УДК 519.95

ТЕСТИРОВАНИЕ МОДУЛЬНОГО ПОДХОДА К ОБУЧЕНИЮ НЕЙРОННЫХ СЕТЕЙ НА ПРИМЕРЕ АФФИННОГО ШИФРОВАНИЯ

© В.П. Рыков

Ключевые слова: искусственные нейронные сети; модульный принцип обучения; аффинный шифр.
Рассматривается новый подход к обучению искусственных нейронных сетей (модульный принцип) на примере аффинного шифрования.

ВВЕДЕНИЕ

Систем паролей и разграничения прав доступа явно недостаточно для эффективной организации защиты информационных ресурсов. Шифрование может обеспечить дополнительный уровень безопасности конфиденциальных данных, защитить файлы на компьютере и передаваемую по сети закрытую информацию от всех, кому не разрешен к ней доступ. Шифрование необходимо для всех особо важных данных, обрабатываемых и хранящихся на жестких дисках, переносных устройствах, содержащихся в электронных письмах, файлах, папках и других местах.

Шифром называется пара алгоритмов, реализующих соответственно шифрование и расшифрование данных. Эти алгоритмы применяются над данными с использованием специального ключа. Ключи для шифрования и для расшифрования могут отличаться, а могут и быть одинаковыми. Секретность второго (расшифровывающего) из них делает данные недоступными для несанкционированного ознакомления, а секретность первого (шифрующего) делает невозможным навязывание ложных данных [1].

Вопросом применения *искусственных нейронных сетей* (ИНС) и стохастических алгоритмов для проблем шифрования и криптоанализа занимается специальный раздел криптографии – *нейрокриптография*.

В криптоанализе используется способность нейронных сетей исследовать пространство решений. При этом используются такие свойства нейронных сетей, как низкая чувствительность к шуму, неточностям (искажения данных, весовых коэффициентов, ошибки в программе). Они позволяют решать проблемы криптографии с открытым ключом, распределения ключей, хеширования и генерации псевдослучайных чисел.

При использовании ИНС модель того или иного объекта строится на основании эмпирических данных, параметры нейронной сети необходимо выбирать из условия минимума следующей функции [2–4]:

$$E = \frac{1}{M}\sum_{i=1}^{M}(y_i - d_i)^2, \qquad (1)$$

где M – число строк в обучающей выборке; d_i – реальные выходные значения временного ряда; y_i – выходное значение, вычисленное ИНС.

Искусственные нейронные сети позволяют решать широкий круг задач, в числе которых прогнозирование временных рядов, распознавание образов и т. д. [5]. Однако использование нейронных сетей на практике предполагает ряд проблем, одной из которых является необходимость значительных временных затрат на их обучение. Одним из вариантов повышения скорости обучения является обучение сети отдельными частями – *модулями*. Такой подход представляет собой поиск решения не во всем пространстве весовых коэффициентов (например, размерности n), а лишь в некоторой его части (в пространстве $n - k$, где k – число неизменяемых весов) [6].

Целью данной работы является сравнение классического (обучение сети полностью) и модульного (обучение сети частями) подходов к обучению ИНС на примере аффинного шифрования.

ПОДГОТОВКА ДАННЫХ ДЛЯ ВЫЧИСЛИТЕЛЬНОГО ЭКСПЕРИМЕНТА

Исходные данные для проведения вычислительного эксперимента составим на основании анализа алгоритма аффинного шифра [7–8]. В аффинном шифре каждой букве алфавита (с количеством символов m) ставится в соответствие число из диапазона $[0; m-1]$.

Затем, каждому такому числу ставится в соответствие новое число, заменяющее его в шифротексте, вычисляемое при помощи функции шифрования:

$$E(x) = (ax + b) \bmod m, \qquad (2)$$

Таблица 1

Представление алфавита для вычислительного эксперимента

Буква алфавита	*a*	*b*	*c*	…	*z*
Индекс	0	1	2	…	25

где x – индекс кодируемого символа в алфавите; m – количество символов в алфавите; a и b – ключ шифрования, причем число a – взаимно простое с m, b – любое число.

Функция расшифрования в данном алгоритме имеет вид:

$$D(x) = a^{-1}(x-b) \bmod m, \quad (3)$$

где a^{-1} – число, обратное к a по модулю m, т. е. удовлетворяющее уравнению:

$$1 = aa^{-1} \bmod m. \quad (4)$$

Для построения нейронной структуры и составления обучающей выборки для сети, реализующей алгоритм аффинного шифрования и расшифрования, необходимо определить, какие параметры принимать в качестве входных данных. Наиболее верным кажется решение, когда на вход шифрующей нейронной сети подаются индекс кодируемого символа в алфавите (x), а также ключ шифрования (a и b). Соответственно для сети расшифрования на вход следует подавать значения x, b и a^{-1}. В таком случае нейронная сеть сможет осуществлять кодирование посимвольно. Нейронная сеть должна иметь 2 выхода – соответственно результатам шифрования и расшифрования.

Для вычислительного эксперимента был выбран английский алфавит длиной 26 символов, представленный в табл. 1. Согласно условию, ключ шифрования a – это число, взаимно простое к длине алфавита, в нашем случае – взаимно простое к 26, для эксперимента возьмем a, равное 3. Ключ b сгенерируем случайным образом в диапазоне [0; 10]. Значение a^{-1} в данном случае будет равняться 9.

Ввиду сложности реализации арифметической операции поиска остатка от деления при помощи нейронной сети, в дальнейшем вычислительном эксперименте будем пользоваться гибридным подходом – первую часть формул шифрования (2) и расшифрования (3) реализуем с помощью нейронной сети, а остаток от деления вычислим позднее с помощью табличного редактора. Таким образом, обучающая выборка для нашего вычислительного эксперимента представлена в табл. 2.

Таблица 2

Обучающая выборка для эксперимента

x	a	b	a^{-1}	$(ax + b)$	$a^{-1}(x - b)$
0	3	8	9	8	–72
1	3	9	9	12	–72
2	3	2	9	8	0
3	3	3	9	12	0
4	3	1	9	13	27
5	3	0	9	15	45
6	3	0	9	18	54
7	3	4	9	25	27
8	3	0	9	24	72
9	3	4	9	31	45
10	3	8	9	38	18
11	3	3	9	36	72
12	3	3	9	39	81
13	3	3	9	42	90
14	3	5	9	47	81
15	3	8	9	53	63
16	3	9	9	57	63
17	3	8	9	59	81
18	3	4	9	58	126
19	3	1	9	58	162
20	3	4	9	64	144
21	3	4	9	67	153
22	3	6	9	72	144
23	3	3	9	72	180
24	3	1	9	73	207
25	3	0	9	75	225

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ МОДУЛЬНОГО ПОДХОДА К ОБУЧЕНИЮ ИНС

Модульный подход к обучению нейронных сетей реализован в программном комплексе, предназначенном для моделирования ИНС, разработанном на языке программирования C++ в визуальной среде Qt Creator (кроссплатформенная среда разработки, предназначенная для запуска на персональном компьютере под управлением ОС GNU/Linux или MS Windows). Программный комплекс защищен свидетельством о регистрации.

Вычислительный эксперимент проводился на персональном компьютере под управлением ОС GNU/Linux.

ВЫЧИСЛИТЕЛЬНЫЙ ЭКСПЕРИМЕНТ

Для формирования ИНС оптимальной структуры в нашем вычислительном эксперименте применяется конструктивный метод, который заключается в поэтапном увеличении количества нейронов, начиная с минимальной структуры до достижения желаемого значения невязки [9]. Таким образом, сеть для эксперимента выбиралась так, чтобы обеспечить минимальное значение невязки и наименьшее количество итераций при обучении. Наилучшие результаты показала сеть, представленная на рис. 1.

Видно, что нейронная сеть представляет собой 2 блока: соответственно блок шифрования и блок расширования, по 2 нейрона в скрытом слое в каждом. Такая сеть позволяет получить хорошие результаты при наименьшем количестве итераций для полного обучения.

Модульный подход к обучению нейронных сетей может дать существенный эффект в скорости обучения именно для «составных» сетей, включающих в себя несколько объектов (в нашем случае объектами являются шифратор и дешифратор). Идея заключается в том, чтобы обучать поочередно каждый из блоков нейронной сети до достижения желаемого значения невязки. Все нейроны в сети, представленной на рис. 1, имеют линейную активационную функцию.

Целью вычислительного эксперимента является сравнение модульного и классического подхода к обучению нейронных сетей. Следовательно, вычислительный эксперимент должен состоять из нескольких этапов: на первом этапе проведем обучение нейронной

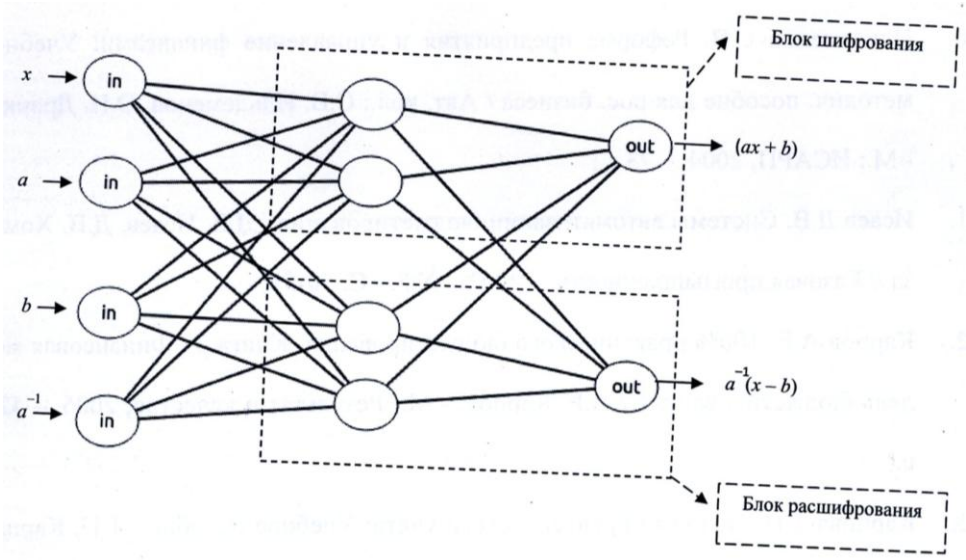

Рис. 1. ИНС, соответствующая наименьшему значению невязки

сети, представленной на рис. 1, полностью (классический подход) и подсчитаем количество итераций; на втором этапе будем проводить отдельно обучение каждого из блоков сети до тех пор, пока не добьемся желаемого значения невязки (модульный подход), а также подсчитаем количество итераций, необходимое для обучения сети частями. После проведения подсчетов сравним количество итераций в обоих случаях. Для обучения сети будем использовать метод Монте–Карло с шагом 0,01. Значение желаемой погрешности также составляет 0,01.

При обучении нейронной сети, представленной на рис. 1, классическим методом (обучение полностью) было затрачено 8026 итераций:

$$N_{full} = 8026. \quad (5)$$

Далее необходимо найти остаток от деления значений выходов сети (Out_{Crypt} – выход блока шифрования; $Out_{Decrypt}$ – выход блока расшифрования) на 26 (длина алфавита). Сравнение результатов представлено в табл. 3.

При этом следует отметить, что обучение нейронной сети частями происходило в несколько последовательных этапов: обучение первой части сети до тех пор, пока процесс минимизации значения невязки не замедлится, что говорит о том, что обучающий модуль сети близок к предельному значению невязки; далее обучение сети останавливалось, происходила фиксация нейронов и связей данного модуля. Затем аналогично производилось обучение второго модуля сети. Данные действия были произведены несколько раз над каждым из модулей ИНС до тех пор, пока невязка не достигла среднего значения, меньшего 0,01. Идея заключается в постепенном подборе весовых коэффициентов для каждого из блоков сети на каждом шаге обучения.

В случае обучения нейронной сети частями (поочередно каждого из блоков) количество итераций составило 7331:

$$N_{part} = 7331. \quad (6)$$

Результаты обучения нейронной сети частями представлены в табл. 4 (Out_{Crypt} – выход блока шифрования; $Out_{Decrypt}$ – выход блока расшифрования).

Таблица 3

Результат эксперимента в случае обучения сети полностью

Out_{Crypt} mod 26	Реальное значение	$Out_{Decrypt}$ mod 26	Реальное значение
8,03556477	8	6,01028422	6
11,958722	12	6,0136642	6
8,35834067	8	0,007213	0
12,2814979	12	0,00383301	0
13,3833281	13	0,99045053	1
15,4256007	15	18,9877662	19
18,4083156	18	1,98811405	2
25,1527997	25	1,00059047	1
24,3737454	24	19,9888097	20
5,11822952	5	19,0012861	19
11,8627137	12	18,0137626	18
10,143217	10	19,9989497	20
13,1259319	13	2,99929749	3
16,1086468	16	11,9996453	12
20,9722463	21	3,00605746	3
0,7762881	1	11,0155017	11
4,6994453	5	11,0188817	11
6,74171788	7	3,0161974	3
5,96266352	6	22,0044166	22
6,12405147	6	5,995668	6
11,9280933	12	14,0051123	14
14,9108082	15	23,0054601	23
19,7744077	20	14,0118723	14
19,9357957	20	24,0031237	24
21,0376259	21	24,9974072	25
23,0798985	23	16,9947229	17

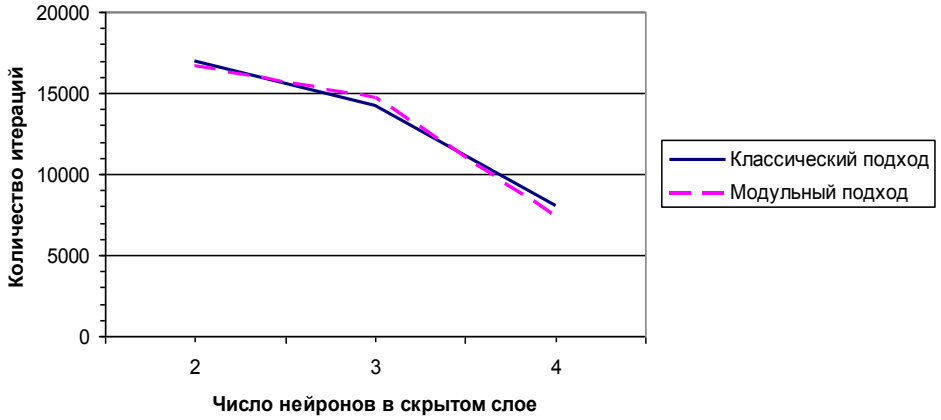

Рис. 2. Зависимость количества итераций от числа нейронов в слое

Таблица 4

Результат эксперимента в случае обучения сети частями

Out_{Crypt} mod 26	Реальное значение	$Out_{Decrypt}$ mod 26	Реальное значение
7,95205643	8	6,09764737	6
11,8713659	12	6,1122885	6
8,33435604	8	0,00277503	0
12,2536655	12	0,0118661	0
13,3768553	13	0,97786798	1
15,4320849	15	18,960083	19
18,4193545	18	1,958511	2
25,1347838	25	1,02179137	1
24,3938937	24	19,9553671	20
5,10932292	5	19,0186475	19
11,8247522	12	18,0819278	18
10,1518222	10	19,9992905	20
13,1390917	13	2,99771853	3
16,1263613	16	11,9961466	12
20,9777107	21	3,02700079	3
0,76110006	1	11,0740681	11
4,68040956	5	11,0887092	11
6,73563921	7	3,07092418	3
5,9947491	6	22,0044999	22
6,18589891	6	5,9542887	6
11,9692883	12	14,001356	14
14,9565578	15	22,999784	23
19,8079073	20	14,0306382	14
19,9990571	20	23,9804271	24
21,1222468	21	24,9464289	25
23,1774764	23	16,9286439	17

Очевидно, что в обоих случаях были получены результаты, близкие к реальным, при этом в случае использования модульного подхода было затрачено меньшее количество итераций на обучение сети, что говорит о его преимуществе над классическим подходом.

Рис. 2 иллюстрирует зависимость количества итераций от числа нейронов в скрытом слое для данного вычислительного эксперимента.

По рис. 2 видно, что в случае если число нейронов в скрытом слое равно 3, то обучение сети частями дает обратный эффект – на обучение затрачивается большее количество итераций. Это объясняется тем, что в данном случае при делении сети на две части, в одной из них остается лишь один скрытый нейрон, а этого недостаточно для эффективного обучения модуля. В том случае если число нейронов в скрытом слое сети больше 4, то сеть является избыточной для данной задачи.

При обучении нейронной сети отдельными модулями, нам хотелось бы узнать, насколько такой подход эффективнее полного обучения. В нашем эксперименте мы нашли количество итераций, необходимое для обучения сети полностью, и количество итерации при обучении частями. Вычислить эффективность модульного подхода можно, найдя отношение количества итераций при полном обучении (5) к количеству итерации при обучении частями (6):

$$J = \frac{N_{full}}{N_{part}} = \frac{8026}{7331} \approx 1{,}094\,. \qquad (7)$$

Согласно формуле (9), в данной задаче модульный принцип обучения оказался приблизительно на 9,4 % эффективнее классического метода.

В общем случае:

– если $J = 1$, то обучение сети частями не дало эффекта над классическим подходом (равное число итераций в обоих случаях);

– если $J > 1$, то обучение сети частями получилось эффективнее;

– если $J < 1$, то обучение сети частями не дало эффекта.

ВЫВОД

В результате сравнения модульного и классического подходов к обучению ИНС на примере аффинного шифрования можно сделать вывод о целесообразности использования модульного подхода, т. к. в ряде случаев это может дать существенный эффект в увеличении скорости обучения нейронных сетей.

ЛИТЕРАТУРА

1. Шифрование и шифры. URL: http://www.familytree.ru/es/cipbooks /book005/part3.htm. Загл. с экрана.
2. Лекция № 4. Традиционные шифры с симметричным ключом. URL: http://www.intuit.ru/department/security/mathcryptet/4/3.html. Загл. с экрана.
3. *Арзамасцев А.А., Зенкова Н.А.* Искусственный интеллект и распознавание образов: учеб. пособие. Тамбов: ИМФИ ТГУ им. Г.Р. Державина, 2010.
4. *Арзамасцев А.А., Крючин О.В., Козадаев А.С., Слетков Д.В.* Тестирование параллельных алгоритмов обучения искусственных нейронных сетей на примере данных изменения температуры воздуха в городе Тамбове // Вестник Тамбовского университета. Серия Естественные и технические науки. Тамбов, 2011. Т. 16. Вып. 2. С. 461-467.
5. *Осовский С.* Нейронные сети для обработки информации / пер. с польск. И.Д. Рудинского. М.: Финансы и статистика, 2002. 344 с.
6. *Арзамасцев А.А., Рыков В.П.* Модель искусственной нейронной сети (ИНС) с реализацией модульного принципа обучения // Вестник Тамбовского университета. Серия Естественные и технические науки. Тамбов, 2012. Т. 17. Вып. 4. С. 1219-1224.
7. Нейронные сети: обучение с учителем. URL: http://www.scorcher.ru /neuro/science/perceptron/mem32.htm. Загл. с экрана.
8. Аффинная система подстановок Цезаря и шифр Цезаря. URL: http://crypto.hut2.ru/cesar.html. Загл. с экрана.
9. Лекции. Интеллектуальные информационные системы. URL: http://gendocs.ru/v98/лекции_-_интеллектуальные_информационные_системы?page=3. Загл. с экрана.

Поступила в редакцию 23 ноября 2012 г.

Rykov V.P. TESTING OF MODULAR APPROACH TO NEURAL NETWORKS TRAINING ON EXAMPLE OF AFFINE ENCRYPTION

A new approach to learning artificial neural networks (modular) on example of an affine encryption is considered.

Key words: artificial neural network; modular training; affine cipher.