ні у професійній підготовці електронних засобів навчання та пакетів прикладних програм виникає розрив в дидактичній логіці навчання; пропонується заповнити цей розрив за допомогою спеціальних програм (інтелектуальних тренажерів), що створюються на основі математичних або імітаційних моделей об'єктів, що вивчаються. При створенні інтелектуальних тренажерів пропонується використовувати наступні принципи: вибір типового класу завдань; організація циклічного, замкнутого управління пізнавальною діяльністю; обов'язкове евристичне рішення завдань, з наступним співставленням результатів з машинним варіантом рішення; створення ситуацій змагань для активізації пізнавальної діяльності.

ПРО ТЕХНОЛОГІЮ ОБРОБКИ ВЕЛИКИХ ОБ'ЄМІВ ДАНИХ

В.В. Бараннік, д.т.н., проф.; В.Ф. Третяк, к.т.н., доц.;
А.В. Власов; А.В. Тристан, к.т.н.
Харківський університет Повітряних Сил імені Івана Кожедуба

В наш час, нове покоління технологій повинно задовольняти вимогам, які часто визначаються критерієм 4V: добувати цінні знання (Value) з великих об'ємів даних (Volume) різного типу (Variety) шляхом швидкого доступу (Velocity). Прогнозується, що інвестиції в технології BD ростимуть щорічно на 40% і до 2015 р. досягнуть 17 млрд. долл. Особливість обробки "великих даних" полягає в тому, що: великі об'єми даних треба зберігати бажано дешевше, ніж в традиційних системах управління базами даних; можуть не в повному обсязі використовуватися багато можливостей розподілених систем управління базами даних; для того, щоб знайти необхідну інформацію, треба виконати переробку величезного об'єму даних; немає необхідності в екстремальній продуктивності. Слід зазначити, що серед загальних принципів побудови Big Data систем виділяють: використання великої кількості (до десятків тисяч) вузлів, на основі відносно дешевого обладнання; кожен вузол є сервером зберігання і обробки даних; обробка даних ведеться в масивно-паралельному режимі; дані зберігаються в декількох копіях (зазвичай в трьох) і відмова вузла або двох не веде до втрати даних; система практично необмежено масштабується. Сфера використання BD: соціальні мережі (Linkedln, Facebook, Digg, Google+), персоналізація (Amazon, Ebay, Yahoo), обслуговування у веб (обслуговування клієнтів і пристроїв), банки і фінанси (виявлення шахрайства), пошук в документах, безпека (аналіз лог файлів, відео, аудіо), наука.

АНАЛИЗ МЕТОДОВ СОКРЫТИЯ ИНФОРМАЦИИ В ИЗОБРАЖЕНИЯХ И ВЫЯВЛЕНИИ ФАКТОВ ПЕРЕДАЧИ СКРЫТЫХ СООБЩЕНИЙ, ВСТРОЕННЫХ В НИХ

И.В. Рубан, д.т.н., проф.; А.Ю. Несмиян; Ю.Н. Рябуха
Харьковский университет Воздушных Сил имени Ивана Кожедуба

В условиях современного развития телекоммуникационных и компьютерных сетей, возникает острая необходимость обеспечения безопасности систем обмена данными. Одним из важных направлений защиты сетей является борьба со скрытой передачей информации. Для реализации подобного рода передачи каких-либо данных, «злоумышленники» умело используют самые разнообразные средства и методы, базирующиеся на алгоритмах стеганографии. Стеганография – это метод организации связи, который собственно скрывает само наличие связи. В последнее время стремительно растет актуальность обеспечения информационной безопасности, что в свою очередь способствует развитию новых направлений и методов стеганографии. В связи с этим, возникает острая необходимость разработки особых подходов к стегоанализу

систем передачи данных для обнаружения скрытой информации. Определение факта наличия скрытого сообщения в вызывающем подозрение контейнере (речи, видео, изображении), является основной задачей стегоанализа. Если в качестве контейнера используется изображение, то наименее стойким к стегоанализу является метод замены наименьших значащих битов или LSB-метод. Известен тот факт, что распределение младших битов сигналов имеет, как правило, шумовой характер (ошибки квантования). Они могут использоваться для внедрения скрытого сообщения, т.к. несут наименьшее количество информации о сигнале. Более стойким к геометрическому преобразованию и обнаружению канала передачи скрытых сообщений является метод, использующий сжатие с потерей данных (например JPEG), так как имеется возможность в широком диапазоне варьировать качество сжатого изображения, что делает невозможным определение происхождения искажения. Исходя из анализа стеганографических методов, можно сделать вывод о необходимости разработки методов установления факта наличия внедренной информации в изображение на основе определения аномальных несвойственных реальным изображениям закономерностей.

ВЫБОР ПРИЗНАКОВ ТЕКСТУРНЫХ ИЗОБРАЖЕНИЙ ТИПА «МАСКИРОВОЧНАЯ СЕТЬ»

И.В. Рубан[1], д.т.н., проф.; О.В. Шитова[1], к.т.н; А.М. Пухляк[2]
[1]Харьковский университет Воздушных Сил имени Ивана Кожедуба;
[2]Министерство Обороны Украины

Сложность использования известных подходов к задаче распознавания на изображениях замаскированных объектов, получаемых оптическими средствами в результате воздушной разведки, определяется тем, что целенаправленные мероприятия по маскировке объектов существенно снижают видимость объектов на изображениях. В работе рассматривается метод маскировки военной техники маскировочной сетью. Одним из этапов автоматизированного распознавания объектов, скрытых маскировочной сетью, является отделение на аэрофотоснимке участка земной поверхности изображения маскировочной сети от фона – травы, грунта, снега, песка и т.д. Существующие методы распознавания становятся неприменимыми по причине отсутствия механизмов обработки текстурных областей типа «маскировочная сеть». Исходя из этого, актуальной задачей является исследование свойств маскировочных сетей с целью выявления их характеристических особенностей и дальнейшей разработки методов, позволяющих локализовывать области интереса на аэрофотоснимках в условиях маскировки. Представление изображения маскировочной сети в виде текстуры позволяет использовать набор признаков, характеризующих текстуру маскировочных сетей. Под текстурными признаками, как правило, понимают характерные признаки, общие для текстур одного класса. В работе для выбора признаков были проанализированы гистограммы 40 изображений земной поверхности четырех классов (травы, грунта, снега и песка) и такое же количество изображений соответствующих им маскировочных сетей. Для сегментации изображений маскировочных сетей в работе проанализированы статистические признаки текстур, а именно энтропия, однородность и средняя яркость. Выбор именно этих признаков обусловлен соответствием требованиям помехоустойчивости, инвариантности к масштабу и повороту изображения маскировочной сети, а также тем, что их расчет не требует высоких вычислительных затрат. При расчетах были использованы изображения одинаковых размеров с глубиной цвета 8 бит на пиксель (полутоновые изображения с 256 градациями яркости). Расчеты показали, что наиболее информативными признаками текстуры для сегментации маскировочной