ется. Еще больше информации теряется при преобразовании сил и совершаемой ими работы в тепловую энергию. Именно поэтому из двух видов сигналов (температура и вибрация) в диагностике предпочтение следует отдать вибрации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Александров А.А., Барков А.В, Баркова А.В., Шафранский Н.А.*Вибрация и вибродиагностика судового электрооборудования. Л.: Судостроение, 1986.
2. *Барков А.В., Баркова Н.А., Азовцев А.Ю.* Мониторинг и диагностика роторных машин по вибрации. Рекомендации для пользователей систем диагностики. Спб: СПбГМТУ, 2000.
3. *Барков А.В., Баркова Н.А* Интеллектуальные системы мониторинга и диагностики машин по вибрации. СПб: Изд-во СПбГМТУ. 1999.Вып. 9,

И.П. Мирошниченко, В.И. Мирошниченко, В.В. Нестеров

МЕТОДИКА РЕГИСТРАЦИИ ИНФОРМАЦИИ С ОПТИЧЕСКИХ ИНТЕРФЕРОГРАММ

Использование интерференционно-голографических методов в настоящее время для проведения высокоточных измерений различных параметров достаточно хорошо известно. Существующие схемы регистрации информации с оптических интерферограмм основаны на использовании фотоприемников, обеспечивающих измерение интенсивности излучения в некоторой заданной области интерферограммы. В этом случае геометрические характеристики апертуры фотоприемника ограничивают функциональные возможности измерительного устройства, что приводит к снижению информативности и точности результатов измерений, особенно при использовании оптических голограмм.

Разработана и реализована методика регистрации информации с оптических интерферограмм при проведении экспериментальных исследований. В состав аппаратных средств, реализующих методику, входят унифицированный экран, аналоговая или цифровая видеотехника и персональный компьютер.

Предлагаемая методика позволяет произвести регистрацию изображения интерферограммы по всей ее поверхности в пределах области экрана, выделить из изображения исследуемые фрагменты интерферограммы и произвести идентификацию полученной информации, соответствующей изменению измеряемого параметра.

Методика использована в процессе проведения экспериментальных исследований для создания оптимальных структур чувствительных элементов перспективных средств измерений малых перемещений поверхностей объектов испытаний, а также при разработке новых видов детекторов для оптических каналов связи.

А.В. Аграновский, С.В. Геращенко, Н.Ю. Полушкин

НОСИТЕЛИ ИНФОРМАЦИИ СО ВСТРОЕННЫМИ СИСТЕМАМИ ЗАЩИТЫ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА, РЕАЛИЗОВАННЫЕ НА МИКРОСХЕМАХ FLASH–ПАМЯТИ

Защищенные твердотельные носители информации являются одним из наиболее перспективных направлений для хранения и переноса конфиденциальной информации.

Защищенные твердотельные носители информации базируются на микросхемах FLASH-памяти со скоростью записи/чтения до 1 Мб/с и объёмом до 512 Мб, для под-

ключения к компьютеру используется, в основном, интерфейс USB – как наиболее подходящий по пропускной способности и удобству для пользователя.

Существующие решения в области твердотельных накопителей довольно однотипны. Наиболее известным является зарубежный ЗТН DiskOnKey фирмы M-Systems, USBDrive фирмы JMTek, ASUS Ai-Flash, Luwen EasyDisk .

Использование DiskOnKey и всех остальных устройств на Windows 98 требует установки дополнительного драйвера. По умолчанию вся память устройства является общедоступной. Для обеспечения конфиденциальности используется программное обеспечение KeySafe. Данный программный модуль представляет собой виртуальный шифродиск с возможностью закрытия данных от чтения/записи в самой микросхеме Flash памяти (в спецификациях к нему не указаны алгоритмы и способы преобразования хранимой информации, что указывает на возможное наличие уязвимых мест в данных устройствах).

USBDrive и аналогичные ему устройства фирм ASUS - Ai-Flash, Luwen – EasyDisk для обеспечения конфиденциальности используют специальный драйвер, создающий виртуальный шифродиск. Эти устройства характеризуются объемами памяти от 32 до 512Мб и средней скоростью обмена 600 – 700 кб в секунду [1,2].

Учитывая, что микросхемы Flash-памяти имеют ограниченные ресурсы записи/стирания информации, очевидной проблемой становится проблема рационального использования ячеек памяти.

Для обеспечения максимального срока службы устройства в условиях ограниченного числа допустимых циклов стирания/записи должен использоваться статистический подход, при котором стираемые ячейки максимально равномерно распределяются по области памяти и используются для записи приблизительно равновероятно.

Исходя из физических принципов работы запоминающего устройства, запись и чтение информации сопровождаются сравнительно высокой вероятностью возникновения ошибок. Поэтому в состав программного обеспечения должен входить модуль обнаружения и коррекции ошибок.

Защиту твердотельного носителя можно разделить на две части:

1. Программная защита – создание на носителе виртуального шифродиска с возможностью различных видов аутентификации [4,5].
2. Аппаратная защита – шифрование небольшого объёма данных, по выбору пользователя, при прохождении, их через микроконтроллер накопителя, экстренное уничтожение ключевой информации необходимой для работы с накопителем и расшифровки остальных данных, находящихся в накопителе, аппаратное закрытие микросхемы памяти от записи и/или чтения.

Высокая скорость обмена данными с микросхемами flash памяти и необходимость простого подключения к компьютеру обязывает эти устройства работать по протоколу USB. [3]

При использовании в качестве компоненты системной интеграции интерфейса USB, предназначенного для подключения периферийных устройств, твердотельный носитель информации опознается операционной системой как мобильный жесткий диск. Для реализации более эффективного варианта интегрирования устройства с поддержкой взаимодействия с подсистемами авторизации и защиты ОС Windows NT/2000/XP следует использовать специально разработанные драйверы клиентской части USB.

Твердотельный носитель информации в этом случае будет представлен как некомпозитное USB-устройство, драйвер которого автоматически устанавливается в виде драйвера минипорта на рабочей станции пользователя. В перечень сервисных функций драйвера минипорта входят функции взаимодействия с подсистемой безопасности Windows а также обеспечение обращения к данным на flash-диске как к обычным файлам, на

уровне драйвера операционной системы. Драйвер должен обеспечивать необходимую трансляцию виртуальной блочной структуры файла в конкретные физические адреса запоминающего устройства. Прикладная программа может просто производить чтение и запись в запоминающее устройство, будто бы она работает с обыкновенным жестким диском.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. M-Systems, DiskOnKey, DiskOnChip technical description, http://www.m-sys.com.
2. ASUS, Ai-Flash technical description, http://www.asus.com/.
3. "USB Standard Specifications", USB Consortium Press, 2000.
4. *Чмора А.Л.* Современная прикладная криптография. - М.: Гелиос АРВ, 2001.
5. *Goldreich O.* Towards a theory of software protection, Proc. 19thAnn. ACM Symp. on Theory of Computing 1987. p. 182–194.

А.В. Аграновский, Р.Э. Арутюнян, Р.А. Хади

СРЕДСТВА ПОИСКА В ТЕКСТОВЫХ БАЗАХ ДАННЫХ

Проблема поиска в базах данных, состоящих из текстовых документов, является одной из наиболее востребованных в современном мире. Поиск обычно осуществляется по запросу пользователя, который либо является предложением на естественном языке, либо набором ключевых слов.

Классическими методами поиска являются булев, векторный и вероятностный поиски. Булева модель основана на построении инвертированного индекса, в котором для каждого ключевого слова указываются документы, содержащие его. Поиск в этом случае сводится к получению множеств документов, содержащих все слова запроса. Векторная модель основана на построении для каждого документа вектора, элементами которого являются веса ключевых слов в этом документе. Для выборки документов при поиске аналогичный вектор составляется для запроса, после чего вычисляются косинусы углов между этим вектором и вектором каждого документа. Вероятностная модель основана на максимизации апостериорной вероятности релевантности каждого документа запросу, вычисляемой с точностью до постоянного множителя α по формуле

$$P = \alpha P(\text{документ D релевантен}) P(\text{запрос Q} \mid \text{документ D релевантен}) .$$

В реальных задачах указанные модели могут объединяться и дополняться для достижения лучших результатов.

Важными являются вопросы кластеризации текстовых документов. Одним из алгоритмов, применяемых для решения этой проблемы, является алгоритм k средних, в котором представителями документов являются векторы, аналогичные рассмотренным в векторной модели поиска. Кластеризация может быть полезной для подготовки множества документов к поиску. Также кластеризованное множество документов может быть и результатом поиска, если прямой поиск не привел к успеху.

Одной из важных проблем при поиске является предоставление пользователю именно тех документов, которые его интересуют. При этом встает вопрос о том, что некоторые из найденных поисковой системой документы могут быть уже известны пользователю. Для отслеживания этой ситуации и соответствующей пересортировки результатов поиска, вводятся вероятности того, что каждый из документов уже известен пользователю. Эти вероятности зависят от информации о конкретном пользователе и документе.