ТЕХНОЛОГИЯ ЗАЩИТЫ ФОТОГРАФИЧЕСКИХ ДОКУМЕНТОВ: ГОЛОГРАФИЧЕСКИЙ ПОДХОД PHOTOWATERMARK

Евгений КАЧУРОВ,
Всероссийская государственная налоговая академия,
(Российская Федерация)

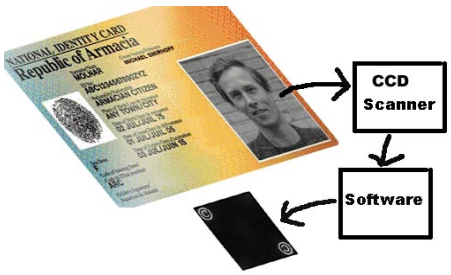
Противодействие методам подделки и фальсификации бумажных, а в последнее время и пластиковых документов является традиционной и актуальной задачей защиты носителей информации. Одним из ключевых элементов для многих документов является фотография. Можно не говорить какой экономический и правовой вред наносит фальсификация и подделка фотографий на таких документах как паспорт, водительское удостоверение, кредитная или идентификационная карта, медицинский полис и другие.

В настоящее время интенсивно разрабатываются новые средства защиты, основанные на последних достижениях физики, химии, микроэлектроники. Наиболее привлекательным решением выглядит встраивание микрочипов. Цифровое представление данных, обеспечивает удобный ввод и редактирование данных, высокую помехоустойчивость записи, простоту считывания данных. Однако подобная простота привлекательна и для взломщиков. Эксперименты с взломом микрочипов, встроенных в паспорт, продемонстрировали весьма низкую безопасность этой технологии - все данные, хранящиеся в электронном виде, стали доступны "злоумышленникам", включая отпечатки пальцев, фотографию и весь шифрованный и открытый текст.

Основной недостаток существующих средств защиты документов с фотографиями состоит в отсутствии условной зависимости между событием подмены объекта идентификации (фотографии владельца документа) и состоянием элемента защиты (например: оптической голограммы или встроенного микрочипа). В этом случае, подмена фотографии на карте при сохранении защитного элемента не приводит к выводу о подделке документа.

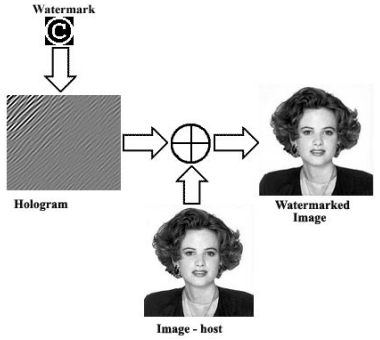
В этом контексте проиллюстрируем технологию PhotoWaterMark для защиты фотографических документов на бумажной или пластиковой основе.

Технология PhotoWaterMark представляет собой сочетание стеганографического подхода сокрытия и криптографического подхода шифрования данных, что обеспечивает практическую невозможность взлома. Причем, основное неудобство для взлома заключается в аналоговом представлении скрываемых данных. Сущность стеганографическго подхода состоит в сокрытии самого факта передачи или внедрения информации в носитель. Один из таких методов встраивания скрытых водяных знаков в фотографии положен в основу настоящей технологии.

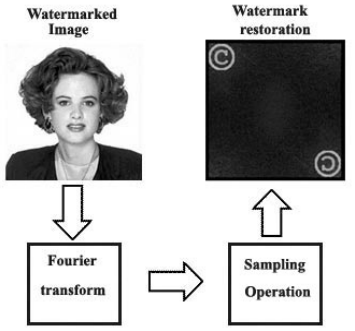


Рассмотрим процедуру контроля документов. Схематично процесс идентификации, например владельца ID карты, можно представить как совокупность программных и технических средств, работающих в режиме реального времени, когда фотоизображение считывается сканером на ПЗС матрице, подвергается некоторым преобразованиям с целью выделения сокрытого водяного знака, а затем скрытая информация визуализируется на экране монитора. На схеме, скрытые данные представлены в виде графического изображения знака копирайта ©.

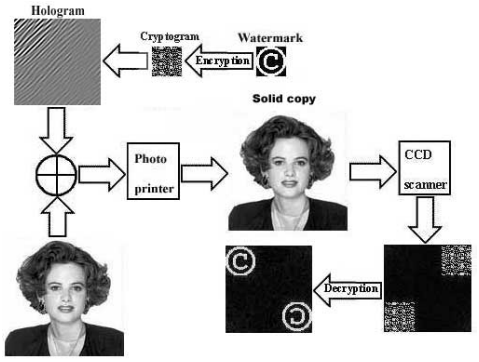
В основу метода встраивания, скрываемых данных, положен принцип интерференции. Сущность метода состоит в синтезе цифровой голограммы водяного знака и аддитивно-мультипликативном смешивании полученной голограммы с изображением-контейнером (смотри рисунок):



Для реализации обратной процедуры - процедуры восстановления водяного знака из голограммы, достаточно выполнить двумерное преобразование Фурье, если конечно известны параметры синтеза голограммы, и в частности пространственная несущая. В реальном времени, эта функция реализуется с помощью цифровых сигнальных процессоров (ЦСП). Например, ЦСП фирмы Texas Instruments, позволяют выполнить эту процедуру за доли секунды. В процессе восстановления водяного знака, можно наблюдать как восстановленный объект, так и его голографическое изображение (смотри рисунок):



Важнейшим элементом любой информационной системы является шифрование конфиденциальной информации. Рассматриваемый подход не является исключением - двумерные криптограммы органически встраиваются в цепочку преобразований двумерных изображений (смотри рисунок):



Стойкость шифра определяется исключительно стойкостью секретного ключа. Таким образом, аналоговое исполнение средства защиты объекта идентификации (фотографии владельца) и скрытый характер встраиваемых данных представляет собой малопривлекательный объект для цифрового взлома, а подключение криптографической подсистемы к стеганографической системе сокрытия данных обеспечивает мощный барьер несанкционированному вмешательству.

В заключение, стоит отметить, что предложенную технологию можно рассматривать как дополнительную степень защиты документов к существующим технологиям. И в этом смысле, на PhotoWaterMark возлагается защита фотографических материалов на аналоговом уровне, а за микрочипами остается их неоспоримое преимущество - простой и удобный способ работы с цифровыми массивами данных.

"TIME CARD" - БЕЗОПАСНОСТЬ ВАШЕЙ КОМПАНИИ В ВАШИХ РУКАХ!

Станислав ЖУК, Евгения ЗГАРДАН
Теоретический Лицей им. "Михаил Когэлничану"
(Республика Молдова)

Information security is the process of protecting information. It protects its availability, privacy and integrity. "TIME CARD" - the software for the account of working hours of the personnel of the company which possesses following advantages: gives possibility of automation of the account of working hours and protection against deliberate infringement of the data.

Кто владеет информацией, тот владеет миром! Пренебрежение этой истиной может обойтись в миллионы и миллиарды убытков. Даже в современной истории можно найти массу красноречивых примеров, когда один единственный файл или документ вершил судьбы сотен тысяч людей и целых корпораций. В силу этих причин защита информации сегодня многими бизнес структурами считается главным