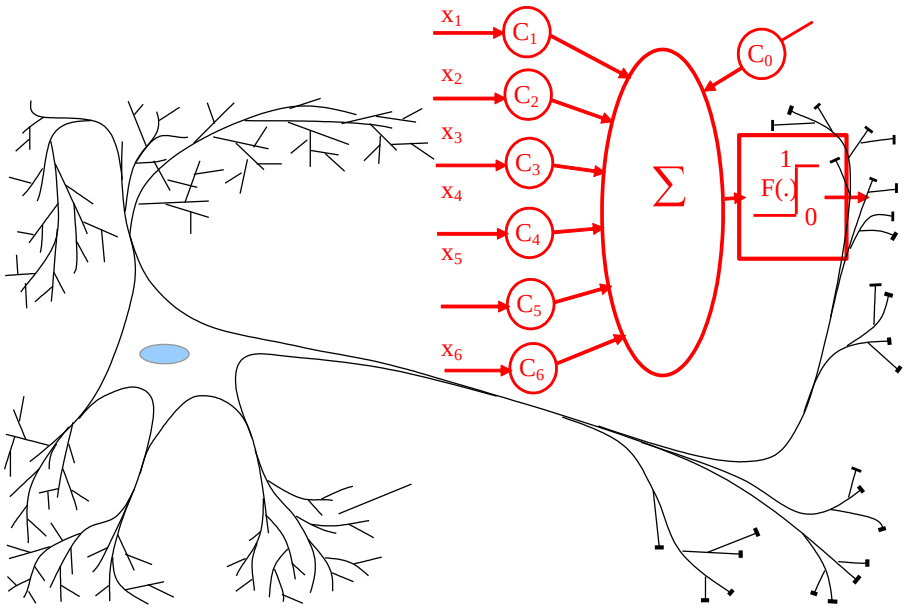
МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Пензенский государственный университет» (ПГУ)

А. И. Иванов, А. П. Иванов, К. А. Ратников

СТАТИСТИКО-НЕЙРОСЕТЕВОЙ АНАЛИЗ БИОМЕТРИЧЕСКИХ ОБРАЗОВ В ПРОСТРАНСТВАХ СПЕКТРОВ КРОССВЕРТОК И АВТОСВЕРТОК ХЭММИНГА

Препринт



Пенза
Издательство ПГУ
2021

УДК 519.24; 53; 57.017
ББК 32.818
И18

Р е ц е н з е н т ы :

доктор технических наук, профессор,
заведующий кафедрой «Компьютерные технологии»
Пензенского государственного университета
В. И. Горбаченко;

доктор технических наук, профессор,
ученый секретарь научно-технического совета
научно-производственного предприятия «Рубин» (г. Пенза)
М. М. Бутаев

Иванов, Александр Иванович.

И18 Статистико-нейросетевой анализ биометрических образов в пространствах спектров кроссверток и автосверток Хэмминга : препринт / А. И. Иванов, А. П. Иванов, К. А. Ратников. – Пенза : Изд-во ПГУ, 2021. – 56 с.

ISBN 978-5-907364-94-3

Доверенный сильный искусственный интеллект и доверенный слабый искусственный интеллект отличаются кардинально по затратам ресурсов на их тестирование. При тестировании сильного искусственного интеллекта обычными методами затраты памяти и вычислительных ресурсов оказываются огромны.

Классическая статистика активно использует коэффициенты корреляции двух переменных или коэффициенты автокорреляции одной переменной. Нейросетевой статистический анализ применим к данным очень высокой размерности, он строится как некоторое подобие классического низкоразмерного статистического анализа. В этом отношении кроссвертки и автосвертки кодов по Хэммингу являются, в некотором смысле, высокоразмерными аналогами обычных двухмерных коэффициентов корреляции.

Издание предназначено для обучающихся, аспирантов, преподавателей, инженеров, занимающихся проблемами применения нейросетевого искусственного интеллекта для решения задач биометрии и иных приложений искусственного интеллекта в защищенном от исследования исполнении.

УДК 519.24; 53; 57.017
ББК 32.818

ISBN 978-5-907364-94-3

СОДЕРЖАНИЕ

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Биометрический образ – уникальный образ человека (лицо, рисунок отпечатка пальца, рукописный автограф, голосовой пароль, рисунок радужной оболочки глаза и т.д.), имеющий высокую сложность (высокую размерность по числу контролируемых биометрических параметров).

Биометрический параметр – параметр, извлекаемый из биометрического образа путем предварительной обработки данных (очистки, центрирования, масштабирования) и последующего вычисления некоторого функционала, как правило, свертывающего данные всего примера в одно число.

Биометрический образ «Свой» – биометрический образ человека, параметры которого порождают с высокой вероятностью на выходах обученной нейронной сети код его личного криптографического ключа.

Биометрический образ «Чужой» – случайный биометрический образ, параметры которого порождают на выходах обученной нейронной сети случайный выходной код.

Искусственный нейрон – математическая конструкция, относящаяся к преобразователям континуума высокой входной размерности или «сырых» данных с низкой информативностью в одномерный континуум данных более высокой информативности (нейроны с гладкими функциями возбуждения). Также это иная конструкция, выполняющая преобразование континуум/цифра, например, персептрон, несколько рассмотренных в данной книге нейронов, являющихся аналогами классических статистических критериев.

Качество нейросетевых решений – соотношение вероятностей ошибок первого и второго рода. Сравнение качества двух разных нейросетевых приложений выполняют при одинаковых значениях одной из вероятностей либо при совпадении вероятностей первого и второго рода.

Нейросетевой преобразователь биометрия-код – преобразователь, заранее автоматически обученный (например, по ГОСТ Р 52633.5–2011) преобразовывать многомерные континуумы примеров биометрического образа «Свой» в почти однозначный выходной код криптографического ключа или длинного пароля доступа. Нейросетевые преобразователи биометрия-код являются хорошо исследованными искусственными нейросетевыми молекулами (на сегодня разработано и введено в действие на территории России семь национальных стандартов).

Сверхсильный нейросетевой искусственный интеллект – программное приложение, существенно превышающее по качеству принимаемых им решений либо по скорости принятия им «хороших» решений, по сравнению с решениями группы «ведущих» специалистов предельно высокого уровня квалификации.

Сильный нейросетевой искусственный интеллект – программное приложение, существенно превышающее по качеству принимаемых им решений, по сравнению с параллельно принимающему решения «средним» человеком (специалистом среднего уровня квалификации).

Слабый нейросетевой искусственный интеллект – программное приложение, существенно уступающее по качеству принимаемых им решений, по сравнению с параллельно принимающему решения «средним» специалистом-человеком (специалистом среднего уровня квалификации).

ОБОЗНАЧЕНИЯ

$E(.)$ – математическое ожидание;

$\sigma(.)$ – стандартное отклонение;

$P_1(.)$ – вероятность появления ошибок первого рода (ошибочного отказа в подтверждении основной гипотезы);

$P_2(.)$ – вероятность появления ошибок второго рода (ошибочного принятия альтернативной гипотезы);

$P_{EE}(.)$ – вероятность появления одинакового значения ошибок первого и второго рода $P_1(.) = P_2(.) = P_{EE}(.)$;

$P(«0_i»)$ – вероятность появления состояния «0» в i-том разряде кода;

$P(«1_i»)$ – вероятность появления состояния «1» в i-том разряде кода;

$H(.,.)$ – энтропия кода;

$h(.)$ – расстояние Хэмминга;

$\oplus$ – сложение по модулю два;

$\neg$ – операция инвертирования кода;

$.|.$ – операция конкатенации двух кодов;

$\Psi(«.»)$ – амплитуда вероятности появления кода «.».

ВВЕДЕНИЕ

Президент России В. В. Путин своим указом № 460 от 10.10.19 «О развитии искусственного интеллекта в Российской Федерации» задал вектор движения отечественной науки на ближайшее время. Следует отметить, что момент рождения нейросетевой ветви искусственного интеллекта обычно относят к 1943 г., в литературе принято подтверждать это, ссылаясь на публикацию Маккалока и Питца [1], как на пионерскую работу, т.е. логические вычислительные машины (цифровые вычислительные машины) и аналоговые (нейросетевые вычислительные машины) начали свое развитие примерно в одно и то же время. На текущий момент мы наблюдаем очевидное доминирование цифровых логических машин над аналоговыми вычислителями (аналого-цифровыми нейросетевыми преобразователями континуумов очень высокой размерности).

Причина доминирования логико-цифровых вычислителей понятна. Их работа понятна людям, понятно как их программировать и их удобно программировать. Люди (программисты) для себя придумали специальные языки программирования, причем во всех языках программирования континуальные переменные и логические переменные строго разделены. Логические или текстовые или целые переменные при программировании обычно помечают кавычками, отделяя их от континуальных (непрерывных переменных). Человек, пишущий программы может и не понимать, что непрерывные (континуальные) переменные внутри цифровой логической машины всегда представлены дискретно. Каждый из процессоров имеет свою разрядную сетку (8, 16, 32, 64 бита и т.д.). Вычисления всегда выполняются с некоторой точностью (приближенно), а ошибки вычислений, как правило, накапливаются. Совместное использование дискретных и непрерывных переменных за исключением нескольких частных случаев приводит к плохо обусловленным задачам. Решение таких задач следует рас-

сматривать как искусство программирования плохо обусловленных задач общего вида.

Сегодня считается большим успехом, если удается написать корректно работающую 5-мерную программу управления роботом. Фактически мы столкнулись с фактом наличия барьера размерности решаемых задач для современных логико-цифровых вычислителей. Такие вычислители плохо работают (виснут) при решении задач низкой размерности $f(x_1,x_2,\ldots,x_5)$, тогда как человек легко решает 10 000-мерные задачи $f(x_1,x_2,\ldots,x_{10000})$ [2].

Исследования мозга человека показали, что у нас есть естественные нейроны с 10 000 входов (так называемые пиромидальные нейроны), следовательно, мы можем решать 10 000-мерные задачи. Насколько велика размерность в 10 000 переменных можно ощутить, отказавшись от многоточия в записи $f(x_1,x_2,\ldots,x_{10000})$. Такая запись коротка из-за того, что она сводится всего к трем переменным и многоточию между ними. Если мы откажемся от многоточия и будем перечислять все переменные подряд, то для записи потребуется примерно 5 страниц.

Зачем людям решать задачи столь высокой размерности легко понять, взглянув на свои руки. Только кисть нашей руки имеет порядка 50 приводов (мышц), всеми ими нужно слаженно (параллельно) управлять, решая задачи очень высокой размерности. Мы сами очень сложные (высокоразмерные) и окружающий нас мир тоже очень сложен. Чтобы выжить, нам приходится решать в реальном времени задачи очень высокой размерности. В частности, когда нас в детском возрасте учили чистописанию, мы с вами самостоятельно отрабатывали свой индивидуальный рукописный почерк. Теперь, когда мы стали взрослыми, всех нас можно легко узнать по индивидуальным особенностям наших индивидуальных почерков. По сути дела с конца прошлого века по настоящее время США, Китай, страны Евросоюза, Россия активно занимаются развитием нейросетевых техноло-

гий применительно к решению задач многомерного статистического анализа с обучением нейросетевых приложений искусственного интеллекта на очень маленьких выборках. За последние 30 лет ведущие в информационном отношении страны потратили на развитие биометрии ресурсы большие, чем было потрачено за весь XX в. на **развитие**[1] классической математической статистики.

Подтверждением значительности произведенных затрат может служить число разработанных и введенных в действие национальных и международных стандартов по биометрии в сравнении с такими же стандартами по классической статистике. Так, в России действуют 43 международные стандарта комитета ISO/IEC JTC1 sc 37 («Биометрия»), кроме того, в России введены в действие семь национальных стандартов технического комитета Госстандарта России № 362 («Техника защиты информации»). Получается, что сегодня в России действует 50 стандартов по нейросетевой статистической обработке биометрических данных. В то же время в России действует всего один документ в двух частях [3, 4], регламентирующий применение примерно десятка из 200 известных статистических критериев [5]. Получается, что нейросетевая биометрия регламентируется 50 стандартами, тогда как обычным статистическим критериям соответствует всего один документ. Мы наблюдаем ситуацию, когда в 50 раз затраты по стандартизации нейросетевой биометрии в XXI в. в России оказались больше затрат на стандартизацию обычного классического статистического анализа. Эта разница должна в ближайшее время усилится в силу того, что в России в 2019 г. создан еще один специализи-

[1] Речь идет именно о **развитии**, а не о **поддержке** математической статистики. Затраты на **поддержку** легко оценить, исходя из того, что в России работает примерно 1000 университетов и в каждом из них работает хотя бы одна кафедра математической статистики с 20 квалифицированными преподавателями. По закону об образовании 10 % своего времени преподаватели должны тратить на научные исследования в рамках выполнения госбюджетных работ.

рованный технический комитет по стандартизации ТК 164 («Искусственный интеллект»).

Положение усугубляется тем, что примерно с 2009 г. к специалистам пришло осознание очень высокой эффективности больших искусственных нейронных сетей, автоматически обученных стандартизованным в России алгоритмом ГОСТ Р 52633.5 [6]. Этот алгоритм позволяет автоматически обучать 256 нейронов и использовать их при многомерном статистическом анализе нечетких биометрических данных, преобразованных в 256-битный выходной код однозначного криптографического ключа.

Принципиально важным является также то, что в приложениях нейросетевой биометрии глубоко проработан вопрос защиты информации решающих правил. Оказалось, что далеко не любое решающее правило удается эффективно защитить без создания дорогой и сложной инфраструктуры поддержки криптографических ключей. В этом отношении нейросетевые решающие правила оказались на сегодняшний день наиболее эффективными. Таблицы обученных нейронных сетей оказалось намного проще шифровать [7] в сравнении с биометрическими шаблонами международных биометрических стандартов [8–10].

Следует отметить, что доверие к нейросетевому искусственному интеллекту возникает только после его тестирования. При этом доверенный сильный искусственный интеллект и доверенный слабый искусственный интеллект отличаются кардинально по затратам ресурсов на их тестирование. При тестировании сильного искусственного интеллекта обычными методами затраты памяти и вычислительных ресурсов оказываются огромны.

В данной работе мы попытаемся показать, что возникающие при тестировании искусственных нейронных сетей эффекты экспоненциального ускорения вычислений и экспоненциального сокращения требуемой памяти возникают за счет использования малых тестовых выборок и реализуются только за счет перехода от статистического анализа обычных кодов

к кросскорреляционным сверткам и автокорреляционным сверткам Хэмминга. В этом отношении пионерским оказался национальный стандарт ГОСТ Р 52633.3 [11], ставший первым в мировой практике документом, рекомендовавшим переход к тестированию больших нейронных сетей на малых выборках.

Классическая статистика активно использует коэффициенты корреляции двух переменных или коэффициенты автокорреляции одной переменной. Нейросетевой статистический анализ применим к данным очень высокой размерности, он строится как некоторое подобие классического низкоразмерного статистического анализа. В этом отношении кроссвертки и автосвертки кодов по Хэммингу являются, в некотором смысле, высокоразмерными аналогами обычных двухмерных коэффициентов корреляции. Видимо, без использования спектров кроссверток кодов по Хэммингу и спектров автосверток кодов по Хэммингу нельзя упростить описание и тестирование нейродинамических вычислителей ближайшего будущего.

ГЛАВА ПЕРВАЯ

ЭКСПОНЕНЦИАЛЬНОЕ УСКОРЕНИЕ ВЫЧИСЛИТЕЛЬНЫХ ОПЕРАЦИЙ С ИСПОЛЬЗОВАНИЕМ НЕЙРОННЫХ СЕТЕЙ ПРИ ПЕРЕХОДЕ ОТ СТАТИСТИК ОБЫЧНЫХ КОДОВ В ПРОСТРАНСТВО АНАЛИЗА СПЕКТРА КРОССВЕРТОК ХЭММИНГА

1.1. Быстрое тестирование нейросети по ГОСТ Р 526553.3 при переходе от обычных кодов в пространство кроссверток Хэмминга

В случае создания и использования слабого нейросетевого искусственного интеллекта, например, обеспечивающего равные вероятности ошибок первого и второго рода на уровне 0,01, достаточно его тестирования на тестовой базе состоящей из 300 примеров образов «Чужой». Тестовую базу такого объема может собрать пользователь самостоятельно и проверить заявленное качество производителем самостоятельно.

Ситуация кардинально меняется, если производитель настаивает на том, что его приложение сильного нейросетевого интеллекта обеспечивает $P_1 \approx 0{,}05$ и $P_2 \approx 0{,}00001$. В этом случае тестовая база должна состоять из 300 000 примеров биометрических образов. Собирать тестовую базу такого размера биометрических образов рядовому пользователю запрещает его национальное законодательство о защите персональных данных.

В случае, если речь идет о распознавании рисунков отпечатков пальцев, то, обучив систему защиты на одном рисунке отпечатка пальца, пользователь может использовать как тестовые 9 оставшихся пальцев. Если пользователь уговорит жену помочь ему, то получит тестовую базу из 19 образов. Кажется, что столь малой базы недостаточно даже для тестирования слабого нейросетевого интеллекта, однако это не так. Если пользоваться рекомендациями отечественного стандарта ГОСТ Р 52633.3 [11],

то от анализа обычных кодов необходимо переходить в пространство расстояний Хэмминга.

На рис. 1 приведена блок-схема нейросетевого преобразователя биометрического образа в код ключа, длиной 256 бит.

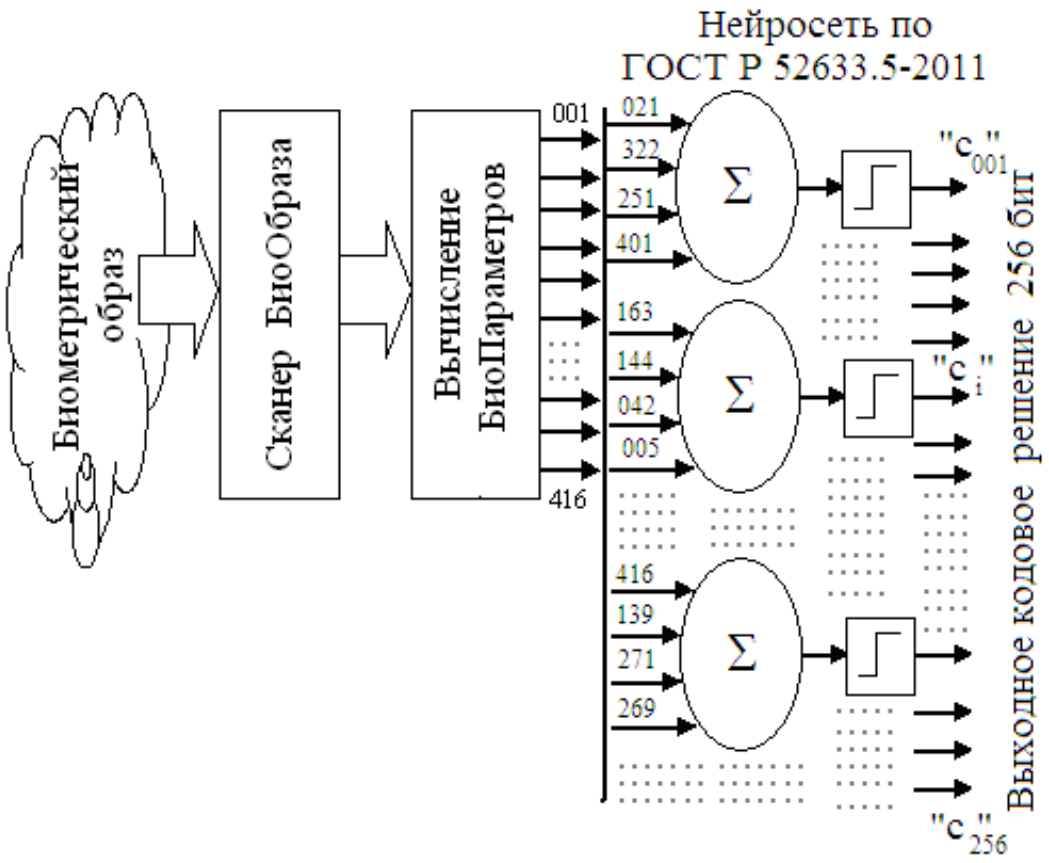


Рис. 1. Нейросетевой преобразователь биометрии в код ключа, длиной 256 бит, обученный автоматически по стандарту [6]

Если на обученный нейросетевой преобразователь подавать примеры образа «Свой», то на выходе нейросети будут появляться коды с высокой вероятностью 0,95 и выше ключа «$\bar{c}$». Состояния кода ключа «$\bar{c}$» повторяется с высокой вероятности во всех 256 битах, т.е. естественная энтропия входных данных биометрического образа «Свой» практически полностью устраняется обученной сетью искусственных нейронов. Энтропия состояний выходного кода «Свой» оказывается практически нулевой $H(«c_1,c_2,\ldots,c_{256}») \approx 0{,}0$.

Совершенно иная ситуация возникает, когда мы будем предъявлять по одному примеру 19 образов «Чужой». Для каждого из этих примеров нейросеть будет выдавать случайные коды – «$\overline{x}_i$» со случайным состоянием их 256 разрядов. Так как разряды кодов «Чужой» изменяются случайно, энтропия этих кодов должна быть значительно больше нуля:

$$H(«x_1,x_2,\ldots,x_{256}») > H(«c_1,c_2,\ldots,c_{256}») \approx 0{,}0. \quad (1)$$

Кажется, что вычислить вероятность ошибок второго рода и энтропию кодов «Чужой» при их длине в 256 бит очень сложно. Однако при тестировании после обучения нейросети эта задача оказывается вполне выполнима по стандарту ГОСТ Р 52633.3 [6], так как во время обучения известен код «Свой». Этот код уничтожается только после обучения нейросети и только после тестирования обученной нейросети.

Для выполнения тестирования необходимо переходить от анализа обычных кодов к анализу кроссверток Хэмминга кодов «Чужой» с единственным кодом образа «Свой»:

$$«h_{c,i}» = \sum_{j=1}^{256} \begin{bmatrix} «c_j» \\ \oplus \\ «x_{j,i}» \end{bmatrix}. \quad (2)$$

Очевидно, что кроссвертка Хэмминга является дискретной величиной и может принимать 257 состояний от минимального значения – «0», когда разряды совпадают, до максимального значения – «256», когда свертываются прямой код и его инверсия.

На рис. 2 приведены примеры реакции «слабой» и «сильной» нейросетевой защиты на 19 одинаковых тестовых воздействий.

Для оценки вероятности ошибок второго рода следует от дискретного распределения с линиями амплитуды вероятности $\Psi(«h»)$ перейти к эквивалентному непрерывному распределению p(h). Для этой цели необхо-

димо математическое ожидание E(«h») и стандартное отклонение σ(«h»). Для эквивалентного непрерывного и дискретного распределений первые статистические моменты совпадают E(«h») = E(h); σ(«h») = σ(h).

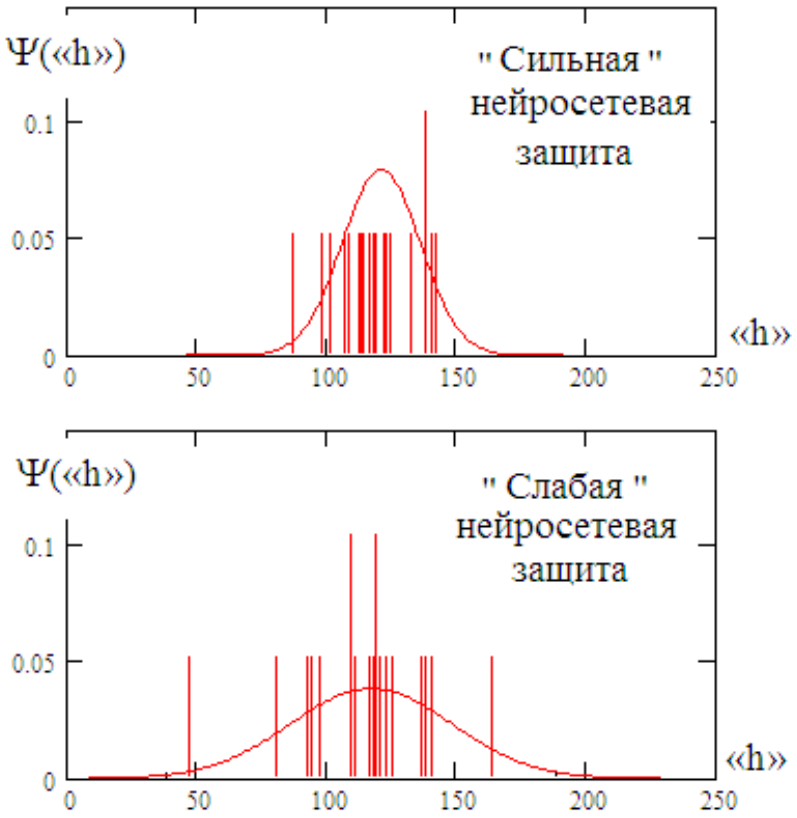


Рис. 2. Слабая и сильная нейросетевая защита, откликающаяся 19-ю спектральными линиями с разным стандартным отклонением

Вероятность ошибок второго рода оценивается следующим образом:

$$P_2 \approx \frac{1}{\sigma(\text{«h»})\sqrt{2\pi}} \int_{-\infty}^{1} \exp\left\{ \frac{(E(\text{«h»}) - u)^2}{2 \cdot \sigma(\text{«h»})^2} \right\} \cdot du \,. \qquad (3)$$

Из соотношения (3) следует, что при одинаковых значениях математических ожиданий двух распределений (см. рис. 2) значения вероятностей ошибок второго рода зависит от стандартных отклонений. Чем выше стандартное отклонение, тем больше должна быть вероятность ошибок второго рода.

Многомерная энтропия выходных кодов нейросетей вычисляется следующим образом:

$$H(«x_1,x_2,\ldots,x_{256}») \approx -\log_2(P_2). \qquad (4)$$

В конечном итоге мы получили эффективный алгоритм вычисления энтропии на малой выборке, обеспечивающий экспоненциальное снижение вычислительной сложности.

1.2. Оценка выигрыша по ускорению вычислений и выигрыша по необходимому объему памяти при переходе от статистического анализа обычных кодов в пространство спектра кроссверток Хэмминга

Следует отметить, что стойкость к атакам случайной подстановки образов «Чужой» будет эффективной, если нейросеть или ее образ «Свой» «слабы» (см. нижнюю часть рис. 2). Для «слабых» нейросетей или для «слабых» образов «Свой», на которых они обучены, вычислить вероятность ошибок второго рода (3), используя, например, 32-разрядное математическое приложение, несложно.

Очевидным является то, что те же самые вычисления (3) при попытке оценок вероятностей ошибок второго рода «сильной» нейросетевой защиты перестают работать. На рис. 3 приведен пример вычисления вероятностей ошибок второго рода при стандартном отклонении распределения Хэмминга в 15 бит и значениях математического ожидания $E(«h») \approx \{20, 40, 60, 80, 100, \ldots\}$ бит.

Если использовать для вычислений 32-разрядное приложение, то такой разрядной сетки хватает только для вычислений вероятности появления ошибок второго рода для математических ожидания в 100 бит и менее. Для больших значений математических ожиданий 32-разрядные приложения не работают. В этом случае вероятность ошибок второго рода оценивается через использование линейной экстраполяции и составляет $P_2 \approx 10^{-15,6}$ (15 нулей после запятой 0,00….).

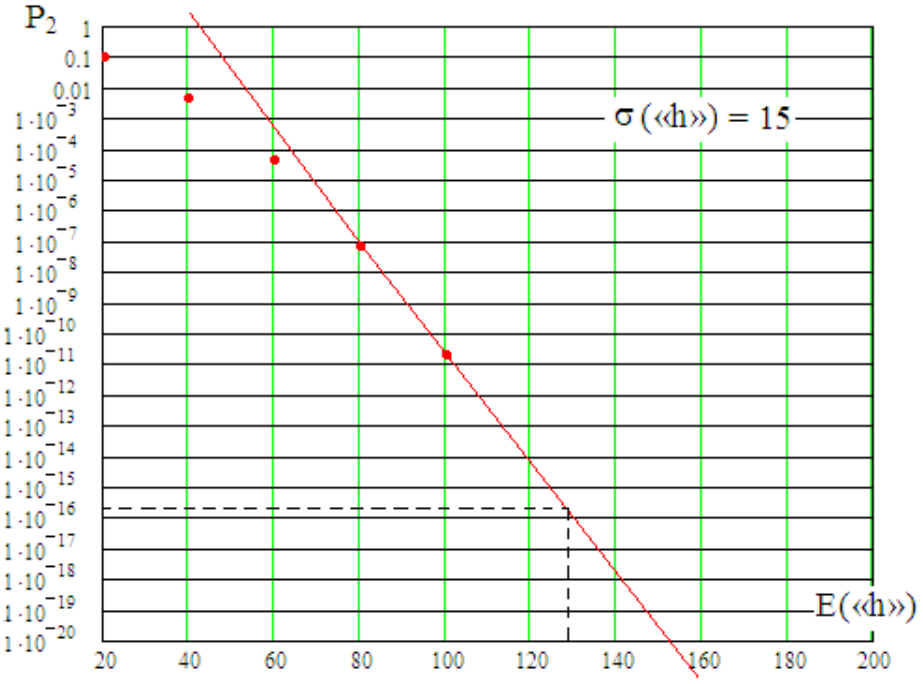


Рис. 3. Вероятность ошибок второго рода, оцениваемая линейной экстраполяцией данных, вычисленных в 32-разрядной сетке

Совершенно такая же ситуация возникает и при оценках энтропии по формуле (4). Соответствующие оценки для малых значений математических ожиданий приведены на рис. 4.

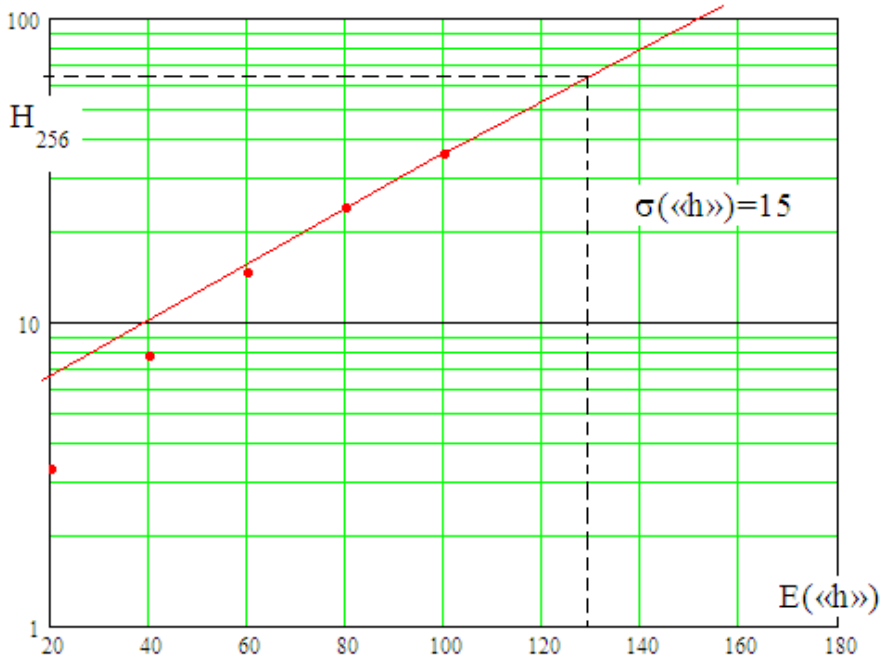


Рис. 4. Энтропия выходных состояний нейросети, оцениваемая линейной экстраполяцией данных, вычисленных в 32-разрядной сетке

На рис. 4 точками помечены энтропии без проблем, оцениваемые 32-разрядными приложениями. Энтропия математического ожидания E(«h») ≈ 128 бит дает оценку в 64 бита (пунктирные линии).

В конечном итоге получается, что отказ от накопления статистик при анализе кодов, длиной в 256 бит, и переход в пространство кроссверток Хэмминга позволяет ускорить вычисления более чем в один миллион миллиардов раз (16 нулей). То же самое относится и к сокращению потребностей в памяти вычислителя (быстрой оперативной и медленной долговременной памяти).

Также следует отметить, что доверенный искусственный интеллект биометрических приложений, как правило, размещают в доверенную малогабаритную, мало потребляющую, вычислительную среду, построенную на использовании малоразрядных контроллеров [12, 13] SIM-карт, микро-SD-карт, RFID-карт. Соответственно, для малоразрядных контроллеров SIM-карт, микро-SD-карт, RFID-карт придется писать приложения, ориентированные на обработку 4-, 8-, 16-, 32-бинарных биометрических данных. Если в таких приложениях вычисления (3) и (4) выполнять таблично, то технических трудностей не возникает. Программы оказываются компактными и для их выполнения достаточно очень скромных вычислительных ресурсов [12, 13].

1.3. Вычисление кроссверток Хэмминга через оценку кодового центра образа «Чужой-π»

Описанные выше алгоритмы тестирования по ГОСТ Р 52633.3 [11] предполагают знание кода «Свой», что вполне естественно, если тестирование выполняет хозяин средства биометрической защиты. Если же новыми возможностями миллиардных ускорений перебора пытается воспользоваться хакер, то код ключа «Свой» ему неизвестен. Тем не менее, хакер

вполне может достичь успеха, опираясь на новые технологические возможности.

Для реализации атаки направленного подбора необходимо сформировать тестовую базу из 10 000 образов «Чужой» в соответствии с рекомендациями ГОСТ Р 52633.1 [14]. Если теперь подавать на вход обученной нейронной сети примеры тестового биометрического образа «Чужой-π», то на выходе нейросети появится последовательность дрожащих состояний каждого из 256 бит. Разобраться в этом шуме случайных выходных кодов нейросети сложно. Не менее сложно вычислить энтропию кодов «Чужой-π» по выборке в 20 примеров. Если пользоваться формулой Шеннона, то для вычисления энтропии потребуется огромная выборка примеров образа «Чужой-π».

Для решения этой проблемы национальный стандарт ГОСТ Р 52633.3 [11] рекомендует переходить от анализа обычных кодов к анализу расстояний Хэмминга между кодом «Свой» и кодами «Все Чужие». В нашем случае поступим так же: для этой цели необходимо вычислить центр кодов «Чужой-π». Смета численного эксперимента по вычислению кодового центра иллюстрируется на рис. 5.

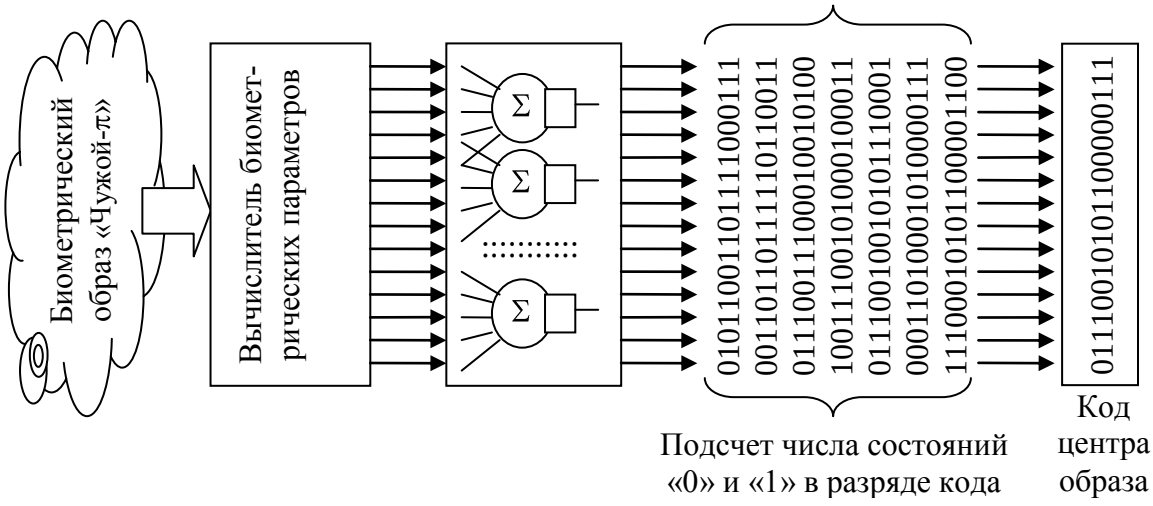


Рис. 5. Поразрядное накапливание состояний кода примеров образа «Чужой-π» при выявлении центра этого множества

Фактически выполняется подсчет состояний «0_i» и состояний «1_i» в каждом i-том разряде кода. Код центра вычисляется по следующему правилу:

$$\begin{cases} E(«x_{\pi,i}») \leftarrow «0_i» \ \text{if} \ \sum «0_{\pi,i}» \geq \sum «1_{\pi,i}» \\ E(«x_{\pi,i}») \leftarrow «1_i» \ \textit{if} \ \sum «0_{\pi,i}» < \sum «1_{\pi,i}». \end{cases} \quad (5)$$

Далее следует для кодового центра образа «Чужой-π» вычислить расстояния Хэмминга для всех других образов «Чужой-j»:

$$«h_{\pi,j}» = \sum_{i=1}^{256} \begin{bmatrix} E(«x_{\pi,i}») \\ \oplus \\ «z_{j,i}» \end{bmatrix}, \quad (6)$$

где «$z_{j,i}$» – кодовое состояние i-го разряда одного из примеров образа «Чужой-j» при $j \neq \pi$; $\oplus$ – символ операции сложения по модулю два.

Если сравнивать выражения (2) и (6), то мы наблюдаем их похожесть. И то, и другое выражение являются кроссвертками Хэмминга. Разница состоит только в том, что мы точно не знаем центр кодов образа «Чужой-π» и вынуждены его восстанавливать усреднением (5). Появляется промежуточная очень неточная операция.

Тем не менее, зная распределение значений кроссверток Хэмминга между центром кодов «Чужой-π» и другими тестовыми образами «Чужой», воспользовавшись формулами (3) и (4), мы оказываемся способными оценить энтропию образа «Чужой-π».

1.4. Извлечение знаний из нейросети через использование энтропии кроссверток Хэмминга в первом поколении

Так же, как мы оценили энтропию одного образа «Чужой-π», мы способны оценить энтропию и других 9999 образов «Чужой» тестовой базы.

Естественно, что эти образы будут давать разные значения энтропии. На рис. 6 приведены взаимно упорядоченные значения энтропий, полученные при реализации атаки извлечения знаний из нейросети [15–17]. Упорядочивание двухмерно и выполнено сортировкой полученных значений энтропии. Затем образу «Чужой» с минимальным значением энтропии был присвоен номер «Чужой-0». Далее, при взаимном упорядочивании образов «Чужой», учитывалась близость между кодовыми центрами образов и значениями их энтропии. Взаимно упорядоченные данные приведены на рис. 6.

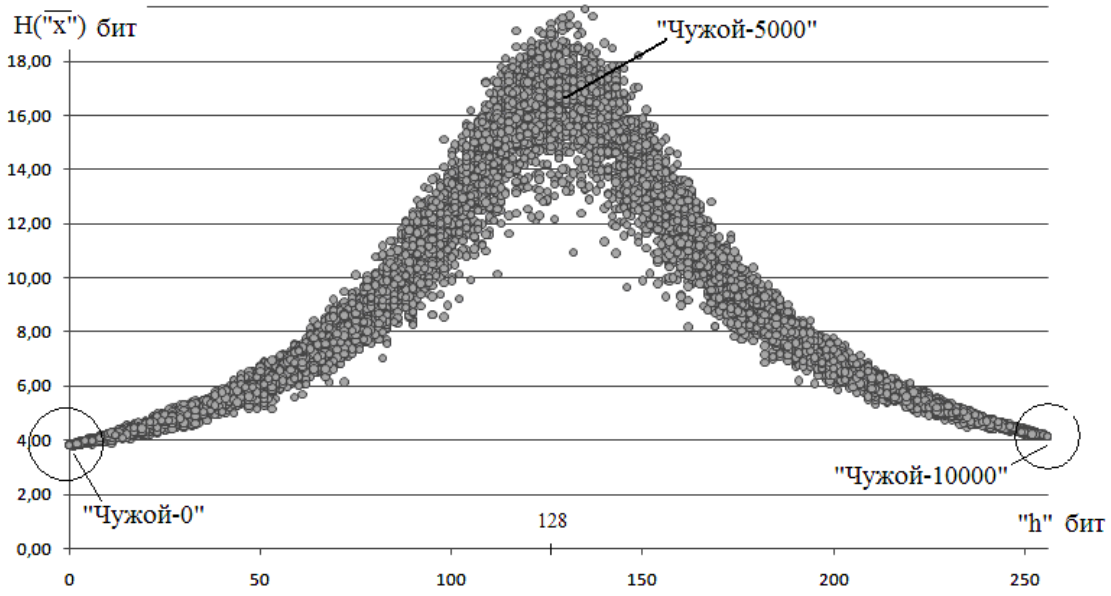


Рис. 6. Пример распределения энтропии упорядоченных образов «Чужой»

Из рис. 6 видно, что после двухмерного взаимного упорядочивания образов «Чужой» образуются две далеко расположенные области с низкой энтропией (эти области выделены окружностями). Наличие двух таких областей – это фундаментальное свойство сетей искусственных нейронов, автоматически обученных алгоритмом ГОСТ Р 52633.5 [3].

Эта симметрия имеет удобную графическую интерпретацию, приведенную на рис. 7, где отображены в виде линий проекции гиперплоскостей 13 нейронов, обрабатывающих пару «сырых» входных биометрических данных.

Любое сечение многомерной гиперсферы «Все образы» по любой паре входных данных дает похожие картины, одно из этих сечений приведено на рис. 7. Все линии проекции, разделяющих пространство, не пересекают эллипс нормально распределенных данных образа «СВОЙ». Именно по этой причине все примеры образа «СВОЙ», на которых обучена нейросеть, всегда имеют один и тот же выходной код.

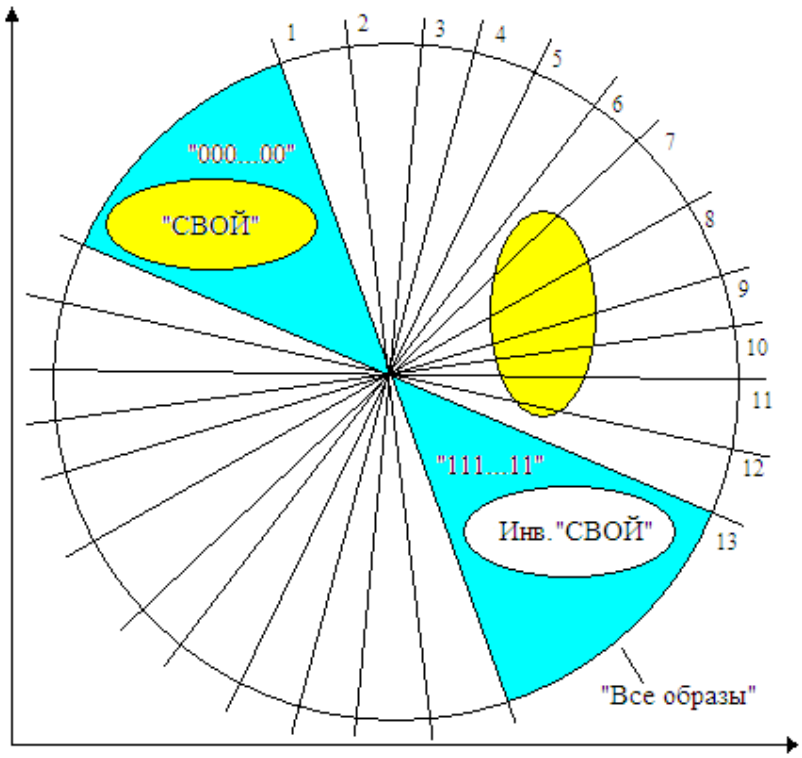


Рис. 7. Симметрия образа «СВОЙ» с выходным кодом «000…00»
и его противоположности (инверсным выходным кодом «111….11»)

Параллельно со стабильным гиперсектором «СВОЙ» обязательно существует его инверсный аналог, попадание в который данных образов стабильно дает инверсный выходной код нейросети. Если мы обучим нейросеть откликаться кодом из 265 состояний «0», то инверсный образ «Свой» будет откликаться инверсным, состоящим только из единиц «1». Мы имеем два очень стабильных гиперсектора с нулевой энтропией, все иные гиперсектора дают коды с высоким значением энтропии при малых вариациях входных данных. Чем большее число гиперплоскостей пересе-

кает классифицируемый образ, тем выше энтропия порождаемых им выходных кодовых состояний.

1.5. Извлечение данных из нейросети в последующих поколениях направленного подбора

Очевидно, что правые и левые коды «Чужой» с низкой энтропией будут давать коды наиболее близкие к коду «Свой» или к его инверсному коду. Для организации атаки по извлечению знаний из нейросети нужно выделить две группы образов «Чужой» с минимальной энтропией, объемом примерно по 50 образов, как это показано на рис. 6.

Далее следует восстановить численность выделенных образов путем их скрещивания между собой алгоритмом ГОСТ Р 52633.2 [18]. На рис. 8 иллюстрируется процедура скрещивания между собой двух образов-родителей и получение от них одного, двух, трех образов-потомков.

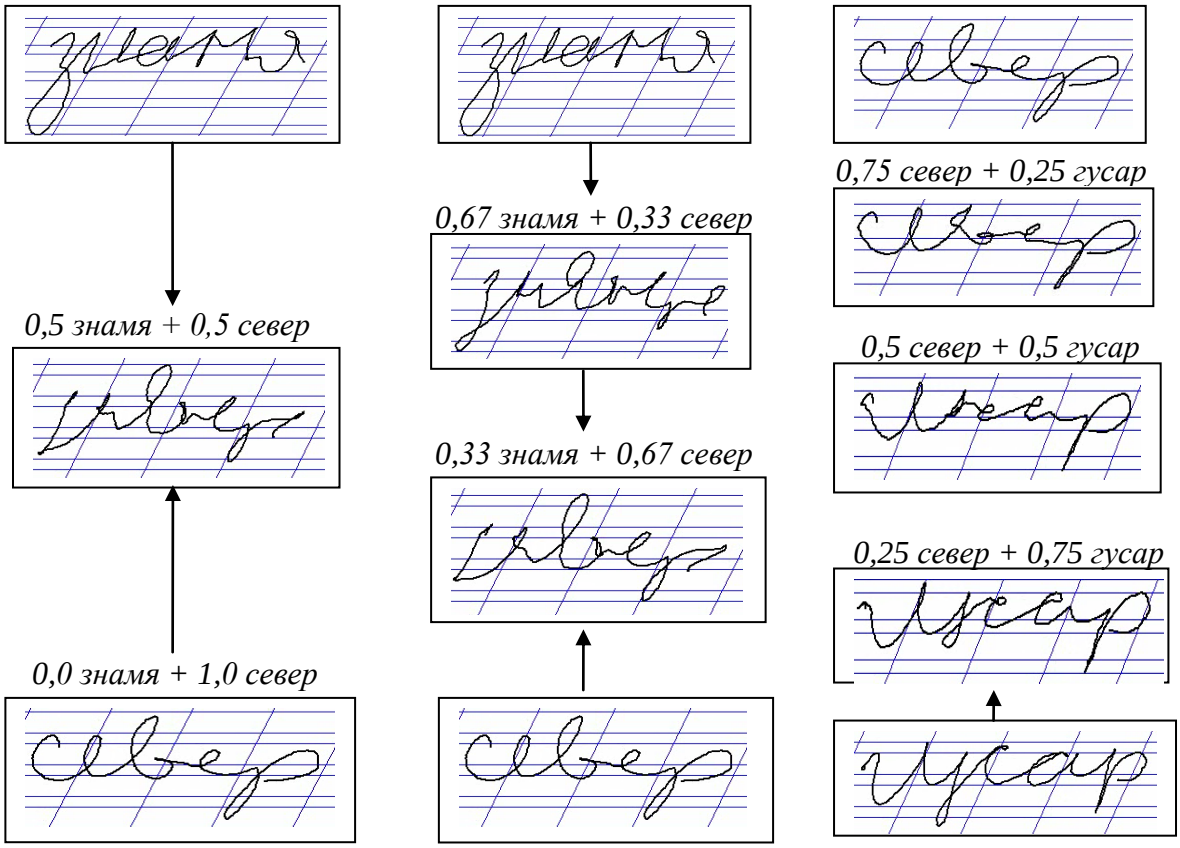


Рис. 8. Примеры синтеза одного, двух и трех образов-потомков скрещиванием двух образов-родителей

После восстановления численности тестовых образов «Чужой» во втором поколении следует повторить атаку подбора. Если повторять атаку направленного подбора порядка 50 поколений, то в итоге удается извлечь из нейросети порядка 97 % знаний о размещенном в ней коде ключа «Свой» и о биометрических параметров образа «Свой».

ГЛАВА ВТОРАЯ

АВТОКОРРЕЛЯЦИОННЫЙ ПОДХОД К ОЦЕНКЕ ПОКАЗАТЕЛЕЙ НЕЙРОСЕТЕВОЙ ДИНАМИКИ ВЫХОДНЫХ СОСТОЯНИЙ ПРЕОБРАЗОВАТЕЛЕЙ БИОМЕТРИИ В КОД КРИПТОГРАФИЧЕСКОЙ АУТЕНТИФИКАЦИИ

2.1. Квантовая сцепленность длинных выходных кодов сети искусственных нейронов с существенно зависимыми состояниями разрядов

Следует отметить, что в предыдущей главе рассматривалась ситуация, когда на входы нейросети подавалось множество образов «Чужой». В этой ситуации изменяются все выходные разряды кода нейросети, а вероятности появление состояний «0» и состояний «1» в каждом разряде практически совпадают. Выполнение этого условия обусловлено тем, что все гиперплоскости нейронов проходят через центр многомерной гиперсферы «Чужой», как это показано на рис. 7.

Формально выполнение условия $P(«0_i») \approx P(«1_i») \approx 0{,}5$ приводит к нулевому показателю стабильности кодовых состояний [6] по каждому разряду:

$$w_i \approx 2\left|0{,}5 - P(«0_i»)\right| = 2\left|0{,}5 - P(«1_i»)\right| \approx 0{,}0. \qquad (7)$$

На рис. 9 приведена простая графическая иллюстрация корреляционной сцепленности между разрядами изменяющихся состояний кода в виде вращающихся окружностей.

Из рис. 9 видно, что ровно половина вращающихся дисков помечена темной заливкой. Наблюдение темной заливки соответствует состояние «1», светлая часть диска соответствует состояние «0». Если разметка вращающихся дисков инверсная, то корреляция между разрядами оказывается единично отрицательной. Повторение разметки дает высокий положительный коэффициент корреляции.

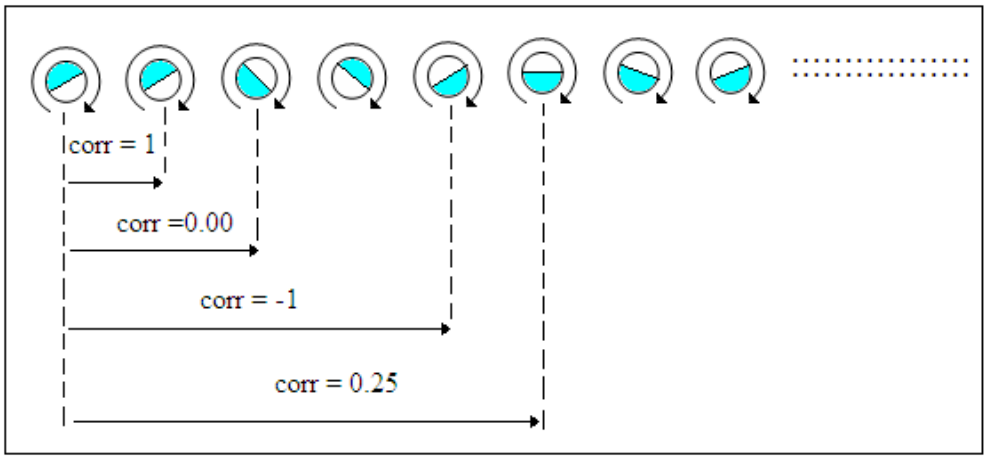


Рис. 9. Модель корреляционной сцепленности первого разряда
с другими разрядами длинного кода при нулевом показателе стабильности

Следует отметить, что ситуация кардинально меняется, если на обученную сеть искусственных нейронов подавать примеры одного образа «Чужой-π». В этом случае на ряду с нестабильными разрядами появляются абсолютно стабильные разряды, как это показано на рис. 10.

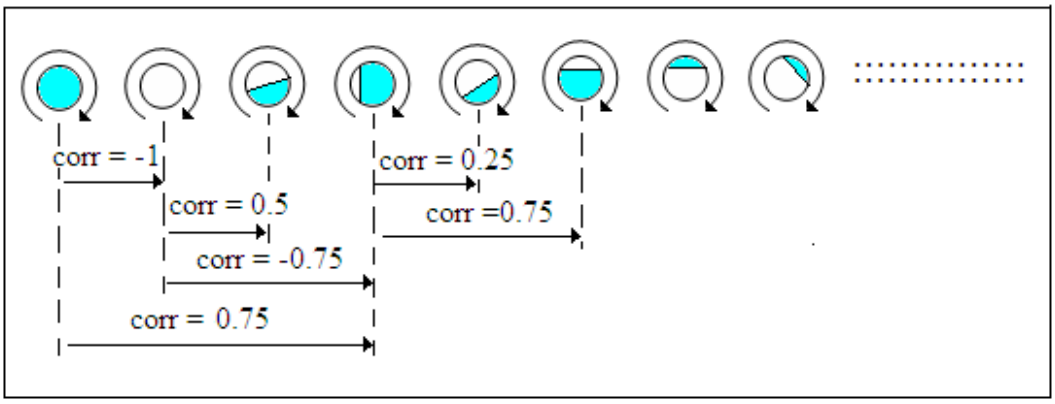


Рис. 10. Появление полностью стабильных разрядов кода для примеров
единственного образа «Чужой-π» (полная заливка или вообще нет заливки)

По мере того, как число абсолютно стабильных разрядов увеличивается, образ «Чужой» становится все больше и больше похож на образ «Свой», у которого все разряды кода обладают высокой стабильности. На рис. 11 отображена эта ситуация. Часть разрядов примеров образа «Свой» могут оставаться не абсолютно стабильными, в правой части рис. 11 показан не абсолютно стабильный разряд («слабый» разряд).

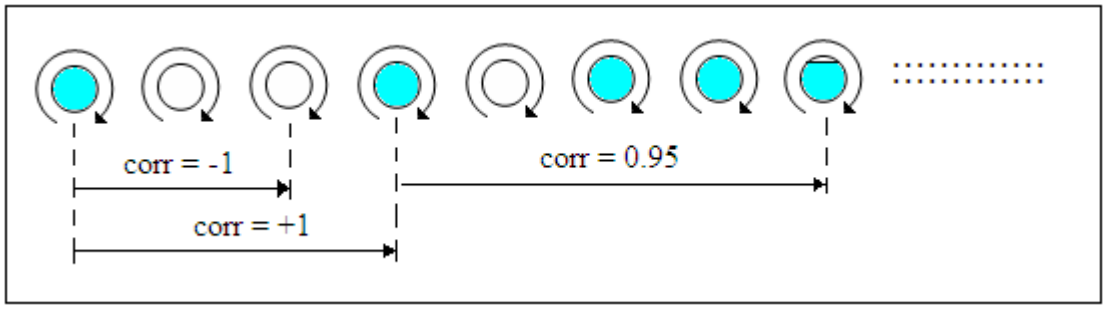


Рис. 11. Сильно коррелированные разряды кода для примеров образа «Свой» с высоким уровнем стабильности $w_i \approx 0{,}999$

В первом приближении модуль коэффициента корреляции можно оценить через усреднение показателей стабильности его разрядов:

$$|R| \approx \frac{1}{256} \sum_{i=1}^{256} w_i . \qquad (8)$$

Естественно, что для разных значений корреляционной сцепленности разрядов кода получаются разные картины распределений значений показателей стабильности, что отражено на рис. 12.

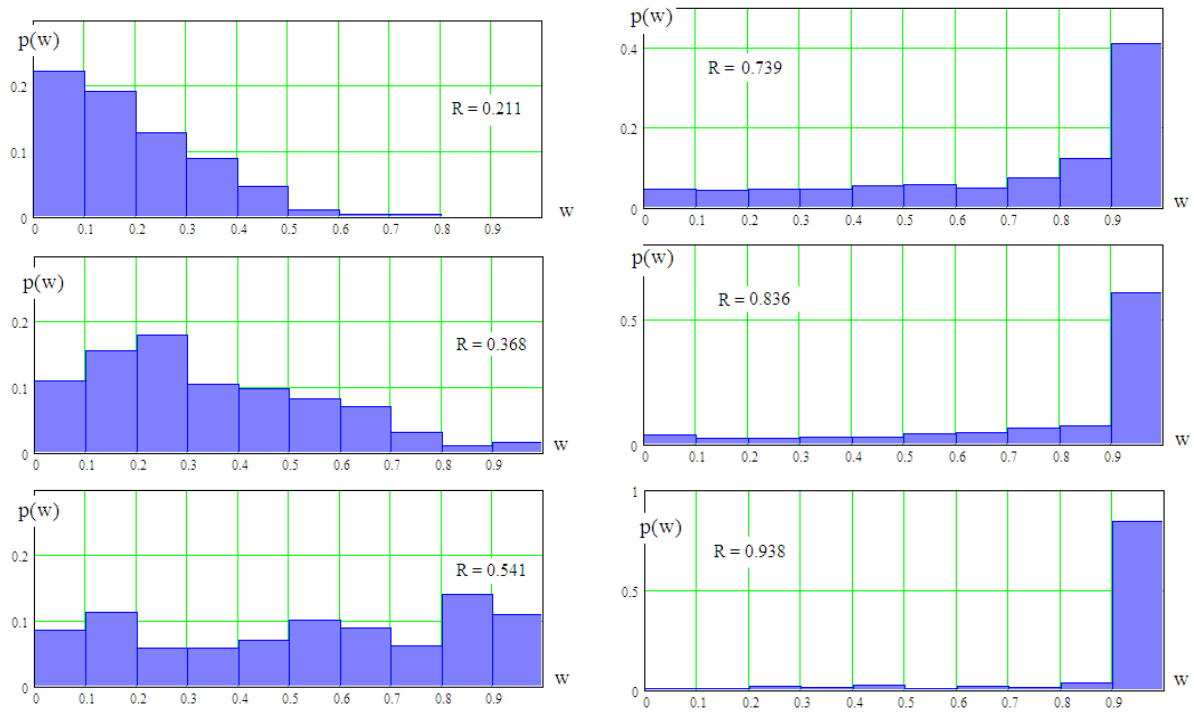


Рис. 12. Примеры типовых распределений значений показателей стабильности разрядов выходных кодов для образа «Чужой-π»

В правом верхнем углу рисунка отображен пример распределения показателей, характерный для слабо коррелированных данных при низкой стабильности разрядов выходного кода. По мере повышения стабильности состояний кода, а также по мере роста модуля коррелированности состояний разрядов, происходит размывание распределений. Максимум размывания распределений возникает при корреляции R = 0,50. При больших выборках числа примеров образа «Чужой-π» и при выполнении условия R = 0,50 распределение показателей стабильности становится равномерным (нижняя левая часть рис. 12).

Численный эксперимент, позволивший получить данные рис. 12, выполнен программным кодом, приведенным в прил. 2. В правой части рисунка отображены распределения показателей стабильности разрядов, характерные для сильно коррелированных данных с высокой стабильностью состояний разрядов.

2.2. Автосвертки Хэмминга, вычисленные по парам кодов-откликов на примеры одного образа «Чужой-π»

В первой главе данной работы показано, что кроссвертки Хэмминга разных образов «Чужой» позволяют в миллиарды раз сократить вычислительные затраты при оценках энтропии длинных кодов. Скорее всего, автосвертки Хэмминга обладают похожими свойствами:

$$\begin{cases} «h_{1,z}» = \sum_{i=1}^{256} \left[(«x_{1,i}») \oplus («x_{z,i}») \right] \quad \text{при} \quad z = \{2, 3, ..., k = 20\} \\ «h_{2,z}» = \sum_{i=1}^{256} \left[(«x_{1,i}») \oplus («x_{z,i}») \right] \quad \text{при} \quad z = \{3, 4, ..., k = 20\} \\ \quad :::, \end{cases} \qquad (9)$$

где k = 20 – объем малой выборки примеров образа «Чужой».

Вычисления вида (9) дают данных больше, чем используется при вычислении кодового центра по формуле (5). Это означает, что потенциал роста точности оценок на малых выборках значителен. На рис. 13 иллюстрируется связь математического ожидания расстояний Хэмминга с уровнем корреляционной сцепленности данных.

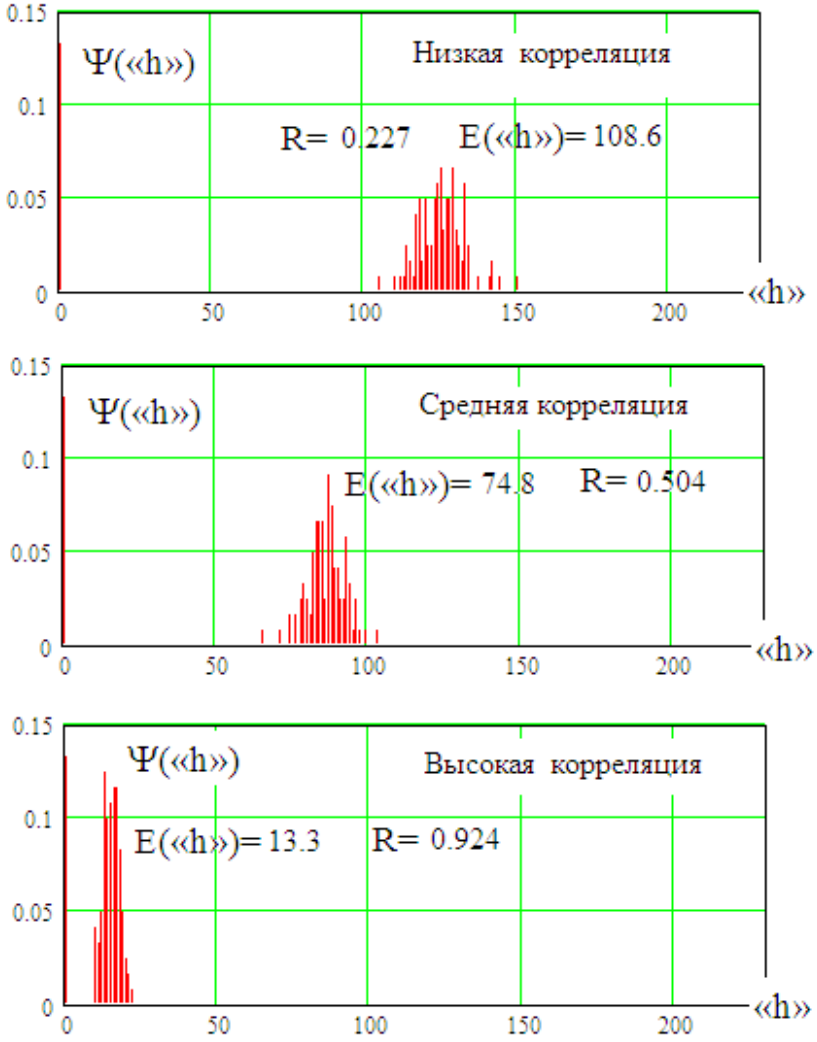


Рис. 13. Зависимость математического ожидания спектров автосверток Хэмминга от уровня корреляционной сцепленности

Параллельно с уменьшением математического ожидания с ростом показателя корреляционной сцепленности уменьшается и стандартное отклонение распределений расстояний Хэмминга. Эта ситуация отображена на рис. 14.

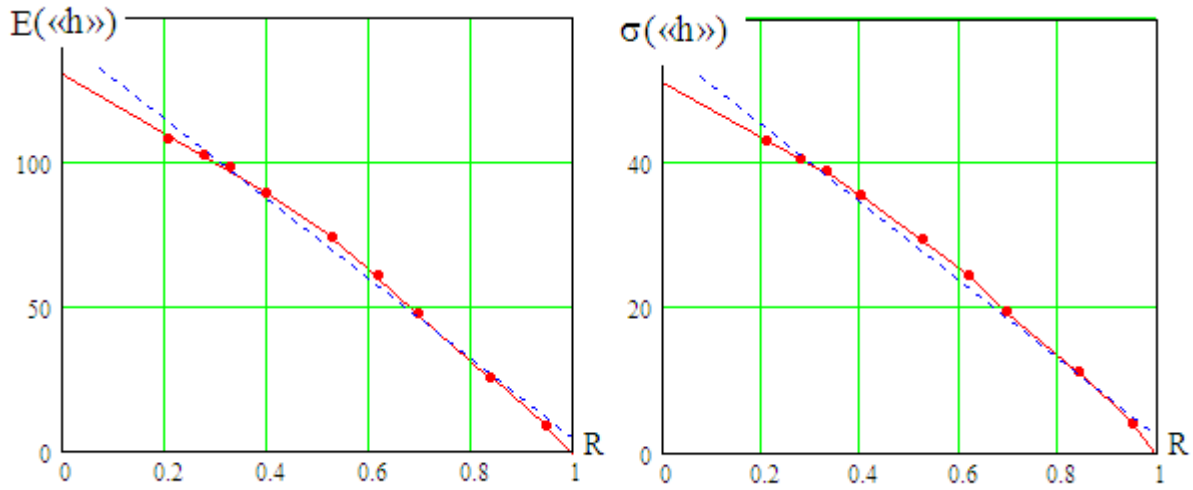


Рис. 14. Связь математического ожидания и стандартного отклонения с показателем корреляционной сцепленности

2.3. Оценка связанности коэффициентов корреляции, вычисленных линейным преобразованием математического ожидания, стандартного отклонения и среднего показателя стабильности

Из рис. 14 видно, что математическое ожидание E(«h») и стандартное отклонение σ(«h») почти линейно связаны с коэффициентом корреляционной сцепленности – R. Вычисления выполняются по следующей формуле:

$$\begin{cases} RE = \dfrac{142 - E(«h»)}{138} \\ R\sigma = \dfrac{56 - \sigma(«h»)}{54}. \end{cases} \qquad (10)$$

Очевидно, что два способа оценки коэффициентов корреляционной сцепленности (10) потенциально могут повысить точность оценки, если они имеют достаточно существенную независимую компоненту. В прил. 3 приводится программное обеспечение, оценивающее корреляционную сцепленность двумя разными способами (10).

К сожалению, рассмотренные выше два способа вычисления оценок сильно коррелированы corr(RE, Rσ) ≈ 0,996. Имеет смысл использовать

только один из этих параметров. То же самое относится и к показателю средней стабильности, он сильно связан с автосвертками Хэмминга corr(RE,E(w)) $\approx$ 0,95. Нельзя тройку этих параметров использовать для усреднения, точность оценок практически не увеличится.

2.4. Автосвертки Хэмминга образа «Чужой-π», построенные на вычислении среднего, взвешенного показателями стабильности разрядов кода

Из-за сильной зависимости по-разному вычисленные параметры нельзя использовать для компенсации погрешностей. По этой причине необходимо искать достаточно независимые преобразования, использование которых дополняет уже рассмотренные автосвертки Хэмминга. К таким преобразованиям следует отнести вычисление расстояний Хэмминга, взвешенных показателями стабильности свертываемых между собой разрядов кода:

$$\begin{cases} hw_{1,z} = \sum_{i=1}^{256}\Big[(«x_{1,i}»)\oplus(«x_{z,i}»)\Big]\cdot w_i, \quad \text{при} \quad z=\{2, 3, ..., k=20\} \\ hw_{2,z} = \sum_{i=1}^{256}\Big[(«x_{2,i}»)\oplus(«x_{z,i}»)\Big]\cdot w_i, \quad \text{при} \quad z=\{3, 4, ..., k=20\}, \\ \vdots \end{cases} \qquad (11)$$

где k = 20 – объем малой выборки примеров образа «Чужой».

Численный эксперимент, описание которого дано в прил. 4, показатель корреляционной сцепленности (8) и функционалы Хэмминга (11) обладают существенной независимостью. При этом математическое ожидание спектра автосверток Хэмминга связано с коэффициентом корреляционной сцепленности квадратичной функцией, как это показано на рис. 15.

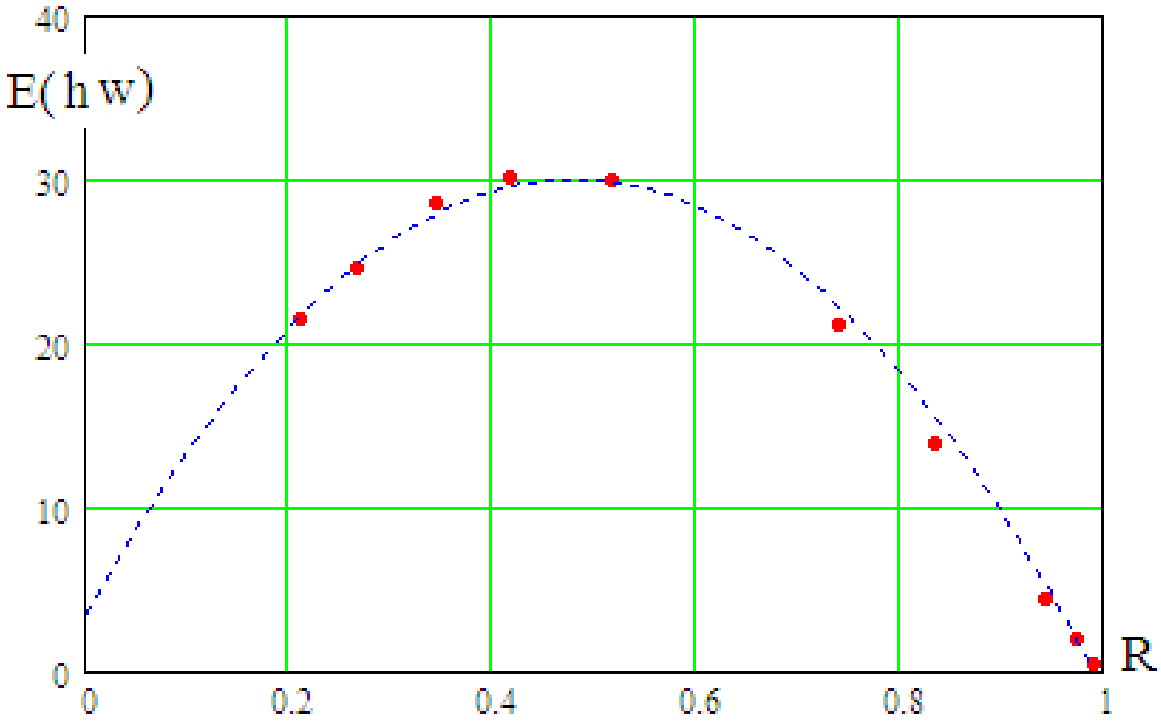


Рис. 15. Квадратичная связь среднего автосверток Хэмминга, взвешенных значениями показателей стабильности

Пересчет математического ожидания в коэффициент корреляции выполняется по следующей квадратичной формуле:

$$\begin{cases} Rw = \sqrt{\dfrac{\left|E(h \cdot w) - 30\right|}{115}} - 0,48 \ \text{ при } E(h \cdot w) < 0,48 \\ Rw = \sqrt{\dfrac{\left|E(h \cdot w) - 30\right|}{115}} + 0,48 \ \text{ при } E(h \cdot w) \geq 0,48. \end{cases} \quad (12)$$

Данные, вычисленные по формулам (12) и (8), отрицательно коррелированны corr(R,Rw) = –0,33. Если бы корреляция между данными полностью отсутствовала, то, усредняя эти данные, возможно было бы снизить интервал ошибок в 1,41 раза (снизить ошибку на 41 %). Остаточная корреляция corr(R, Rw) = –0,33 снижает эффективность усреднения. Ошибку удается снизить только на 21 %.

2.5. Получение существенно независимых оценок расширением окна свертывания кодовых последовательностей

Как было показано в предыдущем параграфе, появление независимой компоненты в разнотипных оценках корреляционной сцепленности является предпосылкой повышения точности при их усреднении. При этом, чем больше независимая компонента, тем больше повышение точности при усреднении.

Очевидным является также то, что рост числа достаточно независимых, оцениваемых компонент, так же будет приводить к повышению точности за счет их усреднения. В этом отношении необходимо осознавать то, каким образом целесообразно модифицировать автосвертки Хэмминга.

Одним из путей модификации автосверток является изменение ширины скользящего окна свертываемых кодов. Например, окно в один бит обычных сверток Хэмминга (9), (11) может быть увеличено до окна в два скользящих бита:

$$\begin{cases} «h2_{1,z}» = \sum_{i=1}^{255}\left[\begin{pmatrix} «x_{1,i}» \\ \oplus \\ «x_{1,i+1}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \end{pmatrix}\right] \quad \text{при} \quad z = \{2, 3, ..., k = 20\} \\ «h2_{2,z}» = \sum_{i=1}^{255}\left[\begin{pmatrix} «x_{2,i}» \\ \oplus \\ «x_{2,i+1}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \end{pmatrix}\right] \quad \text{при} \quad z = \{3, 4, ..., k = 20\} \quad (13) \\ :: \\ :: \\ :: \end{cases}$$

При такой модификации возникает достаточно значимая независимая компонента corr(E(«h2»), E(w)) = –0,754 по данным прил. 5.1.

Очевидной является возможность увеличения ширины скользящего окна, например, до окна в три скользящих бита, как это показано в формуле (14).

$$
\begin{cases}
«h3_{1,z}» = \sum\limits_{i=1}^{254}\left[\begin{pmatrix} «x_{1,i}» \\ \oplus \\ «x_{1,i+1}» \\ \oplus \\ «x_{1,i+2}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \\ \oplus \\ «x_{z,i+2}» \end{pmatrix}\right] \text{ при } z = \{2,3,...,20\} \\
«h3_{2,z}» = \sum\limits_{i=1}^{254}\left[\begin{pmatrix} «x_{2,i}» \\ \oplus \\ «x_{2,i+1}» \\ \oplus \\ «x_{2,i+2}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \\ \oplus \\ «x_{z,i+2}» \end{pmatrix}\right] \text{ при } z = \{3,4,...,20\} \\
:: \\
:: \\
:: \\
:::
\end{cases} \quad (14)
$$

Формально свертки Хэмминга должны вычисляться только с использованием операций сложения по модулю два, однако модуль вычислительных операций может быть увеличен [19–22].

$$
\begin{cases}
«\tilde{h}2_{1,z}» = \sum\limits_{i=1}^{255}\left[\begin{pmatrix} «x_{1,i}» \\ \oplus \\ «x_{1,i+1}» \end{pmatrix} + \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \end{pmatrix}\right] \quad \text{при} \quad z = \{2,3,....,k=20\} \\
«\tilde{h}2_{2,z}» = \sum\limits_{i=1}^{255}\left[\begin{pmatrix} «x_{2,i}» \\ \oplus \\ «x_{2,i+1}» \end{pmatrix} + \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \end{pmatrix}\right] \quad \text{при} \quad z = \{3,4,....,k=20\} \\
:: \\
:: \\
:::
\end{cases} \quad (15)
$$

Формула (15) соответствует вычислению автосверток по скользящему окну шириной в два бита. Соответствующий численный эксперимент,

описаннный в прил. 5. ч. 2, обеспечивает корреляционную сцепленность corr(E(«h2»), E(w)) = –0,219. Следующая формула (16) построена на окне свертывания в три бита.

$$\begin{cases} «\tilde{h}3_{1,z}» = \sum\limits_{i=1}^{254} \left[\begin{pmatrix} «x_{1,i}» \\ \oplus \\ «x_{1,i+1}» \\ \oplus \\ «x_{1,i+2}» \end{pmatrix} + \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \\ \oplus \\ «x_{z,i+2}» \end{pmatrix} \right] \text{ при } z = \{2, 3, ..., 20\} \\ «\tilde{h}3_{2,z}» = \sum\limits_{i=1}^{254} \left[\begin{pmatrix} «x_{2,i}» \\ \oplus \\ «x_{2,i+1}» \\ \oplus \\ «x_{2,i+2}» \end{pmatrix} + \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \\ \oplus \\ «x_{z,i+2}» \end{pmatrix} \right] \text{ при } z = \{3, 4, ..., 20\} \\ :: \\ :: \\ :: \\ :: \end{cases} \quad (16)$$

Еще одним вариантом выполнения сверток является их взвешивание показателями стабильности разрядов:

$$\begin{cases} «h2w_{1,z}» = \sum\limits_{i=1}^{255} \left[\begin{pmatrix} «x_{1,i}» \\ \oplus \\ «x_{1,i+1}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \end{pmatrix} \right] \cdot \sqrt{w_i \cdot w_{i+1}} \quad \text{при} \quad z = \{2, 3, ..., k = 20\} \\ «h2w_{2,z}» = \sum\limits_{i=1}^{255} \left[\begin{pmatrix} «x_{2,i}» \\ \oplus \\ «x_{2,i+1}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \end{pmatrix} \right] \cdot \sqrt{w_i \cdot w_{i+1}} \quad \text{при} \quad z = \{3, 4, ..., k = 20\} \\ :: \\ :: \\ :: \end{cases} \quad (17)$$

Как показано далее в формулах (17–19) вариантов вычисления автосверток Хэмминга достаточно много. Результаты численного моделирования этого типа вычислений даны в прил. 5 (части 3–5).

$$
\begin{cases}
«h3_{1,z}» = \sum_{i=1}^{254} \left[\begin{pmatrix} «x_{1,i}» \\ \oplus \\ «x_{1,i+1}» \\ \oplus \\ «x_{1,i+2}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \\ \oplus \\ «x_{z,i+2}» \end{pmatrix} \right] \cdot \sqrt[3]{w_i \cdot w_{i+1} \cdot w_{i+2}} \quad \text{при} \quad z = \{2, 3, ..., 20\} \\
«h3_{2,z}» = \sum_{i=1}^{254} \left[\begin{pmatrix} «x_{2,i}» \\ \oplus \\ «x_{2,i+1}» \\ \oplus \\ «x_{2,i+2}» \end{pmatrix} \oplus \begin{pmatrix} «x_{z,i}» \\ \oplus \\ «x_{z,i+1}» \\ \oplus \\ «x_{z,i+2}» \end{pmatrix} \right] \cdot \sqrt[3]{w_i \cdot w_{i+1} \cdot w_{i+2}} \quad \text{при} \quad z = \{3, 4, ..., 20\} \\
:: \\
:: \\
:: \\
:: \\
\end{cases}
\tag{18}
$$

По мере увеличения окна свертывания корреляционная сцепленность данных снижается с данными, вычисленными на малых значениях окна. В этом контексте необходимо стремиться не только к использованию сверток, вычисленных на окнах разной длины, но и к ортогонализации этих сверток [23]. На текущий момент общие принципы ортогонализации нейросетевых вычислений понятны, однако публикаций в этом направлении крайне мало.

ЗАКЛЮЧЕНИЕ

Искусственные нейронные сети так же, как и естественные нейронные сети, способны решать задачи огромной размерности. Мы – свидетели быстрого развития новых эффективных технологий обработки информации. В первой главе данной работы показано, что переход от анализа выходных кодов нейросети в статике и переход к анализу спектров Хэмминга дает миллиардный выигрыш по ускорению вычислений. При этом, перевод искусственной нейросети из статики в динамику хорошо отражает практику использования естественных нейронных сетей человеком. В наших головах вообще нет использования нейросетевых вычислений в статике. Мы с вами все реальные очень сложные вычисления осуществляем в нейродинамике, о чем свидетельствуют электроэнцефалограммы работы нашего головного мозга.

Видимо, наши огромные интеллектуальные возможности обусловлены именно тем, что наши естественные нейронные сети постоянно находятся в нейродинамике и тем самым многократно ускоряют свои вычислительные возможности. То, что в нейродинамике удается в миллиарды раз ускорить вычисления, было понятно давно (на использовании этого эффекта был создан ГОСТ Р 52633.3–2011), однако все построенные 10 лет назад вычислительные процедуры построены на кроссвертках Хэмминга.

Данный препринт является осознанной попыткой закрыть этот однобокий взгляд на проблему. Автосвертки Хэмминга – это не менее эффективный вычислительный инструмент. На их использовании могут быть построены не менее эффективные вычислительные процедуры. Авторы данной работы надеются привлечь внимание специалистов к использованию для создания нейросетевых вычислителей как кроссверток Хэмминга, так и автосверток Хэмминга.

СПИСОК ЛИТЕРАТУРЫ

1. McCulloch W.S., Pitts W. A logical calculus of the ideas imminent in nervous activities // Bulletin of Mathematical Biophysics. 1943. № 5. P. 115–133.

2. Хайкин С. Нейронные сети: полный курс. М. : Вильямс, 2006. С. 1104.

3. Р 50.1.037–2002. Рекомендации по стандартизации. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Ч. I. Критерии типа χ2. Госстандарт России. М., 2001. 140 с.

4. Р 50.1.037–2002. Прикладная статистика. Правила проверки согласия опытного распределения с теоретическим. Ч. II. Непараметрические критерии. Госстандарт России. М., 2002. 123 с.

5. Кобзарь А. И. Прикладная математическая статистика. Для инженеров и научных работников. М. : ФИЗМАТЛИТ, 2006. 816 с.

6. ГОСТ Р 52633.5–2011. Защита информации. Техника защиты информации. Автоматическое обучение нейросетевых преобразователей биометрия-код доступа.

7. Техническая спецификация «Системы обработки информации. Криптографическая защита информации. Защита нейросетевых биометрических контейнеров с использованием криптографических алгоритмов», принята 19.11.2020 на XXV заседании технического комитета № 26.

8. ISO/IEC 24745:2011 Information technology. Security techniques. Biometric information protection.

9. ISO/IEC 24761:2009 Information technology. Security techniques. Authentication context for biometrics.

10. ISO/IEC 19792:2009 Information technology. Security techniques. Security evaluation of biometrics.

11. ГОСТ Р 52633.3–2011. Защита информации. Техника защиты информации. Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора.

12. Possibility of Decrease in a Level of Data Correlation During Processing Small Samples Using Neural Networks by Generating New Statistic Tests / A. I. Ivanov, A. G. Bannykh, P. S. Lozhnikov, A. E. Sulavko, D. P. Inivatov // Journal of Physics: Conference Series (2020 J. Phys.: Conf. Ser. 1546 012080).

13. Иванов А. И., Банных А. Г. Быстрая оценка энтропии длинных кодов с зависимыми разрядами на микроконтроллерах с малым потреблением и низкой разрядностью (обзор литературы по снижению размерности задачи) // Инженерные технологии и системы, 2020. Т. 30, № 2. С. 300–312.

14. ГОСТ Р 52633.1–2009. Защита информации. Техника защиты информации. Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

15. Волчихин В. И., Иванов А. И. Нейросетевая молекула: решение обратной задачи биометрии через программную поддержку квантовой суперпозиции на выходах сети искусственных нейронов // Вестник Мордовского университета. 2017. Т. 27, № 4. С. 518–523.

16. Волчихин В. И., Иванов А. И., Банных А. Г. Регуляризация вычисления энтропии выходных состояний нейросетевого преобразователя биометрия-код, построенная на размножении малой выборки исходных данных // Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 4. С. 14–23.

17. Майоров А. В., Сомкин С. А., Юнин А. П., Акмаев А. Ж. Оценка стойкости защищенных нейросетевых преобразователей биометрия-код с использованием больших баз синтетических биометрических образов //

Безопасность информационных технологий : сб. науч. ст. по матер. I Всерос. науч.-техн. конф. (24 апреля, г. Пенза), 2019. С. 130–136.

18. ГОСТ Р 52633.2–2010. Защита информации. Техника защиты информации. Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации.

19. Иванов А. И., Юнин А. П. Эмбрион искусственного интеллекта: компактная нейросетевая проверка качества случайных последовательностей, полученных из биометрических данных. Пенза : Изд-во ПГУ, 2021. 62 с.

20. Волчихин В. И., Иванов А. И., Юнин А. П., Малыгина Е. А. Многомерный портрет цифровых последовательностей идеального «белого шума» в свертках Хэмминга // Известия высших учебных заведений. Поволжский регион. Технические науки. 2017. № 4. С. 4–13.

21. Юнин А. П., Иванов А. И., Ратников К. А., Кольчугина Е. А. Оценка качества «белого» шума: реализация теста «стаи обезьян» через множество сверток Хэмминга, построенных на разных системах счисления // Известия высших учебных заведений. Поволжский регион. Технические науки. 2018. № 4 (48). С. 54–64.

22. Иванов А. И., Юнин А. П., Бояршинов М. А. Оценка энтропии длинных кодовых слов на выходе нейросетевого преобразователя биометрии в пространствах множества сверток Хэмминга // Интеллектуальные системы в производстве. 2019. Т. 17, № 2. С. 30–36.

23. Иванов А. И., Куприянов Е. Н. Защита искусственного интеллекта: ортогонализация статистико-нейросетевого анализа малых выборок биометрических данных : препринт. Пенза : Изд-во ПГУ, 2020. 72 с.

Часть 1. Программное обеспечение численного эксперимента, связывающего малую выборку из 21 примера кодов образа «Чужой» с разным уровнем модуля средней коррелированности

$x := rnorm(256, 0, 1)$

$ss5(rr) := \left| \begin{array}{l} y \leftarrow rnorm(256, 0, 5 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss5(rr_i)$

$i := 0..255$

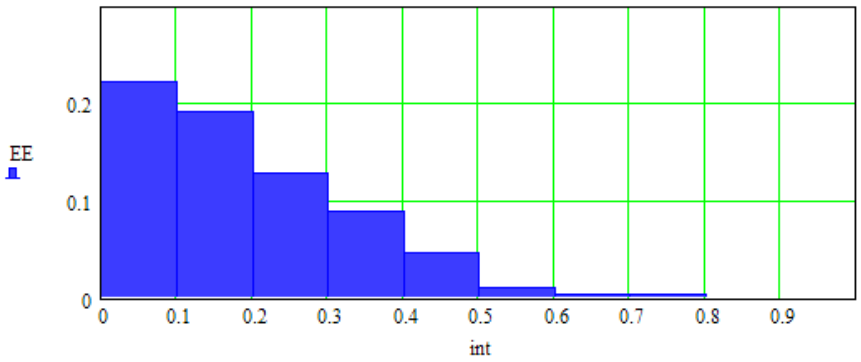
$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

$mean(w) = 0.211$

$i := 0..20$

$int_i := 0.05 + 0.1 \cdot i$ $\quad EE := \frac{hist(int, w)}{256}$



$ss2(rr) := \left| \begin{array}{l} y \leftarrow rnorm(256, 0, 2 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss2(rr_i)$

$i := 0..255$

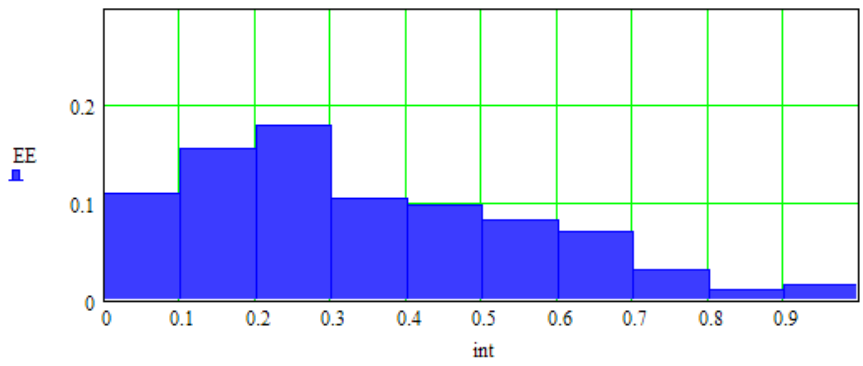
$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

$mean(w) = 0.368$

$i := 0..20$

$int_i := 0.05 + 0.1 \cdot i$ $\quad EE := \frac{hist(int, w)}{256}$



Приложение 1

Часть 2. Программное обеспечение численного эксперимента, связывающего малую выборку из 21 примера кодов образа «Чужой» с разным уровнем модуля средней коррелированности

$$ss1(rr) := \left| \begin{array}{l} y \leftarrow rnorm(256, 0, 1 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss1(rr_i)$

$i := 0..255$

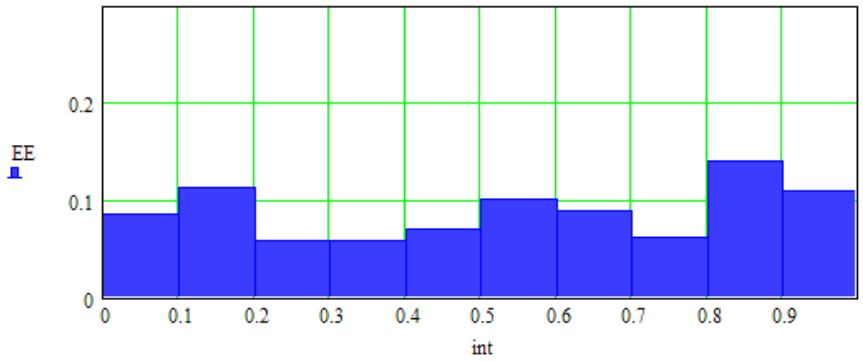
$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

$mean(w) = 0.54$

$i := 0..20$

$int_i := 0.05 + 0.1 \cdot i$ $\quad EE := \frac{hist(int, w)}{256}$



$$ss05(rr) := \left| \begin{array}{l} y \leftarrow rnorm(256, 0, 0.5 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss05(rr_i)$

$i := 0..255$

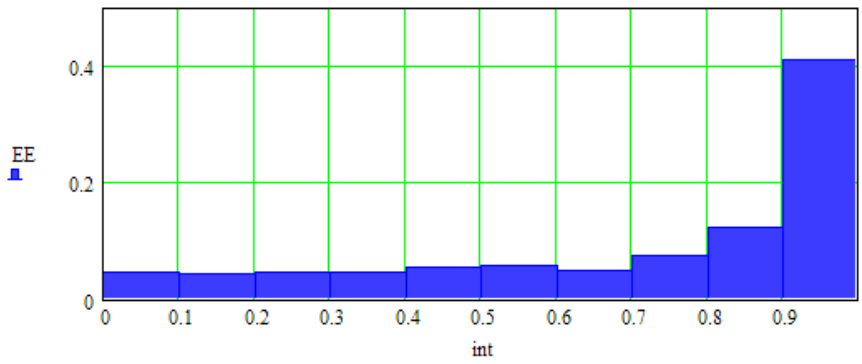
$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

$mean(w) = 0.739$

$i := 0..20$

$int_i := 0.05 + 0.1 \cdot i$ $\quad EE := \frac{hist(int, w)}{256}$



Часть 3. Программное обеспечение численного эксперимента, связывающего малую выборку из 21 примера кодов образа «Чужой» с разным уровнем модуля средней коррелированности

$$ss03(rr) := \left| \begin{array}{l} y \leftarrow mom(256, 0, 0.3 + rr) \\ \text{for } i \in 0..255 \\ \quad z_i \leftarrow 0 \\ \quad z_i \leftarrow 1 \text{ if } y_i \geq x_i \\ z \end{array} \right.$$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss03(rr_i)$

$i := 0..255$

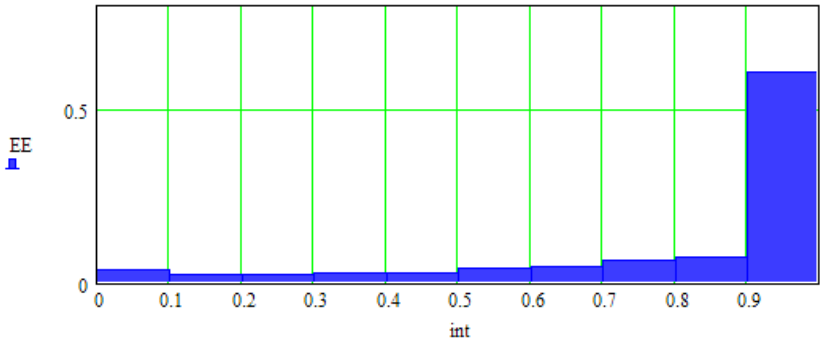
$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

mean(w) = 0.836

$i := 0..20$

$int_i := 0.05 + 0.1 \cdot i$ $\quad EE := \frac{hist(int, w)}{256}$



$$ss01(rr) := \left| \begin{array}{l} y \leftarrow mom(256, 0, 0.1 + rr) \\ \text{for } i \in 0..255 \\ \quad z_i \leftarrow 0 \\ \quad z_i \leftarrow 1 \text{ if } y_i \geq x_i \\ z \end{array} \right.$$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss01(rr_i)$

$i := 0..255$

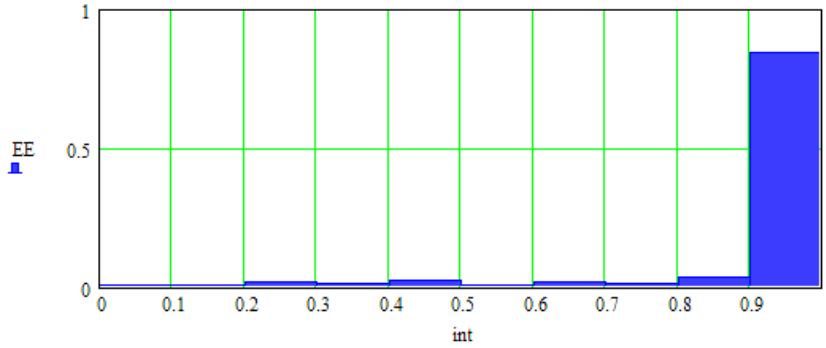
$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

mean(w) = 0.936

$i := 0..20$

$int_i := 0.05 + 0.1 \cdot i$ $\quad EE := \frac{hist(int, w)}{256}$



Приложение 2

Часть 1. Связь математических ожиданий автосверток Хэмминга с усредненным показателем стабильности. Слабая корреляционная сцепленность

$x := \mathrm{rnorm}(256, 0, 1)$

$ss5(rr) :=$ | $y \leftarrow \mathrm{rnorm}(256, 0, 5 + rr)$ | for $i \in 0..255$ | $z_i \leftarrow 0$ | $z_i \leftarrow 1$ if $y_i \geq x_i$ | z

$i := 0..20$

$rr_i := \mathrm{rnd}(0.001)$ $\quad z^{\langle i \rangle} := ss5(rr_i)$

$i := 0..255$

$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

$\mathrm{mean}(w) = 0.227$

$HH :=$ | for $i \in 1..20$

$h_i \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 0 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$

for $i \in 2..20$

$h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 1 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$

for $i \in 3..20$

$h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 2 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$

for $i \in 4..20$

$h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 3 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$

for $i \in 5..20$

$h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 4 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$

for $i \in 6..20$

$h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 5 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$

h

$HH =$

	0
105	0
106	123
107	125
108	125
109	125
110	120
111	142
112	132
113	120
114	133
115	133
116	121
117	133
118	118
119	130
120	129

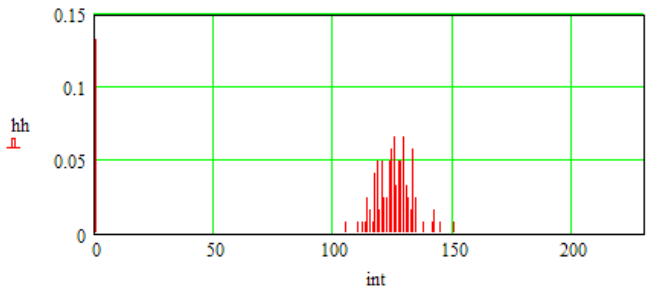
$\mathrm{mean}(HH) = 108.645$

$\mathrm{stdev}(HH) = 42.961$

$i := 0..250$

$int_i := 0 + i$

$hh := \frac{\mathrm{hist}(int, HH)}{120}$



Часть 2. Связь математических ожиданий автосверток Хэмминга с усредненным показателем стабильности. Корреляционная сцепленность R = 0,504

$$ss1(rr) := \left| \begin{array}{l} y \leftarrow rnorm(256, 0, 1 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss1(rr_i)$

$i := 0..255$

$zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$

$mean(w) = 0.504$

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 0 \rangle}\right)_j \right] \oplus \left[\left(z^{\langle i \rangle}\right)_j \right] \right] \\ \text{for } i \in 2..20 \\ \quad h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 1 \rangle}\right)_j \right] \oplus \left[\left(z^{\langle i \rangle}\right)_j \right] \right] \\ \text{for } i \in 3..20 \\ \quad h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 2 \rangle}\right)_j \right] \oplus \left[\left(z^{\langle i \rangle}\right)_j \right] \right] \\ \text{for } i \in 4..20 \\ \quad h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 3 \rangle}\right)_j \right] \oplus \left[\left(z^{\langle i \rangle}\right)_j \right] \right] \\ \text{for } i \in 5..20 \\ \quad h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 4 \rangle}\right)_j \right] \oplus \left[\left(z^{\langle i \rangle}\right)_j \right] \right] \\ \text{for } i \in 6..20 \\ \quad h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 5 \rangle}\right)_j \right] \oplus \left[\left(z^{\langle i \rangle}\right)_j \right] \right] \\ h \end{array} \right.$$

$HH =$

	0
105	0
106	87
107	88
108	65
109	79
110	85
111	103
112	92
113	92
114	83
115	93
116	88
117	81
118	88
119	88
120	82

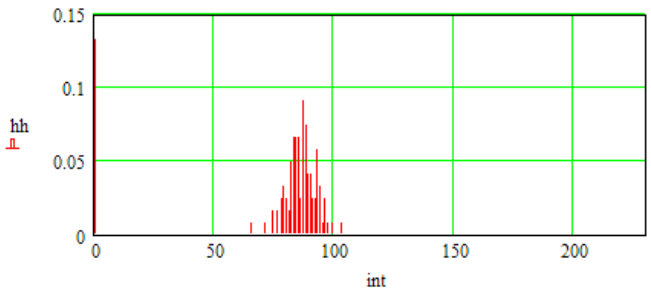
$mean(HH) = 74.843$

$stdev(HH) = 29.75$

$i := 0..250$

$int_i := 0 + i$

$hh := \frac{hist(int, HH)}{120}$



Часть 3. Связь математических ожиданий автосверток Хэмминга с усредненным показателем стабильности. Высокая корреляционная сцепленность R = 0,924

$$ss01(rr) := \left| \begin{array}{l} y \leftarrow rnorm(256, 0, 0.1 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$$

$i := 0..20$

$rr_i := rnd(0.001)$ $\quad z^{\langle i \rangle} := ss01(rr_i)$

$i := 0..255$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$ $\quad zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

$mean(w) = 0.924$

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 0 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \\ \text{for } i \in 2..20 \\ \quad h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 1 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \\ \text{for } i \in 3..20 \\ \quad h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 2 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \\ \text{for } i \in 4..20 \\ \quad h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 3 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \\ \text{for } i \in 5..20 \\ \quad h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 4 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \\ \text{for } i \in 6..20 \\ \quad h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 5 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \\ h \end{array} \right.$$

$HH =$

	0
105	0
106	15
107	16
108	17
109	10
110	15
111	13
112	18
113	21
114	16
115	13
116	15
117	16
118	16
119	12
120	17

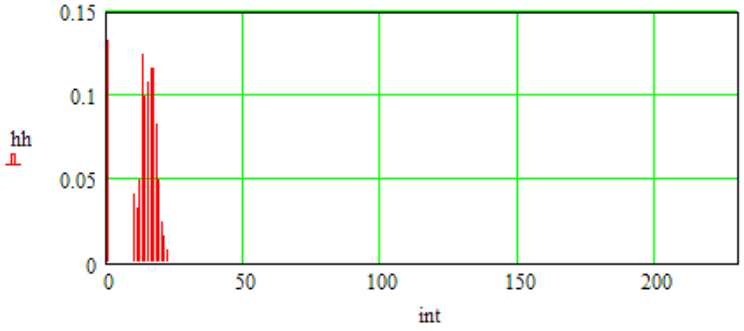
$mean(HH) = 13.256$

$stdev(HH) = 5.749$

$i := 0..250$

$int_i := 0 + i$

$hh := \frac{hist(int, HH)}{120}$



Приложение 3

Оценка показателя связанности двух вариантов вычисления показателей корреляционной сцепленности через математическое ожидание E(«h») и σ(«h») и среднего показателей стабильности

$x := \mathrm{rnorm}(256, 0, 1)$

$ss1(rr) :=$ | $y \leftarrow \mathrm{rnorm}(256, 0, 1 + rr)$ | for $i \in 0..255$ | $z_i \leftarrow 0$ | $z_i \leftarrow 1$ if $y_i \geq x_i$ | z

$i := 0..20$

$rr_i := \mathrm{rnd}(0.001)$ $\quad z^{\langle i \rangle} := ss1(rr_i)$

$i := 0..255$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$ $\quad zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$HH :=$ | for $i \in 1..20$ | $h_i \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 0 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$ | for $i \in 2..20$ | $h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 1 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$ | for $i \in 3..20$ | $h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 2 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$ | for $i \in 4..20$ | $h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 3 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$ | for $i \in 5..20$ | $h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 4 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$ | for $i \in 6..20$ | $h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 5 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right]$ | $HH \leftarrow \left(\frac{142 - \mathrm{mean}(h)}{138} \quad \frac{56 - \mathrm{stdev}(h)}{54}\right)$

$HH = (0.504 \quad 0.502)$ $\quad \mathrm{mean}(w) = 0.539$

$$RRR := \begin{pmatrix} 0.495 & 0.491 & 0.524 \\ 0.451 & 0.446 & 0.478 \\ 0.494 & 0.486 & 0.532 \\ 0.467 & 0.464 & 0.502 \\ 0.447 & 0.443 & 0.493 \\ 0.486 & 0.482 & 0.512 \\ 0.516 & 0.51 & 0.541 \\ 0.499 & 0.492 & 0.53 \\ 0.502 & 0.5 & 0.529 \\ 0.488 & 0.481 & 0.518 \\ 0.485 & 0.484 & 0.523 \\ 0.458 & 0.456 & 0.491 \\ 0.495 & 0.494 & 0.522 \\ 0.469 & 0.467 & 0.497 \\ 0.513 & 0.508 & 0.553 \\ 0.535 & 0.53 & 0.555 \\ 0.482 & 0.478 & 0.517 \\ 0.488 & 0.486 & 0.525 \\ 0.499 & 0.494 & 0.52 \\ 0.504 & 0.502 & 0.539 \end{pmatrix}$$

$\mathrm{corr}\left(RRR^{\langle 1 \rangle}, RRR^{\langle 2 \rangle}\right) = 0.95$

$\mathrm{corr}\left(RRR^{\langle 0 \rangle}, RRR^{\langle 1 \rangle}\right) = 0.996$ $\quad \mathrm{corr}\left(RRR^{\langle 0 \rangle}, RRR^{\langle 2 \rangle}\right) = 0.955$

Приложение 4

Оценка показателя связанности двух вариантов вычисления показателей корреляционной сцепленности через взвешевание показателем стабильности математических ожиданий разрядов кода автосверток Хэмминга и средней корреляции

$$x := \mathrm{rnorm}(256, 0, 1)$$

$$ss1(rr) := \left| \begin{array}{l} y \leftarrow \mathrm{rnorm}(256, 0, 1 + rr) \\ \text{for } i \in 0..255 \\ \quad \left| \begin{array}{l} z_i \leftarrow 0 \\ z_i \leftarrow 1 \text{ if } y_i \geq x_i \end{array} \right. \\ z \end{array} \right.$$

$$i := 0..20 \qquad rr_i := \mathrm{rnd}(0.001) \qquad z^{\langle i \rangle} := ss1\left(rr_i\right)$$

$$i := 0..255 \qquad zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i \qquad w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$$

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 0 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \cdot w_j \\ \text{for } i \in 2..20 \\ \quad h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 1 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \cdot w_j \\ \text{for } i \in 3..20 \\ \quad h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 2 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \cdot w_j \\ \text{for } i \in 4..20 \\ \quad h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 3 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \cdot w_j \\ \text{for } i \in 5..20 \\ \quad h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 4 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \cdot w_j \\ \text{for } i \in 6..20 \\ \quad h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{255} \left[\left[\left(z^{\langle 5 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right]\right] \cdot w_j \\ h \end{array} \right.$$

$$\mathrm{mean}(HH) = 25.997 \qquad \mathrm{mean}(w) = 0.52$$

$$RR := \begin{pmatrix} 28.105 & 0.524 \\ 27.667 & 0.478 \\ 28.285 & 0.532 \\ 28.559 & 0.502 \\ 28.324 & 0.532 \\ 30.369 & 0.493 \\ 26.919 & 0.512 \\ 26.781 & 0.541 \\ 27.078 & 0.53 \\ 26.96 & 0.529 \\ 28.565 & 0.518 \\ 28.417 & 0.523 \\ 28.273 & 0.491 \\ 26.896 & 0.522 \\ 27.28 & 0.497 \\ 28.174 & 0.553 \\ 26.763 & 0.555 \\ 27.955 & 0.517 \\ 27.761 & 0.525 \\ 25.997 & 0.52 \end{pmatrix}$$

$$\mathrm{corr}\left(RR^{\langle 0 \rangle}, RR^{\langle 1 \rangle}\right) = -0.333$$

Приложение 5

Часть 1. Автосвертки Хэмминга, вычисленные на скользящем окне в два разряда, свертываемых кодов

$x := \mathrm{rnorm}(256, 0, 1)$

$ss1(rr) :=$ | $y \leftarrow \mathrm{rnorm}(256, 0, 1 + rr)$ | for $i \in 0..255$ | $z_i \leftarrow 0$ | $z_i \leftarrow 1$ if $y_i \geq x_i$ | z

$i := 0..20$

$rr_i := \mathrm{rnd}(0.001)$ $\quad z^{\langle i \rangle} := ss1(rr_i)$

$i := 0..255$

$w_i := 2 \cdot \left| \frac{zz_i}{21} - 0.5 \right|$ $\quad zz_i := \sum_{j=0}^{20} \left(z^{\langle j \rangle}\right)_i$

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$HH :=$ | for $i \in 1..20$

$$h_i \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 0 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle 0 \rangle}\right)_{j+1}\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]$$

for $i \in 2..20$

$$h_{i+20\cdot 1} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 1 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle 1 \rangle}\right)_{j+1}\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]$$

for $i \in 3..20$

$$h_{i+20\cdot 2} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 2 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle 2 \rangle}\right)_{j+1}\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]$$

for $i \in 4..20$

$$h_{i+20\cdot 3} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 3 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle 3 \rangle}\right)_{j+1}\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]$$

for $i \in 5..20$

$$h_{i+20\cdot 4} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 4 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle 4 \rangle}\right)_{j+1}\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]$$

for $i \in 6..20$

$$h_{i+20\cdot 5} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 5 \rangle}\right)_j\right] \oplus \left[\left(z^{\langle 5 \rangle}\right)_{j+1}\right] \oplus \left[\left(z^{\langle i \rangle}\right)_j\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]$$

h

$\mathrm{mean}(HH) = 96.05$

$\mathrm{mean}(w) = 0.524$

$RR :=$

96.149	0.532
100.992	0.493
97.702	0.512
95.785	0.541
98.959	0.53
98.149	0.529
98.826	0.518
99.24	0.523
101.107	0.491
98.529	0.522
99.537	0.497
97.306	0.553
95.174	0.555
100.893	0.517
101.438	0.525
98.215	0.52
96.694	0.539
99.736	0.52
98.893	0.511
100.033	0.504

$\mathrm{corr}\left(RR^{\langle 0 \rangle}, RR^{\langle 1 \rangle}\right) = -0.754$ $\quad \mathrm{mean}\left(RR^{\langle 1 \rangle}\right) = 0.522$

Приложение 5

Часть 2. Автосвертки Хэмминга, вычисленные на скользящем окне в два разряда, свертываемых кодов с привлечением двух сложений по модулю два и одного обычного суммирования

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 0 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 0 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \right] \\ \text{for } i \in 2..20 \\ \quad h_{i+20\cdot 1} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 1 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 1 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \right] \\ \text{for } i \in 3..20 \\ \quad h_{i+20\cdot 2} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 2 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 2 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \right] \\ \text{for } i \in 4..20 \\ \quad h_{i+20\cdot 3} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 3 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 3 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \right] \\ \text{for } i \in 5..20 \\ \quad h_{i+20\cdot 4} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 4 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 4 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \right] \\ \text{for } i \in 6..20 \\ \quad h_{i+20\cdot 5} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 5 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 5 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \right] \\ h \end{array} \right.$$

$\text{mean}(HH) = 213.008$

$\text{mean}(w) = 0.524$

$$RR := \begin{pmatrix} 222.132 & 0.538 \\ 213.802 & 0.528 \\ 217.967 & 0.536 \\ 221.24 & 0.531 \\ 205.884 & 0.521 \\ 212.909 & 0.522 \\ 218.496 & 0.482 \\ 233.554 & 0.516 \\ 224.612 & 0.486 \\ 214.76 & 0.524 \\ 221.421 & 0.478 \\ 229.372 & 0.506 \\ 217.702 & 0.536 \\ 222.76 & 0.529 \\ 230.843 & 0.51 \\ 212.43 & 0.539 \\ 223.008 & 0.509 \\ 227.174 & 0.53 \\ 229.025 & 0.518 \\ 223.388 & 0.546 \end{pmatrix}$$

$\text{corr}\left(RR^{\langle 0 \rangle}, RR^{\langle 1 \rangle}\right) = -0.219$

$\text{mean}\left(RR^{\langle 1 \rangle}\right) = 0.519$

Приложение 5

Часть 3. Автосвертки Хэмминга, вычисленные на скользящем окне в два разряда, свертываемых кодов с привлечением двух сложений по модулю два и одного обычного суммирования и взвешивания средним геометрическим показателей стабильности

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 0 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 0 \rangle} \right)_{j+1} \right] \oplus \left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 2..20 \\ \quad h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 1 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 1 \rangle} \right)_{j+1} \right] \oplus \left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 3..20 \\ \quad h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 2 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 2 \rangle} \right)_{j+1} \right] \oplus \left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 4..20 \\ \quad h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 3 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 3 \rangle} \right)_{j+1} \right] \oplus \left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 5..20 \\ \quad h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 4 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 4 \rangle} \right)_{j+1} \right] \oplus \left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 6..20 \\ \quad h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{254} \left[\left[\left(z^{\langle 5 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 5 \rangle} \right)_{j+1} \right] \oplus \left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ h \end{array} \right.$$

mean(HH) = 41.609

mean(w) = 0.524

$$RR := \begin{pmatrix} 39.827 & 0.504 \\ 40.219 & 0.527 \\ 40.988 & 0.508 \\ 42.363 & 0.532 \\ 43.623 & 0.548 \\ 43.807 & 0.545 \\ 42.743 & 0.549 \\ 41.437 & 0.51 \\ 43.176 & 0.536 \\ 39.16 & 0.484 \\ 40.482 & 0.523 \\ 40.744 & 0.508 \\ 42.458 & 0.542 \\ 40.884 & 0.536 \\ 41.328 & 0.516 \\ 38.367 & 0.48 \\ 41.783 & 0.525 \\ 44.677 & 0.531 \\ 43.5 & 0.541 \\ 43.563 & 0.538 \end{pmatrix}$$

$\text{corr}\left(RR^{\langle 0 \rangle}, RR^{\langle 1 \rangle}\right) = 0.832$ $\quad$ $\text{mean}\left(RR^{\langle 1 \rangle}\right) = 0.524$

Приложение 5

Часть 4. Автосвертки Хэмминга, вычисленные на скользящем окне в два разряда, свертываемых кодов с привлечением двух сложений по модулю два и одного обычного суммирования

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 0 \rangle}\right)_i\right] \oplus \left[\left(z^{\langle 0 \rangle}\right)_{j+1}\right]\right] + \left[\left[\left(z^{\langle i \rangle}\right)_i\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]\right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 2..20 \\ \quad h_{i+20\cdot 1} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 1 \rangle}\right)_i\right] \oplus \left[\left(z^{\langle 1 \rangle}\right)_{j+1}\right]\right] + \left[\left[\left(z^{\langle i \rangle}\right)_i\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]\right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 3..20 \\ \quad h_{i+20\cdot 2} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 2 \rangle}\right)_i\right] \oplus \left[\left(z^{\langle 2 \rangle}\right)_{j+1}\right]\right] + \left[\left[\left(z^{\langle i \rangle}\right)_i\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]\right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 4..20 \\ \quad h_{i+20\cdot 3} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 3 \rangle}\right)_i\right] \oplus \left[\left(z^{\langle 3 \rangle}\right)_{j+1}\right]\right] + \left[\left[\left(z^{\langle i \rangle}\right)_i\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]\right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 5..20 \\ \quad h_{i+20\cdot 4} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 4 \rangle}\right)_i\right] \oplus \left[\left(z^{\langle 4 \rangle}\right)_{j+1}\right]\right] + \left[\left[\left(z^{\langle i \rangle}\right)_i\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]\right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 6..20 \\ \quad h_{i+20\cdot 5} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 5 \rangle}\right)_i\right] \oplus \left[\left(z^{\langle 5 \rangle}\right)_{j+1}\right]\right] + \left[\left[\left(z^{\langle i \rangle}\right)_i\right] \oplus \left[\left(z^{\langle i \rangle}\right)_{j+1}\right]\right]\right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ h \end{array} \right.$$

$\text{mean}(HH) = 101.505$

$\text{mean}(w) = 0.524$

$$RR := \begin{pmatrix} 110.126 & 0.548 \\ 105.865 & 0.533 \\ 96.103 & 0.496 \\ 99.151 & 0.497 \\ 106.878 & 0.538 \\ 99.844 & 0.504 \\ 96.83 & 0.529 \\ 110.828 & 0.523 \\ 99.547 & 0.494 \\ 97.807 & 0.498 \\ 106.848 & 0.535 \\ 109.041 & 0.544 \\ 109.322 & 0.519 \\ 99.902 & 0.506 \\ 108.874 & 0.552 \\ 100.172 & 0.508 \\ 110.371 & 0.545 \\ 102.219 & 0.531 \\ 97.023 & 0.507 \\ 97.843 & 0.498 \end{pmatrix}$$

$\text{corr}\left(RR^{\langle 0 \rangle}, RR^{\langle 1 \rangle}\right) = 0.8$

$\text{mean}\left(RR^{\langle 1 \rangle}\right) = 0.52$

Приложение 5

Часть 5. Автосвертки Хэмминга, вычисленные на скользящем окне в два разряда, свертываемых кодов с привлечением двух сложений по модулю два и одного обычного суммирования и дополнительного взвешивания

Повторить_запуск_20_раз_и_перенести_данные_в матрицу

$$HH := \left| \begin{array}{l} \text{for } i \in 1..20 \\ \quad h_i \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 0 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 0 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot 2 \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 2..20 \\ \quad h_{i+20 \cdot 1} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 1 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 1 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot 2 \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 3..20 \\ \quad h_{i+20 \cdot 2} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 2 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 2 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot 2 \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 4..20 \\ \quad h_{i+20 \cdot 3} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 3 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 3 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot 2 \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 5..20 \\ \quad h_{i+20 \cdot 4} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 4 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 4 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot 2 \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ \text{for } i \in 6..20 \\ \quad h_{i+20 \cdot 5} \leftarrow \sum_{j=0}^{254} \left[\left[\left[\left(z^{\langle 5 \rangle} \right)_i \right] \oplus \left[\left(z^{\langle 5 \rangle} \right)_{j+1} \right] \right] + \left[\left[\left(z^{\langle i \rangle} \right)_i \right] \oplus \left[\left(z^{\langle i \rangle} \right)_{j+1} \right] \right] \cdot 2 \right] \cdot \sqrt{w_j \cdot w_{j+1}} \\ h \end{array} \right.$$

mean(HH) = 152.401

mean(w) = 0.524

$$RR1 := \begin{pmatrix} 146.055 & 0.498 \\ 145.74 & 0.489 \\ 152.74 & 0.516 \\ 150.743 & 0.526 \\ 158.372 & 0.537 \\ 165.387 & 0.538 \\ 143.651 & 0.508 \\ 155.706 & 0.52 \\ 160.708 & 0.519 \\ 149.307 & 0.498 \\ 151.962 & 0.508 \\ 150.967 & 0.522 \\ 162.029 & 0.525 \\ 152.759 & 0.52 \\ 152.21 & 0.532 \\ 147.846 & 0.523 \\ 164.788 & 0.537 \\ 157.443 & 0.507 \\ 163.97 & 0.513 \\ 164.09 & 0.515 \end{pmatrix}$$

$\text{corr}\left(RR1^{\langle 0 \rangle}, RR1^{\langle 1 \rangle}\right) = 0.56$ $\quad$ $\text{mean}\left(RR1^{\langle 1 \rangle}\right) = 0.518$

Научное издание

Иванов Александр Иванович,
Иванов Алексей Петрович,
Ратников Кирилл Андреевич

СТАТИСТИКО-НЕЙРОСЕТЕВОЙ АНАЛИЗ БИОМЕТРИЧЕСКИХ ОБРАЗОВ В ПРОСТРАНСТВАХ СПЕКТРОВ КРОССВЕРТОК И АВТОСВЕРТОК ХЭММИНГА

Редактор *Е. В. Шмелева*
Технический редактор *Ю. В. Анурова*
Компьютерная верстка *Ю. В. Ануровой*
Дизайн обложки *А. А. Стаценко*

Подписано в печать 05.04.2021.
Формат 60×84 1/16. Усл. печ. л. 3,25.
Заказ № 97. Тираж 300.

Издательство ПГУ
440026, Пенза, Красная, 40.
Тел. 66-60-49, 66-67-77; e-mail: iic@pnzgu.ru