# НЕЙРОННЫЕ СЕТИ В БИОМЕТРИИ

**Часть 2.**

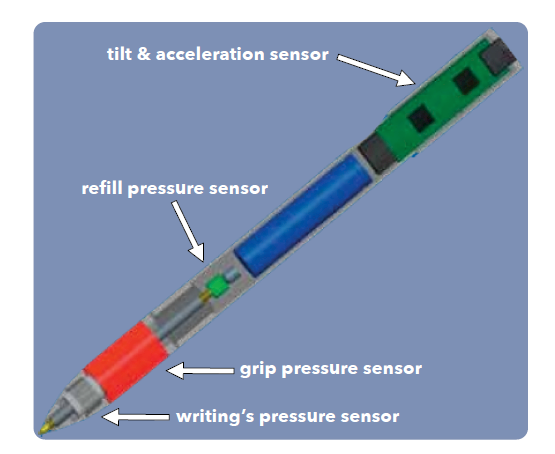
# Распознавание по динамике письма с помощью сверточной нейронной сети

([1] Книга 1, раздел 10)[[1]](#footnote-1)

Люди пишут по-разному, имеют не только различный почерк, но и разный способ письма, кто-то сжимает ручку сильно, кто-то небрежно, оказывают разное давление на лист бумаги.

Эти характеристики письма – *динамические,* они изменяются во времени.

Существуют инструменты, специальные ручки, которые могут измерять динамические параметры письма. Пример на рисунке (см. также Книга 1, раздел 10).



**Рисунок 1. Специальная ручка с сенсорами для измерения динамики подписи**

Такая ручка имеет 6 сенсоров:

1. Микрофон

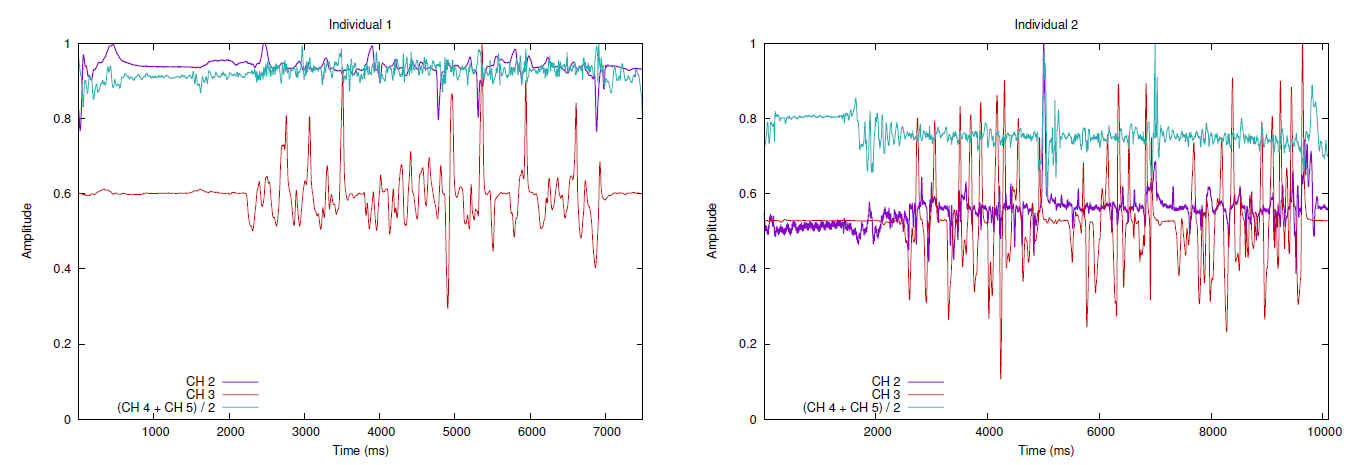
2. Датчик силы сжатия ручки

3. Датчик осевого (вдоль ручки) давления на бумагу (и в резервуаре с чернилами)

4-6. Наклон и ускорение по трем осям X, Y, Z.

Используя такую ручку можно измерить динамические характеристики письма, для этого испытуемых просят написать некоторый текст, например, свое ФИО, подпись и т.п.

Данные сенсоров записываются. В эксперименте показания микрофона (CH1) не учитываются, также обнаружили что показания датчика наклона и ускорения по оси X (CH4) практически не различаются, его показания тоже не будут учитываться. Для датчиков по осям Y и Z взяли среднее значение, таким образом оставив три показания. На рис. 2 изображены эти показания для двух разных испытуемых, откуда видно, что они различны.



**Рисунок 2. Записи показаний датчиков для двух испытуемых** (на рис. опечатка, третья линия графика (CH5+CH6)/2)

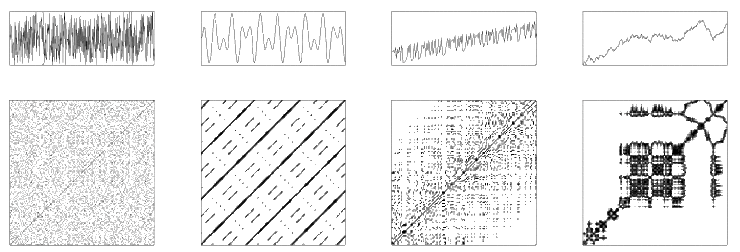
Мы с вами привыкли что для обработки динамических данных используются рекуррентные или динамические сети, но авторы решили использовать 2D сверточную сеть. Для этого необходимо преобразовать временные последовательности – записи датчиков – в изображения. Осталось три временных последовательности, логично их представить R, G, B каналами изображения (собственно ради этого авторы и взяли среднее между каналами CH5 и CH6, чтобы оставить три последовательности и использовать в дальнейшем уже готовые удобные фреймворки для обучения сверточных сетей).

**Как представить последовательность (одномерный вектор) изображением (двумерная матрица)?**

Для этого авторы использовали так называемый «график рекуррентности»[[2]](#footnote-2) (recurrence plot)[[3]](#footnote-3).

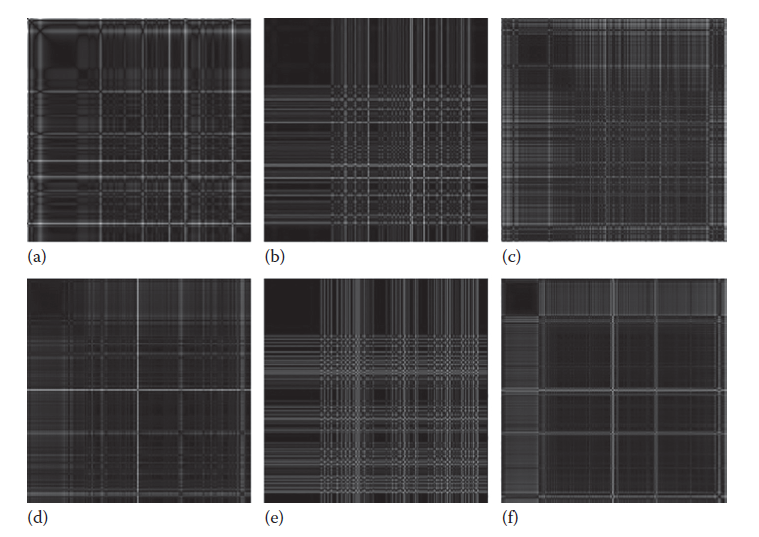
Он строится следующим образом. Пусть последовательность **X(n)** имеет **М** отсчетов, матрица **R** соответствующего ему изображения будет иметь размер **М\*М**. Для каждого элемента матрицы считаем

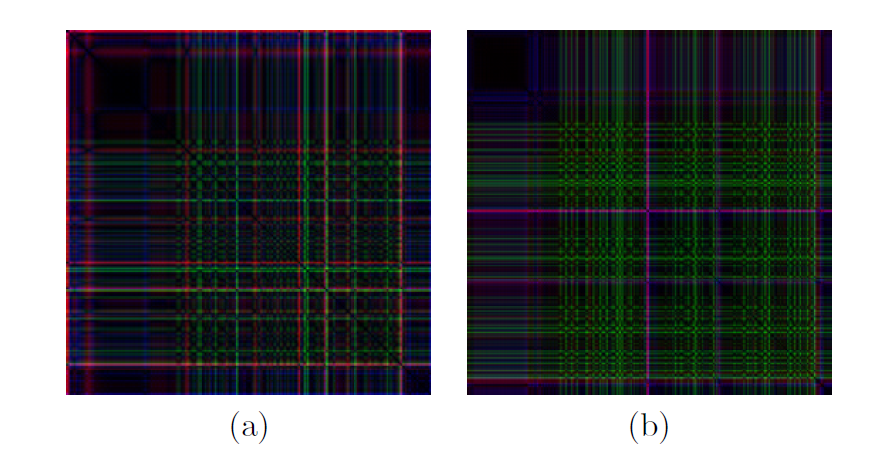
То есть, элемент матрицы (пиксель) с координатами (i,j) будет не нулевым если элементы последовательности с этими номерами примерно совпадают, с точностью до заданного порога **е.** Для некоторых последовательностей (сигналов) такие матрицы приведены на рис. 3. Очевидно, главная диагональ матрицы всегда равна 1.



**Рисунок 3. Примеры графиков рекуррентности.** (черный цвет – соответствует единичному значению пикселя)

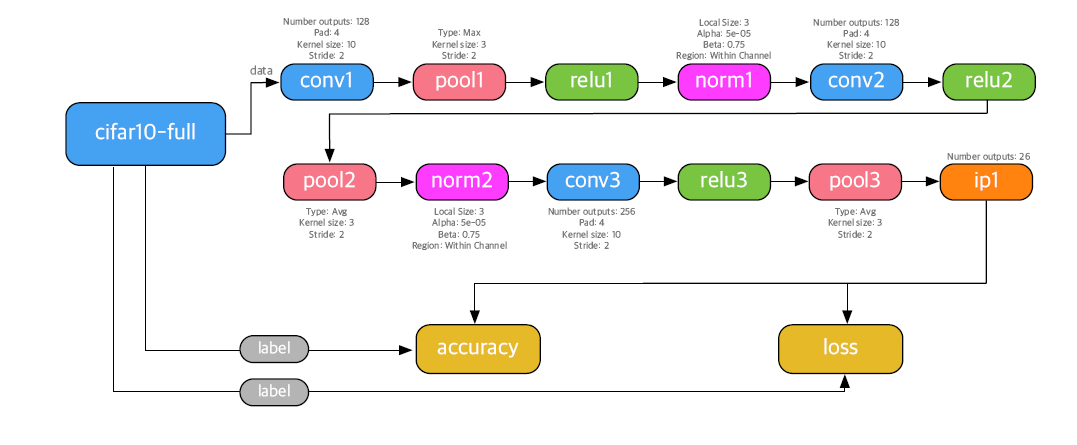
На рис.4 показаны графики рекуррентности для двух испытуемых, R, G и B каналы. Видно, что они различаются меду собой. Цветовые каналы затем объединены в одно RGB изображение.

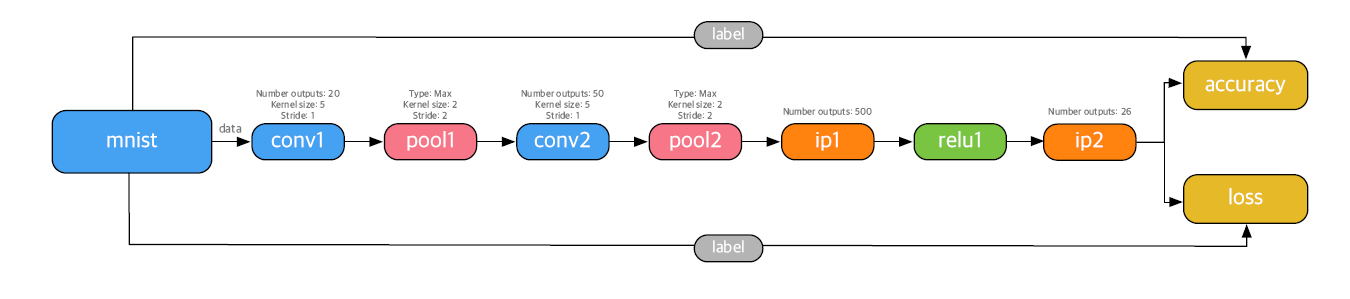




**Рисунок 4. Графики рекуррентности для двух испытуемых.** Сверху – R, G и B каналы по отдельности (белый цвет соответствует единичному значению пикселя), снизу – каналы объединены в одно цветное изображение.

Теперь, когда мы перевели наши данные в изображения, можно создать и обучить сверточную сеть для их распознавания. Для этого был создан набор данных из 260 изображений размером 256\*256 пикселей (отмасштабированы), по 10 изображений на каждого испытуемого. 90% данных для обучения, 10% для теста. Использовались некоторые архитектуры нейронных сетей из библиотеки Caffe [[4]](#footnote-4), их вид приведен на рис. 5, с некоторыми небольшими модификациями, подробности см. в работе ([1], раздел 10).

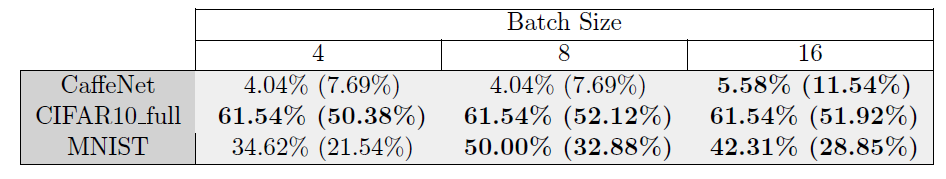
а) CIFAR10\_full

б) MNIST

**Рисунок 5. Архитектуры CIFAR10\_full и MNIST**

Результаты приведены в таблице (mean average precision) и на рис.6 (confusion matrix).

Конечно, результаты не столь впечатляющи как, скажем, для отпечатков пальцев, тем не менее имеют перспективу.





**Рисунок 6. Матрица потерь для эксперимента**

# Послесловие

Системы биометрии постоянно развиваются, появляются новые измерители и измерения, улучшаются методы, растет производительность вычислительных систем и количество внедрений. Нельзя останавливаться лишь на одном каком-то методе, всегда есть вероятность что его могут скомпрометировать, провести атаку. Мы видели с вами такие примеры. Приведенные здесь материалы лишь маленькая часть возможностей, которые доступны сегодня. Многие исследователи стремятся объединить различные способы измерения, чтобы повысить защищенность системы.

В качестве примера приведу работу моего студента-курсовика, который пытался распознать смену пользователя смартфона по показаниям датчика ускорения. Ведь люди по-разному держат, по-разному нажимают на экран, имеют разную походку. Этого может быть достаточно чтобы определить, что пользователь сменился. Но как всегда, «дьявол кроется в деталях», различить, скажем двух пользователей (студента и меня) проблем не составило (и получить свою отличную оценку), но означает ли это что такая система может любых пользователей различить? Конечно нет! Выбор или разработка метода должны исходить из конкретных требований, нет и не может быть универсальных решений. Сделать систему распознавания лиц на 100 или на миллион человек — это кардинально разные задачи, и потребуют разных методов.

# Что нужно вынести с этой лекции:

1. Понимать, как строится график рекуррентности.
2. Понимать, как можно использовать динамические характеристики письма для идентификации.

**Самостоятельная работа:**

Подумать о том, что биометрические системы подвержены атакам, почитать как такие атаки можно проводить, как защищаться, как оценить степень защищенности.

# Список литературы

1. Vatsa M., Singh R., Majumdar A. (ed.). Deep Learning in Biometrics. – CRC Press, 2018.
2. Richard Jiang, Chang-Tsun Li, Danny Crookes, Weizhi Meng, Christophe Rosenberger. Deep biometrics. Springer, 2020

1. Для цветных картинок см. https://www.researchgate.net/publication/331210201\_Person\_Identification\_Using\_Handwriting\_Dynamics\_and\_Convolutional\_Neural\_Networks/link/5c6c4d44a6fdcc404ebee23a/download [↑](#footnote-ref-1)
2. Называют по-разному, рекуррентный график, кросс-рекуррентный график и пр. [↑](#footnote-ref-2)
3. <https://en.wikipedia.org/wiki/Recurrence_plot> [↑](#footnote-ref-3)
4. http://caffe.berkeleyvision.org [↑](#footnote-ref-4)