Протокол аутентификации данных на основе стеганографического встраивания информации

Предотвращение подмешивания некорректных данных в процессе обучения интеллектуальной системы

В распределенных системах актуальна задача аутентификации данных, поступающих от участников обучения, а также авторизации узлов, предоставляющих информацию, чтобы исключить подмену источника. Большие объемы информации требуют минимизации вычислительных ресурсов, затрачиваемых на проверку ее подлинности. Использование незначительного искажения исходных данных (стеганографии) гарантирует надёжность происхождения этих данных.

ЦЕННОСТНОЕ ПРЕДЛОЖЕНИЕ

Ресурсоэффективная аутентификация и авторизация узлов, гарантирующие валидность данных в распределенной среде

ОБЛАСТИ ПРИМЕНЕНИЯ

Системы безопасности финансового сектора, производственных компаний, провайдеры облачных платформ для ML, системы передачи изображений

КОНКУРЕНТНЫЕ ПРЕИМУЩЕСТВА

Минимизация вычислительных ресурсов для проверки валидности данных

СТАДИЯ РАЗРАБОТКИ

Разработана программа, проведено тестирование

ОСНОВНЫЕ ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ

- PSNR (соотношение сигнал/шум) 46,1 Дб
- Встраивание информации идет на вейвлетах Хаара
- Типы данных: файлы .jpg

Фото и вносимое искажение

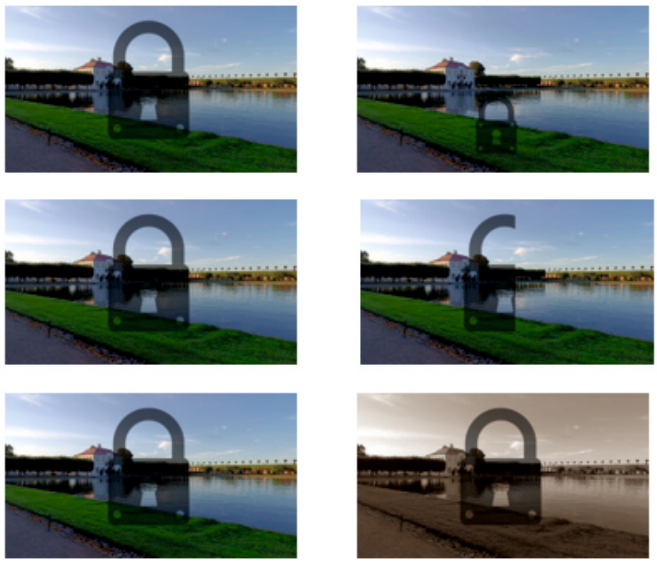

Фото с внесенной стеганографической меткой