тели каждого из филиалов либо структурных подразделений (директора, главные инженеры). Обсуждение дополнений и изменений в ПИБ проводится с учетом результатов текущего анкетирования начальников отделов филиалов (структурных подразделений) предприятия по вопросам обеспечения информационной безопасности на вверенных им объектах. Отчет о результатах проведения данного анкетирования по каждому из филиалов (структурных подразделений) должен представляться их директорами. Кроме того, на стадии планирования для каждого из филиалов (структурных подразделений) из списка его сотрудников должны выбираться лица, ответственные за контроль выполнения положений стратегической и тактической ПИБ.

Стадия реализации должна быть связана с осуществлением, внедрением и поддержкой стратегической и тактических ПИБ. На данной стадии с внесенными комиссией изменениями и дополнениями в стратегическую ПИБ предприятия и тактическую ПИБ филиала должен быть под роспись ознакомлен каждый сотрудник, имеющий доступ к информационной системе данного предприятия. Дополнительно на данной стадии лицами, назначенными ответственными за контроль выполнения положений стратегической и тактической ПИБ, должен по согласованию с директором и главным инженером филиала (структурного подразделения) разрабатываться перечень мер, которые будут предприниматься по отношению к сотрудникам, допускающим нарушения положения ПИБ. С утвержденным перечнем так же, как и с принятыми изменениями и дополнениями ПИБ, должен быть своевременно ознакомлен каждый сотрудник.

На стадии проверки оценивается и, если необходимо, измеряется эффективность процессов МИБ организации на соответствие требованиям ПИБ, а также подготавливаются отчеты генеральному директору о результатах проведения соответствующего анализа. Повысить уровень объективности результатов измерения эффективности процессов МИБ возможно путем проведения независимого аудита системы информационной безопасности филиала (структурного подразделения), при котором в состав аудиторской группы не входят сотрудники филиалов (структурных подразделений) РУП «Белтелеком». При этом отчет генеральному директору о результатах проведения данного измерения представляется руководителем аудиторской группы. Предварительно положения этого отчета должны быть обсуждены с директором филиала (структурного подразделения), в котором был проведен аудит.

Результаты стадии проверки определяют необходимость внеочередного заседания комиссии по обсуждению и установлению дополнений и изменений в ПИБ и, как следствие, комплекс мероприятий для стадии совершенствования СМИБ. В случае, если принимается отрицательное решение по вопросу проведения внеочередного заседания комиссии, то перечень мер, корректирующих и совершенствующих СМИБ филиала (структурного подразделения), разрабатывается его директором и главным инженером, и согласуется с руководителем аудиторской группы. Наряду с результатами аудита системы информационной безопасности филиала (структурного подразделения), при составлении данного перечня мер следует учитывать данные о планируемых сроках проведения очередного заседания комиссии по обсуждению и установлению дополнений и изменений в ПИБ. По факту принятия и реализации мер, корректирующих и совершенствующих СМИБ филиала (структурного подразделения), его директор должен представить отчет генеральному директору предприятия. Завершающими мероприятиями стадии совершенствования СМИБ должны являться анкетирование начальников отделов филиалов (структурных подразделений) по вопросам обеспечения информационной безопасности на вверенных им объектах и составление отчетов по результатам данного анкетирования.

Таким образом, продолжительность и комплекс мероприятий каждой последующей стадии жизненного цикла СМИБ филиалов (структурных подразделений) многофилиального предприятия определяется результатами комплекса мероприятий его предыдущих стадий.

К ВОПРОСУ ОЦЕНКИ ЭФФЕКТИВНОСТИ ПРИМЕНЕНИЯ ТЕХНОЛОГИИ CAPTCHA ДЛЯ ЗАЩИТЫ СЕТЕВЫХ РЕСУРСОВ

Н.Н. Кузьмицкий, С.С. Дереченник, Д.А. Костюк,
БрГТУ, г. Брест

Введение

История использования графических изображений в качестве основы теста Тьюринга (Completely Automated Public Turing tests to tell Computers and Humans Apart или CAPTCHA), призванного предотвратить массовую автоматизированную эксплуатацию сервисов, предоставляемых посетителям сетевого ресурса для единичного использования, насчитывает более 10 лет [1]. Исходная сфера применения CAPTCHA-тестов – развлекательные веб-сайты и цифровые медиа, окупаемость которых построена на периодическом показе посетителям рекламы и предложении более комфортных платных вариантов сервиса – предполагала незначительный ущерб в случае обхода данного вида защиты. Однако по мере внедрения веб-сервисов государственными и иными учреждениями (например, услуг сетевой регистрации) возможный ущерб становится гораздо более серьезным, меняясь от сравнительно небольших коммерческих убытков и издержек массовой рассылки несанкционированной рекламы к возможности затруднить либо полностью парализовать работу медицинских учреждений, банков и др. организаций. Показателен пример блокирования электронной регистрации в консульствах Республики Польша, осуществляемого злоумышленниками для перехвата и последующей перепродажи мест в очереди на собеседование, в результате чего для граждан Беларуси оказался практически недоступен установленный порядок получения визы [2].

Подход к защите от подобных вредоносных программ построен на применении тестов, легко выполнимых че-

ловеком и непреодолимых автоматизированными системами. При этом в настоящее время подавляющая часть CAPTCHA-тестов основана на вводе субъектом строки текста, в полной мере (порядок символов, регистр) соответствующей образам графических изображений (см. примеры на рисунке 1).

Рукописный текст имеет ряд принципиальных отличий от машинописного (разнообразие стилей письма, геометрических, топологических свойств символов др.). Кроме того, затруднено решение большинства задач в его автоматическом анализе (распознавание символов, сегментация). Поэтому изображения рукописных слов являются наиболее подходящими для создания CAPTCHA-тестов.

Хотя для обхода нередко применяются и непрямые способы (поиск уязвимостей веб-сайта, привлечение массового человеческого ресурса), судить о принципиальной эффективности защиты CAPTCHA-тестами можно только на основе возможности прохождения теста с помощью технологий искусственного интеллекта. Разнообразие сфер практического применения систем OCR (Optical Character Recognition) приводит к постоянному совершенствованию имеющихся и разработке новых методик распознавания текста. В связи с незначительными изменениями типов искаженных изображений, используемых для защиты, и расширением сфер их применения до критически важных, становится актуальным вопрос, насколько надежны на текущий момент CAPTCHA-тесты для блокирования автоматизированных атак. В русле данного исследования и находится представленная работа. При этом основное внимание уделяется оценке возможности созданию универсального классификатора цифровых образов на основе нейросетевого подхода, который является одним из наиболее гибких механизмов, перспективных для работы с искаженными образами символов.

Классификатор цифровых образов

Под универсальностью классификатора будем понимать его способность сохранять высокую точность распознавания на произвольной выборке входных данных. В зависимости от способа получения рассмотрим три типа текстовых образов: машинописные, рукописные и синтезированные. Изображения последнего типа подобны символам CAPTCHA, т. к. являются результатом применения пространственных преобразований к образам первых двух. Для их генерации была разработана методика, основанная на технике «волновых искажений», позволяющих имитировать эффекты от воздействия неблагоприятных окружающих условий или дефектов аппаратуры [3]. Примеры изображений выделенных типов приведены на рисунке 2.

В качестве базовой для решения задачи распознавания нами выбрана представленная на рисунке 3 сверточная нейросетевая архитектура (CNN), особенностями которой являются:

1) локальные рецептивные поля (нейроны получают входной сигнал от окрестностей нейронов предыдущего слоя, за счет чего сеть обучается двумерной структуре входного образа);

2) разделяемые веса (нейроны слоя объединены картами, в которых они обладают общими весами, при этом карты генерируют различные признаки и сокращают количество параметров, настраиваемых в ходе обучения);

3) пространственные подвыборки (локальное усреднение откликов карт приводит к синтезу высокоуровневых признаков и повышает инвариантность сети к искажениям) [4].

Рисунок 1 – Примеры графических CAPTCHA-тестов

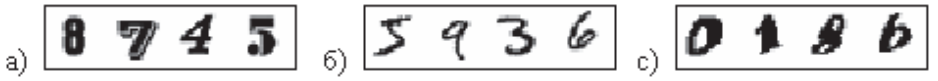

Рисунок 2 – Примеры машинописных (a), рукописных (б) и синтезированных (c) образов

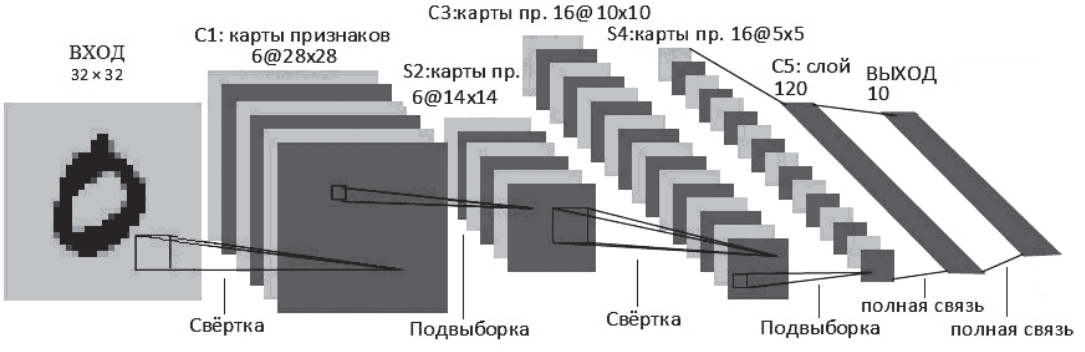

Рисунок 3 – Сверточная нейросетевая архитектура (CNN)

Таблица 1 – Точность распознавания (в %) CNN-экспертами образов

CNN эксперт	MNIST _train	FONT _train	KNI _train	Среднее для 3-х	MNIST_ test	FONT_ test	KNI _test	Среднее для 3-х
CNN_MNIST	99.68	96.75	85.21	93.88	99.39	95.23	85.06	93.22
CNN_FONT	86.68	99.88	88.34	91.63	87.23	99.58	88.06	91.62
CNN_KNI	86.48	94.54	99.38	93.46	86.52	92.97	99.29	92.92
Среднее	90.94	97.05	90.97	92.99	91.04	95.92	90.80	92.58

Таблица 2 – Точность распознавания (в %) комитетами образов тестовых частей баз

Комитет CNN	MNIST _test	FONT _test	KNI _test	Среднее для 3-х
MAX_COM	98.23	98.62	98.56	98.47
AVER_COM	97.64	99.11	98.10	98.28
MAJOR_COM	93.82	98.50	98.86	97.06
MKF	99.15	99.56	99.86	99.52
KADMOS	95.84	98.68	84.95	93.15

Выделенные типы изображений послужили прообразами к созданию трех видов экспертов, под которыми понимаются CNN, специализирующиеся в распознавании изображений одного из типов. Для построения экспертов использовалась рукописная (MNIST, 60000/10000 образов в тренировочной/тестовой части), машинописная (FONT, 20000/5000 образов) и синтезированная (KNI, 60000/10000 образов) базы данных. Результаты тестирования экспертов представлены в таблице 1, на основании данных которой можно отметить:

1) использованная архитектура CNN и методика ее обучения позволили достичь более 99% точности распознавания экспертами образов своих баз;

2) максимальный уровень ошибок был показан экспертами на множестве KNI_train, соответствующем символам CAPTCHA;

3) эксперт, обученный на основе MNIST, обладал лучшей средней точностью как на тренировочных (93.88%), так и на тестовых (93.22%) частях баз;

4) средняя точность экспертов (92.58%) на тестовых множествах показала низкую универсальность нейросетевой модели (аналогичное замечание справедливо и для других методов машинного обучения, в частности, метода опорных векторов (SVM)).

Для повышения обобщающих характеристик CNN использовались технологии коллективного распознавания, представленные двумя подходами:

– эксперты объединены в три комитета, названия которых соответствуют применяемой ими схеме голосования членов: MAX_COM, AVER_COM, MAJOR_COM;

– базы образов объединены в одну смешанную (по 20 000 примеров из каждой типовой), на основе которой с использованием процедуры «регулярного масштабирования» [5] построены несколько CNN, сформировавших комитет MKF, имеющий усредняющую схему голосования.

Результаты тестирования полученных комитетов и системы KADMOS (коммерческий продукт, специализирующийся в решении OCR задач) представлены в таблице 2. Отметим, что с помощью второго подхода также был создан комитет для заглавных букв английского языка, средняя точность распознавания которого на трех типовых базах составила 98,44%.

Анализ данных таблицы приводит к следующим выводам:

1) интеграция знаний CNN в комитеты позволяет существенно повысить точность распознавания (минимум – на 4,48%, максимум – на 6,94%);

2) наиболее эффективным оказался комитет, CNN в котором были обучены на смешенной базе образов, что позволило им сформировать более информативные признаки классов;

3) средняя точность комитета MKF (99,52%) показывает его высокую универсальность и стабильность характеристик, в отличие от модуля KADMOS (особенно на синтезированной базе символов, подобных CAPTCHA (84,95%)).

Заключение

Результаты проведенных исследований показали, что современные технологии искусственного интеллекта способны приблизиться к созданию универсального классификатора алфавитно-цифровых данных, что помимо своей безусловной практической пользы может привести к необходимости разработки новых путей выявления автоматизированных атак.

Литература:

1. L. von Ahn, M. Blum, J. Langford. Telling humans and computers apart automatically // Communications of the ACM. Vol. 47, No. 2. – 2004. – P. 57–60.

2. Посол Польши признал наличие проблем с электронной регистрацией на получение визы. // Новости Беларуси. Белорусское телеграфное агентство. 14 ноября 2012 г. http://tinyurl.com/bq3vsxc

3. N. Kuzmitsky, S. Derechennik. The problem of «brittleness» of convolutional neural networks in recognition of digit patterns with different writing styles // Proceedings of the 7th International Conference Neural Networks and Artificial Intelligence (ICNNAI). – 2012. – P. 235-238.

4. Y. LeCun, L. Bottou, Y. Bengio and P. Haffner. Gradient-Based Learning Applied to Document Recognition // Proceedings of the IEEE, 86(11). – 1998. – P. 2278-2324.

5. Н.Н Кузьмицкий. Об одном значимом результате в распознавании образов рукописных цифр // Материалы Международной научной конференции «Информационные технологии и системы». – 2012. – С. 228–229.