ИСПОЛЬЗОВАНИЕ ФИЗИЧЕСКИ НЕПОВТОРИМЫХ ОСОБЕННОСТЕЙ В БОРЬБЕ С КОНТРАФАКЦИЕЙ

Автор: Сергей ОЛЕЙНИК

Universitatea Tehnică a Moldovei

Аннотация: *В данной работе рассматриваются типы ценных документов и основные способы их защиты. Описываются преимущества и недостатки наиболее популярных методов защиты. Определено перспективное направление по борьбе с контрафакцией.*

Ключевые слова: *защита документов, физически неповторимые особенности, особенности поверхности бумаги, алгоритмы валидации документов, борьба с контрафакцией.*

1. ВВЕДЕНИЕ

Биометрия сегодня является наиболее эффективным средством для идентификации и аутентификации физических лиц. Схожий подход может быть применён для проверки подлинности ценных бумаг, банкнот, произведений искусства, этикеток и упаковок различной продукции, так как поверхность почти каждого изделия имеет свои естественные изъяны, например, для бумажных документов такими изъянами является хаотичное перекрытие волокон.

2. ЦЕННЫЕ ДОКУМЕНТЫ

Ценный документ – это любой документ, имеющий материальную ценность.

Существуют следующие типы документов [1]:

- **Официальные документы** – сертификаты (рождения, собственности и т.д.), дипломы, идентификационные и членские карты, сертификаты компаний (ISO), разрешения и лицензии (водительские, на охоту, рыбалку, строительство и т.д.), регистрация автомобиля.
- **Оригинальные документы** – входные билеты и билеты на мероприятия, сертификаты подлинности, этикетки и упаковки, бланки с рецептами, страховые документы.
- **Оборотные документы** – авиабилеты, посадочные талоны, чеки, купоны, подарочные сертификаты, ваучеры, денежные переводы и дорожные чеки.

3. НЕОБХОДИМОСТЬ В ЗАЩИТЕ

Существуют различные методы мошенничества и для того, чтобы защитить документы необходимо понимать от чего их нужно защищать. Следует понимать различные виды мошенничества, чтобы выбрать правильное решение для защиты.

Различают следующие виды мошенничества [1]:

- **Кража –** присвоение документов с целью последующего их использования или продажи.
- **Контрафакция** – репродукция оригинального документа с изменением исходных данных.
- **Подделка –** изменение существующего документа.

4. ЭЛЕМЕНТЫ ЗАЩИТЫ ДОКУМЕНТОВ

Элементы защиты документов делятся на разные категории, и основными категориями защиты документов являются:

- **Аннулирующие особенности** – это особенности, проявляющиеся на документе при сканировании или цветном копировании.
  Преимущества: относительно низкая стоимость.
  Недостатки: Существуют сканеры, справляющиеся с аннулирующими особенностями.
- **Микропечать** – это напечатанный текст, сливающийся в прямую линию при рассмотрении невооружённым взглядом, однако он читается при использовании увеличительного стекла.
  Преимущества: Низкая стоимость, простые принтеры не могут качественно её воспроизвести.
  Недостатки: Необходимость в использовании увеличительного стекла для проверки.
- **Радужная печать** – разновидность печати, при которой краски разного цвета плавно переходят друг в друга и смешиваясь образуют новые цвета.
  Преимущества: Смесь красок затрудняет работу старых копиров и сканеров.
  Недостатки: Увеличение стоимости, печать воспроизводится современной техникой.

- **Рамки высокого разрешения** – напечатанные на документах рамки высокого разрешения.
  Преимущества: Сложные линии плохо поддаются копированию, низкая стоимость.
  Недостатки: Лицо, проверяющая документ должно иметь образец для сравнения.
- **Водяной знак** – наносится специальной препрозрачной или непрозрачной белой краской. При освещении бумаги с обратной стороны переменная плотность бумаги приводит к прохождению света через неё с различной интенсивностью.
  Преимущества: Практически невозможно воспроизвести копиром или сканером.
  Недостатки: Воспроизводится с использованием резиновой печати и специальной краски.
- **Тиснение фольгой** – тиснение документа отражающим изображением из фольги.
  Преимущества: При копировании изображение выглядит тёмным и неотражающим.
  Недостатки: Значительно увеличивает стоимость документа.
- **Чеканка** – создание выступающего изображения на документе.
  Преимущества: Невозможно дублировать документ сканированием или копированием.
  Недостатки: Умеренное увеличение стоимости документа.
- **Голограмма** относится к классу изображений, известных как дифракционные оптически изменяемые устройства изображений. Проявляется в результате интерференции света от разных источников по шаблону. [2] Она высоко оценивается с точки зрения безопасности.
  Преимущества: Воспроизводится только специализированным дорогим оборудованием.
  Недостатки: Не предотвращает возможное подделывание, но значительно усложняет его.
- **Видимые и невидимые флуоресцентные волокна** – синтетические волокна, добавляемые в процессе изготовления бумаги с целью усложнить процесс копирования. Метод основывается на характеристиках проводимости света оптическими волокнами и уникальной конфигурации волокон, внедрённых в бумагу. При освещении одного конца волокна происходит свечение второго конца. Положение обоих освещённых концов определяет “подпись волокон”. Документ сканируется с одинаковым освещением волокон и, если данные полученные при сканировании совпадают с ранее закодированными, то документ является подлинным (рисунок 1). [2]
  Преимущества: Затрудняет контрафакцию и характеризуется высокой степенью защиты.
  Недостатки: Требуется использования ультрафиолетового света для верификации. Применение оптических волокон добавляет значительную стоимость в процесс производства документов. [1]

Примеры аннулирующих особенностей и микропечати представлены на рисунке 1.

Рисунок 1 – Аннулирующие особенности “VOID” [1], микропечать [1] и сканирование внедрённых волокон [2]

5. ФИЗИЧЕСКИ НЕПОВТОРИМЫЕ ОСОБЕННОСТИ

5.1 ОСОБЕННОСТИ ПОВЕРХНОСТИ БУМАГИ

При детальном рассмотрении поверхности бумаги, используя электронный микроскоп, можно наблюдать трёхмерную структуру переплетающихся волокон. Эти структуры не повторяются, и рисунок принимает разнообразные формы на различных участках поверхности бумаги (смотри рисунок 2a).

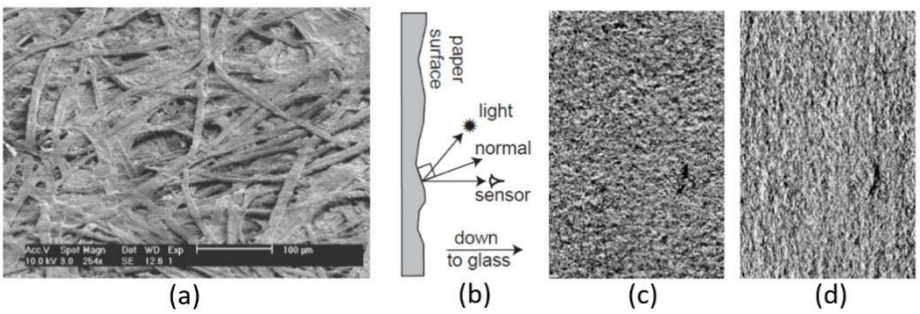

Рисунок 2 – a) поверхность бумаги; b) отрезок бумаги длиной 10 мм при сканировании сверху вниз; c), d) сканированный регион слева направо и соответственно справа налево. [3]

Физический документ может быть аутентифицирован на основе естественно сформированных неровностей структуры. [3] Существует метод, позволяющий оценить трёхмерную структуру бумаги, используя сканер. В результате сканирования при различной ориентации документа будут получены различные изображения. Свет попадающий на сенсор сканера зависит от угла между источником света и нормалью к поверхности (рисунок 2b). На основании извлечённых особенностей поверхности формируется отпечаток бумаги, который уникально идентифицирует его. Отпечаток документа сохраняется в базе данных для дальнейшей верификации или же может быть нанесён на документ вместе с цифровой подписью для дальнейшей верификации. Отпечаток может быть использован для проверки того, что векторы особенностей документов совпадают без необходимости раскрытия вектора особенностей исходного документа. Процесс регистрации и проверки документа представлены на рисунке 3. При регистрации документ сканируется, оценивается его трёхмерная структура поверхности и генерируется вектор особенностей V, который описывает уникальную структуру документа. Полагается, что два документа с одинаковыми векторами особенностей являются идентичными. Для защиты вектора особенностей и препятствованию подделыванию путём воспроизведения вектора особенностей используется хеширование H(V) извлечённого вектора особенностей. Для надёжности работы измерения ошибки вектора особенностей в процессе регистрации извлекается информации о коррекции ошибки из вектора V и сохраняется в отпечатке. Отпечаток также содержит случайное число для инициализации генератора псевдослучайных чисел, используемого при расчёте вектора особенностей.

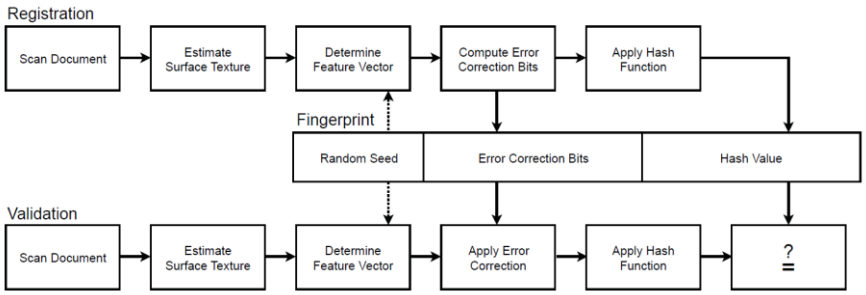

Рисунок 3 – Процесс регистрации и валидации [3]

В процессе валидации доступ к исходному вектору особенностей отсутствует. Валидация документа требует определения вектора особенностей, используя случайное число, сохранённое в отпечатке. При валидации учитывается потенциальная порча вектора характеристик $\tilde{V}'$ и при получении вектора $\tilde{V}$ используются биты коррекции ошибок. Рассматриваемый документ считается валидным, если на основании вектора особенностей рассчитывается хеш значение, совпадающее со значением, хранимым в отпечатке, то есть $H(\tilde{V}) = H(V)$.

Описанный подход удовлетворяет следующим критериям:

- *Уникальность* – каждый документ идентифицируется и отличается от других по своей структуре.
- *Согласованность*. Отпечаток бумаги может быть многократно проверен различными сторонами на протяжении всего периода существования документа.
- *Выразительность*. Отпечаток документа короткий и может быть легко рассчитан.
- *Надёжность*. Документ может быть проверен по отпечатку даже после небрежного отношения с документом.
- *Сопротивляемость к подделыванию*. Воспроизведение отпечатка бумаге очень сложно и дорого.

Данный метод может быть использован при проверке подлинности ценных бумаг, билетов, паспортов, этикеток и может применять до нанесения на бумагу содержимого документа, однако необходимо наличие сканера, что делает применение этого метода не всегда возможным.

5.2 ОСОБЕННОСТИ ПРОИЗВЕДЕНИЙ ИСКУССТВА

На поверхности любого произведения искусства есть особенности, которые могут быть использованы для его идентификации. Эти структуры могут быть выявлены. На рисунке 4a представлена картина маслом с выделенной области-сертификата, на рисунке 4b – для скульптуры и 4c для каменной литографии. Весь процесс проверки подлинности произведения искусства представлен на рисунке 4d.

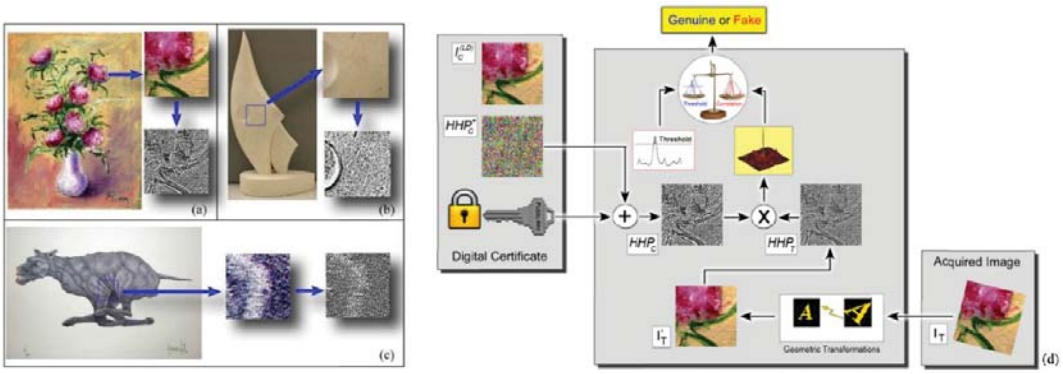

Рисунок 4 – a) картина маслом; b) скульптура; c) каменная литография; (d) полная схема проверки произведения искусства на подлинность [4]

Процесс создания хилеметрического [4] сертификата состоит в извлечении с определённой области произведения искусства случайного шаблона, который сложно повторить. Первым шагом является выбор области и точек доверия внутри неё. Точки доверия используются для коррекции геометрической дисторсии на этапе верификации. На следующем этапе создаётся хилеметрический хеш шаблон для области интереса, переведённой в оттенки серого с применением фильтра высоких частот, нормализацией и последующим выделением границ. Выбранная область в низком разрешении записывается в цифровой сертификат аутентификации. В сертификат также записывается хеш шаблон, соответствующий выбранной области. Для того, чтобы не допустить подделку сертификата, он подписывается цифровой подписью DSS (Digital Signature Standard), основывающейся на инфраструктуре PKI. [5]

6. ЗАКЛЮЧЕНИЕ

Борьба с контрафактной продукцией и защита ценных бумаг всегда была и остаётся актуальной. Большинство существующих подходов характеризуются дороговизной или недостаточной эффективностью, а подлинность продукции или ценных бумаг преимущественно определяется вручную. Традиционный подход аутентификации предметов, чувствительных к подделке, основываются на присутствии засекреченных идентификаторов или сложном процессе производства, который непросто воспроизвести. Зачастую это неприемлемо, так всё это отражается на стоимости продукции. Новым перспективным направлением для исследований является изучение оптических особенностей структуры поверхности для подтверждения подлинности. Используя биометрический подход, можно увеличить степень защиты ценных документов и упростить процесс проверки подлинности.

БИБЛИОГРАФИЯ

1. Ellen Carter. *Session 40: Are Your Valuable Documents Vulnerable to Fraud?*
2. Declan McAleese. *Counterfeit Currency Detection Techniques.* [Электронный ресурс].– Режим доступа: http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/AV0506/s0128541.pdf.
3. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman and Edward W. Felten. *Fingerprinting Blank Paper Using Commodity Scanners.* – IEEE Symposium on Security and Privacy, May 2009.
4. Lorenzo Cozzella, Giuseppe Schirripa Spagnolo and Fabio Leccese. *Biometric-Like Approach for Verifying Artwork Authenticity.* Canadian Center of Science and Education, 2013.
5. Lorenzo Cozzella. Hylemetric *Techniques for data and Information Security.* – Scuola Dottorale EDEMOM, June 2013.