Исследование совместного использования алгоритмов сжатия и шифрования данных

Сергей Владимирович Антоненко
студент
Московский государственный технический университет им Баумана Н.Э.
Москва, Россия
antonenkosv@student.bmstu.ru

Роман Дмитриевич Сим
студент
Московский государственный технический университет им. Баумана Н.Э.
Москва, Россия
esengulovrt@student.bmstu.ru

Поступила 16.03.2023
Принята 30.04.2023

Аннотация

В данной статье представлено исследование о способах обеспечения скорости и безопасности передачи данных путем комбинированного использования шифрования и сжатия данных. В статье рассматриваются основные принципы и преимущества каждого из этих методов отдельно, а также объясняется необходимость их совместного применения. Авторы статьи анализируют различные алгоритмы сжатия и шифрования данных и исследуют их совместное влияние на производительность и безопасность передачи. Представлены результаты экспериментов и сравнительные анализы различных комбинаций алгоритмов сжатия и шифрования данных. В итоге статьи приводятся рекомендации по выбору оптимальной комбинации алгоритмов для конкретных сценариев передачи данных с целью достижения максимальной эффективности и безопасности. Эта статья является ценным ресурсом для исследователей, разработчиков и специалистов в области информационной безопасности, которые интересуются оптимизацией процесса передачи данных и обеспечением их защиты. Дальнейшее развитие этого программного продукта включает модернизацию и тестирование с целью нахождения более оптимальных последовательностей выполнения действий и подбора более подходящих алгоритмов сжатия и шифрования. Этот процесс позволит продукту достичь лучшей производительности и эффективности при одновременном обеспечении высокого уровня безопасности данных.

Ключевые слова

шифрование, сжатие, совместное использование шифрования и сжатия данных.

Введение

В современном информационном обществе передача данных играет важную роль, охватывая практически все сферы нашей жизни. Будь то обмен информацией через интернет, передача файлов или электронная почта, основные требования при передаче данных остаются неизменными: сохранение целостности, обеспечение безопасности и достижение оптимальной скорости передачи.

Для достижения безопасности при передаче данных используются различные алгоритмы шифрования, а для оптимальной скорости передачи применяют алгоритмы сжатия данных.

Рационально применять не только один отдельный алгоритм или технологию, а совместно использовать несколько подходов. В частности, алгоритмы шифрования и сжатия данных играют ключевую роль в обеспечении безопасности и оптимизации передачи данных.

Исходя из вышесказанного, становится очевидно, что есть необходимость в разработке приложения, которое объединяет в себе алгоритмы шифрования и сжатия данных.

Материалы и методы исследования

Способы обеспечения скорости и безопасности передачи данных.

Алгоритмы шифрования позволяют защитить данные от несанкционированного доступа, обеспечивая их конфиденциальность. Они преобразуют данные в зашифрованный вид, который может быть восстановлен только с помощью соответствующего ключа (Алферов, 2002).

Алгоритмы сжатия данных позволяют уменьшить объем передаваемой информации, что ведет к повышению скорости передачи. Они исследуют структуру данных и удаляют избыточность, повторяющиеся элементы или несущественные детали, сохраняя при этом основную информацию (Бабаш, 2007). Это позволяет сократить время передачи данных и снизить нагрузку на сеть.

Таким образом, совместное применение алгоритмов шифрования и сжатия данных является неотъемлемой частью современных систем передачи данных. Они обеспечивают сохранение целостности, обеспечивают конфиденциальность и эффективность передачи информации различного формата. От выбора и оптимального сочетания этих алгоритмов зависит безопасность и эффективность передачи данных в различных сферах деятельности (Гатченко, 2012).

Целью настоящей работы является разработка, реализация и исследование метода совместного применения алгоритмов сжатия и шифрования данных.

Эффективность предложенного метода зависит от последовательности выполнения его этапов и алгоритмов, реализуемых на каждом их них. Выбор последовательности действий имеет прямое влияние на итоговый текст, получаемый в результате работы метода.

Базовыми операциями разработанного метода являются сжатие и шифрование данных.

Результаты и обсуждение

Выбор алгоритмов сжатия и шифрования в значительной степени обосновывается типом исходных данных. Результат обработки данных также зависит и от последовательности выполнения этих алгоритмов.

Понимая это, мы, для определения наиболее подходящего способа, предложили два варианта, в которых меняется последовательность итераций.

В первом варианте использование шифрования с последующим сжатием данных, а во втором варианте использование сжатия с последующим шифрованием данных.

Для проведения сравнительного анализа двух вариантов, передадим в программные реализации текстовые данные различного объема, где в качестве шифрования данных выберем алгоритм RSA, а для сжатия данных используем алгоритм Хаффмана. Результаты сравнения представлены в таблице 1 (Баричев , 2006; Шнайер, 2002; Сэломон, 2006; Халид Сайуд, 2021; Марк Нельсон, 2022; Коутинхо, 2001; Венбо Мао, 2005):

Таблица 1. Сравнение двух вариантов алгоритма шифрования совместно с сжатием данных

Размер исходного текстового файла	Вариант 1: шифрование с последующим сжатием	Вариант 2: сжатие с последующим шифрованием
8000 байт	5800 байт (72.5%)	6400 байт (80%)
48000 байт	33500 байт (69.7%)	38000 байт (79%)
80 000 байт	54200 байт (68%)	62000 байт (78%)

Для большей наглядности различия между двумя вариантами алгоритма представлены в виде графика, изображенного на рисунке 1.

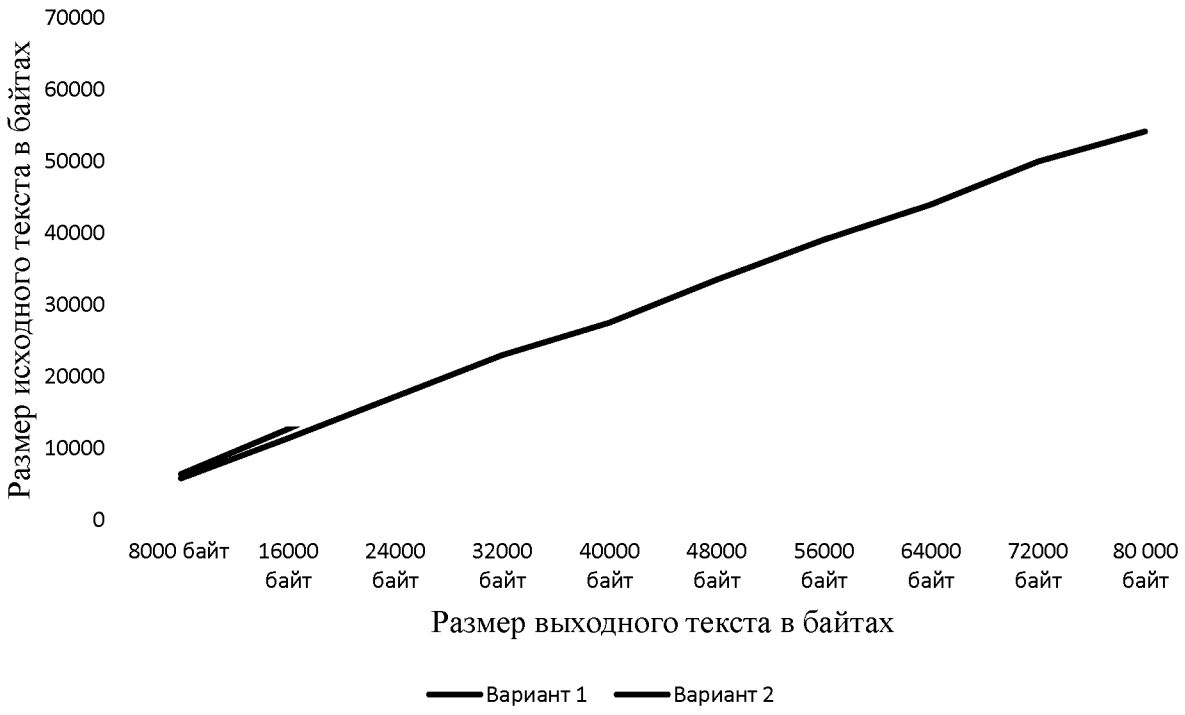

Рисунок 1. Различие между алгоритмами

В результате исследования было обнаружено, что первый вариант демонстрирует более высокую эффективность и лучшие результаты по сравнению со вторым. Это основывается на наблюдениях и анализе данных, полученных в ходе эксперимента.

В результате был разработан программный продукт, который в дальнейшем будет модернизироваться.

Для достижения наиболее эффективного шифрования и оптимального сжатия данных, в зависимости от получаемых данных, программа определяет какой алгоритм шифрования и сжатия данных следует использовать. Таким образом проблема оптимизации скорости передачи данных для быстрой и эффективной коммуникации, а также проблема надежности передаваемых данных решается. Для определения типа данных программа читает расширение файла и в зависимости от расширения подбирает оптимальные алгоритмы.

Заключение

В данной статье был рассмотрен разработанный программный продукт, который представляет функциональность совместного сжатия и шифрования данных. Этот продукт являет собой значимый шаг в направлении обеспечения безопасности и оптимизации хранения информации.

Модернизация программного продукта может включать анализ и сравнение различных алгоритмов сжатия и шифрования, эксперименты с разными параметрами и настройками, а также применение методов машинного обучения и оптимизации для определения оптимальных решений. Тестирование продукта поможет проверить его функциональность, стабильность и безопасность, а также выявить возможные уязвимости и улучшить его производительность.

Таким образом, разработка и модернизация данного программного продукта способствуют развитию и совершенствованию области сжатия и шифрования данных, а также предоставляют пользователю оптимальные и надежные инструменты для обработки и защиты информации.

Список литературы

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С. Основы криптографии. Учебное пособие. 2-е изд. М.: Гелиос АРВ, 2002. 480 с.
2. Бабаш А.В. Криптография. Под редакцией Бабаш А.В., Шанкин Г.П. М.: СОЛОН-Р, 2007. 512 с. (Серия книг «Аспекты защиты»). ISBN 5-93455- 135-3.
3. Гатченко Н.А., Исаев А.С., Яковлев А.Д. Криптографическая защита информации. СПб: НИУ ИТМО, 2012. 142 с.
4. Баричев С.Г., Серов Р.Е. Основы современной криптографии. Учебное пособие. М.: Горячая Линия Телеком, 2006. 152 с.
5. Шнайер Б. Прикладная криптография: Протоколы, алгоритмы, исход. тексты на яз. Си. Москва: Триумф, 2002. 815 с.
6. Сэломон Д. Сжатие данных, изображений и звука: пер. с англ. Чепыжова В.В., Москва: Техносфера, 2006. 365 с.
7. Халид Сайуд. Введение в сжатие данных. Под изд. Моргана Кауфманна. Сан-Франциско: 2000. 636 с.; 25 см.
8. Марк Нельсон, Жан-Лу. Gailly "Data Compression: Techniques and Applications".
9. Коутинхо С. Введение в теорию чисел. Алгоритм RSA. Перевод с англ. Кулешова С.А. под редакцией Ландо С.К. М.: ПОСТМАРКЕТ, Москва, 2001. 328 с.
10. Венбо Мао. Современная криптография: теория и практика; Компания Hewlett-Packard; пер. с англ. и ред. Клюшина Д.А. Вильямс, 2005. ГПП Печ. Двор. 763 с.

Study of joint use of data compression and encryption algorithms

Sergey V. Antonenko
Student
Bauman moscow state technical university
Moscow, Russia
antonenkosv@student.bmstu.ru

Roman D. Sim
Student
Bauman moscow state technical university
Moscow, Russia
esengulovrt@student.bmstu.ru

Received 16.03.2023
Accepted 30.04.2023

Abstract

This article presents a study on how to ensure the speed and security of data transfer through the combined use of encryption and data compression. The article discusses the main principles and advantages of each of these methods separately, and also explains the need for their combined application. The authors of the article analyze various algorithms for data compression and encryption and investigate their combined impact on the performance and security of data transmission. The results of experiments and comparative analyzes of various combinations of data compression and encryption algorithms are presented. As a result of the article, recommendations are given for choosing the optimal combination of algorithms for specific data transfer scenarios in order to achieve maximum efficiency and security. This article is a valuable resource for researchers, developers, and information security professionals who are interested in optimizing the data transfer process and ensuring its protection. Further development of this software product includes modernization and testing in order to find more optimal sequences of actions and select more suitable compression and encryption algorithms. This process will allow the product to achieve better performance and efficiency while maintaining a high level of data security.

Keywords

encryption, compression, combined use of encryption and data compression.

References

1. Alferov A.P., Zubov A.YU., Kuz'min A.S. Osnovy kriptografii. Uchebnoe posobie. 2-e izd. M.: Gelios ARV, 2002. 480 s.
2. Babash A.V. Kriptografiya. Pod redakciej Babash A.V., SHankin G.P. M.: SOLON-R, 2007. 512 s. (Seriya knig «Aspekty zashchity»). ISBN 5-93455- 135-3.
3. Gatchenko N.A., Isaev A.S., YAkovlev A.D. Kriptograficheskaya zashchita informacii. SPb: NIU ITMO, 2012. 142 s.
4. Barichev S.G., Serov R.E. Osnovy sovremennoj kriptografii. Uchebnoe posobie. M.: Goryachaya Liniya Telekom, 2006. 152 s.
5. SHnajer B. Prikladnaya kriptografiya: Protokoly, algoritmy, iskhod. teksty na yaz. Si. Moskva: Triumf, 2002. 815 s.
6. Selomon D. Szhatie dannyh, izobrazhenij i zvuka: per. s angl. CHepyzhova V.V., Moskva: Tekhnosfera, 2006. 365 c.
7. Halid Sajud. Vvedenie v szhatie dannyh. Pod izd. Morgana Kaufmanna. San-Francisko: 2000. 636 s.; 25 sm.
8. Mark Nel'son, ZHan-Lu. Gailly "Data Compression: Techniques and Applications".
9. Koutinho S. Vvedenie v teoriyu chisel. Algoritm RSA. Perevod s angl. Kuleshova S.A. pod redakciej Lando S.K. M.: POSTMARKET, Moskva, 2001. 328 s.
10. Venbo Mao. Sovremennaya kriptografiya: teoriya i praktika; Kompaniya Hewlett-Packard; per. s angl. i red. Klyushina D.A. Vil'yams, 2005. GPP Pech. Dvor. 763 s.