УДК 004.032

ЗАЩИТА ИЗОБРАЖЕНИЙ ОТ РАСПОЗНАВАНИЯ НЕЙРОСЕТЯМИ

П.В. Поляков
ИКБ РТУ МИРЭА
Россия, 107076, Москва, Стромынка ул., 20
E-mail: polyakov.p.v1@edu.mirea.ru

А.Ю. Алешин
ИКБ РТУ МИРЭА
Россия, 107076, Москва, Стромынка ул., 20
E-mail: aleshin@edu.mirea.ru

Abd Ali Husseinn Najm Abd Ali
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: shamsuldaeenhaidar@mail.ru

Shamsuldaeen Haidar Abdulwahhab H.
ТГТУ
392000, Тамбов, ул.Советская, 106
E-mail: ShamsuldaeenHaidar@mail.ru

Ключевые слова: Распознавание изображений, нейронные сети, защита данных, обфускация изображений, угрозы конфиденциальности, технологии распознавания лиц, методы защиты, перспективы развития, шифрование изображений, приватность информации.

Аннотация: Данная статья исследует проблему защиты изображений от нежелательного распознавания нейросетями в контексте современных технологий. Основанный на комплексном обзоре, текст раскрывает методы распознавания изображений, описывая сверточные нейронные сети и технологии идентификации объектов и лиц. Он также обсуждает угрозы и проблемы, связанные с этим явлением, включая нарушения частной жизни и возможности злоупотребления технологиями распознавания. Статья подробно рассматривает различные методы защиты изображений, включая обфускацию, использование шумов и искажений, разработку специальных алгоритмов и интеграцию защиты на этапе создания изображений. Наконец, обсуждаются перспективы развития в этой области, подчеркивая важность разработки новых, более надежных методов защиты изображений от нежелательного распознавания в будущем.

1. Введение

В настоящую эпоху развития искусственного интеллекта и широкого при-менения нейронных сетей в различных сферах жизни стало явным, что защита личной информации и конфиденциальных данных играет ключевую роль. Од-ним из наиболее актуальных вопросов стало обеспечение безопасности изображений от нежелательного распознавания нейросетями. С постоянным улучшением алгоритмов машинного обучения, а также увеличением объема доступной информации, возникает растущая потребность в разработке эффективных методов защиты, предотвращающих

несанкционированное использование изображений для идентификации лиц, объектов или локаций [1].

2. Механизмы обфускации

Современные методы распознавания изображений на базе нейронных сетей включают в себя различные техники обработки и анализа визуальной информации. Одним из ключевых инструментов являются сверточные нейронные сети (CNN). CNN эффективно извлекают признаки из изображений, используя несколько сверточных слоев, пулинга и полносвязных слоев для классификации или распознавания объектов на изображении. Их успешное применение распространяется от задач распознавания объектов на фотографиях до сегментации изображений и детекции лиц.

Кроме того, существует множество технологий распознавания объектов и лиц, основанных на нейросетях. Эти системы используют разнообразные архитектуры сетей для точного определения объектов, их распознавания и классификации. Например, модели Region-Based CNN (R-CNN) или You Only Look Once (YOLO) обеспечивают эффективные методы детекции объектов, при этом способные работать в реальном времени. Также стоит отметить алгоритмы распознавания лиц, которые находят широкое применение в системах безопасности, социальных сетях и других сферах. Эти методы основаны на поиске и сопоставлении уникальных признаков лица, таких как расположение глаз, форма лица и другие характеристики, что позволяет с высокой точностью идентифицировать личности на изображениях.

В современном информационном обществе использование нейросетей для распознавания изображений несет с собой ряд потенциальных угроз и проблем. Одной из основных проблем является нарушение частной жизни. При распознавании лиц или объектов на фотографиях, в том числе в социальных сетях или общественных местах, существует риск несанкционированного сбора и использования персональной информации. Это может привести к утечкам данных, использованию личных изображений без согласия, а также к слежке и нарушению личной жизни [2, 3].

Еще одной угрозой является возможное использование распознавания для целей злоупотребления и мошенничества. Взлом и обход систем безопасности с использованием поддельных или искаженных изображений, обман различных систем идентификации, а также возможность манипулирования фотографиями или видео для создания фейковой информации – все это представляет серьезную угрозу для безопасности и доверия к технологиям распознавания изображений. Эти проблемы акцентируют внимание на важности разработки эффективных методов защиты, предотвращающих потенциальные угрозы и минимизирующих риски, связанные с нежелательным распознаванием нейросетями.

Обфускация изображений: Этот метод предполагает изменение изображений таким образом, чтобы они оставались пригодными для человеческого восприятия, но усложняли процесс распознавания нейросетями. Обфускация может включать в себя добавление шума, изменение цветовых палитр, а также применение геометрических искажений к изображениям. Это позволяет сохранить основные визуальные характеристики изображения, но затрудняет точное распознавание объектов на нем нейронными сетями.

Использование шумов и искажений: Этот метод включает добавление случайных шумов или искажений к изображениям с целью исказить или затруднить процесс распознавания. Такие изменения могут быть применены на уровне пикселей или объектов на изображении, что затрудняет автоматическое распознавание нейросетями

и, в то же время, сохраняет изображение визуально приемлемым для человеческого восприятия.

Защита с помощью техники противодействия атакам: Этот подход включает в себя разработку алгоритмов и технологий, направленных на обнаружение и предотвращение атак, направленных на системы распознавания. Это включает в себя создание защищенных моделей нейронных сетей, способных справляться с попытками обхода или атаки на их структуру и функционирование. Такие техники могут быть основаны на обучении с учителем или без него, а также на внедрении механизмов проверки подлинности данных и аутентификации изображений [4].

Специальные алгоритмы подавления признаков: Этот метод предполагает модификацию изображений таким образом, чтобы удалить или затруднить извлечение ключевых признаков объектов или лиц, что делает их распознавание сложным для нейросетей. Алгоритмы подавления признаков могут использовать различные техники, такие как маскирование или удаление определенных участков изображения, подавление текстур или особенностей, которые могут быть использованы для идентификации объектов.

Использование зашифрованных изображений: Этот метод включает в себя шифрование изображений с помощью различных методов шифрования данных. Зашифрованные изображения представляют собой непонятные для человека и машины данные, которые могут быть восстановлены только с помощью ключа дешифрования. Подобные методы обеспечивают высокий уровень защиты данных на этапе хранения или передачи, предотвращая несанкционированный доступ и распознавание объектов на изображениях.

Интеграция методов защиты в процесс создания изображений: Этот подход предусматривает разработку методов защиты на уровне процесса создания изображений. Он включает в себя использование специализированных алгоритмов или техник при создании изображений, что делает их менее уязвимыми к нежелательному распознаванию. Это может быть встроено в процессы съемки, обработки изображений или генерации содержания таким образом, чтобы сделать распознавание объектов сложным или невозможным для нейронных сетей, сохраняя при этом визуальное качество для человеческого восприятия [5].

Перспективы развития защиты изображений от распознавания нейросетями представляют широкий спектр возможностей для инноваций и усовершенствований. С постоянным развитием технологий и возрастающей сложностью нейросетей для распознавания изображений, важно стремиться к созданию более надежных методов защиты.

Одной из перспектив является дальнейшее усовершенствование алгоритмов защиты. Это включает в себя разработку более эффективных и инновационных подходов к обфускации изображений, созданию новых методов шифрования и разработке интеллектуальных алгоритмов, способных динамически адаптироваться к новым методам распознавания и атакам.

Другой важной перспективой является интеграция многоуровневых систем защиты. Это означает создание комплексных решений, которые объединяют различные методы защиты в единую систему. Например, сочетание обфускации изображений с использованием шифрования и алгоритмами подавления признаков может создать более эффективную защиту, усиливая сложность для нейросетей в процессе распознавания. Также важным аспектом является учет потенциальных слабостей в существующих методах защиты для их последующего усовершенствования и создания более надежных механизмов защиты изображений.

3. Заключение

Защита изображений от нежелательного распознавания нейросетями представляет собой важный и актуальный аспект в контексте развития современных технологий. В свете постоянного улучшения алгоритмов и возросшей значимости вопросов конфиденциальности и безопасности личных данных, необходимость эффективных методов защиты изображений становится все более важной. Продвижение в области защиты изображений требует комплексного подхода. Осознание угроз и проблем, связанных с распознаванием изображений нейросетями, играет важную роль в формировании стратегий защиты. Методы обфускации, использование шумов и искажений, а также разработка специализированных алгоритмов и интеграция защиты на уровне создания изображений – все это лишь начало пути к созданию более надежных механизмов защиты. Несмотря на нынешние достижения в области защиты изображений, важно продолжать исследования и разработки для противодействия возможным атакам и угрозам. Совмещение разнообразных подходов, инновационных решений и учет изменяющейся природы технологий позволят создать более эффективные и надежные методы защиты, что станет ключевым фактором в обеспечении конфиденциальности и безопасности изображений в будущем.

Список литературы

1. Ясницкий Л.Н. Введение в искусственный интеллект.
2. Горбань А.Н., Россиев Д.А. Нейронные сети на персональном компьютере.
3. Rosenblatt F. The Perceptron: A Probabilistic Model For Information Storage And Organization In The Brain.
4. Dupond S. A thorough review on the current advance of neural network structures.
5. Amari Shun-Ichi. Learning patterns and pattern sequences by self-organizing nets of threshold elements.