НОВЫЙ ПОДХОД К ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ: ИСПОЛЬЗОВАНИЕ ЛОКАЛЬНЫХ БИНАРНЫХ ШАБЛОНОВ ДЛЯ ИЗОБРАЖЕНИЙ С ЦЕЛЬЮ ОБЕСПЕЧЕНИЯ ИНВАРИАНТНОСТИ РАЗМЕРОВ И ОРИЕНТАЦИИ

А.К. Крамаренко, А.В. Матиевская

Учреждение образования «Брестский государственный технический университет», Брест, Беларусь

В данном докладе представлен новый подход к технической защите информации, основанный на использовании локальных бинарных шаблонов (LBP) для обработки изображений с целью обеспечения инвариантности их размеров и ориентации. Защита информации является критическим аспектом в современном цифровом мире, где конфиденциальность и целостность данных играют важную роль [1]. Одной из основных проблем в области технической защиты информации является разработка методов, способных обеспечить надежность и инвариантность в условиях изменчивости размеров и ориентации изображений. В данном исследовании мы сосредоточились на обработке изображений с использованием локальных бинарных шаблонов, которые позволяют создавать инвариантные признаки для описания изображений независимо от их размеров и ориентации. Локальные бинарные шаблоны (LBP) являются текстурными признаками, впервые предложенными в 1994 г. Они вычисляются в окрестности каждого пикселя и описывают зависимость между значениями яркости в этой окрестности [2]. В данном исследовании мы предлагаем применить вычисление LBP к пикселям бинарного представления изображений с целью создания инвариантных признаков.

Процедура обработки изображений включает последовательность преобразований, таких как бинаризация изображения, фильтрация, поворот изображения до горизонтальной ориентации, вырезание описывающего прямоугольника и масштабирование в шаблон фиксированного размера. После этого применяется вычисление локальных бинарных шаблонов к пикселям бинарного представления изображения. Полученные LBP значения строят гистограмму, которая представляет собой новый инвариантный признак нормализованного представления изображения. Эксперименты, проведенные в рамках данного исследования, показали, что вычисление корреляции Пирсона между инвариантными признаками, основанными на локальных бинарных шаблонах, позволяет различать изображения различных объектов и обеспечивает надежную защиту информации [3].

Таким образом, представленный подход к технической защите информации на основе локальных бинарных шаблонов открывает новые перспективы для создания инвариантных признаков изображений, которые могут быть использованы в различных областях, связанных с защитой информации. Это может включать обнаружение поддельных изображений, аутентификацию и идентификацию объектов на изображениях, а также защиту цифровых данных. Однако следует отметить, что данное исследование представляет только начальный этап в разработке нового подхода к технической защите информации. Дальнейшие исследования и эксперименты требуются для более полного понимания эффективности и применимости этого подхода в различных сценариях.

В заключение, использование локальных бинарных шаблонов для обработки изображений представляет собой новый и перспективный подход к технической защите информации. Этот подход может быть применим в различных областях, связанных с защитой данных, и имеет потенциал для улучшения надежности и инвариантности признаков изображений.

Список литературы

1. Черноокий, И. В. Тенденции внедрения ИТ в образовательный процесс высшей школы в Республике Беларусь / И. В. Черноокий // Проблемы устойчивого развития регионов Республики Беларусь и сопредельных стран : сборник научных статей XI Международной научно-практической интернет-конференции, Могилев, 1–30 июня 2022 г.; под ред. Н. В. Маковской. – Могилев: МГУ имени А. А. Кулешова, 2022. – С. 111–114.

2. Панов, И. О. Особенности применения локальных бинарных шаблонов в задачах компьютерного зрения / И. О. Панов, А. А. Калинин // Вестник Московского государственного технического университета имени Н. Э. Баумана. Серия: Приборостроение. – 2015. – № 4. – С. 92–106.

3. Шишкина, Е. Анализ и сравнительная оценка методов распознавания текстурных изображений / Е. Шишкина // Известия Самарского научного центра Российской академии наук. – 2016. – № 18(2-2). – С. 583–588.

БИОМЕТРИЧЕСКИЕ ТЕХНОЛОГИИ В ЭЛЕКТРОННЫХ МЕДИЦИНСКИХ КАРТАХ

В.А. Крищенович

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Стремительное развитие технологий и интенсивное использование их в сфере здравоохранения привело к цифровизации медицинских систем. Оцифрованная карта пациентов, содержащая полную историю болезни, называется электронная медицинская карта (ЭМК). ЭМК позволяет непрерывно и качественно оказывать медицинскую помощь пациентам, сокращая вероятность потери данных. В связи с тем, что ЭМК содержит большое количество персональных данных, оцифровка личных медицинских карт сопряжена с рисками для безопасности и конфиденциальности [1].

Исследование HOPAA показало, что в период с 2009 по 2022 год поступило 5 150 обращений о случаях утечки данных из медицинских учреждений. Эти утечки, включавшие более 500 файлов, привели к обнародованию 382 262 109 медицинских записей. А по данным статистики HIPAA Journal в 2023 году поступило 725 сообщений об утечке данных, и в результате этих утечек было раскрыто более 133 млн. записей [2]. Для устранения этих рисков необходима целая техническая и правовая инфраструктура. Например, комбинация национального стандарта HIPAA и международного стандарта ISO 13606-4:2019. Информация о пациентах в ЭМК должна быть защищена, чтобы она не угрожала здоровью пациента и его частной жизни [3].

Внедрение биометрических систем в ЭМК позволяет решить ряд проблем, обеспечивая механизм уникальной идентификации личности и дополнительный уровень безопасности. Распознавание лица, голоса помогает предотвратить несанкционированный доступ к медицинским данным и улучшить процесс идентификации пациентов. А внедрение биометрических технологий в управление цифровыми данными позволяет медицинским учреждениям укрепить свои протоколы безопасности и защитить данные пациентов от злоумышленников. Также упрощается контроль доступа к ЭМК и другой конфиденциальной информации, обеспечивая просмотр и изменение данных пациента только авторизованным персоналом.

Ряд преимуществ такие как: обеспечение высокого уровня безопасности, ввиду сложности подделки физиологических параметров, высокая точность и удобство использования делают биометрическую аутентификацию новым стандартом защиты конфиденциальной информации о пациентах. Согласно исследованиям Exactitude