«Информатика, кибернетика и вычислительная техника»

Научная статья
УДК 004.891.3
DOI: 10.17072/1993-0550-2023-2-65-71

Искусственный интеллект для контроля передачи данных в тактическом звене управления с использованием многослойного и многопотокового шифрования геопространственной обстановки

Ксения Вячеславовна Иванова[1], Алексей Федорович Сальников[2], Роман Викторович Мормуль[3]
[1] Пермский военный институт войск национальной гвардии Российской Федерации, Пермь, Россия
[2] Пермский национальный исследовательский политехнический университет, Пермь, Россия
[3] Пермский военный институт войск национальной гвардии Российской Федерации, Пермь, Россия
[1]ksgorbunova@yandex.ru, https://orcid.org/0000-0003-1007-9237
[2]afsalnikov@mail.ru, https://orcid.org/0000-0002-6345-8137
[3]rmormul@yandex.ru, https://orcid.org/0000-0002-9514-0983

Аннотация. В работе представлена разработка комплекса научно-технических решений, позволяющих контролировать передачу данных. В частности, рассмотрена возможность использования криптографических алгоритмов многослойного шифрования, отображающих геопространственную обстановку местности. Созданы многопотоковые вычислительные программы, позволяющие маскировать геопространственную обстановку с различной интенсивностью белого шума.

Ключевые слова: *шифрование; криптография; AES; RSA; белый шум; маскирование*

Для цитирования: *Иванова К. В., Сальников А. Ф., Мормуль Р. В.* Искусственный интеллект для контроля передачи данных в тактическом звене управления с использованием многослойного и многопотокового шифрования геопространственной обстановки // Вестник Пермского университета. Математика. Механика. Информатика. 2023. Вып. 2(61). С. 65–71. DOI: 10.17072/1993-0550-2023-2-65-71.

Статья поступила в редакцию 05.12.2022; одобрена после рецензирования 06.02.2023; принята к публикации 17.06.2023.

«Computer Science, Cybernetics and Computing»

Research article

Artificial Intelligence for Data Transfer Control in Tactical Command Element Using Multilayer and Multithreaded Geospatial Enviroment Encryption

Kseniya V. Ivanova[1], Aleksei F. Salnikov[2], Roman V. Mormul[3]
[1]Perm Military Institute of National Guard Troops, Perm, Russia
[2]Perm National Research Polytechnic University, Perm, Russia
[3]Perm Military Institute of National Guard Troops, Perm, Russia

[1]ksgorbunova@yandex.ru, https://orcid.org/0000-0003-1007-9237
[2]afsalnikov@mail.ru, https://orcid.org/0000-0002-6345-8137
[3]rmormul@yandex.ru, https://orcid.org/0000-0002-9514-0983

Abstract. The paper presents the development of a scientific and technical solutions to control data transmission set. In particular, the using cryptographic multilayer encryption algorithms possibility is considered. Algorithms can display the geospatial terrain situation. Multithreaded computational programs allowing to mask geospatial environment with various white noise intensity were created.

Keywords: *encryption; cryptographic; AES; RSA; white noise; masking*

For citation: *Ivanova K.V., Salnikov A.F., Mormul R.V.* Artificial Intelligence for Data Transfer Control in Tactical Command Element Using Multilayer and Multithreaded Geospatial Enviroment Encryption. Bulletin of Perm University. Mathematics. Mechanics. Computer Science. 2023;2(61):65-71. (In Russ.). DOI: 10.17072/1993-0550-2023-2-65-71.

The article was submitted 05.12.2022; approved after reviewing 06.02.2023; accepted for publication 17.06.2023.

Введение

В настоящее время войска национальной гвардии России выполняют огромное количество служебно-боевых задач и их успешное выполнение во многом зависит от правильной оценки тактических свойств местности, умелого их использования командирами и военнослужащими в различных условиях обстановки, умения быстро и правильно ориентироваться на местности. Вопросами изучения и оценки местности в интересах организации и проведения служебно-боевых задач, ориентирования на ней в различных условиях обстановки занимается военная топография. Результаты исследования будут заключаться в экономической эффективности применения технологии искусственного интеллекта при многослойном шифровании геопространственной обстановки и минимизации временных затрат при формировании зашифрованных данных.

Рассмотрим анализ существующих криптографических алгоритмов многопотокового шифрования графических данных.

1. Анализ существующих криптографических алгоритмов многопотокового шифрования графических данных

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы [1].

В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения. Криптографические методы могут помочь обеспечить безопасность, но только на эти методы надеяться не следует [1].

Шифрование – процесс преобразования исходного текста, который носит также название открытого текста, в шифрованный текст.

Расшифровывание – процесс, обратный шифрованию. На основе ключа шифрованный текст преобразуется в исходный.

Криптографические методы могут применяться для решений следующих проблем безопасности:

1) конфиденциальности передаваемых/хранимых данных;
2) аутентификации;
3) целостности хранимых и передаваемых данных;
4) обеспечения подлинности документов.

Существующие алгоритмы шифрования:

1. Симметричное шифрование:
   – потоковый шифратор;
   – блочный шифратор;
   – алгоритм блочного шифрования AES.
2. Асимметричное шифрование:
   – алгоритм шифрования RSA.

В работе [2] предлагается рассмотреть преимущества и недостатки симметричных и асимметричных алгоритмов шифрования.

Алгоритмы симметричного шифрования намного быстрее и требуют меньше вычислительной мощности, но их недостатком является распределение ключей. В свою очередь, асимметричное шифрование решает проблему распределения ключей, используя открытые ключи для шифрования, а приватные – для дешифрования [2].

В результате, алгоритмы симметричного шифрования намного быстрее и требуют меньше вычислительной мощности, но их основным недостатком является распределение ключей.

Поскольку один и тот же ключ используется для шифрования и дешифрования информации, этот ключ нужно передать всем, кому потребуется доступ, что естественно создает определенные риски, на рис. 1 представлено сравнение симметричного и асимметричного шифрования [3].

Критерий сравнения	Ассиметричное шифрование	Симметричное шифрование
Вид ключа	Применяется открытый и закрытый ключи	Применяется один ключ для защиты данных несколькими адресатами
Способ обмена ключами	Открытый ключ общедоступен, закрытый ключ доступен только владельцу	Применяется защищенный механизм нестандартный
Производительность	Сложный алгоритм негативно отражается на скорости передачи данных	Простота реализации алгоритма положительно отражается на скорости передачи данных
Сфера применения в отношении векторного изображения	Цифровая подпись	Комплексный характер шифрования
Сервисы защиты данных	Аутентификация, авторизация, неотказуемость	Конфиденциальность данных

Рис. 1. *Преимущества и недостатки симметричных и асимметричных алгоритмов шифрования*

В работе [3] предлагается рассмотреть алгоритм AES.

Далее сравнили асимметричный алгоритм шифрования RSA с симметричным алгоритмом AES [4]. Выбор используемого алгоритма шифрования происходил на основе анализа и сравнения алгоритмов RSA и AES [4].

Опираясь на результаты сравнения алгоритмов шифрования, приведенных на рис. 2, делаем вывод, что наиболее высокий уровень защиты и скорость шифрования имеет алгоритм AES [5].

Шифр	Алгоритмы шифрования			
	Длина ключа	Размер блока	Скорость преобразований	Степень защиты данных
RSA	Количество бит числа N	Переменный	Очень низкая	Низкая
AES	128, 192, 256 бит	128 бита	Высокая	Высокая

Рис. 2. *Анализ алгоритмов RSA и AES*

2. Применения алгоритма шифрования AES

В исследованиях М.Ф. Баймухамедова приводится структура алгоритма AES, которая представляет блок данных, представленных массивом, имеющим размер 4x4, представленных на рис. 3.

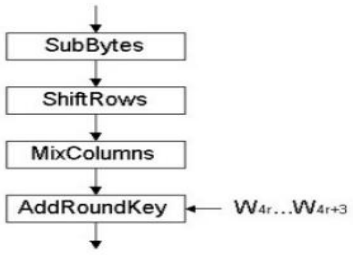

Рис. 3. *Структура алгоритма AES*

Рассмотрим операции, входящие в алгоритм AES более детально. С помощью операции SubBytes производится замена каждого байта в массиве, как это показано на рис. 4.

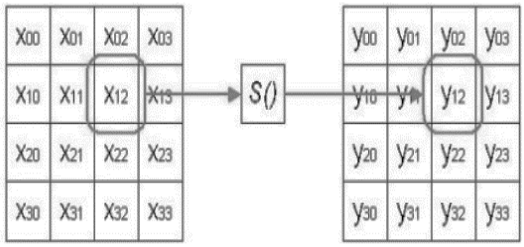

Рис. 4. *Процедура замены каждого байта в массиве с помощью операции SubBytes*

Для осуществления циклического сдвига влево строк массива, кроме нулевой с применением операции ShiftRows, производится циклический сдвиг влево i-той строки массива (где i = 1, 2, 3) на i байт.

Для умножения каждого столбца массива, представленного в виде полином поля GF(28) на полином a(x) = 3x3+x2+x+2 по модулю x 4+1, применяется операция MixColumns (показана на рис. 5).

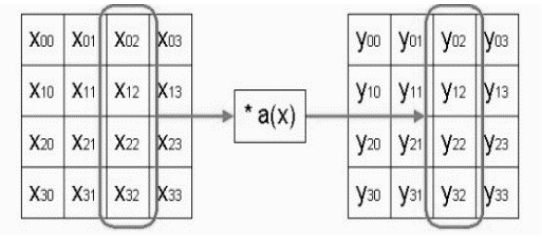

Рис. 5. *Результаты применения операции MixColumns*

Для наложения на массив данных ключа с алгоритмом AES необходимо применять операцию AddRoundKey [5]. В данном случае на -й столбец массива данных происходит наложение определенного слова расширенного ключа W4r+i, где r – это номер раунда алгоритма, зависящий от размера ключа.

В случае применения алгоритма AES в отношении векторного изображения возникает задача расширения ключа, и для этого применяется операция AddRoundKey с формированием 4*(R+1) слов.

Для расширения ключа на первоначальном этапе необходимо выполнить его инициализацию с заданием исходного ключа по алгоритму AES Nk и добавлением его расширения Wi, как это показано на рис. 6.

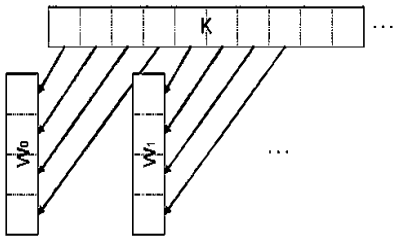

Рис. 6. *Инициализация расширенного ключа по алгоритму AES*

Для формирования дальнейшего расширения ключа AES используется следующая последовательность операций i=Nk… 4*(R+1)-1. Для этого вначале формируется временная переменная T=Wi+1. Для модификации данной переменной принимается условие кратности i к Nk.

Преимуществом процедуры расширения ключа по алгоритму AES является то, что расширение ключа может происходить параллельно с защитой данных [5].

3. Оцифровка и маскирование геопространственной обстановки

Маскирование – технологический прием, предназначенный для повышения криптостойкости маскируемых данных. Маскирование геопространственной обстановки будет производиться с применением двумерного белого шума. Разберемся, что это такое.

Белый шум – случайный сигнал, несущий равную интенсивность на разных частотах в заданном направлении в виде волн. Двумерный белый шум в нашем случае говорит о том, что распространение случайного сигнала происходит не только по горизонтали (оси x), но и по вертикали (оси y).

Исходный вид изображения геопространственной обстановки, исполненной с использованием компьютерного зрения, мы видим на рис. 7, далее на рис. 8 и 9 представлены те же самые изображения, но уже с различной интенсивностью маскирования.

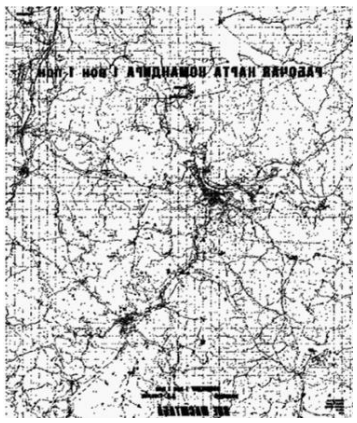

Рис. 7. *Отображение цифрового кода исходного изображения*

Далее представлен результат маскированием геопространственной обстановки с интегральным отношением 1/20 и 1/45.

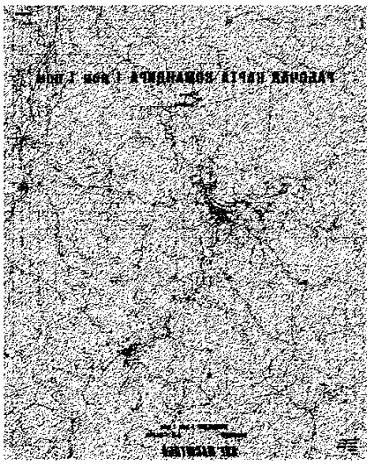

Рис. 8. *Результат маскированием геопространственной обстановки с частотой шума 1/20*

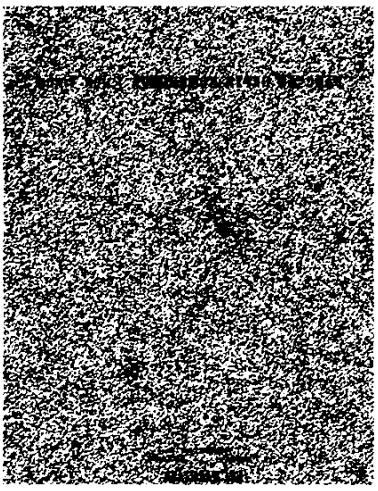

Рис. 9. *Результат маскированием геопространственной обстановки с частотой шума 1/45*

4. Пример аппаратной реализации данной статьи

Передача зашифрованной геопространственной обстановки может производиться через потоки Е1, при помощи коммутационного оборудования входящего в комплект машины управления и комплексной аппаратной связи П-144МСН соединенных между собой витой парой через штатные разъемы.

Пример организации взаимодействия представлен на рис. 10.

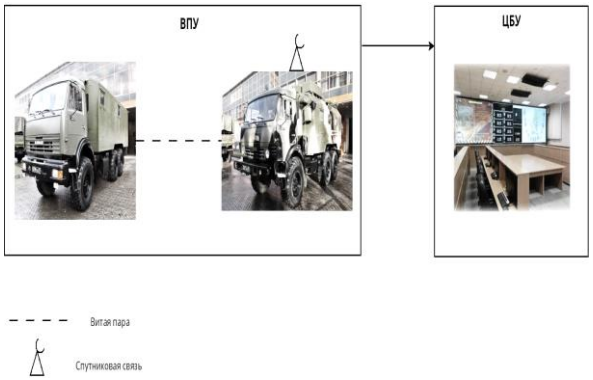

Рис. 10. *Схема организации передачи данных*
а – Машина управления,
б – Комплексная аппаратная связи П-144МСН,
в – Центр боевого управления

Отображение топографической карты в машине управления происходит с использованием документ-камеры WolfVision EYW-12 (рис. 11).

Рис. 11. *Документ-камера WolfVision EYW-12 [6]*

Документ-камера WolfVision EYE-12 представляет собой видеокамеру высокого разрешения для прямой передачи изображений [6]. Она может использоваться для разных целей, предусматривающих презентацию прямых изображений.

Например, в качестве документ-камеры или для передачи прямых изображений из одного помещения в другое.

Кроме того, телекамеры можно установить на штатив, панорамные опоры или настенные опоры, предназначенные для видео- или охранных камер [6].

Технические характеристики представлены в таблице.

Технические характеристики камеры WolfVision EYE-12

Вес	0,8 кг
Напряжение питания	100-240 В.
Оптическое увлечение	48х
Потребляемая мощность	8 Вт
Разрешение	1280х960
Цифровая память	9 кадров
Тип камеры	Стационарная, потолочная

5. Фильтрация изображения с помощью вейвлетов

Исходными данными для цифровой фильтрации являются отсчеты (значения) "точного" сигнала или изображения, которые зашумлены (искажены) случайным шумом (погрешностью) различной природы. Фильтрация заключается в построении алгоритма фильтрации (вычислительной процедуры), которая позволила бы достигнуть наилучших результатов в удалении шума из исходного (зашумленного) изображения.

Построение алгоритма фильтрации опирается на использование вероятностных моделей сигнала или изображения и шума, а также на применение различных статистических критериев оптимальности. Очевидно, что фильтрация используется для того, чтобы в максимальной степени удалить шумы из исходного сигнала, внося при этом минимальные искажения значений "точного" сигнала. Итак, фильтрация заключается в построении алгоритма фильтрации (вычислительной процедуры), которая позволила бы достигнуть наилучших (с точки зрения принятого критерия) результатов в удалении шума из зашумленного сигнала.

Построение алгоритмов фильтрации в значительной степени опирается на вероятностные модели сигнала и шума измерения и зависит от используемого критерия оптимальности, который позволяет оценить оптимальность того или иного алгоритма [7].

Алгоритмы Фурье-фильтрации основываются на предположении, что коэффициенты дискретного преобразования Фурье с большими индексами l (высокие частоты) в основном обусловлены шумами измерения и, зануляя эти коэффициенты, удается отфильтровать (в большей или меньшей степени) шум измерения [7].

Алгоритмы вейвлет-фильтрации основаны на следующих свойствах вейвлет-разложения [7]:

- информация о "точном" сигнале f(x) содержится только в небольшом количестве коэффициентов вейвлет-разложения (информативные коэффициенты). Остальные коэффициенты равны нулю либо незначительно отличаются от нуля по абсолютной величине, и их можно назвать *незначимыми (шумовыми) коэффициентами разложения.* Это свойство также широко используется для сжатия сигналов и изображений;
- шум измерения равномерно "перераспределяется" по всем коэффициентам вейвлет-разложения. В частности, если значения шума ηi не коррелированы и имеют одинаковую дисперсию σ2, то коэффициенты разложения этого шума по базису ортогональных вейвлетов также не коррелированы между собой и имеют одинаковую дисперсию [7].

Заключение

В данной статье рассмотрены вопросы сравнения симметричных и асимметричных систем шифрования. Произведен анализ алгоритмов шифрования AES и RSA. Рассмотрено применение алгоритма шифрования AES. Приведен пример аппаратной реализации данной статьи. Оцифровано изображения геопространственной обстановки с применением компьютерного зрения. Выполнена операция маскирования геопространственной обстановки с различной интенсивностью белого шума.

Список источников

1. *Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В.* Основы криптографии. М.: Гелиос АРВ, 2002. 480 с.
2. *Гуненков М.Ю.* Сравнительный анализ современных криптографических шифров // Молодежь, наука, творчество. 2019. С. 338–342. Банк данных угроз ФСТЭК URL: https://bdu.fstec.ru (дата обращения: 16.10.2022).
3. *Зикратова Т.В., Соловьев А.Л.* Метод криптографической защиты информации на основе гамма-шифрования // Актуальные проблемы защиты и безопасности: Труды XXIV Всерос. науч.-практ. конф. Санкт-Петербург. 01–04 апреля 2021 года. Т. 3. СПб.: ФГБУ "Российской академии ракетных и артиллерийских наук", 2021. С. 94–97. EDN UVDSFU.
4. *Коутинхо С.* Введение в теорию чисел. Алгоритм RSA. М.: Постмаркет, 2001. 328 с.
5. *Баймухамедов М.Ф.* Алгоритм шифрования AES как средство обеспечения информационной безопасности // Актуальные научные исследования в современном мире. 2019. № 9. С. 24–29.
6. *Руководство* по эксплуатации КУТСУ.
7. *Воскобойников Ю.Е.* Вейвлет-фильтрация сигналов и изображений. Новосибирск, 2015. С. 5, 61.

References

1. *Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V.* Fundamentals of cryptography. M.: Gelios ARV, 2002. 480 p.
2. *Gunenkov M.Yu.* Comparative analysis of modern cryptographic ciphers // Youth, science, creativity, 2019. P. 338–342. FSTEC Threat Data Bank URL: https://bdu.fstec.ru (accessed: 10.16.2022).
3. *Zikratova, T.V., Soloviev A.L.* Method of cryptographic protection of information based on gamma encryption // Actual problems of protection and security: Proceedings of the XXIV All-Russian Scientific and Practical Conference, St. Petersburg. April 01-04, 2021. Vol. 3. St. Petersburg: FSBI "Russian Academy of Rocket and Artillery Sciences", 2021. P. 94–97. EDN UVDSFU.
4. *Coutinho S.* Introduction to number theory. Algo-rhythm RSA. M.: Postmarket, 2001. 328 p.
5. *Baymukhamedov M.F.* AES encryption algorithm as a means of ensuring information security // Actual scientific research in the modern world. 2019. № 9. P. 24–29.
6. *UTSU* Operation Manual.
7. *Voskoboynikov Yu.E.* Wavelet filtering of signals and images. Novosibirsk, 2015. P. 5, 61.

Информация об авторах:

К.В. Иванова – инженер учебной лаборатории подвижных средств управления, факультет связи, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д. 1);

А.Ф. Сальников – доктор технических наук профессор кафедры "Ракетно-космическая техника и энергетические системы", Пермский национальный исследовательский политехнический университет (614990, Россия, г. Пермь, ул. Комсомольский проспект, 29), AuthorID 558165;

Р.В. Мормуль – кандидат технических наук, доцент кафедры вычислительных машин комплексов систем и сетей, Пермский военный институт войск национальной гвардии Российской Федерации (614112, Россия, г. Пермь, ул. Гремячий Лог, д. 1), AuthorID 1002143.

Information about the authors:

K. V. Ivanova – Engineer of the Mobile Control Tools Training Laboratory, Faculty of Communications, Perm Military Institute of National Guard Troops (1 Gremyachy Log st., Perm, Russia, 614112);

A. F. Salnikov – Doctor of Technical Sciences, Professor of the Department "Rocket and Space Technology and Power Systems", Perm National Research Polytechnic University (29 Komsomolsky Ave., Perm, Russia, 614990) AuthorID 558165;

R. V. Mormul – Candidate of Technical Sciences, Associate Professor of the Department of Computing Machines of Systems and Networks Complexes, Perm Military Institute of National Guard Troops (1 Gremyachy Log st., Perm, Russia, 614112), AuthorID 1002143.