

УДК 004.056.57

РАЗРАБОТКА АЛГОРИТМА ОБНАРУЖЕНИЯ НЕПРАВОМЕРНОГО ИСПОЛЬЗОВАНИЯ ИЗОБРАЖЕНИЙ

*Явтушенко Е. Д., выпускник физического факультета кафедры
радиофизики и электроники, ФГБОУ ВО «ЧелГУ»,
Ручай А. Н., кандидат физ.-мат. наук, доцент кафедры
компьютерной безопасности и прикладной алгебры
ФГБОУ ВО «ЧелГУ», Челябинск, Россия*

Ключевые слова: безопасность изображений, хеш изображения, поиск изображений, перцептивный хеш.

Статья посвящена проблеме неправомерного использования изображений. Был проведён анализ нормативно-правовых актов, регулирующих охрану изображений в отношении защиты персональных данных, авторского права, распространения запрещённой информации. Рассмотрены существующие подходы к поиску изображений по заданным шаблонам. Разработан и протестирован алгоритм обнаружения неправомерного использования изображений на основе перцептивного хеша.

Введение. В настоящее время в большинстве стран мира существует проблема незаконного использования изображений. К изображениям человека относятся его фотографии, видеозаписи или произведения изобразительного искусства, на которых он изображен [1]. Кража и повторная публикация изображений без согласия автора является нарушением авторских прав и кражей личной собственности. С распространением социальных сетей возросла актуальность охраны и защиты персональных данных граждан. Правоохранительные органы контролируют утечку любой недостоверной информации, а также провоцирующих материалов, представляющих угрозу жизни и здоровью населению (например, сведения экстремистского характера) [2]. Поиск изображений неправомерного характера осуществляется на базе имеющегося набора шаблонов. Происходит проверка наличия схожих или однотипных изображений на том или ином ресурсе.

Цель работы – изучить существующие системы поиска и разработать оптимальный алгоритм обнаружения неправомерного использования изображений по заданным шаблонам.

Материал и методика исследований. В работе был проведён анализ существующих методов поиска. Побайтовое сравнение двух файлов (*Template Matching*) неэффективно, так как изображения могут быть изменены (иметь различный размер, качество) и при этом являться в достаточной мере схожими. Более эффективным методом является использование *нейронных сетей*. Предварительно сеть обучается с помощью тренировочного множества. Главное преимущество нейронных систем состоит в возможности находить не только копии изображений, но и просто похожие (например, фотографии, снятые с другого ракурса) [3]. Недостаток в большом количестве обучающих данных и высоких вычислительных затратах. Для реализации поиска также существует метод построения *цветовой гистограммы* — вектора, каждый элемент которого — количество пикселей изображения, имеющих определённый цвет [3]. Гистограммы не содержат данных о положении элементов в пространстве сцены, поэтому изображения с похожими гистограммами могут сильно отличаться. Поиск по данному методу эффективно работает на маленьких базах изображений. В данной работе для задачи поиска используются алгоритмы *перцептуального хеширования* [4, 5]. Происходит преобразование изображений (изменение размера, перевод в градации серого и др.), вычисляются хеши и сравниваются на основании расстояния Хемминга.

Работа была выполнена на основе базы данных, содержащей 10000 изображений и различных перечней их модификаций, таких как смена цветовой модели с RGB на XYZ, изменение размера, размытие фильтром Гаусса, поворот на небольшой угол, добавление шума. Размер хеша -1024 бита. Был исследован «короткий» хеш, который вычисляется путём сортировки бит полного хеша в порядке убывания информативности бит и взятия первых (наиболее значимых) 64 бита. Данный подход по результатам экспериментов показал самое низкое качество работы. Третьим рассмотренным методом является поиск по отсортированному хешу с последовательным сравнением блоков. После сортировки 1024-битный хеш был разбит на блоки определённого размера. Сравнение происходит блок за блоком с фильтрацией изображений. Оценка эффективности алгоритмов проводилась на основе расчёта значений ошибок первого и второго рода. В контексте данной работы *ошибка первого рода* - вероятность того, что в результате действия алгоритма не найдено изображений, подобных шаблону, несмотря на то, что они там есть. Данная ошибка может появляться при повышении

**Таблица 1 - Пороговые значения для каждого блока
отсортированного хеша**

Блок хеша	Порог	Число ложно найденных изображений
phash0 (8 бит)	5	6218
phash1 (8 бит)	4	2828
phash2 (16 бит)	8	1714
phash3 (32 бита)	14	934
phash (960 бит)	250	23

порога чувствительности или при сильном различии между изображениями. *Ошибка второго рода* - вероятность «пропустить чужого», то есть алгоритм находит изображения, которые не являются схожими с входным объектом [3].

Результаты исследований. В ходе исследования было выявлено, что оптимальным методом является поиск по отсортированному хешу с последовательным сравнением блоков. При поиске фильтр на первых 8 битах отбрасывает порядка 80% процентов ложных хешей изображений (Таблица 1). Для каждого блока были экспериментально подобраны пороговые значения таким образом, чтобы находились все модификации тестовых изображений. При данном подходе средняя ошибка составляет 0,00385, а среднее время работы 0,35 с. Однако данный алгоритм поиска не подходит для выявления отдельных фрагментов рисунка и изображений, повернутых на большой угол. При поиске по полному 1024 битному хешу средняя ошибка составляет 0.0054, время обработки одного изображения - 0,49 с.

Значения ошибок первого и второго рода для каждого блока представлены в Таблице 2.

Заключение. На сегодняшний день существует множество систем поиска изображений с различными возможностями. Однако многие из них основываются на имени файла, его формате, что не решает проблему неправомерного использования информации. В работе было исследовано и реализовано три алгоритма поиска изображений с помощью перцептивного хеша. Представленный алгоритм поиска по отсортированному хешу с последовательным сравнением блоков эффективнее поиска по 1024 битному хешу, так как имеет более высокую скорость работы. Таким образом разработанный подход блочного сравнения хешей может применяться на практике.

Таблица 2 - Значения ошибок для пяти блоков.

№ каскада	Ошибка 1 рода	Ошибка 2 рода
1	0,0011	0,6218
2	0,0070	0,2828
3	0,0016	0,1714
4	0,0006	0,0934
5	0,0052	0,0025

Библиографический список:

1. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ (ред. от 28.03.2017) //Статья 152.1. Охрана изображения гражданина.
2. Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 N 436-ФЗ (последняя редакция) Статья 5. Виды информации, причиняющей вред здоровью и (или) развитию детей.
3. Н.С.Байгарова, Ю.А.Бухштаб, Н.Н.Евтеева, Д.А.Корягин. Некоторые подходы к организации содержательного поиска изображений и видеоинформации//Институт прикладной математики имени М.В.Келдыша Российской академии наук.-2002
4. Zauner, C., Steinebach, M., and Hermann, E.. Rihamark: perceptual image hash benchmarking//Proc.SPIE 7880, 78800X–15.-2011.
5. Zhen-kun, W., Wei-zong, Z., Ouyang-Jie, Peng-fei, L., Yi-hua, D., Meng, Z., and Jin-hua, G. A robust and discriminative image perceptual hash algorithm//2010 Fourth International Conference on Genetic and Evolutionary Computing//2010.-С. 709–712 .

PROTECTION ALGORITHM DESIGN AGAINST IMAGE ILLEGAL EXPLOITATION*Yavtushenko E. D., Ruchay A. N.***Key words:** *image security, image hash, image search, perceptual hash.*

The paper considers the issue of image illegal exploitation. We analyzed the legally enforceable enactments regulating the copyright law (author's right), personally identifiable information, dissemination of secret information. Existing image pattern search algorithms were considered. The technology of perceptual hash was taken for realization. The algorithm of protection against image illegal exploitation was designed on the data analyze basis. The main advantage of our algorithm is low time expenditures.