2. Алефиренко, В. М. Выбор состава технических средств для систем обеспечения безопасности / В. М. Алефиренко // Доклады БГУИР. – 2017. – № 2 (104). – С. 39–44.

3. Алефиренко, В. М. Комплексный анализ технических характеристик блокираторов сотовой связи и беспроводного доступа / В. М. Алефиренко, А. Д. Денскевич, А. М. Асиненко // Журнал «Science Time»: Материалы Междунар. науч.-практ. мероприятий Общества Науки и Творчества за июнь 2022 года / Казань, 2022. – № 6 (102). – С. 5–9.

4. Акустические сейфы для защиты от перехвата конфиденциальной информации [Электронный ресурс]. – Режим доступа: https://detsys.ru/catalog/zashchita_telefonov/. – Дата доступа: 21.09.2024.

УДК 004.9, 519.688

ЭФФЕКТИВНОСТЬ ИСПОЛЬЗОВАНИЯ КРИПТОМОДУЛЯ С ПРИМЕНЕНИЕМ МИНИМАЛЬНО ИЗБЫТОЧНЫХ МОДУЛЯРНЫХ СИСТЕМ СЧИСЛЕНИЯ ДЛЯ ШИФРОВАНИЯ ДАННЫХ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ

Ломако А. А., Козлова Е. И.

НИУ «Институт прикладной физических проблем имени А. Н. Севченко» БГУ
Минск, Республика Беларусь

Аннотация. На сегодняшний день одним из актуальных направлений в шифровании информации является использование модулярных систем счисления. В работе описываются минимально избыточные модулярные системы счисления и их применение для шифрования изображений, регистрируемых при дистанционном зондировании Земли. На основании экспериментальных вычислений выявлено, что скорость шифрования данных за счет использования параллельных вычислений повышается в 3,8 раза.

Ключевые слова: обработка изображений, параллельные вычисления, беспилотные летательные аппараты, модулярная арифметика.

THE CRYPTOMODULE WITH MINIMALLY REDUNDANT MODULAR NUMBER SYSTEMS EFFECTIVENESS FOR REMOTE SENSING DATA ENCRYPTING

Lamaka A., Kazlova A.

A. N. Sevchenko Institute of Applied Physical Problems of Belarusian State University
Minsk, Republic of Belarus

Abstract. One of the most relevant directions in information encryption is the use of the mathematical apparatus of elliptic curves and modular number arithmetic systems. The paper describes minimally redundant modular number systems and their application to encrypt images recorded during remote sensing. It was revealed after the experimental calculations that the data encryption speed increases by 3.8 times due to the use of parallel computing.

Key words: image processing, parallel computing, unmanned aerial vehicles, modular arithmetic.

Адрес для переписки: Ломако А. А., пр. Независимости, 65, г. Минск 220113, Республика Беларусь
e-mail: remsens@mail.ru

В последнее время получили развитие исследования в области криптографии, направленные на согласование математического аппарата эллиптических кривых и арифметики модулярных систем счисления [1; 2]. Этот подход позволяет разрабатывать высокопроизводительные криптосистемы различного назначения [2]. Одной из областей применения такого криптомодуля может быть шифрование данных, получаемых при дистанционном зондировании Земли (ДЗЗ). При этом шифрование может использоваться как для засекречивания данных космической съемки (в том числе, мульти- или гиперспектральных изображений), так и для обработки видеопотоков данных, передаваемых от беспилотных летательных аппаратов их операторам по радиоканалу. При этом использование особенности модулярных вычислительных систем как архитектурно параллельных в совокупности с характерной для данных ДЗЗ целочисленностью значений в пикселях изображений позволяет существенно увеличить скорость обработки информации. Целью данного исследования стала численная оценка увеличения скорости шифрования изображений за счет использования параллельных вычислений.

Минимально избыточные модулярные системы счисления. Использование в различного рода числовых системах кодовой избыточности позволяет существенно улучшить арифметические и другие свойства таких систем. Для минимально избыточных модулярных систем счисления (МИМСС) отображение, описывающее кодирование, определяется следующим образом:

$$\nu: D \to Z_{m_1} \times Z_{m_2} \times \ldots \times Z_{m_k}, \qquad (1)$$

где m_1, m_2, …, m_k – модули МИМСС, D – кодируемое множество (прообраз кодового пространства), Z_{M_k} – диапазон таких целых чисел, что набору модулей m_1, m_2, …, m_k числа $X \in Z$ отвечает некий модулярный код (χ_1, χ_2,…, χ_k). При этом мощность диапазона D меньше, чем у диапазона $Z_{\bar{M}_k}$ классической неизбыточной модулярной системы счисления с тем же базисом [2].

Главным преимуществом МИМСС по сравнению с неизбыточными модулярными системами счисления является значительное упрощение вычисления интервально-индексной характеристики за счет упрощения вычислительных процедур до тривиальных (одной модульной операции) при использовании табличной реализации [2].

Программный модуль шифрования. Для оценки эффективности разработан программный модуль (ПМ) шифрования RGB изображений (24 bit). В силу того, что для МИМСС при преобразовании одного целого числа требуется одна модульная операция, в ПМ в качестве операции пересчета значения интенсивности пикселя используется операция деления по модулю.

Управляющие устройства целевой нагрузки систем ДЗЗ, как правило, не обладают большими вычислительными мощностями, исходя из чего их возможности по шифрованию данных в реальном времени весьма ограничены. Одним из применяемых аппаратных решений может быть использование микрокомпьютеров Raspberry Pi, которые имеют до 4 ядер процессора (например, [3]). Это учитывалось при проведении анализа.

Анализ эффективности. Для оценки эффективности были использованы данные обзорной камеры беспилотного комплекса авиационного спектрометрирования [3]. Исходное разрешение изображений камеры составляет 1920×1080 пк. Производилось ресемплирование изображений с использованием билинейной интерполяции, в результате чего были сгенерированы 5 наборов изображений различного разрешения для анализа. Количество изображений в каждом из наборов данных равно 40. Разрешения изображений в различных наборах представлено в таблице 1.

Таблица 1 – Пиксельные разрешения в наборах данных для анализа

Номер набора	5	4	3	2	1
Ширина, пк	2592	1920	1280	960	640
Высота, пк	1520	1080	720	540	360

Без использования параллельных вычислений скорость шифрования данных должна падать прямо пропорционально количеству пикселей в изображении. При использовании многопоточности технических средств, применяемых для расчетов, вычислительная эффективность будет увеличиваться при росте числа параллельно запущенных процессов. Однако количество потоков и скорость шифрования может изменяться не в прямой пропорциональности, так как в данном случае вероятно возникновение эффекта замедления вычислений в процессе слияния результатов расчетов в различных потоках в единое изображение. Тем не менее, этого замедления можно избежать за счет хранения данных о числовых значениях пикселей в последовательной области памяти. В таком случае при вычислениях можно передавать указатели на отдельные области памяти в каждый поток для независимого шифрования. Результаты экспериментальной оценки среднего времени шифрования для групп изображений различного разрешения представлены на рисунке 1.

Как видно на рисунке 1, без применения многопоточности наблюдается ожидаемая линейная зависимость времени вычислений от количества пикселей в изображении. При этом использование параллельных вычислений позволяет существенно уменьшить время шифрования.

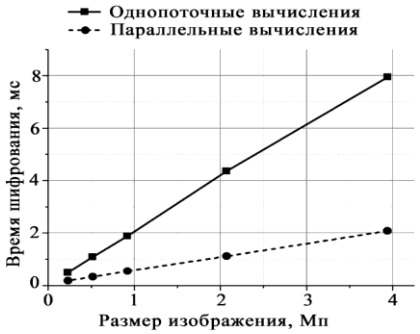

Рисунок 1 – Сравнительные графики зависимости среднего времени шифрования изображений от их разрешения

Так, например, для разрешения кадров 2592×1520 пк при использовании 4 вычислительных потоков среднее значение времени шифрования одного изображения уменьшается с величины 7,95 мс с СКО 0,06 мс до 2,08 мс с СКО 0,06 мс. Таким образом, за счет архитектурной возможности модулярных систем счисления по разбиению вычислений на независимые потоки возможно повышение скорости шифрования изображений до 3,8 раз.

Выводы. Анализ эффективности использования криптомодуля с применением МИМСС при шифровании данных ДЗЗ показал, что разработанный ПМ, использующий особенности модулярных вычислительных структур как архитектурно параллельных, позволяет в зависимости от разрешения изображений повысить скорость шифрования информации от 2,6 до 3,8 раз.

Благодарности. Работа выполнена в рамках государственной программы научных исследований «Цифровые и космические технологии, безопасность общества и государства» подпрограммы «Цифровые технологии и космическая информатика» по заданию 1.9.2 (№ государственной регистрации 20212656).

Литература

1. Инютин, С. А. Основы модулярной алгоритмики / С. А. Инютин. – Ханты-Мансийск : Полиграфист, 2009. – 347 с.

2. Червяков, Н. И. Модулярная арифметика и ее приложения в инфокоммуникационных технологиях / Н. И. Червяков [и др.]. – М.: ФИЗМАЛИТ, 2017. – 400 с.

3. Lamaka, A. A. Photospectral Data Obtaining with the Unmanned Aerial Spectrometry Vehicle / A. A. Lamaka [et al.] // Devices and Methods of Measurements. – 2023. – V. 14, № 1. – P. 7–17.