УДК 004.94

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ПРОЦЕССОВ ВЕРИФИКАЦИИ В ДОКУМЕНТООБОРОТЕ ОРГАНИЗАЦИИ

Кадильникова Татьяна Михайловна, д.т.н., профессор
Минюк Ольга Николаевна, к.с.-х.н., доцент
Полесский государственный университет
Kadilnikova Tatyana Mikhailovna, Ph.D, Kadilnikovatm@ukr.net
Minyuk Olga Nikolaevna, PhD, minola86@mail.ru
Polessky State University

Аннотация. Предложено решение проблемы защиты информации, содержащейся в электронном документе, путем верификации электронной цифровой подписи с помощью нейронных сетей. Построена структура базы данных программного приложения.

Ключевые слова: электронная цифровая подпись, нейронная сеть, документооборот, бинарное изображение, классификатор.

С развитием информационных технологий для документооборота открылись огромные возможности. С появлением и развитием глобальной сети Интернет и его важным атрибутом – электронной почтой, проблема транспортировки и хранения практически перестала быть проблемой. По электронной почте электронный документ приходит к получателю в считанные минуты. Но, с устранением одной проблемы, появилась другая – защита информации, которую содержит электронный документ, безопасность информации которого особенно важна в наше время.

Электронный документ, в отличие от бумажного документа, невозможно закрепить печатью или подписью. Поэтому в нем их функции выполняет электронная цифровая подпись (ЭЦП), проверка подлинности которой представляет значительный интерес. Документы, которые поступают в организацию, проходят следующие стадии: передача на исполнение; предварительное рассмотрение; первичная обработка; рассмотрение руководством; регистрация [1].

Для организации на сервере организации электронного документооборота создают базу данных, где хранят все созданные документы. Возможен доступ как через интернет (внешний), так и по локальной сети (внутренней). Документы загружаются или сохраняются в определённые выделенные папки организации. Папки распределяются соответственно с иерархической структурой подразделения организации. Модифицировать, создавать, удалять созданные документы может лицо, которое наделено соответствующими правами.

В настоящее время используется электронная цифровая подпись и шифрование. У каждого сотрудника имеется два ключа (ключевая пара) – закрытый и открытый. При помощи закрытого ключа формируется ЭЦП и расшифровывается информация, предназначенная данному пользователю. Закрытый ключ должен быть доступен только его владельцу. Открытый ключ служит для проверки ЭЦП и шифрования и доступен любому пользователю информационной системы.

Следуя из вышесказанного, полностью полагаться на одну лишь электронную цифровую подпись нельзя. Поэтому предлагается разработка и внедрение системы верификации документов в систему электронного документооборота (СЭД) с использованием биометрической защиты, а именно – проверка рукописной подписи на документе с помощью компьютерного зрения и нейронных сетей.

Распознавание рукописной подписи происходит в несколько этапов.

1. **Предварительная обработка изображения** (processing): на этом этапе происходит обработка изображения с целью повышения его качества и приведения его к виду, удобному для извлечения признаков. Задачу можно сформулировать следующим образом: по изображению текста A необходимо построить бинарное изображение B того же размера такое, что:

$$f(i,j)\begin{cases}1, \text{если } I(i,j) \geq d,\\ 0, \text{если } I(i,j) < d,\end{cases} \qquad 1)$$

где d называется порогом бинаризации.

При этом на гистограмме яркости изображения текста наблюдается два пика: высокий пик в области светлых пикселей (бумага) и низкий пик в области тёмных пикселей (текст). Поэтому задача поиска порогового значения яркости, т. е. такого, что пиксели с яркостью выше этого значения (фон) будут считаться чёрными, а ниже (подпись) – белыми (такое «инвертирование» цвета делается в целях упрощения применения многих алгоритмов в дальнейшем), является задачей поиска оптимального значения между двумя пиками гистограммы.

Если цвет пикселя (его код от 0 до 255) меньше цвета порога бинаризации (в нашем случае – оттенки белого, код – приблизительно 240 – 255), то этот пиксель удаляется с изображения. В бинарном инверсионном методе такие пиксели наоборот, сохраняются на изображении, а остальные удаляются. Результатом этапа предварительной обработки изображения является бинарное изображение черной подписи на белом фоне, соответствующей исходному изображению.

2. Извлечение признаков (feature extraction): на этом этапе формируются признаковые описания, по которым можно сравнивать подписи. Пусть $\boldsymbol{X}$ – множество рассматриваемых объектов, $\boldsymbol{Y}$ – конечное множество. Существует функция $\boldsymbol{y} : \boldsymbol{X} - \boldsymbol{Y}$, значения которой известны только на конечной выборке $X = \{(x_1, y_1), \ldots ,(x_m, y_m)\}$. Требуется построить функцию $a : \boldsymbol{X} \to \boldsymbol{Y}$, близкую к $\boldsymbol{y}$. Функция a называется *классификатором*.

Признаком называется отображение $f : \boldsymbol{X} \to D_f$, где D_f — множество значений признака. Если заданы признаки $f_1, \ldots , f_n$, то вектор $(f_1(x), \ldots , f_n(x))$ называется *признаковым описанием* объекта $x \in \boldsymbol{X}$. Построение признакового описания для объекта x также носит название *извлечение признаков*.

Обычно классификаторы строят в виде $a(x) = b(\mathbf{f}(x))$, где $\mathbf{f}(x) = (f_1(x), \ldots , f_n(x))$ – некоторое признаковое описание объекта. Удачный выбор признакового описания для объекта позволяет резко повысить качество системы распознавания. Для задачи распознавания объектов на изображении вообще и распознавания подписи в частности существует три основных класса признаков: статистические (признаки, хранящие информацию о распределении пикселей на изображении), геометрические (признаки, хранящие информацию о геометрических свойствах объекта), структурные (признаки, описывающие структуру объекта, т.е. наличие составных частей и связей между ними).

3.Классификация (classification): на этом этапе по признаковым описаниям, построенным на этапе извлечения признаков, система принимает решение о том, к какому заранее известному классу отнести выделенный на этапе сегментации элемент (в нашем случае – этот ли человек поставил эту подпись?). Для обучения используются стандартные методы, чаще всего метод обратного распространения ошибки [2]. Функция активации нейронов (передаточная функция) – любая, по выбору исследователя. Для задачи классификации используется свёрточная нейронная сеть.

Данная сеть состоит из двух повторяющихся участков, которые содержат по два слоя свёртки и по одному слою подвыборки. Данные участки предназначены для выделения основных признаков рукописной подписи. В

конце сети расположен классификатор, который состоит из одного полносвязного слоя, который содержит 512 нейронов, и выходного слоя, который содержит 10 нейронов.

На вход сети поступают полутоновые изображения размером 250 на 150 пикселей в одном канале. На первом слое свёртки используется 32 карты признаков размера 2 на 2. То есть каждый нейрон свёрточного слоя подключен к квадратному участку изображения размером 2 на 2. После этого идёт слой подвыборки (пуллинга), на котором выполняется уменьшение размерности изображения. Следующий свёрточный слой по сравнению с первым имеет похожую архитектуру: 64 карты признаков с ядром свёртки 1 на 1. Затем используется снова такой же слой пуллинга. Третий сверточный слой имеет 128 карт признаков с ядром свёртки 1 на 1, и за ним идет третий слой пуллинга. После нескольких прохождений свёртки изображения и уплотнения с помощью пулинга система перестраивается от конкретной сетки пикселей с высоким разрешением к более абстрактным картам признаков, как правило, на каждом следующем слое увеличивается число каналов и уменьшается размерность изображения в каждом канале. В конце концов, остаётся большой набор каналов, хранящих небольшое число данных (даже один параметр), которые интерпретируются как самые абстрактные понятия, выявленные из исходного изображения.

Эти данные объединяются и передаются на обычную полносвязную нейронную сеть, которая тоже может состоять из нескольких слоёв. При этом полносвязные слои уже утрачивают пространственную структуру пикселей и обладают сравнительно небольшой размерностью (по отношению к количеству пикселей исходного изображения) [3].

4.Обработка результатов (postprocessing): на этом этапе происходит выдача результатов по результатам классификации.

Принципиальная схема, описывающая процесс подписания и передачи документа в системе электронного документооборота с внедрением биометрической верификации представлена на рисунке 1.

Для внедрения метода биометрической верификации достаточно:

1. поставить свою подпись на электронном документе при его создании/отправлении;

2. занести свою подпись в базу данных подписей, если ее там нет, в нескольких экземплярах;

3. при получении документа из информационной системы проверить не только ЭЦП, но и подпись.

При работе с подписью, которая уже есть в базе, нейронная сеть выявляет «степень похожести» – насколько точно эта подпись похожа на подпись в базе – и выдает пользователю СЭД результат.

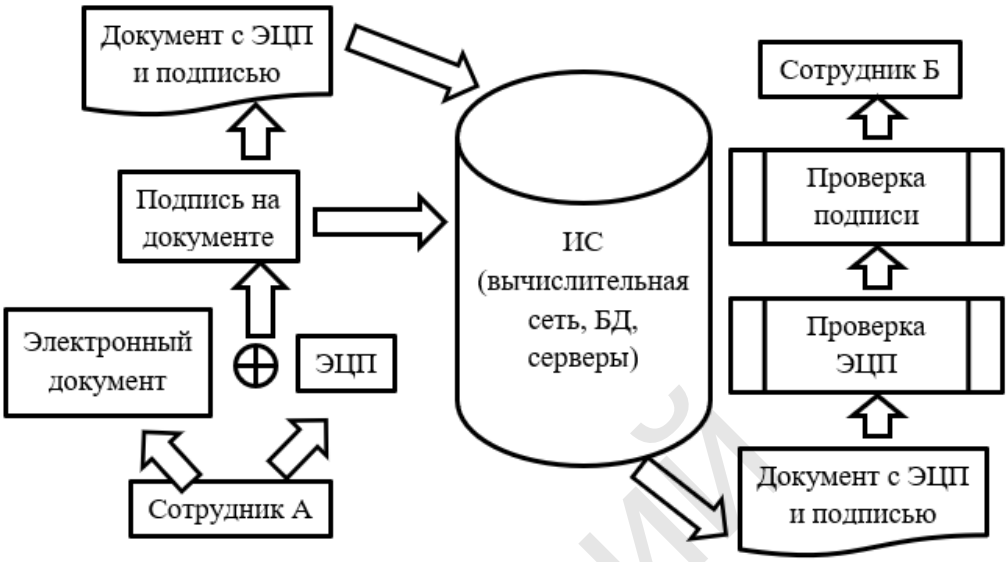

Рисунок 1. – Принципиальная схема документооборота с биометрической верификацией

Структура данных в базе представлена на рисунке 2.

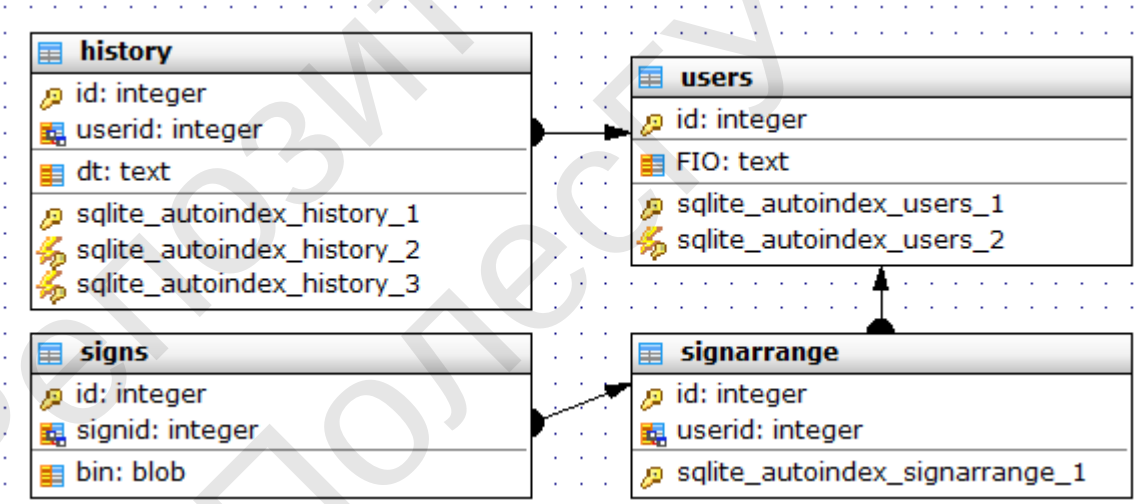

Рисунок 2. – Структура данных в базе приложения

В данной БД есть четыре таблицы:

1. Таблица **history** – в ней хранится история обработанных подписей:

1.1. Поле **id –** идентификатор. Является первичным ключом.

1.2. Поле **userid** – идентификатор пользователя. Определяет, чья подпись была обработана (проверена или добавлена).

1.3. Поле **dt –** дата и время операции над подписью.

2. Таблица **users –** таблица людей, чьи подписи хранятся в базе данных приложения:

2.1. Поле **id.** Является первичным ключом.

2.2. Поле **FIO –** ФИО человека, чья подпись хранится в БД.

3. Таблица **signarrange** – так как для работы программы необходимо определенное количество подписей человека, т.е. в БД на каж-

дого человека приходится не одна, а несколько подписей, то необходима таблица-агрегатор, определяющая, к какому человеку относится массив подписей БД:

3.1. Поле **id.** Является первичным ключом.

3.2. Поле **userid –** определяет отношение массива подписей к конкретному человеку (его идентификатору из таблицы людей).

4. Таблица **signs** – таблица с изображениями подписей:

4.1. Поле **id.** Является первичным ключом.

4.2. Поле **signid –** определяет отношение подписи к определенному массиву подписей.

Если пользователь хочет верифицировать подпись, то он загружает файл с подписью в программу. Если в программе есть обученная нейронная сеть, то файл с подписью проверяется, и в окне с результатами верификации показывается изображение подписи, ее владелец, должность владельца и степень владения. Если степень владения меньше 0.9, то программа считает, что подпись поддельная. Программа верифицирует подписи гораздо лучше, если в базе данных есть достаточное количество наборов подписей. Рекомендуется переобучить нейронную сеть с помощью соответствующей функции программы, если часто появляются ошибки верификации.

Список использованных источников

1. Горлушкина Н. Н. Системный анализ и моделирование информационных процессов и систем / Н. Н. Горлушкина. – СПб : Университет ИТМО, 2016. – 120 с.

2. Козлов Г. О., Новикова С. В. Распознавание рукописных подписей при помощи свёрточной нейронной сети / Г.О. Козлов, С. В. Новикова // Технические и физико-математические науки: сб. ст. – М.: МЦНО, 2018. – С. 17–20.

3. Козлов, В. Д. Алгоритмы оффлайн-распознавания рукописных цифр: выпускная квалификационная работа / В. Д. Козлов. – М. : МГУ им. М. В. Ломоносова, 2015. – 26 с.