Вопросы оценки стойкости нейросетевой системы биометрической аутентификации

Григорий Маршалко

Биометрическая аутентификация

- Классический подход – требуется защита шаблона

Биометрическая аутентификация

- Классический подход – требуется защита шаблона
- 'Защищенный' подход – нечеткие экстракторы и т.д.
  - защищенные эскизы (secure sketches): пара преобразований $SS(w) = s$ и $Rec(w', s) = w,\ w \approx w'$, где w – вектор биометрических параметров, s – открытый вспомогательный параметр.

Биометрическая аутентификация

- Классический подход – требуется защита шаблона
- 'Защищенный' подход – нечеткие экстракторы и т.д.
  - защищенные эскизы (secure sketches): пара преобразований $SS(w) = s$ и $Rec(w', s) = w,\ w \approx w'$, где w – вектор биометрических параметров, s – открытый вспомогательный параметр.
  - нечеткие экстракторы (fuzzy extractors): пара преобразований $Gen(w) = (R, P)$ и $Rep(w', P) = R,\ w \approx w'$, где w – вектор биометрических параметров, R – секретный ключ, P – открытый вспомогательный параметр.

Свойства биометрических данных

1. Неоднородность и зависимость биометрических параметров – тяжело получить равновероятный ключ (Ушмаев, 2011)
2. Очевидная возможность компрометации

Свойства биометрических данных

1. Неоднородность и зависимость биометрических параметров – тяжело получить равновероятный ключ (Ушмаев, 2011)
2. Очевидная возможность компрометации

Пути решения (ПНИЭИ, ПГУ)

1. Использование нейронных сетей
2. Использование 'тайного' биометрического образа (рукописного пароля, произносимой фразы)

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.2 Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.2 Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.3 Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.2 Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.3 Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора
- ГОСТ Р 52633.4 Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.2 Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.3 Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора
- ГОСТ Р 52633.4 Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа
- ГОСТ Р 52633.5 Автоматическое обучение нейросетевых преобразователей биометрия-код доступа

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.2 Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.3 Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора
- ГОСТ Р 52633.4 Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа
- ГОСТ Р 52633.5 Автоматическое обучение нейросетевых преобразователей биометрия-код доступа
- ГОСТ Р 52633.6 Требования к индикации близости предъявленных биометрических данных образу «Свой»

Стандарт ГОСТ Р 52633. Высоконадежная биометрическая аутентификация

- ГОСТ Р 52633.0 Требования к высоконадежной биометрической аутентификации
- ГОСТ Р 52633.1 Требования к формированию баз естественных биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.2 Требования к формированию синтетических биометрических образов, предназначенных для тестирования средств высоконадежной биометрической аутентификации
- ГОСТ Р 52633.3 Тестирование стойкости средств высоконадежной биометрической защиты к атакам подбора
- ГОСТ Р 52633.4 Интерфейсы взаимодействия с нейросетевыми преобразователями биометрия-код доступа
- ГОСТ Р 52633.5 Автоматическое обучение нейросетевых преобразователей биометрия-код доступа
- ГОСТ Р 52633.6 Требования к индикации близости предъявленных биометрических данных образу «Свой»

Общая схема нейросетевой системы биометрической аутентификации

Типы используемых нейронных сетей. ГОСТ Р 52633.5

- ориентированные на работу с непрерывными биометрическими параметрами, имеющими, как правило, низкое среднее качество (однослойные, двухслойные)
- ориентированные на работу с дискретными биометрическими параметрами, имеющими, как правило, хорошее среднее качество

Типы используемых нейронных сетей. ГОСТ Р 52633.5

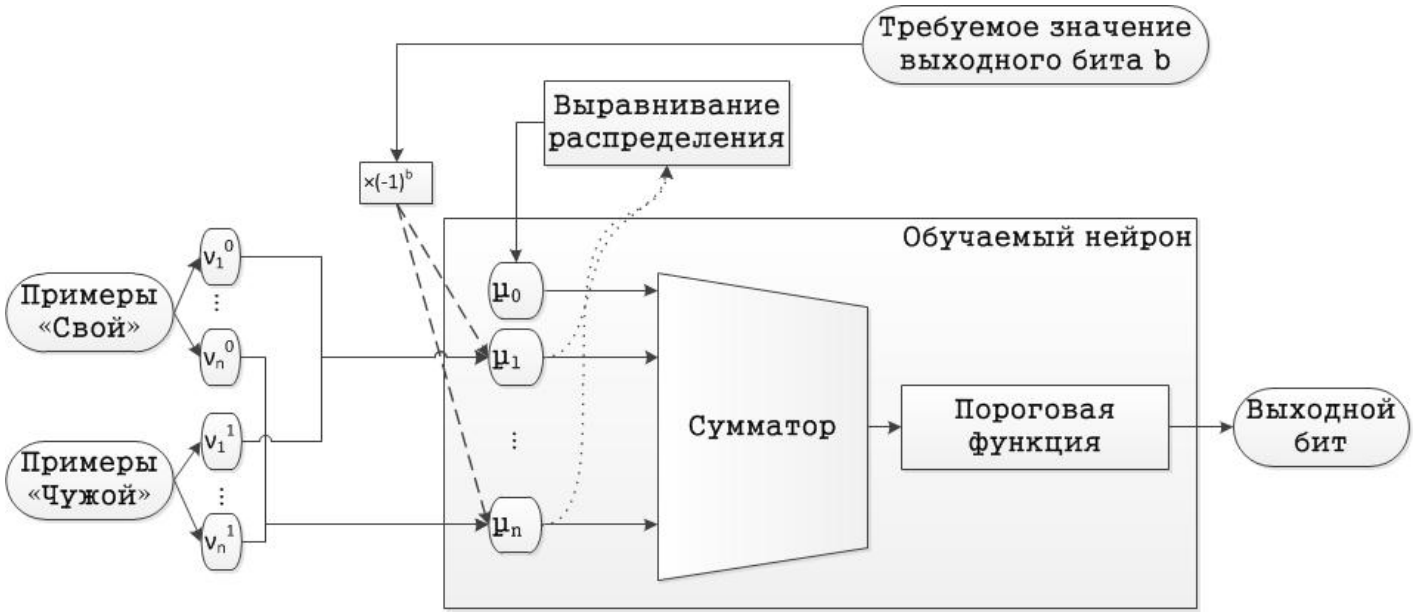
- ориентированные на работу с непрерывными биометрическими параметрами, имеющими, как правило, низкое среднее качество (однослойные, двухслойные)
- ориентированные на работу с дискретными биометрическими параметрами, имеющими, как правило, хорошее среднее качество

Далее будем рассматривать однослойные нейронные сети, ориентированные на работу с непрерывными биометрическими параметрами

Обозначения

- N_0 – число контролируемых параметров (число входов нейронной сети), которое зависит от используемой биометрической технологии ($N_0 = 416$);
- N_1 – число нейронов в сети, соответствующее длине секретного ключа, поступающего на вход протокола аутентификации;
- n – число входов каждого из нейронов, определяемое на основе анализа качества биометрических данных ($n = 16$);
- $\vec{\nu} = (\nu_1, \ldots, \nu_{N_0})$ – вектор входных биометрических данных;
- $\mathcal{M} = \left(\mu_i^j, i = \overline{0, n}, j = \overline{1, N_1}\right)$ – весовые коэффициенты на входе j-го нейрона, при этом, входы с номерами $1, \ldots, n$ соединены со входами сети, а нулевой вход используется для выравнивая выходного распределения на выходе нейрона;
- $\mathcal{D} = \left(d_i^j, i = \overline{1, n}, j = \overline{1, N_1}\right)$ – таблица соответствий (связей) входов нейронов сети и координат входного вектора биометрических данных;
- $\vec{b} = (b_1, ..., b_{N_1})$ – криптографический ключ;
- a_i – некоторые вспомогательные весовые коэффициенты.

Задание весовых коэффициентов нейронов осуществляется посредством оценки выборочных средних $\overline{\nu_t^c}$ и дисперсий $S^2(\nu_t^c)$ t-го биометрического параметра $t = 1, \ldots, \nu_{N_0}$ для образов «Свой» $(c = 0)$ и «Чужой» $(c = 1)$ с последующей фиксацией выходного значения для образа «Свой».



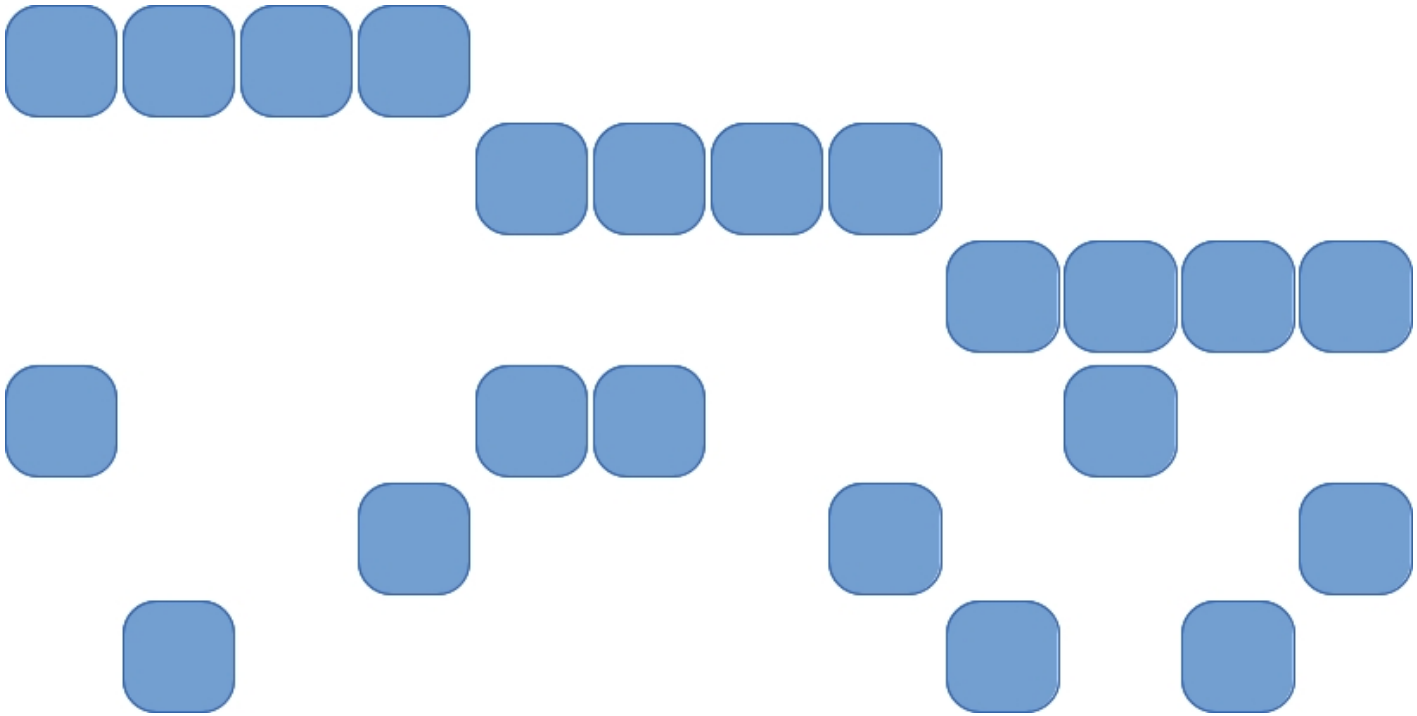
Алгоритм обучения

1. обнулить таблицы $\mathcal{M}$ и $\mathcal{D}$
2. Для $j = 1, \ldots, \left[\frac{N_0}{n}\right]$ выполнить шаг 3
3. Для $i = 1, \ldots, n$ выполнить шаг 4
4. $\mu_i^j = \frac{(-1)^{b_j}\left(\overline{\nu_{jn+i}^1} - \overline{\nu_{jn+i}^0}\right)}{a_2\sqrt{S^2(\nu_{jn+i}^1)} + \sqrt{S^2(\nu_{jn+i}^0)}}$, $d_i^j = jn + i$
5. Для $j = \left[\frac{N_0}{n}\right] + 1, \ldots, N_1$ выполнить шаг 6
6. Для $i = 1, \ldots, n$ выполнить шаги 7 и 8
7. $\tau = prnd\left(\mathcal{D}\right)$
8. $\mu_i^j = \frac{(-1)^{b_j}\left(\overline{\nu_\tau^1} - \overline{\nu_\tau^0}\right)}{a_2\sqrt{S^2(\nu_\tau^1)} + \sqrt{S^2(\nu_\tau^0)}}$
9. Для $j = 1, \ldots, N_1$ выполнить шаг 10
10. $\mu_0^j = norm\left(\mu_1^j, \ldots, \mu_n^j\right)$

Изложенный алгоритм использует вызов двух функций:

- $prnd\left(\vec{d}\right)$, которая осуществляет псевдослучайный выбор координат вектора биометрических параметров таким образом, чтобы выполнялись два условия:
  - минимальная частота использования входа нейронной сети отличается от максимальной не более чем на 2,
  - отсутствуют общие связи к 2,3,4 рядом расположенным нейронам;
- $norm\left(\mu_1^j, \ldots, \mu_n^j\right)$, которая вычисляет значение порогового элемента нейрона.

Результат обучения



Угрозы безопасности нейросетевых систем биометрической аутентификации. ГОСТ Р 52633.0

1. подбора нарушителем вектора входных биометрических данных $\vec{\nu}$;
2. извлечение нарушителем конфиденциальной информации из структуры и параметров нейронной сети (таблицы M и $\vec{d}$);
3. подбора нарушителем криптографического ключа $\vec{b}$;

Угрозы безопасности нейросетевых систем биометрической аутентификации. ГОСТ Р 52633.0

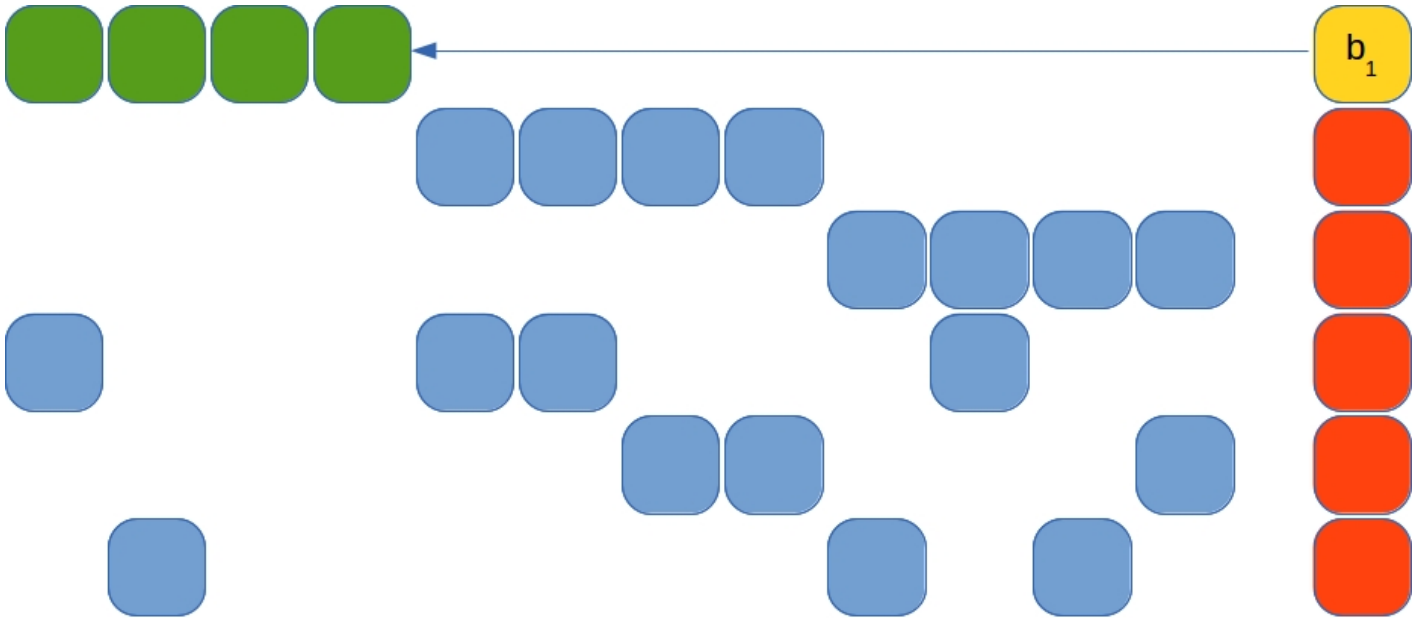
1. подбора нарушителем вектора входных биометрических данных $\vec{\nu}$;
2. извлечение нарушителем конфиденциальной информации из структуры и параметров нейронной сети (таблицы M и $\vec{d}$);
3. подбора нарушителем криптографического ключа $\vec{b}$;

Способы противодействия

- контроль целостности ПО
- аудит процессов
- увеличение размеров нейронной сети (1)
- ограничения доступа к таблицам значений M и $\vec{d}$ (2)
- увеличения размерности таблиц (2)
- создания уникальной конфигурации связей нейронной сети для каждого пользователя (2)

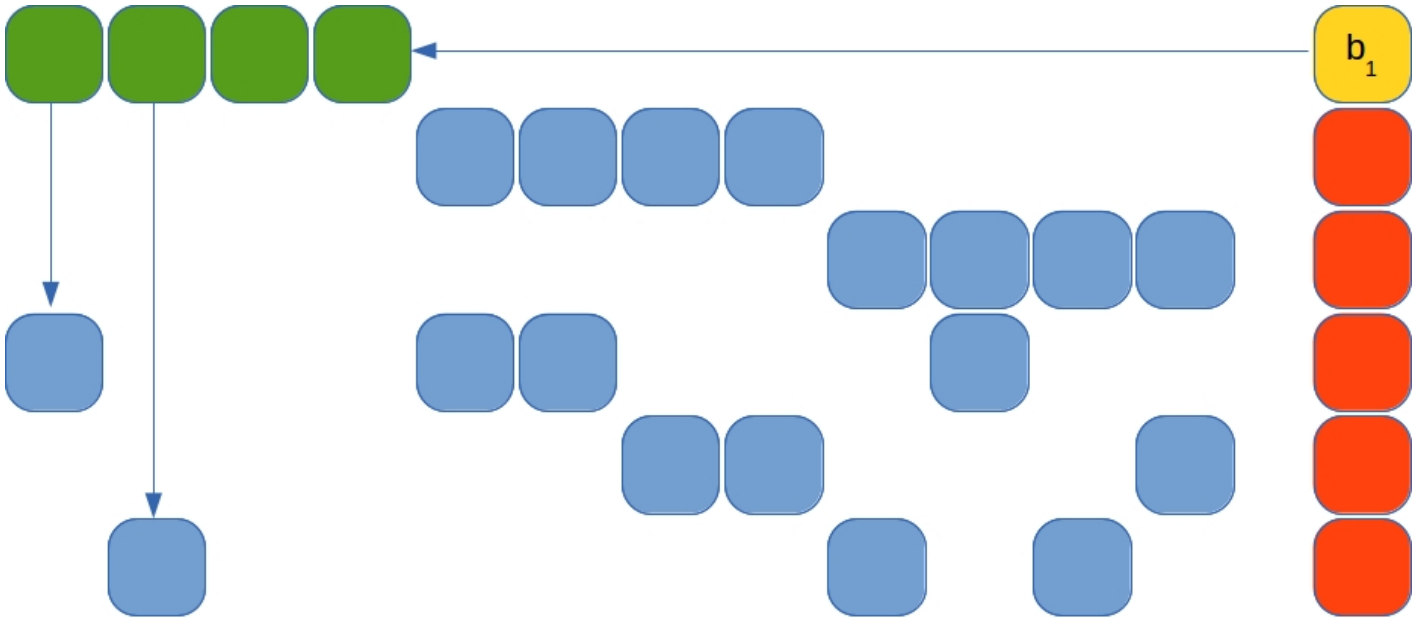
Компрометация таблиц нейронной сети

Значения коэффициентов нейронов зависят только от соответствующего биометрического параметра и бита ключа: мы можем последовательно определять биты секретного ключа!



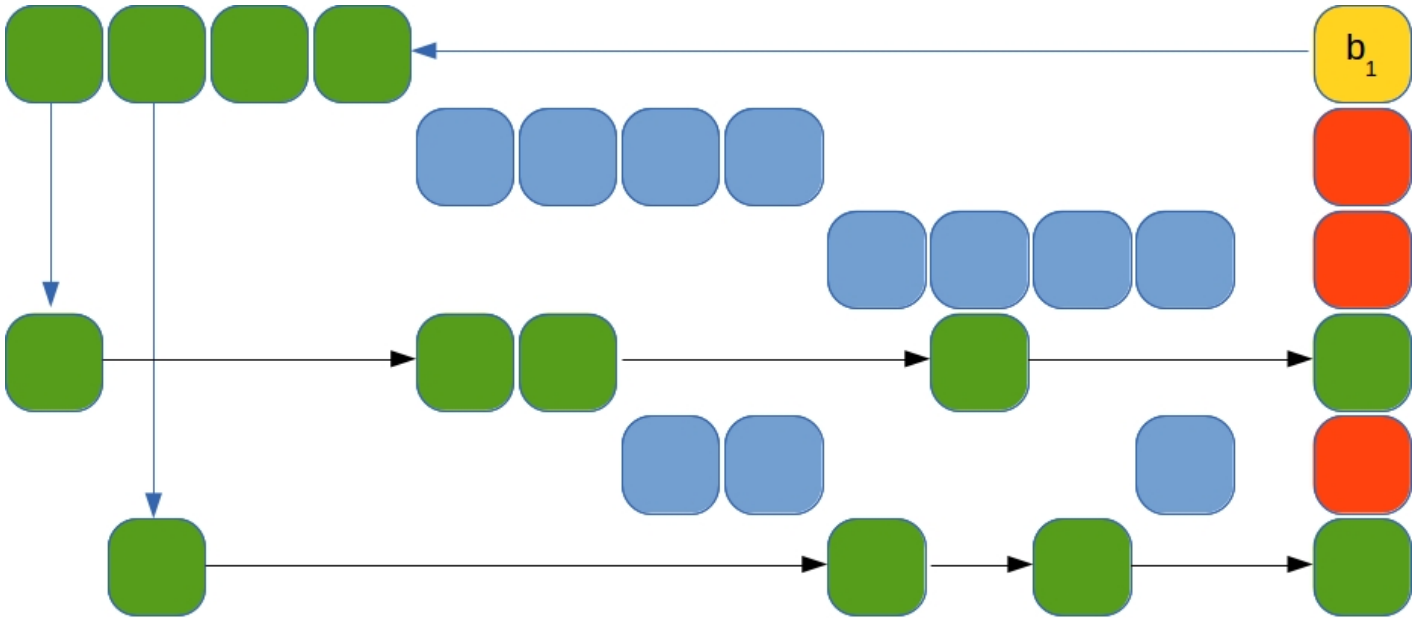
Компрометация таблиц нейронной сети

Значения коэффициентов нейронов зависят только от соответствующего биометрического параметра и бита ключа: мы можем последовательно определять биты секретного ключа!



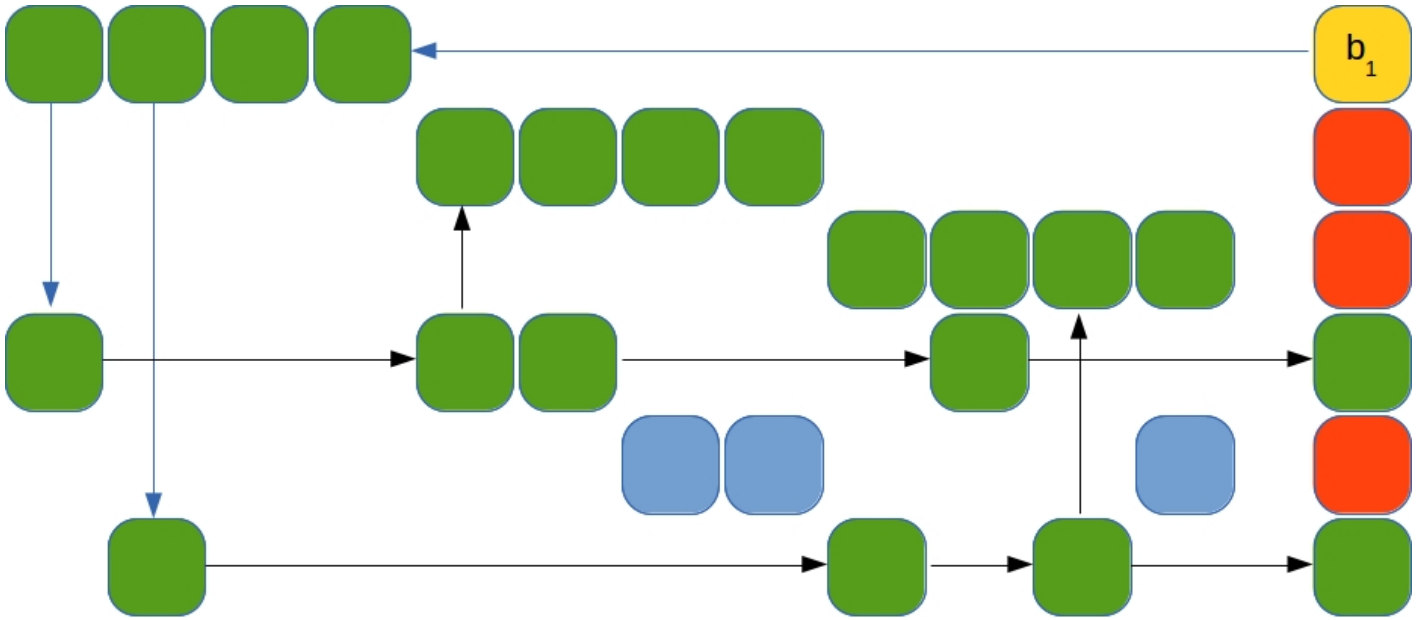
Компрометация таблиц нейронной сети

Значения коэффициентов нейронов зависят только от соответствующего биометрического параметра и бита ключа: мы можем последовательно определять биты секретного ключа!



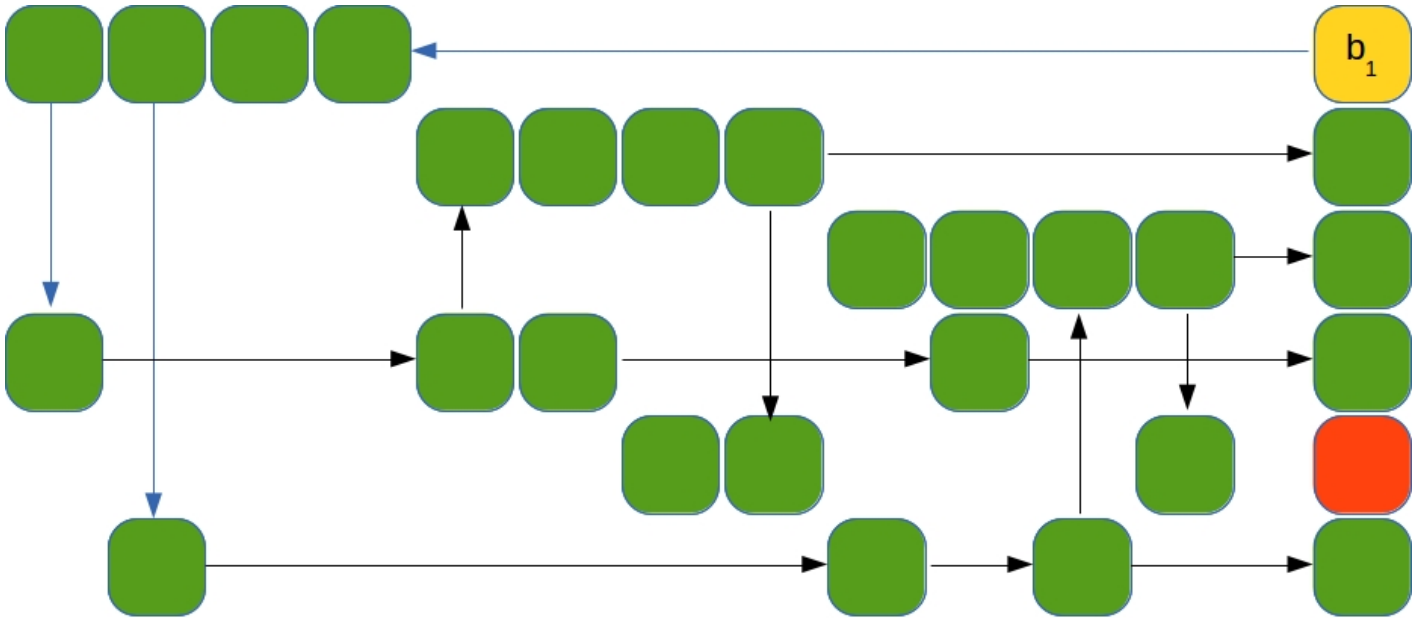
Компрометация таблиц нейронной сети

Значения коэффициентов нейронов зависят только от соответствующего биометрического параметра и бита ключа: мы можем последовательно определять биты секретного ключа!



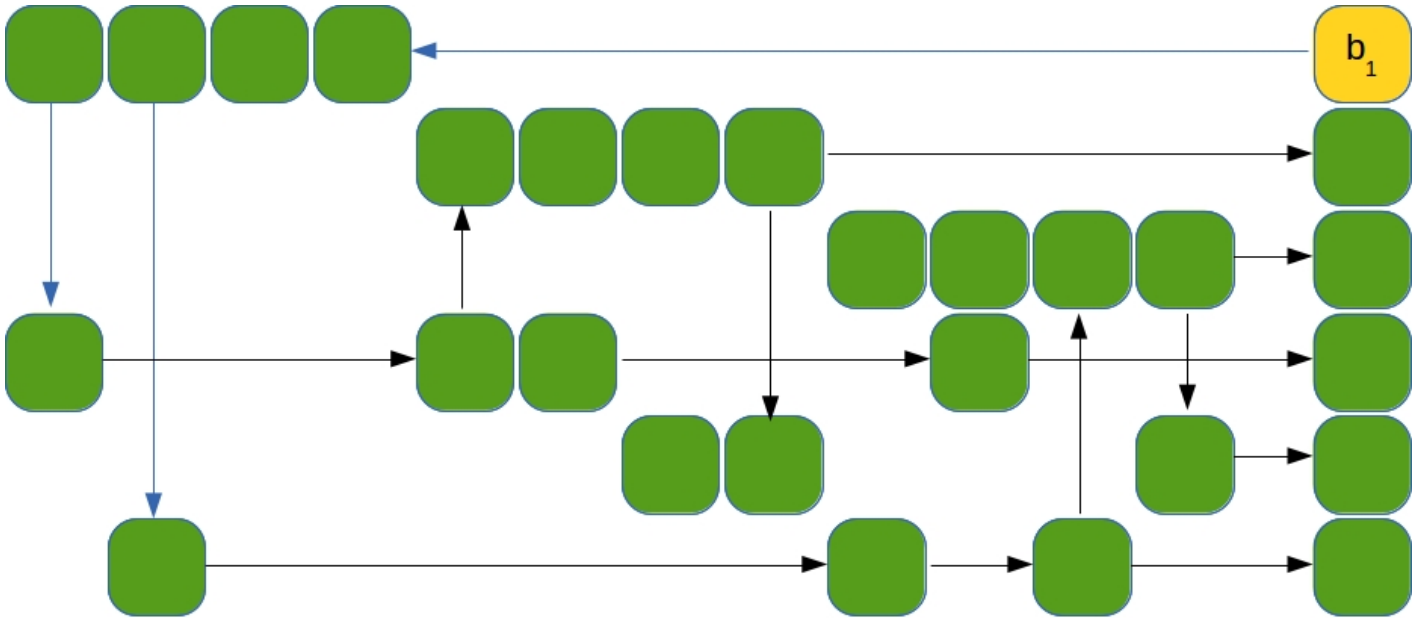
Компрометация таблиц нейронной сети

Значения коэффициентов нейронов зависят только от соответствующего биометрического параметра и бита ключа: мы можем последовательно определять биты секретного ключа!



Компрометация таблиц нейронной сети

Значения коэффициентов нейронов зависят только от соответствующего биометрического параметра и бита ключа: мы можем последовательно определять биты секретного ключа!



При компрометации таблиц секретный ключ доступен в двух вариантах (истинный и его отрицание)!

Определение биометрического образа при компрометации таблиц нейронной сети

- Нейронная сеть описывается системой линейных неравенств

Определение биометрического образа при компрометации таблиц нейронной сети

- Нейронная сеть описывается системой линейных неравенств
- Майоров 2009: трудоемкость решения СЛН алгоритмом Черниковой $O\left(N_0^{\frac{N_1}{2}+1}\right)$

Определение биометрического образа при компрометации таблиц нейронной сети

- Нейронная сеть описывается системой линейных неравенств
- Майоров 2009: трудоемкость решения СЛН алгоритмом Черниковой $O\left(N_0^{\frac{N_1}{2}+1}\right)$
- Приведенная оценка получена для алгоритма описания всего множества решений СЛН для «экстремального» случая конусов решений, задаваемых системой линейных неравенств, имеющих максимальное число векторов в остове (Золотых 1998)

Определение биометрического образа при компрометации таблиц нейронной сети

- Нейронная сеть описывается системой линейных неравенств
- Майоров 2009: трудоемкость решения СЛН алгоритмом Черниковой $O\left(N_0^{\frac{N_1}{2}+1}\right)$
- Приведенная оценка получена для алгоритма описания всего множества решений СЛН для «экстремального» случая конусов решений, задаваемых системой линейных неравенств, имеющих максимальное число векторов в остове (Золотых 1998)
- Нам достаточно найти хотя бы одно решение

Решение СЛУ

- Даже экспоненциальные алгоритмы линейного программирования эффективно применяются на практике

Решение СЛУ

- Даже экспоненциальные алгоритмы линейного программирования эффективно применяются на практике
- Алгоритмы внутренних точек, центрального пути – эффективно применяются для задач со сходными размерами(Зоркальцев 2003)

Решение СЛУ

- Даже экспоненциальные алгоритмы линейного программирования эффективно применяются на практике
- Алгоритмы внутренних точек, центрального пути – эффективно применяются для задач со сходными размерами(Зоркальцев 2003)
- Решение случайно выработанных систем линейных неравенств (128 уравнений от 416 неизвестных) не вызывают никаких трудностей с использованием стандартных математических пакетов на персональной ЭВМ (использовался математический пакет Mathematica 7 на нетбуке Asus EeePC 1003 с процессором Atom N208 и 1 Гб ОЗУ)

При компрометации нейронной сети допустимый биометрический образ эффективно восстанавливается!

Атака при неизвестных таблицах – 'черный' ящик

Основное свойство - коэффициенты различных нейронов определяются независимо.

- Выбираются N_0 биометрических векторов, на которых значение нейрона равно единице

Атака при неизвестных таблицах – 'черный' ящик

Основное свойство - коэффициенты различных нейронов определяются независимо.

- Выбираются N_0 биометрических векторов, на которых значение нейрона равно единице
- Выбираются N_0 биометрических векторов, на которых значение нейрона равно нулю

Атака при неизвестных таблицах – 'черный' ящик

Основное свойство - коэффициенты различных нейронов определяются независимо.

- Выбираются N_0 биометрических векторов, на которых значение нейрона равно единице
- Выбираются N_0 биометрических векторов, на которых значение нейрона равно нулю
- Дихотомическим алгоритмом, с заданной погрешностью находится уравнение гиперплоскости, задаваемой нейроном

- При $N_0 = 416, N_1 = 128$ сложность метода составляет порядка $4.8 \cdot 10^8$ операций.
- Алгоритм может быть существенно улучшен

Выводы

- В таблицах нейронной сети содержится вся информация о секретных параметрах системы (таблицы – секретный ключ)

Выводы

- В таблицах нейронной сети содержится вся информация о секретных параметрах системы (таблицы – секретный ключ)
- Нейросетевое преобразование не может рассматриваться как нечеткий экстрактор

Выводы

- В таблицах нейронной сети содержится вся информация о секретных параметрах системы (таблицы – секретный ключ)
- Нейросетевое преобразование не может рассматриваться как нечеткий экстрактор
- Нейросетевое преобразование может применяться только в защищенной среде

Выводы

- В таблицах нейронной сети содержится вся информация о секретных параметрах системы (таблицы – секретный ключ)
- Нейросетевое преобразование не может рассматриваться как нечеткий экстрактор
- Нейросетевое преобразование может применяться только в защищенной среде
- Часть требований стандарта ГОСТ Р 52633 по противодействию угрозам является недостаточными

Спасибо за внимание