It should be noted that the Algorithm class implements the function of cryptographic encryption based on RSA. The RSA functions were written using security and crypto libraries. The first one is responsible for creating a pair of keys based on the size of 2048 bits. These keys are, of course, public and private.

The programming environments that were used in the creation of the application were Intellij IDEA and NetBeans. Intellij IDEA was used to create our database.

Currently developed application is being tested.

REFERENCES

1 Urbanowicz, P. Bazy danych: teoria i praktyka / Paweł Urbanowicz, Marcin Płonkowski, Dmitry Urbanowicz. – Lublin: KUL, 2010. – 382 s.

2 Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin: KUL, 2004. – 150 s.

3 Urbanovich, P. P. Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii/ P.P. Urbanovich: ucheb.-metod. posobiye dlya stud. – Minsk: BGTU, 2016. –220 s.

УДК 004.85

В. К. Сенюк, магистрант;
В. Л. Колесников, проф., д-р техн. наук (БГТУ, г. Минск)

БЕГРАДИЕНТНЫЙ МЕТОД ОБУЧЕНИЯ ПОЛНОСВЯЗНОЙ НЕЙРОННОЙ СЕТИ ПРЯМОГО РАСПРОСТРАНЕНИЯ

Градиентные методы обучения нейронных сетей при обратном распространении ошибки требуют больших затрат времени при сложных вычислениях частных производных, градиентов, изменений весов, моментов и скорости обучения. В виду большого объема вычислений при использовании градиентных методов хорошая сходимость алгоритмов достигается за большое количество эпох [1].

При решении тестовой задачи классификации нейронной сетью (при обучении градиентным методом) на вход подавалась относительно малая выборка данных, для активации нейронов использовалась сигмоидальная функция, методом «проб и ошибок» выбирались значения момента и скорости обучения. При этом, «приемлемые результаты», – сходимость и энергия ошибки достигались при обучении, примерно, за 10 – 15 тысяч эпох.

Представлялось целесообразным проанализировать «неградиентные» методы обучения нейронных сетей с целью выявления их достоинств и недостатков по сравнению с другими методами обучения.

Для решения задачи была разработана нейронная сеть с самоорганизацией, а для ее обучения использовался алгоритм «WTA» (победитель получает всё), который является аналогом алгоритма Ллойда для решения задачи кодирования. Целью обучения сети с самоорганизацией на основе конкуренции нейронов считается такое упорядочение нейронов (подбор значений их весов), которое минимизирует значение ожидаемого искажения, оцениваемого погрешностью аппроксимации входного вектора значениями весов нейрона-победителя. При P входных векторах X и применении евклидовой метрики эта погрешность, называемая также погрешностью квантования, может быть выражена в виде

$$E = \frac{1}{P}\sum_{i=1}^{P}\|x^i - w_w \qquad (1)$$

где w_{win} – вес нейрона-победителя при предъявлении вектора x^i.

В соответствии с алгоритмом после предъявления вектора x рассчитывается активность каждого нейрона. Победителем признается нейрон с самым сильным выходным сигналом, т.е. тот, для которого скалярное произведение весов синапсов на входные значения является наибольшим. Это произведение соответствует наименьшему евклидовому расстоянию между входным вектором и весовым вектором нейрона. Победитель получает право уточнить свои веса в направлении вектора x согласно правилу Кохонена [2]

$$w_{win} \leftarrow w_{win} + \alpha\,[x - w_{win}], \qquad (2)$$

где α – коэффициент скорости обучения.

Одно из достоинств алгоритма заключается в том, что коэффициент скорости обучения не подбирается «случайным образом», а в начале обучения инициализируется значением приблизительно равным единице и уменьшается в процессе обучения до значения близкого к нулю.

В полном виде анализируемый алгоритм можно представить следующим образом:

1. Нормализация данных обучающей выборки. На вход нейронной сети подаются нормализованные переменные.

2. Весовые коэффициенты нейронной сети инициализируются случайными значениями. Обычно эти значения находятся в диапазоне [-0.5; 0.5].

3. На входы сети подается нормализованный входной вектор одного из примеров обучающей выборки. Производится прямое распространение сигналов по нейронной сети.

4. Среди всех нейронов скрытых слоев осуществляется поиск нейрона с самым большим выходным значением *Nwin* (нейрон-победитель).

5. В соответствии с пунктом 2 осуществляется обновление весового вектора нейрона-победителя.

6. Цикл повторяется с шага 3 до исчерпания количества эпох обучения.

Анализ алгоритма обучения производился на примере той же тестовой задачи классификации и обучающей выборки (таблица 1). При обучении в тысячу эпох сеть уже выдавала правильный результат, что доказывает быструю сходимость алгоритма.

Таблица 1 – Сравнение методов обучения НС

Параметры	Обучение с вычислением градиента	Обучение без вычисления градиента
Скорость обучения (V)	Подбирается вручную до достижения оптимального результата	Устанавливается примерно равным единице и уменьшается в процессе обучения до значения близкого к нулю $\alpha -= \frac{\alpha}{N}$, где N – количество эпох обучения
Градиент (G)	Вычисляется в процессе обучения НС	Не используется
Количество эпох обучения (E)	Зависит от порога ошибки. В тестовой задаче E равно 10-15 тысячам эпох	E равно одной тысяче эпох
Конечное значение ошибки	Равно пороговому значению	На тестовой задаче равно примерно 0.0002

Таким образом, обучение на основе неградиентного метода позволяет отказаться от подбора гиперпараметров сети, градиента и других величин, вычисление которых является достаточно ресурсоемким без потери качества классификации и скорости обучения. На рис.1 показаны значения ошибки сети по эпохам обучения. Можно видеть, что уже на сотой эпохе сеть выдавала достаточно малую ошибку, что говорит о том, что после ста эпох обучение сети можно было бы остановить и, при этом, классификация осуществлялась бы правильно.

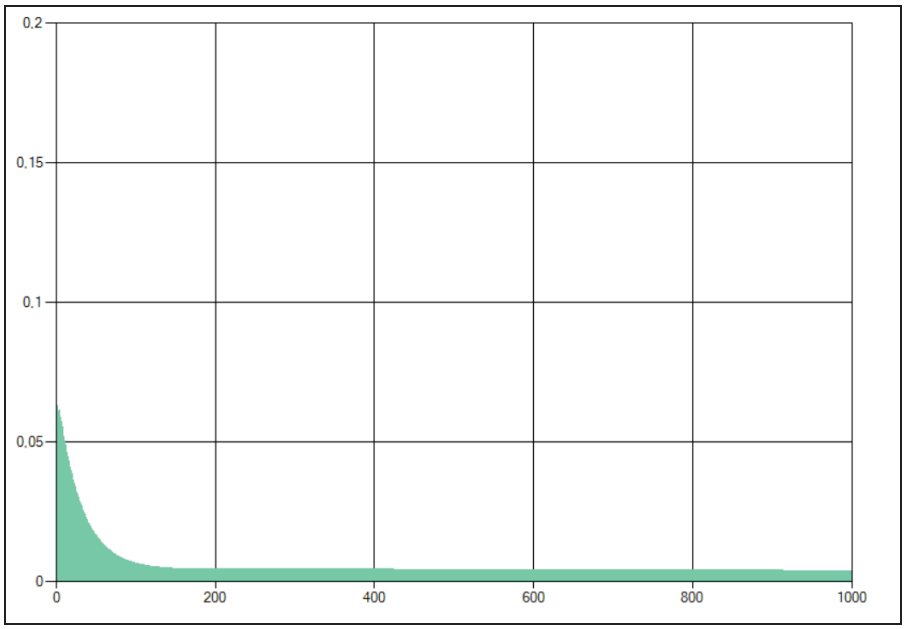

Рисунок 1 – Сходимость алгоритма

Также следует отметить простоту программной реализации описанного неградиентного метода обучения, по сравнению с методом градиентного спуска с обратным распространением ошибки. Неградиентные методы требуют меньше вычислительных ресурсов, что обусловлено применением простейших структур данных и тривиальных математических операций. Среднее количество тактов времени, затраченное на обучение нейронной сети равно трем млн.

ЛИТЕРАТУРА

1 Rojas R. Neural Networks. A Systematic Introduction / R.Rojas. – Springer, 1996. – 220 с.

2 Хайкин С. Нейронные сети / Саймон Хайкин. – Вильямс, 2006. – 1104 с.

УДК 003.26+004.056

В. О. Берников, асп.;
П. П. Урбанович, проф., д-р техн. наук (БГТУ, г. Минск)

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ СТЕГАНОГРАФИЧЕСКОЙ СТОЙКОСТИ МНОГОКЛЮЧЕВОЙ СИСТЕМЫ

Под стеганографической стойкостью информационных систем понимается уровень их защищенности перед попытками несанкционированного извлечения, разрушения, искажения или удаления осажден-