

3. Вертикальный и горизонтальный контроль по паритету. Исходные данные рассматриваются в виде матрицы, строки которой составляют байты данных. Контрольный разряд подсчитывается отдельно для каждой строки и для каждого столбца матрицы.

4. Коды Хэмминга. Самостоятельно находят и исправляют ошибки, даже изолированные, то есть искаженные отдельные биты которые могут быть разделены большим количеством правильных битов.

Построение кодов Хэмминга основано на принципе проверки на четность числа единичных символов: к последовательности добавляется такой элемент, чтобы число единичных символов в получившейся последовательности было четным, ($S = 0$ – ошибок нет, $S = 1$ – однократная ошибка). Матрица преобразования соответствующей размерности умножается на матрицу-столбец кодового слова и каждый элемент полученной матрицы-столбца берется по модулю 2. На аппаратном уровне, в Optix OSN 8800, коды Хэмминга реализуются в модуле OTN tributary unit, на плате TN52TOG.

ИСПОЛЬЗОВАНИЕ ЖУРНАЛА ИЗМЕНЕНИЙ ФАЙЛОВ NTFS В КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЕ

О.Р. Мысливец

При проведении компьютерно-технической экспертизы, а именно при анализе файловой системы NTFS, часто встает необходимость в поиске удаленных файлов и их анализе. Несмотря на то, что методы поиска удаленных файлов и их восстановления для файловой системы NTFS [1] не представляют особой сложности, не всегда возможно полностью восстановить файл для последующего анализа. В подобных случаях, если не удастся восстановить файл полностью либо частично, существует возможность получить информацию о том, хранился ли файл в файловой системе в определенный промежуток времени и определить действия, проводимые над файлом. Информацию такого рода можно получить из журнала изменений файлов NTFS. Наряду с именами файлов и информацией об их MFT-записях, данный метафайл хранит в себе информацию о действиях, произведенных над файлами, а также временные метки произведенных действий [2]. С помощью данной информации можно однозначно установить факт хранения и использования некоторого файла, вплоть до получения полной последовательности произведенных над файлом действий за определенный промежуток времени. Недостатками данного подхода можно считать возможное отсутствие метафайла, вследствие его преднамеренного удаления или отключение опции журналирования для конкретного тома, а также ввиду ограничений на размер журнала изменений файлов, некоторые записи в журнале могут быть перезаписаны более новыми, что может повлиять на конечный результат. Несмотря на все недостатки данного подхода, в ходе исследований выяснилось, что в процессе анализа журнала изменений файлов NTFS существует вероятность получения информации о файлах, удаленных более 3 месяцев назад, но и не более 6 месяцев с момента удаления при условии активного использования накопителя информации.

Литература

1. Кэрриэ, Б. Криминалистический анализ файловых систем/ Кэрриэ Б. – СПб.: Питер, 2007. – 470 с.
2. USN_RECORD_V2 structure [Электронный ресурс] / Microsoft TechNet – Режим доступа: [https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa365722\(v=vs.85\).aspx](https://msdn.microsoft.com/ru-ru/library/windows/desktop/aa365722(v=vs.85).aspx) – Дата доступа: 17.05.2017.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОГО ХРАНЕНИЯ И ЗАЩИТЫ ИНФОРМАЦИИ БАЗЫ ДАННЫХ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

Е.А. Нестерович, С.А. Зайкова

В современных условиях любая деятельность сопряжена с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в настоящее время значения информации стали высокие требования к конфиденциальности данных. Системы управления базами данных (СУБД), в особенности реляционные, стали доминирующим инструментом в этой области. Обеспечение информационной безопасности СУБД приобретает решающее

значение при выборе средства обеспечения необходимого уровня защиты для компании либо предприятия в целом. Организация защиты требует комплексного подхода и учета всех возможных коммуникационных каналов, обеспечение физической безопасности, шифрование резервных копий и информации, покидающей периметр компании, а также ряда организационных мероприятий. В работе проведен анализ предметной области, связанной с обеспечением безопасного хранения и защиты от несанкционированного доступа в базу данных, а также разработаны инструменты защиты базы данных в соответствии с требованиями к безопасности хранения и передачи данных. Спроектирована функциональная модель базы данных, предназначенная для хранения зашифрованных данных, введенных пользователем (на примере военного комиссариата Гродненской области). Решены следующие задачи: рассмотрены и проанализированы наиболее популярные уязвимости баз данных MySQL, спроектирована архитектура базы данных для специализированного программного обеспечения «Модуль социальной защиты ветеранов» военного комиссариата Гродненской области, разработан и испытан прототип приложения, произведена оценка его эффективности, даны рекомендации по организации обеспечения безопасного хранения и защиты информации от несанкционированного доступа.

Литература

1. Смирнов, С Безопасность систем баз данных / С. Смирнов. – Гелиос АРВ, 2007. – 352 с.
2. Шустова, Л. Базы данных / Л. Шустова, О. Тараканов. – М.: Инфра-М, 2016. – 304 с.

ПОВЫШЕНИЕ РАЗРЕШЕНИЯ ИЗОБРАЖЕНИЙ, ПОЛУЧАЕМЫХ ПРИ АЭРОКОСМИЧЕСКОМ МОНИТОРИНГЕ ЗЕМЛИ

П.М. Никуленко, В.Ю. Цветков, Д.Ю. Туча

В настоящее время все большую необходимость получают алгоритмы повышения разрешения изображений. Алгоритмы супер-разрешения позволяют повышать качество изображений, не затрагивая аппаратуру космических аппаратов. Супер-разрешение – технология, позволяющая повышать разрешающую способность изображений (способность передавать мелкие детали). Алгоритмы супер-разрешения основаны на получении дополнительной информации из каких-либо источников (копии снимков со смещениями и под другим ракурсом, база данных изображений). Супер-разрешение на основе обучающегося множества имеет преимущество над другими методами в виду того, что не требует модификаций съемочной аппаратуры, так как использует информацию, хранящуюся в базе данных при наземной обработке. Основной принцип предлагаемого алгоритма заключается в нахождении среди изображений базы данных наиболее схожих и подходящих высоких частот для построения повышенного разрешения. Результат повышения детализации будет зависеть от того, насколько большое количество высокочастотных участков будет находиться в базе снимков, при этом даже при небольшой степени сходства четкость изображений будет увеличиваться в виду наложения слоя высоких частот, а возможные ошибки будут корректироваться степенью их прозрачности. Главной проблемой алгоритма является уменьшение ошибок при повышении разрешения, для этого применяется автоматическая коррекция прозрачности накладываемых частот, исходя из степени сходства изучаемых участков. Также существует необходимость развития алгоритма по принципу нейронных сетей, для автоматической выборки из обрабатываемых изображений недостающих в базе высокочастотных участков и последующего накопления их.

УПРАВЛЕНИЕ ДОСТУПОМ И ЗАЩИТА ИНФОРМАЦИИ В СИСТЕМЕ МОНИТОРИНГА ГИДРОЛОГИЧЕСКОГО РЕЖИМА ВОДНЫХ ОБЪЕКТОВ

Е.В. Новиков, Д.А. Мельниченко

Для мониторинга состояния и прогнозирования динамики гидрологического режима водных объектов широко используются данные дистанционного зондирования Земли. Специализированный распределенный сетевой программный комплекс мониторинга русловых процессов и гидрологического режима рек с использованием таких данных в качестве