AWS Thinkbox Deadline- платформа для керування процесом рендерингу, яка дозволяє масштабувати обчислювальні потужності в залежності від потреб проекту.

Платформа Google Zync Render це Інтеграція з Maya, Nuke, Arnold та іншими

Таким чином, хмарні технології для рендерингу надають потужні можливості для графічного дизайну, анімації та інших областей, які вимагають великих обчислювальних ресурсів.

Список використаної літератури

1. Романюк, О. Н.. Борисова К. О., Катєльніков Д. І. Аналіз хмарної технології Google Drive. Матеріали XXI Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів «Стан, досягнення та перспективи інформаційних систем і технологій», Одеса, 22-23 квітня 2021 р. Електрон. текст. дані. Одеса, 2021. С. 65-67.
2. Степанчук П. В., Романюк О. В. Використання хмарних сервісів у мобільній розробці для підвищення захисту, продуктивності та функціональності. Матеріали LIII науково-технічної конференції підрозділів ВНТУ, Вінниця, 20-22 березня 2024 р. Електрон. текст. дані. 2024.
3. Миргородський А. В. Особливості адміністрування баз даних в хмарних середовищах [Електронний ресурс] / А. В. Миргородський, О. В. Романюк // Матеріали XLIX науково-технічної конференції підрозділів ВНТУ, Вінниця, 27-28 квітня 2020 р. – Електрон. текст. дані. – 2020.
4. Романюк О. Н., Павлов С. В., Бобко О. Л., Завальнюк Є. К, Решетнік О. О. Аналіз великих даних у комп`ютерній графіці. Оптико-електронні інформаційно-енергетичні технології. 2024. № 1(47). С. 50–57.
5. Романюк О. Н. Вимоги до побудови систем рендерингу [Текст] / О. Н. Романюк, О. В. Романюк // Електронні інформаційні ресурси: створення, використання, доступ : збірник матеріалів Міжнародної науково-практичної інтернет-конференції. Пам`яті А.М.Петуха, 9-10 грудня 2019 р. – Суми/Вінниця : НІКО/ВНТУ, 2019. – С. 303- 305.
6. Романюк, О. Н. Комп’ютерна графіка [Електронний ресурс] : електронний навч. посіб. / О. Н. Романюк, О. В. Романюк, Р. Ю. Чехместрук. – Вінниця : ВНТУ, 2023. – 147 с.

УДК 004.627

ОСОБЛИВОСТІ ШИФРУВАННЯ ЗОБРАЖЕНЬ НА ОСНОВІ GPU

Романюк О.Н., Майданюк В.П., Нечипорук В.Л. (ran12345@gmail.com)
Вінницький національний технологічний університет (Україна)

Розглянуто використання GPU для шифрування зображень. Показано, що шифрування зображень на GPU продовжує розвиватися, надаючи значні можливості для покращення безпеки, швидкості та ефективності обробки даних у широкому спектрі застосувань.

Шифрування зображень з використанням графічних процесорів (GPU) стало популярним завдяки здатності GPU ефективно виконувати паралельні обчислення.

GPU має багато ядер обробки, які можуть одночасно обробляти різні частини зображення, значно збільшуючи швидкість шифрування [1]. Графічні процесори здатні обробляти великі обсяги даних, що робить їх доцільними для шифрування великих зображень або відео. Використання GPU для шифрування дозволяє основному процесору (CPU) зосередитися на інших завданнях, тим самим покращуючи загальну продуктивність системи. Розроблена NVIDIA, технологія CUDA дозволяє розробникам використовувати мову програмування C/C++ для написання програм, які виконуються на GPU. Фреймворк **OpenCL** розроблено для написання програм, які виконуються на різноманітних платформах, включаючи GPU, від різних виробників [2].

Процес шифрування з використанням GPU включає ряд етапів. Зображення конвертується в формат, який можна ефективно обробляти на GPU, зазвичай, у вигляді масиву байтів або текстур. Дані зображення розділяються на блоки, які можуть бути паралельно оброблені на різних ядрах GPU. Шифрувальний алгоритм імплементується у вигляді кернелу GPU, який виконується

паралельно для кожного блоку або пікселя. Шифровані блоки об’єднуються назад в одне ціле зображення.

Розділення зображень на блоки для обробки на GPU є важливим елементом в ефективному паралельному шифруванні [3]. Перед тим, як зображення можна буде ефективно обробити на GPU, його зазвичай конвертують у формат, зручний для обробки. Зображення конвертується у масив байтів або масив пікселів. Кожен піксель може представляти собою один або кілька байтів залежно від глибини кольору (наприклад, RGB, RGBA). Якщо необхідно, дані можуть бути нормалізовані або стандартизовані для спрощення подальшої обробки. Вибір розміру блоку зазвичай залежить від характеристик GPU і алгоритму шифрування [4]. Наприклад, AES,зазвичай, працює з блоками розміром 128 біт [5]. Загальна кількість блоків визначається на основі розміру зображення і вибраного розміру блоку. Якщо зображення не ділиться націло на блоки, застосовується метод доповнення (padding) для заповнення останнього блоку.

Кожен блок призначається для паралельної обробки на окремих ядрах GPU. Це може бути організовано за допомогою технологій, як CUDA або OpenCL, де розробник може визначити, як блоки розподілятимуться та оброблятимуться. Блоки зображення завантажуються у глобальну пам'ять GPU, де вони стають доступними для обробки ядрами GPU. Для кожного блоку запускається кернел (програма обробки), який виконує шифрування або розшифрування. Оскільки кожен блок обробляється незалежно, GPU може виконувати шифрування паралельно, що значно прискорює процес в порівнянні з послідовною обробкою на CPU. Після завершення обробки результати для кожного блоку збираються та знову складаються в одне ціле зображення, яке тепер є зашифрованим.

Використання GPU для шифрування зображень забезпечує швидку і ефективну обробку, що є особливо корисним для застосувань в реальному часі або для обробки великих наборів даних.

Під час блокового шифрування зображень на GPU можуть виникати деякі проблеми на стиках блоків під час шифрування даних зображення, які не є кратними розміру блоку шифрування, потрібно застосовувати метод доповнення (padding). Неправильне вирівнювання або неправильно вибраний метод доповнення може призвести до того, що останній блок не буде правильно оброблений, що вплине на якість розшифрованого зображення. Також можуть виникати помилки при визначенні країв блоків, особливо якщо зображення має нестандартні розміри або пропорції.

Багато алгоритмів блокового шифрування, таких як AES в режимі ECB (Electronic Codebook), обробляють кожен блок незалежно, що може призвести до того, що ідентичні блоки вхідних даних дають ідентичні зашифровані блоки. Це може створити вразливості, особливо в зображеннях з багатьма повторюваними пікселями. Аби уникнути таких проблем, краще використовувати більш безпечні режими шифрування, такі як CBC (Cipher Block Chaining) або CTR (Counter), де кожен блок шифрується з залежністю від попереднього, що зменшує ризики і забезпечує більшу безпеку.

Правильна реалізація шифрування з урахуванням всіх блоків і їх стиків вимагає додаткової уваги до деталей і може збільшувати складність програмного коду, особливо при використанні більш складних режимів шифрування на GPU.

Загалом, для забезпечення безпеки та ефективності при шифруванні зображень на GPU важливо ретельно планувати методику розділення на блоки, вибір режиму шифрування та вирішення проблем, пов’язаних із стиками блоків.

Технічно блоки можуть перекриватися під час обробки зображень, але це залежить від конкретного завдання та методу, який використовується. У контексті шифрування зображень зазвичай блоки не перекриваються, оскільки кожен блок даних шифрується незалежно для забезпечення безпеки. Однак, існують ситуації, коли перекриття блоків може бути корисним. При застосуванні фільтрів або інших операцій обробки зображень (наприклад, розмиття, підкреслення границь), часто блоки даних мають перекриватися, щоб уникнути видимих швів або артефактів на межах оброблених областей. Тут перекривання блоків дозволяє кожному фрагменту враховувати сусідні дані для згладжування переходів.

У процесах кодування відео, які використовують рухомі блоки або макроблоки, можливе перекриття для точного відстеження руху і мінімізації втрат на межах кадрів.

Оцінка шифрування зображень на GPU включає кілька критеріїв, які визначають якість, ефективність та безпеку шифрувальних рішень. Основні критерії, які слід враховувати такі:

- час шифрування визначає швидкість, з якою GPU може зашифрувати зображення. Це важливо для застосувань в реальному часі, таких як відеоконференції або стрімінг;

- час розшифрування визначає швидкість розшифрування, також важлива, оскільки вона впливає на здатність користувачів швидко отримувати доступ до зашифрованих даних;

- важливим є завантаження GPU, яке визначає міру використання графічного процесора під час шифрування. Оптимальне рішення мінімізує завантаження GPU, залишаючи ресурси для інших задач;

- ефективне шифрування мінімізує вимоги до пам'яті для збереження проміжних станів і ключів;

- стійкість до криптоаналізу визначає здатність алгоритму протистояти різним видам криптоаналітичних атак, таких як атаки з вибраним відкритим текстом або атаки на основі часу;

- алгоритми повинні забезпечувати адаптивність до різних розмірів зображень: Здатність алгоритму ефективно шифрувати зображення різних розмірів і роздільної здатності;

- важливою є сумісність із різними моделями і поколіннями GPU, включаючи ті, що мають різні можливості і обмеження;

- алгоритми шифрування повинні підтримка різні формати зображень;

- після шифрування та наступного розшифрування якість зображення не погіршувалась, особливо при використанні методів шифрування, які вносять зміни в дані зображення;

- шифрувальні рішення на GPU повинні бути легкі у впровадженні та налаштуванні для кінцевих користувачів, без потреби в глибоких знань криптографії або програмування.

Вибір правильної технології шифрування на GPU і алгоритму залежить від конкретних потреб організації або проекту, а також від доступних ресурсів та інфраструктури.

Перспективи розвитку шифрування зображень на GPU є досить обнадійливими, враховуючи постійне зростання обчислювальних потужностей графічних процесорів і розширення їхніх можливостей. З розвитком технологій віртуальної реальності, відеоконференцій високої роздільної здатності та автономних транспортних засобів з'являється потреба в швидкому шифруванні великих обсягів даних в реальному часі. GPU, завдяки своїм високим паралельним обчислювальним можливостям, підходять для цього завдання, оскільки можуть забезпечити необхідну швидкість обробки.

Науковці та розробники працюють над створенням більш ефективних алгоритмів шифрування, які оптимізовані для виконання на GPU. Це включає розробку алгоритмів, які мінімізують завантаження пам'яті та покращують використання кешу, щоб забезпечити більшу швидкість шифрування без втрати безпеки.

Зі зростанням використання хмарних обчислень шифрування даних стає ще більш важливим. GPU на хмарних платформах можуть бути використані для шифрування зображень та інших даних перед їхнім зберіганням або передачею, що дозволяє користувачам ефективно масштабувати свої ресурси шифрування.

Розвиток апаратних засобів для шифрування на базі GPU може включати в себе вбудовані рішення для безпеки, які можуть додатково захистити ключі шифрування та алгоритми від атак. Це може бути здійснено через розробку спеціалізованих мікросхем або безпечних виконавчих середовищ на GPU.

Покращення методів управління ключами, зокрема автоматичне оновлення та розподіл ключів, можуть бути інтегровані з GPU, щоб забезпечити більшу безпеку та гнучкість у застосуваннях шифрування.

Оскільки ринок GPU складається з декількох виробників, розробка універсальних, міжплатформних рішень для шифрування, які можуть ефективно працювати на різноманітному обладнанні, стає критично важливою.

Загалом, шифрування зображень на GPU продовжує розвиватися, надаючи значні можливості для покращення безпеки, швидкості та ефективності обробки даних у широкому спектрі застосувань.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Романюк О. Н. Довгалюк Р. Ю, Олійник С. В. Класифікація графічних відеоадаптерів / Наукові праці ДонНТУ . Серія : інформатика, кібернетика та обчислювальна техніка. – 2011. – Вип. 14 (188). – С. 211-215.

2. Завальнюк Є.К., Романюк О.Н., Снігур А.В., Шевчук Р. П.. Аналіз сучасних архітектур GPU. Стан, досягнення та перспективи інформаційних систем і технологій / Матеріали XXIII Всеукраїнської науково-технічної конференції молодих вчених, аспірантів та студентів. Одеса, 20-21 квітня 2023 р. - Одеса, Видавництво ОНТУ, 2023 р. –с.302-303.
3. Завальнюк Є.К., Романюк О.Н. Реалізація паралелізму потоків команд і даних графічних процесорів. Інноваційні дослідження та перспективи розвитку науки і техніки у XXI столітті, Рівне, 19 жовтня 2023 р. Рівне, Редакційно-видавничий центр Приватного вищого навчального закладу «Міжнародний економіко-гуманітарний університет імені академіка Степана Дем'янчука, 2023 р. Ч3. С.156-158.
4. Майданюк, В. П. Основи теорії інформації та кодування : електронний навчальний посібник комбінованого (локального та мережного) використання [Електронний ресурс] / Майданюк В. П., Романюк О. Н., Тужанський С. Є. – Вінниця : ВНТУ, 2022. – 133 с.
5. Баленко О.І., Семенов С.Г., Можаєв О.О. Дослідження можливостей графічних процесорів при реалізації алгоритмів симетричного шифрування // Інформаційно-керуючі системи на залізничному транспорті – 2015, №4. – С. 44-47..

УДК 911.3:006.6

ВІЗУАЛІЗАЦІЯ ГЕОГРАФІЧНОЇ ІНФОРМАЦІЇ ДЛЯ СТРАТЕГІЧНОГО АНАЛІЗУ ВІЙСЬКОВОГО ТА ГЕОПОЛІТИЧНОГО ПЛАНУВАННЯ

Рябоволенко Е. А., Мормуль М. Ф.,
(rabovolenkoeduard@gmail.com, nikolaj.mormul@gmail.com)
Університет митної справи та фінансів, Україна

У тезах розглядаються географічні інформаційні системи (ГІС) і дистанційне зондування, які відіграють ключову роль у військовому застосуванні завдяки своїй здатності обробляти просторові дані. При їх дослідженні використовується описово-аналітичний підхід для ілюстрації використання ГІС у військових операціях на основі досвіду, розробленого для наземних військових застосувань. Різні військові структури широко використовують надійні і точні інструменти просторового картографування для командування, управління, зв'язку і координації під час військових операцій. У дослідженні розглядається кілька стратегій візуалізації даних, які ефективно передають географічну інформацію для стратегічного аналізу і прийняття рішень у різних секторах, включаючи військове планування і геополітичний аналіз.

Постановка проблеми. Сучасний світ стикається з численними викликами, які вимагають ефективного управління та прийняття рішень на основі об'єктивних даних. Географічна інформація (ГІ) стає важливим інструментом у стратегічному аналізі, оскільки дозволяє візуалізувати складні дані, розкриваючи просторові взаємозв'язки і тенденції. Проте, незважаючи на доступність технологій, таких як ГІС (географічні інформаційні системи) та інструменти візуалізації, існує ряд проблем, що заважають ефективному використанню географічної інформації.

По-перше, недостатнє усвідомлення можливостей, які надають сучасні методи візуалізації, обмежує їхнє впровадження в стратегічний аналіз. Багато організацій все ще покладаються на традиційні методи аналізу, які не здатні врахувати складність геопросторових даних.

По-друге, існує проблема стандартизації та інтеграції даних з різних джерел. Відсутність єдиних стандартів може призводити до неузгодженості в інформації, що ускладнює прийняття рішень.

По-третє, не всі користувачі мають достатню кваліфікацію для роботи з географічною інформацією, що обмежує їхню здатність інтерпретувати результати візуалізації.

Отже, постає необхідність у розробці комплексного підходу до візуалізації географічної інформації, який би враховував ці виклики і сприяв ефективнішому використанню ГІ для стратегічного аналізу. Це відкриває нові можливості для підвищення ефективності управлінських рішень в різних сферах, від економіки до екології.