ПРОГРАММИРОВАНИЕ, 2022, № 6, с. 54–58

ТЕОРИЯ ПРОГРАММИРОВАНИЯ: ФОРМАЛЬНЫЕ МОДЕЛИ И СЕМАНТИКА

УДК 004.891.2

АЛГОРИТМ ХЕШИРОВАНИЯ ИЗОБРАЖЕНИЙ С ИСПОЛЬЗОВАНИЕМ СВЕРТОЧНОЙ НЕЙРОННОЙ СЕТИ

© 2022 г. О. В. Куликова[a],* (https://orcid.org/ 0000-0002-9526-3078),
Г. С. Домбаян[a],(https://orcid.org/ 0000-0002-8890-288X)**

[a] Донской государственный технический университет
344002 Ростов-на-Дону, пл. Гагарина, 1, Россия

**E-mail: kov0768@list.ru*

***E-mail: nuken_96@mail.ru*

Поступила в редакцию 03.03.2022 г.
После доработки 24.06.2022 г.
Принята к публикации 27.06.2022 г.

Цель исследования заключается в разработке алгоритма для хеширования изображений с использованием сверточных нейронных сетей. Алгоритм, предложенный в данной работе, реализуется в три этапа:

1) предварительное обучение нейронной сети на тренировочных данных;

2) настройка нейронной сети для одновременного обучения нейронной сети семантическим признакам изображения и аппроксимирующей хеш-подобной функции для вычисления хеш-кодов;

3) извлечение изображений с помощью предложенного алгоритма иерархического глубокого поиска.

DOI: 10.31857/S0132347422060061

1. ВВЕДЕНИЕ

Хеширование применяется в самых разнообразных областях использования информационных технологий: в базах данных для ускорения поиска по ключу, в криптосистемах, в высокоуровневых языках программирования для реализации разнообразных структур данных и алгоритмов и пр. [1]. В информационной безопасности хеширование становится краеугольным камнем таких задач, как: хранение паролей, создание уникальных криптографических ключей и электронной цифровой подписи, аудит подлинности и целостности документов в ПК. Хеширование и в настоящее время остается достаточно популярной и востребованной областью информационных технологий, а благодаря достижениям в индустрии микротранзисторов и ростом вычислительных мощностей появилась возможность модификации и возможного улучшения алгоритмов хеширования. С ростом общего объема визуальной информации, передаваемой по сети, возросла необходимость в эффективном хранении и поиске изображений в больших базах данных. Для решения данных проблем идеально подходит хеширование изображений с сохранением их семантических признаков. Данная область научного исследования сравнительно молода и развивается всего на протяжении последних десяти лет, поэтому требует дальнейших усовершенствований и модификаций используемых алгоритмов.

2. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ГЛУБОКИХ МЕТОДОВ ХЕШИРОВАНИЯ ИЗОБРАЖЕНИЙ

Подробный сравнительный анализ эффективности применения традиционных методов машинного обучения и сверочных нейронных сетей для решения задачи семантического хеширования представлен в работах [2] и [3]. В таблице 1 представлена в порядке возрастания точность методов глубокого хеширования с 12/16, 32 и 48-битными хеш-значениями. Стоит отметить, что несмотря на высокую точность предложенных в работах [2] и [3] моделях и эффективность алгоритма глубокого иерархического поиска, данные модели предъявляют высокие требования к вычислительным ресурсам обучаемой машины, а это нежелательный фактор при необходимости переобучения использованной модели под конкретные технические спецификации. Также некоторые из рассмотренных моделей дают большую погрешность в извлечении похожих картинок по хеш-кодам.

Как видно, наиболее эффективным является метод глубокого обучения на бинарных хеш-значениях, в связи с чем можно определить следую-

Таблица 1. Сравнительный анализ точности методов глубокого хеширования

Применяемый метод хеширования	Точность метода с 12/16-битным хеш-значением	Точность метода с 32-битным хеш-значением	Точность метода с 48-битным хеш-значением
Неуправляемое глубокое хеширование	19.43%	24.86%	23.95%
Бинарное глубокое обучение	67.32%	69.63%	66.45%
Глубокое попарное обучение	71.3%	74.4%	75.7%
Глубокое обучение на бинарных хеш-значениях	89.3%	89.72%	89.73%

щие требования к искомому хеш-значению для изображения:

– сохранение максимально возможного количества информации из входного изображения;

– минимальные потери информации из входного изображения при извлечении главных признаков;

– инвариантность относительно афинных преобразований [4] и аугментации входных данных [5];

– равномерное распределение битов хеш-значения для увеличения полезной информации.

3. ПРЕДВАРИТЕЛЬНОЕ ОБУЧЕНИЕ НЕЙРОННОЙ СЕТИ НА ТРЕНИРОВОЧНЫХ ДАННЫХ

Для реализации сверточной нейронной сети была выбрана архитектура AlexNet, поскольку не требует больших вычислительных ресурсов для обучения или переобучения сети на пользовательском наборе изображений.

На рис. 1 подробно представлена структура модели. Данная модель была предобучена на базе данных ImageNet, предназначенной для отработки и тестирования методов распознавания образов и машинного зрения. Следует отметить, что модель была модифицирована для выполнения поставленной задачи.

Модель включает в себя пять сверточных слоев, предназначенных для минимизации размерности входного изображения, и три полносвязных слоя, которые занимаются собственной классификацией. Был добавлен еще один слой между седьмым и восьмым полносвязными слоями, задачей которого является обучение хешированию изображений. Данный слой принимает на вход семантические признаки изображения, полученные на предыдущем слое и затем вычисляет хеш-значения изображения.

CONV1 – первый сверточный слой
MAX POOL1 – первый pooling-слой
NORM1 – первый нормализация
CONV2 – второй сверточный слой
MAX POOL2 – второй pooling-слой
NORM2 – вторая нормализация
CONV3 – третий сверточный слой
CONV4 – четвертый сверточный слой
CONV5 – пятый сверточный слой
Max POOL3 – третий pooling-слой
FC6 – полносвязный слой
FC7 – полносвязный слой
FC8 – полносвязный слой

Рис. 1. Порядок слоев в модифицированной модели AlexNet.

4. НАСТРОЙКА И ОБУЧЕНИЕ НЕЙРОННОЙ СЕТИ

Для обучения хеширующего слоя используется погрешность сверточной нейронной сети по классификации изображений. Также, для данной нейронной сети специально была подобрана функция потерь:

$$\arg\min_{W} \alpha\sum_{n=1}^{N} L(y_n, \hat{y}_n) + \lambda\|W\|^2 - \beta\sum_{n=1}^{N}\|a_n^H - 0.5\|^2 + \gamma\sum_{n=1}^{N}(mean(a_n^H) - 0.5)^2$$

Третье слагаемое данной функции служит для бинаризации выходов хеширующего слоя для составления хеш-значения. Четвертое слагаемое предназначается для равномерного распределения битов хеш-значения, чтобы оно переносило максимально возможное количество информации из входного изображения. Также, для обучения нейронной сети был использован метод регуляризации “drop-out” для уменьшения вычислительной сложности и пакетная нормализация.

Обучение СНС происходило традиционным образом с помощью градиентного спуска [6]. Схема алгоритма обучения нейронной сети представлена на рис. 2. На схеме алгоритма обучения можно видеть, что в каждой итерации (эпохе) обучения нейронная сеть выполняет прямой проход, в котором вычисляет значения функций активации для каждого слоя и сохраняет состояния весовых коэффициентов и параметров сдвига, а затем выполняет обратный проход, в котором вычисляет значения производных функций активации. С помощью полученных значений производных

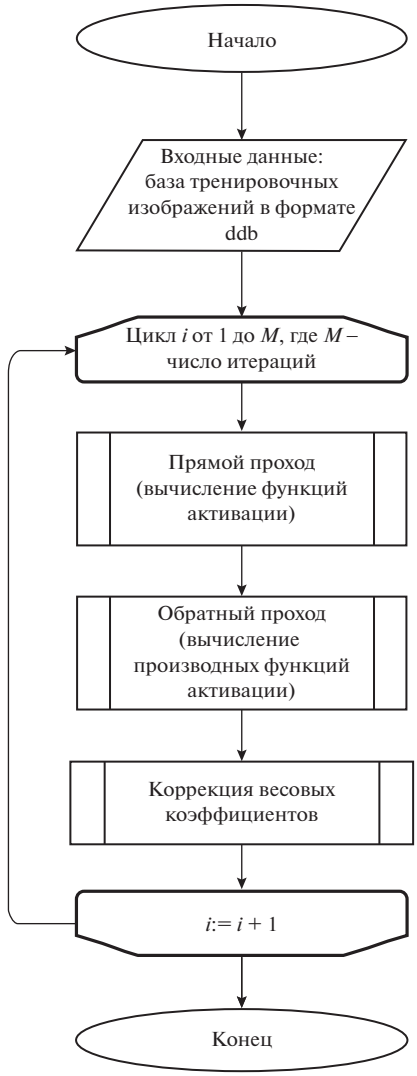

Рис. 2. Схема алгоритма обучения нейронной сети.

нейронная сеть корректирует значения весовых коэффициентов на каждом слое, тем самым минимизируя функцию ошибки.

Недавние исследования [7], [8] и [9] показали, что значения функций активации последних слоев нейронной сети могут служить визуальным дескриптором входного изображения. Использование таких визуальных дескрипторов демонстрирует впечатляющие результаты для задач классификации изображений, поиска и других задач компьютерного зрения. Однако такие визуальные дескрипторы многомерны и требуют больших вычислительных ресурсозатрат. В данной работе предлагается наряду с использованием СНС для извлечения семантических признаков изображения использовать дополнительный скрытый слой, задачей обучения которого будет аппроксимация хеш-функции для заданного вектора семантических признаков.

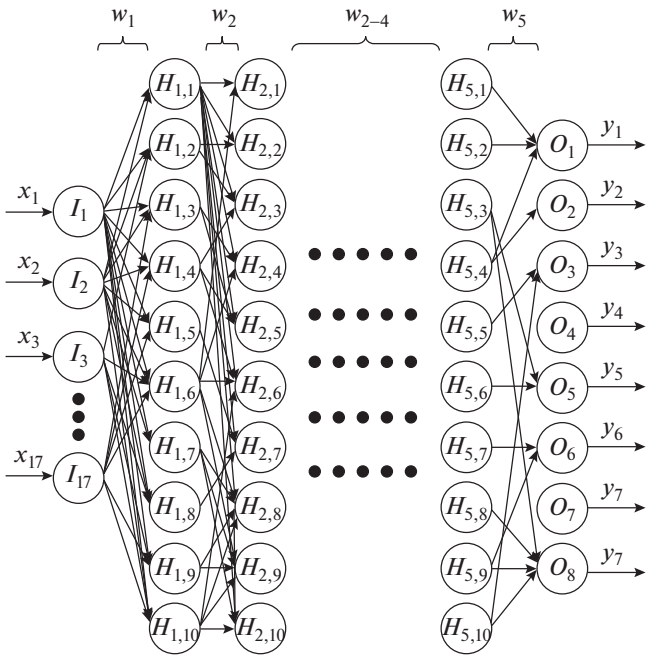

Рис. 3. Структура скрытого слоя СНС для вычисления хеш-значения изображения.

Чтобы облегчить эффективный поиск изображений, используется практичный способ преобразования результатов функций активации в двоичные коды. Такие двоичные компактные коды могут быть использованы для хеширования, а затем, для вычисления расстояния Хэмминга [10]. В данной работе предлагается наряду с использованием СНС для извлечения семантических признаков изображения использовать дополнительный скрытый слой, задачей обучения которого будет аппроксимация хеш-функции для заданного вектора семантических признаков. Обучение скрытого слоя для вычисления хеш-значения будет происходить благодаря имеющимся помеченным тренировочным данным и минимизации функции потерь от погрешности работы СНС. Структура скрытого слоя показана на рис. 3. На данном рисунке видно, что скрытый слой нейронной сети имеет параметры (17, 50, 8). Это означает, что данный слой использует для вычисления двоичных кодов 17 входных семантических признаков, 50 скрытых нейронов и 8 выходных нейронов, значения функции активации которых используются для составления хеш-значения. Указанные выше параметры скрытого слоя нейронной сети являются компромиссом между требуемой точностью извлечения изображений из базы данных и вычислительными ресурсами обучаемой машины.

Настройки модели СНС сохраняются в специальном proto-файле, структура которого пред-

```
name: "AlexNet"
layer {
  name: "data"
  type: "Input"
  top: "data"
  input_param { shape: { dim: 10 dim: 3 dim: 227 dim: 227 } }
}
layer {
  name: "conv1"
  type: "Convolution"
  bottom: "data"
  top: "conv1"
  param {
    lr_mult: 1
    decay_mult: 1
  }
  param {
    lr_mult: 2
    decay_mult: 0
  }
  convolution_param {
    num_output: 96
    kernel_size: 11
    stride: 4
  }
}
layer {
  name: "relu1"
  type: "ReLU"
  bottom: "conv1"
  top: "conv1"
}
```

Рис. 4. Архитектура СНС для хеширования изображений.

ставлена на рис. 4. Лаконичность такого формата позволяет эффективно создавать и сохранять новые архитектуры СНС.

5. ИЗВЛЕЧЕНИЕ ИЗОБРАЖЕНИЙ С ПОМОЩЬЮ ПРЕДЛОЖЕННОГО АЛГОРИТМА ИЕРАРХИЧЕСКОГО ГЛУБОКОГО ПОИСКА

Поиск изображения на основе его хеш-значения основан на алгоритме нахождения приблизительных ближайших соседей. Схему алгоритма поиска можно увидеть на рис. 5.

Извлечение изображения из базы данных происходит в несколько этапов:

– получение списка кандидатов с помощью алгоритма приблизительного ближайшего соседа;

– определение наилучших кандидатов с помощью минимизации расстояния Хэмминга между векторами главных признаков изображений;
– сортировка списка наилучших кандидатов в порядке возрастания расстояния Хэмминга.

Рис. 5. Схема алгоритма вычисления хеш-значения для изображения на основании вектора его семантических признаков.

На основании исследований, проведенных в работах [11], [12] и [13] был сделан вывод о том, что расстояние Хэмминга – оптимальная характеристика определения похожих изображений. Поэтому минимальное расстояние Хэмминга между хеш-значениями изображений указывает на то, что должны быть похожи при условии корректной работы СНС и метода извлечения главных признаков изображения.

6. ВЫВОДЫ

В настоящей работе было проведено алгоритмическое конструирование программного средства хеширования изображений. Также были рассмотрены следующие алгоритмы:

– бинаризация входных данных;

– инициализация нейронной сети;

– обучение нейронной сети;

– извлечение хеш-значения для входного изображения на основе его главных признаков;

– поиск изображения на основе его хеш-значения.

На основании результатов данной работы будет реализовано программное конструирование программного средства хеширования изображений.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная технология. Криптографическая защита информации. Функция хеширования. ГОСТ Р 34.11-2012. Москва, Стандартинформ, 2012.
2. Методика определения угроз безопасности информации в информационных системах. Текст: электронный // Методический документ ФСТЭК России: [сайт]. 2015. https://mindstep.ru/wiki/index.php/Методика_определения_угроз_безопасности_информации_в_информационных_системах (дата обращения 26.09.2020 г.).
3. Защита от несанкционированного доступа к информации. Термины и определения: Руководящий документ ФСТЭК России [утверждено решением председателя Гостехкомиссии при Президенте Российской Федерации от 30 марта 1992 года]. Москва: Кремль, 1992. 8 с.
4. *Ершов А.В.* Линейные и аффинные пространства и отображения. М.: МФТИ, 2016. 69 с.
5. *Емельянов С.О.* Методы аугментации обучающих выборок в задачах классификации изображений / Емельянов С.О., Иванова А.А., Швец Е.А., Николаев Д.П. // Сенсорные системы. 2018. Т. 32. № 3.
6. *Городецкий С.Ю., Гришагин В.А.* Нелинейное программирование и многоэкстремальная оптимизация. Нижний Новгород: Издательство Нижегородского Университета, 2007. С. 357–363.
7. Object recognition from local scale-invariant features / David Lowe. Text: electronic // IEEE (ICCV). – 1999. – https://doi.org/10.1109/ICCV.1999.790410. http://ieeexplore.ieee.org/document/790410 (date of the application: 16.01.2021).
8. Convolutional recurrent neural networks: learning spatial dependencies for image representation / Zhen Zuo, Bing Shuai [et al.]. Text: electronic // IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops (CVRPW). 2015. https://doi.org/10.1109/CVPRW.2015.7301268. http://ieeexplore.ieee.org/document/7301268 (date of the application: 30.01.2021). Access mode: free.
9. Exploiting local features from deep networks for image retrieval / Joe Yue-Hei Ng, Fan Yang [et al.]. Text: electronic // IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshops. 2015. https://doi.org/10.1109/CVPRW.2015.7301272. http://ieeexplore.ieee.org/document/7301272 (date of the application: 30.01.2021).
10. Alex X. Liu, Ke Shen, Eric Torng. Large Scale Hamming Distance Query Processing. ICDE Conference, 2011. P. 553–564.
11. Affinity CNN: learning pixel-centric pairwise relations for figure/ground embedding / Michaile Maire. – Text: electronic // IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVRP). 2016. https://doi.org/10.1109/CVPR.2016.26. http://ieeexplore.ieee.org/document/7780395 (date of the application: 14.01.2021).
12. Object contour detection with a fully convolutional encoder-decoder network / Michaile Maire, Takuya Narihira [et al.]. Text: electronic // IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVRP). 2016. https://doi.org/10.1109/CVPR.2016.28. http://ieeexplore.ieee.org/document/7780397 (date of the application: 14.01.2021).
13. Learning relaxed deep supervision for better edge detection / Yu Liu, Michael Lew [et al.]. Text: electronic // IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVRP). 2016. https://doi.org/10.1109/CVPR.2016.32. http://ieeexplore.ieee.org/document/7780401 (date of the application: 14.01.2021).