на которых были написаны буквы и цифры.

3. Шифровальное колесо Болтона – работало по принципу простой замены одной буквы на другую.

4. Шифровальная машина Конвертер М-209 – зашифрованное сообщение распечатывалось на бумаге в виде пятизначных групп.

5. Шифровальная машина Лоренц – принцип работы был основан на поточном шифре Вернама.

Подготовлен доклад с целью ознакомления студентов с основами криптографии. Данная информация может быть полезна студентам, обучающимся по специальности “Защита информации”, а также тем, кто умеет или учится профессионально программировать, интересуется сжатием данных или занимается исследованием современных средств шифрования. В наши дни криптография используется практически во всех сферах, работающих с приёмом и передачей информации, обеспечивает работу сверхсекретных каналов связи, а также эта наука успешно применяется в банковской деятельности.

Список использованных источников:

1. Василенко, О. Н. Теоретико-числовые алгоритмы в криптографии / О. Н. Василенко. – М. : МЦНМО, 2003. – 326 с.

2. Введение в криптографию / В. В. Ященко [и др.] ; под общ. ред. В. В. Ященко. – 3-е изд., перераб. – М. : МЦНМО, 2003. – 400 с.

3. Математические и компьютерные основы криптологии : учеб. пособие / Ю. С. Харин [и др.]. – Минск : Новое знание, 2003. – 382 с.

4. Стройникова, Е. Д. Основы прикладной алгебры : учеб.-метод. пособие / Е. Д. Стройникова. – Минск : БГУИР, 2010. – 120 с.

5. Шифровальные устройства [Электронный ресурс]. – Режим доступа: http://kryptography.narod.ru/mashiny.html.

ДИАГНОСТИКА НА РАК ПРИ ПОМОЩИ НЕЙРОННЫХ СЕТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пунько В.В., Приходько В.С.

Волорова Н. А. – к.т.н., доцент

Популяция людей на планете с каждым днем увеличивается, как и увеличивается число болезней, не подлежащих лечению и очень трудных в диагностике. Одним из таких заболеваний является рак. Около 13 % всех смертей в мире происходит из-за онкологических заболеваний, которые сегодня считаются самой распространенной патологией после инсульта и ишемии.

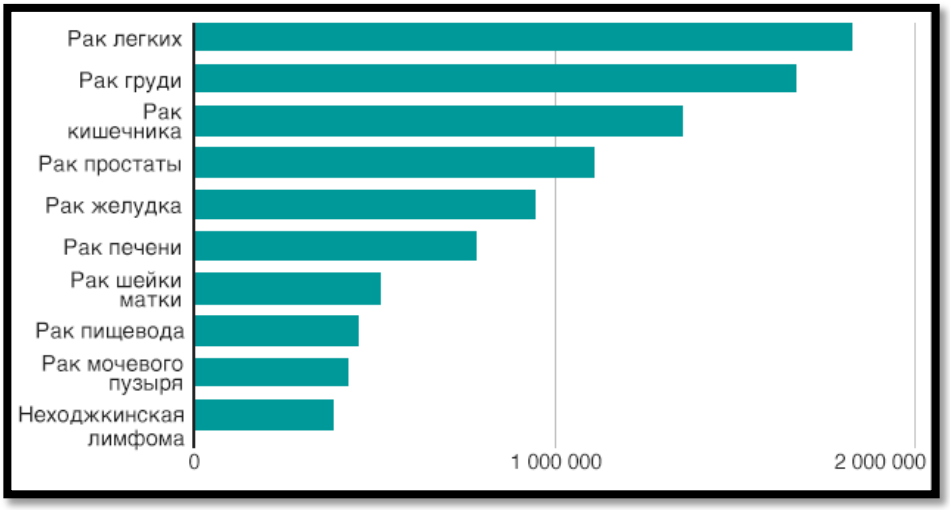

Рис. 1 – Статистика раковых заболеваний на 2012 год

Дело в том, что онкологических заболеваний (того самого рака) — огромное количество разновидностей. Например, раков молочной железы существует более 20 видов, и, кроме этого, у каждого вида рака молочной железы есть характеристики, влияющие на стратегию лечения. Заболеваний, которые называют лимфомы — тысячи видов и подвидов. И, опять же, существует принципиальная разница в их лечении. От правильности постановки диагноза в итоге зависит успешность или не успешность лечения. Пациента можно лечить сколь угодно хорошо, но если его лечат от другого вида рака — лечение не имеет существенного эффекта.

Про онкологическую диагностику много говорят, и, несмотря на это, очень мало знают в среде непрофессионалов. Во-первых, скрининг (ранняя диагностика) и диагностика — это совершенно разные вещи. Во-вторых, от этапа, когда пациент впервые попадает к онкологу, и онколог подозревает у пациента

профильное заболевание, должно пройти несколько принципиально важных этапов для того, чтобы начать лечение. Все эти этапы и называются онкологической диагностикой.

Человек не прозрачен, и даже если обнаружено новообразование, говорить о том, что это рак или не рак, и, тем более, какой это рак, в большинстве случаев очень преждевременно. Роль диагностики в онкологии очень высока. Именно поэтому, после того как есть основания предполагать онкологическое заболевание, пациента направляют на такой этап диагностики, как морфологический.

Он состоит из хирургической процедуры забора материала (биопсии [5]) и, собственно, самого морфологического исследования (гистологический/иммуногистохимический/молекулярный анализ). Именно на основании этих анализов человеку или подтверждают, или корректируют поставленный клинический диагноз. Именно на основании морфологического (патоморфологического) заключения пациента будут потом лечить. И именно от точности этого этапа онкологической диагностики будет зависеть насколько подходит лечение данному пациенту с его заболеванием, насколько оно будет эффективно.

Но человек может ошибиться, и тогда рак может быть не выявлен. Анализ данных биопсии можно передать компьютеру, т.к. машина точнее человека, и многие задачи может решать быстрее и лучше. Цель этого исследования – создание нейронной сети для распознавания раковых заболевания на ранней стадии по анализу биопсии.

Изначально, перед работой с изображением, его нужно подготовить, в этом случае делается его препроцессинг. Сперва мы применим к изображению фильтры для уменьшения шумов и сглаживания. Далее мы представляем каждый пиксель полученного изображения как точку в трёхмерном пространстве (первые 2 координаты – координаты пикселя в изображении, а третья – его цвет в RGB) (Рис. 2).

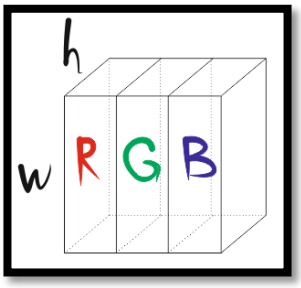

Рис. 2 – Представление картинки в качестве трехмерного куба

Теперь это представление надо нормализовать. Для каждого цветового спектра делим значение цвета в этом пикселе на среднее арифметическое значений всех пикселей в этом цвете. Для более мощной нормализации можно найти среднее значение не на данном изображении, а на всей выборке изображений. Пример нормализации изображения 2 на 2 пикселя:

$$A = \begin{pmatrix} (1,1,1) & (3,1,1) \\ (3,1,1) & (1,1,1) \end{pmatrix} \rightarrow K_n = \frac{\sum_{i=1}^{4} x_i}{4}, \text{где } i - \text{значение пикселя в } R\backslash G\backslash B$$

$$K_n = 1 \rightarrow A_n = \frac{A}{K_n} = \begin{pmatrix} \left(\frac{1}{4},1,1\right) & \left(\frac{1}{4},1,1\right) \\ \left(\frac{1}{4},1,1\right) & \left(\frac{1}{4},1,1\right) \end{pmatrix}$$

Таким образом у нас все значения сместятся ближе к нулю и с ними будет проще подсчитывать веса для нейронной сети (Рис. 3).

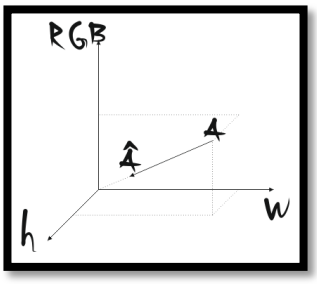

Рис. 3 – Смещение пикселей ближе к нулю в трехмерном пространстве

На изображении биопсии присутствуют не только клетки, но ещё и достаточно большое количество соединительной ткани, которая нам не нужна, и соответственно было бы неплохо её убрать. Для этого мы после препроцессинга сегментируем изображение оставляя только клетки. Сегментирование производится в данной работе при помощи нейронной сети архитектуры UNet [1]. Сети данной архитектуры могут быстро и качественно сегментировать изображения. Недостатком этой сети является долгое обучение. Принцип работы довольно простой: изображение, поданное на вход, проходит несколько слоев свертки поле чего результат разворачивается, учитывая результаты предыдущих слоев свертки. Таким образом на выходе у нас получается изображение с наложенной маской, в данном случае – клетка без соединительной ткани.

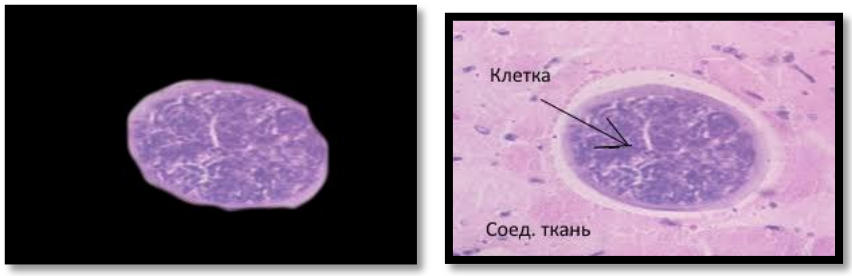

Рис. 4 – Не сегментированная клетка и клетка после сегментации соответственно

Далее мы формируем объект, состоящий из изображения биопсии и тега (кодового названия органа, откуда она была взята). После этого механизм принятия решений по тегу выбирает на какой из ансамблей нейронных сетей передать данную биопсию для анализа. Изображение из этого объекта подаётся на ансамбль из пяти нейронных сверточных сетей [4], которые учились вне зависимости друг от друга. Т.к. они обучались независимо результаты у них могут быть разные. Из полученных результатов считается средний и это среднее значение и есть вероятность нахождения рака на данном органе. Полная схема архитектуры программы приставлена на рисунке 5.

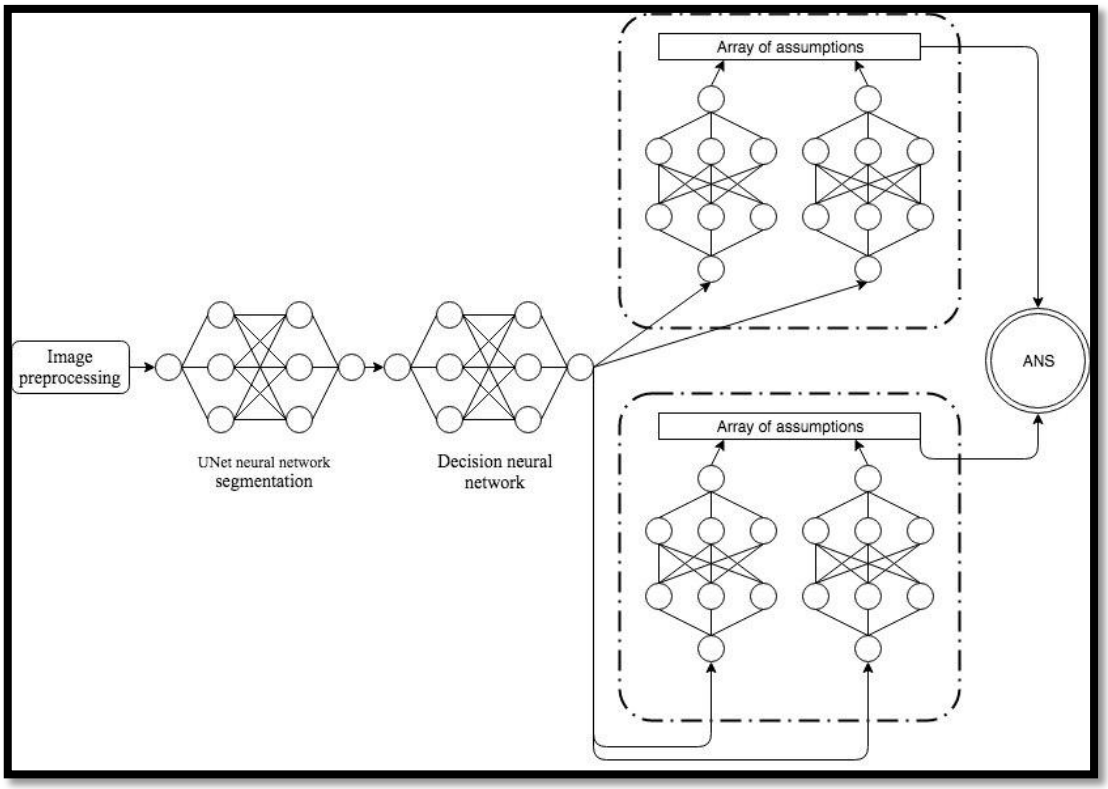

Рис. 5 – Схема взаимодействия между нейронными сетями для анализа картинки

Так как данных, по которым можно обучать нейронную сеть у нас не много (в открытом доступе достаточно мало изображений биопсий пациентов больных раком) сделаем небольшие модернизации всех сетей. Воспользуемся сеткой под названием автокодирование [2], предназначенной для выявления важной информации на изображении. Дело в том, что после каждого пропуска через данную сеть одного и того же изображения мы всегда будем получать нужную информацию с некоторыми отклонениями (например, будут появляться искажения на фото). Тем самым мы усилим тренировочную выборку и обучим сеть более точно. Принцип автокодировщика прост – это однослойный персептрон с одинаковым кол-вом входных нейронов и классов, а единственный скрытый слой имеет размер в 2 раза больше, чем входной. Вставляя такую сетку через каждый слой в нашей сверточной сети, и внося прием Dropout [3] (выбивание нейронов на каждой эпохе для увеличения вариативности сети) мы можем уменьшить тренируемый сет. Для еще большего улучшения используем написанную мной библиотеку neural_fitbox, которая позволяет во время обучения подменять и изменять данные постоянно перемешивая их перед подачей. Таким образом мы имеем модель, в которой каждый слой имеет автокодирование, и мощного учителя, который может во время тренировки менять данные. Имея такую архитектуру, мы можем учить наши сети имея очень малое кол-во данных. Вплоть до 1000 изображений на тренировку и проверку.

После того, как ансамбль сетей делает вывод, составляем отчет и сохраняем. Если все 5 сверток дают не ясные результаты, то мы пробуем подать изображение еще раз. После чего можно сделать вывод. Стоит учитывать, что это – вероятность, полученная на маленьких данных, и для использования в промышленных масштабах потребуется переобучить сеть на больших данных. Это можно сделать достаточно просто, учитывая, что сеть принятия решения уже обучена, а сегментация никак не влияет на результат. Для переобучения на тот или иной рак, нужно переобучить ансамбль нейронных сетей, после чего включить блок в схему и продолжить работу. Данный подход может легко распознавать раковые заболевания точнее и быстрее человека.

Список использованных источников:
1. UNetpaper - https://arxiv.org/abs/1505.04597
2. Autodecoder - https://tensorchiefs.github.io/bbs/files/vae.pdf
3. Dropout - http://jmlr.org/papers/volume15/srivastava14a.old/srivastava14a.pdf
4. CNN - http://cs231n.stanford.edu/slides/2017/cs231n_2017_lecture5.pdf
5. Biopsy - https://www.euroonco.ru/glossary-a-z/biopsy

ПРИМЕНЕНИЕ РЕЖИМА ПОНИЖЕННОГО ЭНЕРГОПОТРЕБЛЕНИЯ ДОЗУ В ИДЕНТИФИКАЦИИ ЦИФРОВЫХ СИСТЕМ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Пучков А.В.

Иванюк А. А. – д-р. техн. наук, доцент

Неотъемлемой частью любой современной цифровой системы является оперативное запоминающее устройство. Таковым нередко выступает динамическое запоминающее устройство (ДОЗУ), которое может использоваться не только по основному назначению, но и, в дополнение к этому, в качестве криптографического примитива для решения задании уникальной неклонируемой идентификации. Классическим подходом является анализ состояния ДОЗУ после включения, но не меньший интерес представляет состояние ДОЗУ после выхода из режима пониженного энергопотребления.

Структурная сложность физических, в частности, электронных систем рассматривается в физической криптографии как основа для построения криптографических примитивов. Основным понятием физической криптографии является физически неклонируемая функция (ФНФ), которую можно понимать как устройство, генерирующее значения ответов на некоторые входные воздействия (запросы), причем, пары запрос-ответ обладают уникальностью, непредсказуемостью и неклонируемостью на других экземплярах интегральных схем, выпущенных в рамках заданного технологического процесса. Процесс производства цифровых устройств и систем предполагает, что значениями отдельных их параметров принципиально невозможно управлять, задавая для них конкретные значения. Такие параметры принимают случайные, уникальные для конкретного экземпляра цифровой системы, значения, а задачей ФНФ является их извлечение и усиление. Классическим примером такого рода параметров являются задержки распространения сигналов [1]. Уникальность пар запрос-ответ означает для ФНФ возможность использовать их в рамках решения задачи неклонируемой идентификации цифровых систем, а также более сложных протоколах аутентификации на их основе. С другой стороны, случайных характер рассмотренных выше параметров позволяет использовать ФНФ для построения генераторов истинно случайных последовательностей, при этом такие генераторы сами будут являются неклонируемыми.

Для оперативных запоминающих устройств, как статических, так и динамических, характерно то, что при включении напряжения питания некоторая часть запоминающих ячеек оказывается в состоянии 1, оставшаяся часть – в состоянии 0. В самом общем случае данный процесс является случайным, а полученное распределение – уникальным со статистической точки зрения. Это даёт возможность говорить об ОЗУ как о ФНФ с ответом, представляющем собой весь массив запоминающих элементов, запросом же выступает включение питания. Поскольку чаще всего в процессе работы цифровой системы ОЗУ непрерывно используется, такой подход сопряжен со сложностями в практической реализации, т.к. использование такого криптографического примитива возможно только непосредственно после включения питающего напряжения ОЗУ, что практически всегда совпадает с включением всей цифровой системы [2]. В этой связи можно выделить ДОЗУ, для которых представляется возможным альтернативный подход – отключение регенерации части запоминающих ячеек. В отличии от предыдущего метода, это может выполняться многократно во время работы цифровой системы. В частном случае, отключение регенерации массива запоминающих элементов выполняется при переходе в режим пониженного энергопотребления, что особенно актуально для мобильных устройств. Несмотря на некоторые недостатки, из-за низкой стоимости ДОЗУ получают широкое распространение в цифровых системах различного назначения.

Для экспериментального исследования были использованы ДОЗУ Micron M45W8MW16, которыми комплектовались имеющиеся в наличии 10 плат быстрого прототипирования Digilent Nexys 4 на основе FPGA Xilinx Artix-7. Данные схемы памяти имеют объем 16 Мбайт и обладают интерфейсом, практически идентичным статическим запоминающим устройствам. При этом регенерация запоминающих ячеек