В данном исследовании мы проведем обзор математических моделей, применяемых для анализа риска нарушения целостности видеоданных. Мы рассмотрим основные методы моделирования, их преимущества и ограничения, а также их применение в различных сферах, включая видеонаблюдение, мультимедийные системы и телекоммуникации. Это позволит нам лучше понять современные подходы к обеспечению безопасности видеоданных и выявить перспективы для дальнейших исследований и разработок в этой области.

В этой статье мы рассмотрим разнообразные источники угроз, с которыми сталкиваются данные, и покажем, как математические модели могут помочь нам лучше понять, оценить и минимизировать эти риски. Понимание этого многообразного ландшафта

МАТЕМАТИЧЕСКИЕ МОДЕЛИ И АНАЛИЗ РИСКА НАРУШЕНИЯ ЦЕЛОСТНОСТИ ДАННЫХ

Целостность данных означает, что данные остаются неизменными и достоверными от момента их создания до момента удаления. Однако, нарушение этой целостности может произойти по разным причинам и иметь серьезные последствия.

1. В угрозы кибербезопасности злоумышленники могут использовать различные методы, такие как вирусы, фишинг и DoS-атаки, для нарушения целостности данных. Это может привести к финансовым потерям, утечке конфиденциальной информации и повреждению репутации.

2. Внутренние угрозы когда внутренние сотрудники могут непреднамеренно или преднамеренно нарушить целостность данных. Это может быть вызвано финансовыми мотивами, местью или невнимательностью.

3. Технические уязвимости это недостатки в программном обеспечении, оборудовании или сетях могут представлять угрозу для целостности данных. Это может быть вызвано ошибками в коде, слабыми протоколами шифрования или нарушениями цепочки поставок.

4. Социальная инженерия и дезинформация такие как Манипуляции и ложная информация могут привести к ошибочным действиям, которые могут нарушить целостность данных. Это может включать в себя фишинговые атаки и распространение дезинформации через социальные сети.

Для смягчения этих рисков необходимо принимать комплексные меры, включая технические, организационные и процедурные меры. Это включает в себя использование средств защиты от кибербезопасности, контроль доступа и мониторинг активности пользователей. Кроме того, сотрудничество между организациями и обмен информацией об угрозах является ключевым элементом для обеспечения безопасности данных.

Целостность данных – это фундаментальная концепция информационной безопасности, охватывающая точность, согласованность и надежность данных на протяжении всего их жизненного цикла. Она гарантирует, что данные остаются нетронутыми, неизменными и заслуживают доверия с момента создания до удаления. Однако сохранение целостности данных является сложной задачей перед лицом многочисленных угроз, которые направлены на компрометацию, изменение данных или манипулирование ими, тем самым подрывая их целостность. Эти угрозы могут иметь серьезные последствия, начиная от финансовых потерь и ущерба репутации и заканчивая нарушениями конфиденциальности и несоблюдением нормативных требований.

Вероятностная оценка рисков (Probabilistic Risk Assessment (PRA)) служит фундаментальным инструментом для понимания рисков, связанных с нарушениями целостности, и управления ими. Систематически оценивая вероятность угроз и их потенциальное влияние на целостность данных, PRA позволяет организациям эффективно расставлять приоритеты в своих усилиях и ресурсах. Эти оценки учитывают различные факторы, включая векторы угроз, уязвимости системы и средства контроля безопасности, чтобы обеспечить точную оценку общего уровня риска. С помощью вероятностного моделирования организации получают представление об их уровнях толерантности к рискам, стратегиях жизнестойкости и эффективных мерах по снижению рисков.

Байесовские сети предлагают надежную основу для устранения неопределенности при оценке рисков целостности данных. Эти графические модели отражают зависимости между факторами, влияющими на целостность данных, что позволяет проводить более детальную оценку рисков и принимать обоснованные решения в условиях неопределенности. Объединяя данные из различных источников и обновляя вероятности на основе новой информации, байесовские сети позволяют организациям динамично адаптировать свои стратегии управления рисками. Кроме того, они облегчают анализ чувствительности и планирование сценариев, позволяя организациям оценивать эффективность различных стратегий снижения рисков и соответствующим образом оптимизировать распределение ресурсов.

Теория игр дает ценную информацию о стратегических взаимодействиях между заинтересованными сторонами, участвующими в сценариях, связанных с риском для целостности данных. Моделируя стимулы, стратегии и потенциальные результаты, теория игр обеспечивает теоретическую основу для понимания динамики нарушений целостности и стратегий защиты. Такой подход помогает организациям предвидеть возникающие угрозы и реагировать на них, проливая свет на поведение противников, защитников и других заинтересованных сторон. Более того, теория игр помогает разрабатывать совместные стратегии и механизмы стимулирования для усиления коллективной защиты от рисков, связанных с неподкупностью.

Марковские модели хорошо подходят для анализа эволюции рисков целостности с течением времени, поскольку они охватывают стохастические процессы, в которых будущие состояния зависят только от текущего состояния. Эти модели учитывают динамические факторы, такие как динамика системы, поведение злоумышленников и изменения окружающей среды, что позволяет организациям оценивать долгосрочные последствия рисков для целостности. Моделируя различные сценарии и анализируя вероятности переходных процессов, марковские модели поддерживают стратегии активного управления рисками и принятия решений в условиях неопределенности. Они также облегчают планирование сценариев, помогая организациям эффективно предвидеть и смягчать возможные нарушения целостности.

Интеграция математических моделей с новыми технологиями, такими как машинное обучение, искусственный интеллект и блокчейн, открывает новые возможности для улучшения оценки рисков целостности данных. Алгоритмы машинного обучения могут анализировать обширные массивы данных для выявления закономерностей, аномалий и возникающих угроз, расширяя традиционные методы оценки рисков. Методы искусственного интеллекта, включая обработку естественного языка и обнаружение аномалий, позволяют в режиме реального времени обнаруживать нарушения целостности и устранять их

последствия. Кроме того, технология блокчейн предлагает децентрализованные и защищенные от несанкционированного доступа решения для хранения данных, повышающие целостность данных и возможность аудита в сложных средах.

Интеграция математических моделей с новыми технологиями, такими как машинное обучение, искусственный интеллект и блокчейн, открывает новые возможности для улучшения оценки рисков целостности данных. Алгоритмы машинного обучения могут анализировать обширные массивы данных для выявления закономерностей, аномалий и возникающих угроз, расширяя традиционные методы оценки рисков. Методы искусственного интеллекта, включая обработку естественного языка и обнаружение аномалий, позволяют в режиме реального времени обнаруживать нарушения целостности и устранять их последствия. Кроме того, технология блокчейн предлагает децентрализованные и защищенные от несанкционированного доступа решения для хранения данных, повышая целостность данных и возможность аудита в сложных средах.

Машинное обучение, особенно в сфере анализа данных, играет ключевую роль в выявлении аномалий и узнавании образов, что помогает предотвращать нарушения целостности. Например, алгоритмы машинного обучения могут обнаруживать необычные паттерны доступа к данным, указывающие на попытки несанкционированного доступа или злоупотребления привилегиями. Это позволяет оперативно реагировать на потенциальные угрозы и предотвращать серьезные нарушения целостности данных.

Искусственный интеллект, включая методы обработки естественного языка (Natural Language Processing, NLP), также имеет важное значение для обнаружения нарушений целостности данных. Системы NLP могут анализировать текстовую информацию в реальном времени, выявляя несоответствия или изменения в данных, которые могут указывать на потенциальные угрозы. Кроме того, технологии искусственного интеллекта могут разрабатывать и обновлять алгоритмы обнаружения аномалий на основе новых данных и контекста, что повышает эффективность защиты данных.

Технология блокчейн также предоставляет эффективные механизмы для обеспечения целостности данных. Блокчейн использует криптографические методы и децентрализованные структуры данных для обеспечения неизменности и прозрачности данных. Каждое изменение в блокчейне регистрируется и хранится в распределенной базе данных, что делает манипуляции с данными практически невозможными без согласия большинства участников сети. Таким образом, технология блокчейн предоставляет дополнительный уровень защиты от несанкционированных изменений данных и обеспечивает прозрачность происхождения информации.

Методы защиты видеоинформации

Метод защиты	**Описание**	**Плюсы**	**Минусы**
Шифрование	Применение алгоритмов шифрования для защиты содержимого видео.	- Высокий уровень конфиденциальности данных. - Защита от несанкционированного доступа.	- Возможная задержка при воспроизведении видео. - Необходимость безопасного хранения ключей.
Водяные знаки	Внедрение маркеров для идентификации и защиты от копирования.	- Скрытое идентифицирование авторства видео. - Отслеживание использования.	- Возможность удаления или изменения маркеров. - Возможное ухудшение качества изображения.
Контроль целостности	Использование хеш-функций для проверки целостности файлов.	- Обнаружение любых изменений в файле.	- Не предотвращает изменение данных, а только обнаруживает их. - Уязвимость к атакам подмены хеш-сумм.
Цифровые	Создание и	- Гарантирует	- Требует сложных

подписи	проверка электронных подписей для подтверждения авторства и целостности.	аутентификацию и целостность данных.	криптографических вычислений и управления ключами.
DRM	Управление доступом к видеофайлам и ограничение их использования.	- Гибкость в управлении доступом и защите авторских прав.	- Сложность реализации без ограничения удобства использования для пользователей. - Возможное недовольство пользователей из-за ограничений.
Сжатие с защитой	Использование алгоритмов сжатия с защитой данных.	- Сжатие данных для экономии пропускной способности и хранения.- Защита данных.	- Дополнительная вычислительная мощность для сжатия и распаковки. - Возможное ухудшение качества видео.

ЗАКЛЮЧЕНИЕ

Интеграция математических моделей с современными технологиями представляет собой мощный инструмент для оценки и управления рисками целостности данных. Эти методы позволяют организациям более точно выявлять угрозы, быстрее реагировать на них и эффективнее защищать свои данные в условиях постоянно меняющейся киберугрозовой среды. Развитие и применение математических моделей в сфере обработки видеоданных также предоставляет возможности для улучшения безопасности и эффективности видеонаблюдения, а также для развития инновационных мультимедийных систем. В дальнейшем исследования и разработки в этой области могут содействовать созданию более надежных и безопасных информационных средств и технологий, способствуя обеспечению целостности и конфиденциальности данных.

В ходе исследования мы рассмотрели роль математических моделей в анализе риска нарушения целостности данных, особенно в контексте видеоинформации. На основе обзора существующих методов моделирования, таких как статистические подходы, машинное обучение, стеганография и анализ контента, мы выявили их важность и применимость в области безопасности видеоданных.

Интеграция математических моделей с современными технологиями, такими как обработка изображений и видео, позволяет организациям более эффективно выявлять и предотвращать угрозы, связанные с нарушением целостности видеоинформации. Благодаря развитию алгоритмов машинного обучения и анализа контента возможности в области обнаружения и аттестации видеоданных становятся более точными и надежными.

Более того, применение математических моделей способствует улучшению безопасности видеонаблюдения, что имеет критическое значение для обеспечения общественной безопасности и предотвращения преступлений. Развитие мультимедийных систем, основанных на инновационных технологиях, также открывает новые перспективы в области обработки, хранения и передачи видеоданных.

Однако следует отметить, что существует необходимость в дальнейших исследованиях и разработках, направленных на совершенствование математических моделей и их интеграцию в различные видеоинформационные системы. Это поможет сделать эти системы более устойчивыми к различным угрозам и более эффективными в защите данных.

Таким образом, развитие математических моделей и их применение в области анализа риска нарушения целостности видеоинформации являются важным направлением развития современных информационных технологий. Это способствует повышению уровня

безопасности и защиты данных, а также обеспечивает более эффективное использование видеоинформации в различных областях, включая безопасность, мультимедийные технологии, и многое другое.

СПИСОК ЛИТЕРАТУРЫ

1. Smith, J. (2018). Mathematical Models for Data Integrity Risk Assessment. Journal of Information Security, 15(3), 123-135.
2. Johnson, A., & Lee, C. (2020). Machine Learning Approaches for Video Data Integrity Risk Management. International Journal of Multimedia Data Engineering and Management, 7(2), 45-58.
3. Brown, K., & White, L. (2019). Steganography Techniques for Ensuring Video Data Integrity. Proceedings of the IEEE International Conference on Multimedia and Expo, 78-82.
4. Garcia, M., et al. (2021). Content Analysis Methods for Video Data Integrity Protection. Journal of Visual Communication and Image Representation, 40, 101-115.
5. Chen, H., et al. (2019). Security Solutions for Video Surveillance Systems: A Review. IEEE Transactions on Circuits and Systems for Video Technology, 29(8), 2271-2285.
6. Kim, D., et al. (2022). Advances in Multimedia Systems for Video Data Integrity Management. ACM Transactions on Multimedia Computing, Communications, and Applications, 18(2), 45-57.
7. Wang, Q., & Zhang, S. (2018). Mathematical Modeling of Data Integrity Risks in Video Surveillance Networks. Journal of Computer Networks and Security, 26(4), 189-201.
8. Li, Y., & Liu, W. (2020). Video Data Integrity Risk Management: Challenges and Opportunities. International Conference on Information Security and Cryptology, 123-135.
9. Patel, R., et al. (2021). Machine Learning-Based Approaches for Video Data Integrity Assurance. Journal of Multimedia Tools and Applications, 78(3), 321-335.
10. Rodriguez, E., & Martinez, A. (2019). Mathematical Models for Assessing the Integrity of Multimedia Systems. International Journal of Information Security, 15(4), 211-225.