УДК 004.056

Железнов Макар Эдуардович
студент кафедры «Институт сквозных технологий (интеллектуальные медиатехнологии)»
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия
Научный руководитель:
Кадомцев Максим Игоревич
доцент кафедры «Институт сквозных технологий»
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

Безопасность мультимедийной информации: технология защиты интеллектуальных медиатехнологий

Аннотация. При увеличении информации в сети, возросли и требования к её защите. На сегодняшний день важной проблемой является обеспечение безопасности информации в сети, так как появляется все больше методов несанкционированного доступа к данным. Мультимедийные данные являются значениями данных во всем потоке информации. Для их защиты необходимо разработать алгоритм аутентификации, который предназначен для обхода любых искажений данных и их кражи. В данной статье проведем анализ методов защиты информации в сети, а также подробно рассмотрим технологии защиты мультимедийных данных. Так, проблема безопасности мультимедийных данных в сети остается актуальной и постоянно усложняется с развитием технологий обработки и передачи информации. Рассмотренные в данной статье методы шифрования данных являются эффективными.

Ключевые слова: мультимедийные данные, шифрование данных, информация, защита данных, несанкционированный доступ, искажение данных, медиатехнологии.

Jeleznov Makar Eduardovich
student of the department "Institute of End to-end Technologies
(Intelligent Media technologies)"
Don State Technical University
Rostov-on-Don, Russia
Scientific Supervisor:
Kadomcev Maxim Igorevich
Associate Professor of the Department of "Institute of End-to-end Technologies"
Don State Technical University
Rostov-on-Don, Russia

Multimedia information security: Smart media technology protection technology

Abstract. With the increase in information on the web, the requirements for its protection have also increased. Today, ensuring the security of information on the network is an important problem, as there are more and more methods of unauthorized access to data. Multimedia data is the meaning of the data in the entire information stream. To protect them, it is necessary to develop an authentication algorithm that is designed to bypass any data distortion and theft. In this article, we will analyze the methods of protecting information on the web, as well as consider in detail the technologies for protecting multimedia data. Thus, the problem of multimedia data security on the Web remains relevant and is constantly becoming more complicated with the development of information processing and transmission technologies. The data encryption methods discussed in this article are effective.

Keywords: multimedia data, data encryption, information, data protection, unauthorized

access, data distortion, media technologies.

Информация играет ведущую роль в любой сфере деятельности. Со временем данных становится все больше, поэтому без внедрения баз данных не обходится ни одна компания. Однако при увеличении информации в сети, возросли и требования к её защите.

На сегодняшний день важной проблемой является обеспечение безопасности информации в сети, так как появляется все больше методов несанкционированного доступа к данным. Данная проблема является актуальной, так как уровень значения информации в современном обществе высок.

Целью данной статьи является анализ методов защиты информации в сети, а также подробное рассмотрение технологии защиты мультимедийных данных.

Мультимедийные данные являются значениями данных во всем потоке информации. К мультимедийным данным относятся изображения, видеозаписи и аудиозаписи. Для их защиты необходимо разработать алгоритм аутентификации, который предназначен для обхода любых искажений данных и их кражи. [1]

Первым методом защиты информации в сети является метод шифрования данных. Процесс шифрования позволяет скрыть содержимое текста, после чего дешифровать его сможет только человек, имеющий правильный закрытый ключ.

При шифровании мультимедийных данных алгоритм, по которому протекает процесс шифровки, должен быть устойчивым к ошибкам и достаточно быстрым. Самым важным требованием к алгоритму шифрования является его «выносливость» к взлому.

Атаки на мультимедийные данные подразделяются на четыре вида:

1. Злоумышленник получил зашифрованный текст, его целью является найти ключ для дешифровки данных и получения оригинального текста;
2. Злоумышленник получил несколько зашифрованных текста и несколько оригинальных текстов, его целью является поиск ключа шифрования для раскрытия им всех зашифрованных данных;
3. Злоумышленник, имея зашифрованный текст, может на выбор получить доступ к дешифрованному тексту, соответственно, может выбрать именно тот текст, который имеет в закрытом виде, следовательно, найдет метод шифрования и получит ключ шифровки;
4. В серверах с открытым ключом злоумышленник, получив доступ к зашифрованному тексту, может дешифровать его, так как дешифрованный текст также хранится на этом сервере.[2]

Так, чтобы противостоят несанкционированному доступу к базам данных, необходимо применять для защиты информации действенную систему шифрования.

Одним из действенных методов является метод хеширования, который заключается в преобразовании данных различной длины в значение определенной длины с помощью хэш-функций или шифрования с открытым ключом. Важно при использовании данного вида шифрования сохранить значение мультимедийных данных, то есть никак их не исказить.

Хеш-функция должна обладать следующими особенностями, чтобы информация была под защитой на необходимом уровне:

1. Хеш-функция не должна искажать данные при небольших изменениях содержания текста;
2. Хеш-функция должна оперативно реагировать на попытку несанкционированного доступа к данным;
3. Хеш-функция должна определять более уязвимые для атаки места, а также определять точное место проникновения в базу данных при несанкционированном доступе;
4. Хеш-функция должна быть под надежной защитой от атак, чтобы она не

была «обманута» злоумышленниками;

5. Получив доступ к значениям, которые были получены с помощью хеш-функции, злоумышленник не должен получить секретный ключ.[3]

Методом защиты авторских прав на созданную информацию, является метод применения водяного знака. Это незаметный символ, который добавляется к данным и является способом идентификации автора текста. Водяные знаки также должны быть защищены от злоумышленников, так как при доступе к таким идентификаторам, мошенники могут создавать тексты различного содержания и подписывать их от имени автора, на чей водяной знак было совершено нападение.

Защита данных в сети – важная задача, которая повышает безопасность мультимедийной информации. Данную проблему часто рассматривают авторы в научных статьях. Действенным методом в области защиты мультимедийной информации от несанкционированного доступа к ним злоумышленников является способ блочного шифрования дискретных данных, предложенный авторами В.М.Масловским, А.А.Молдовян, Н.А.Молдовян. [4]

Целью изобретения является улучшение показателей работы и скорости метода шифрования. Способ шифрования данных предполагает разделение ключа шифрования на совокупность подключей, а также разделение блока данных на подблоки. При использовании данного способа шифрования преобразование информации протекает с уменьшением числа преобразований данных, однако стойкость к несанкционированным атакам должна повышаться, также повышается и скорость шифрования данных.

Авторы предлагают следующую схему шифрования, представленную на рисунке 1.

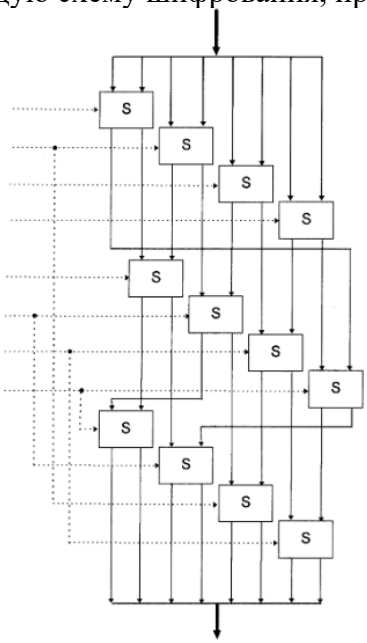

Рисунок 1 – Обобщенная схема шифрования

На рисунке 1 представлен один раунд шифрования. В зависимости от нужной скорости шифрования можно задавать любое количество раундов в диапазоне от 6 до 20 и более раундов.

Таким образом, проблема безопасности мультимедийных данных в сети остается актуальной и постоянно усложняется с развитием технологий обработки и передачи информации. Рассмотренные в данной статье методы шифрования данных являются эффективными. Задача увеличения скорости шифрования достигнута с применением метода разбиения блока данных на подблоки и формирования ключа шифрования в виде совокупности подключей.

Список источников

1. Бабенко, Л. К. Современные алгоритмы блочного шифрования и методы их анализа / Л.К. Бабенко, Е.А. Ищукова. - М.: Гелиос АРВ, 2006. – С. 376-386;
2. Баричев, С. Г. Основы современной криптографии / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов. - Москва: СИНТЕГ, 2011. – С. 176-185;
3. Байер, Доминик Microsoft ASP .NET. Обеспечение безопасности / Доминик Байер. - М.: Питер, Русская Редакция, 2008. – С. 430-448;
4. Патент RU 2140710 C1 – Способ блочного шифрования дискретных данных. В.М.Масловский, А.А.Молдовян, Н.А.Молдовян. https://patents.google.com/patent/RU2140710C1/ru (дата обращения 20.09.2025г.).