ИДЕНТИФИКАЦИЯ ЧЕЛОВЕКА ПО ДИНАМИКЕ НАПИСАНИЯ СЛОВ В КОМПЬЮТЕРНЫХ СИСТЕМАХ

Ложников П.С.
Сибирская государственная автомобильно-дорожная академия, г. Омск

Существующие способы аутентификации пользователя в компьютерных системах делят на следующие:

- по учетной записи пользователя и паролю;
- с применением специализированных устройств (микропроцессорных карточек, токенов и т.д.);
- по биометрическим характеристикам человека.

Первые два способа не является достаточным условием, для того, чтобы со стопроцентной уверенностью можно было утверждать, что аутентифицированный пользователь именно тот, кто является владельцем специального устройства или пароля. Преимущество последнего способа, по сравнению с двумя первыми, заключается в том, что аутентифицируется не внешний предмет, принадлежащий пользователю или запомненная им фраза, а биометрический признак, который невозможно потерять, передать или забыть.

Биометрическая аутентификация согласно [1] может проходить в двух режимах верификации и идентификации. В первом случае пользователь изначально представляется, вводя свою учетную запись, затем происходит сравнение с ранее зарегистрированным его эталоном и предъявленных измерений соответствующего биометрического параметра. При идентификации сравниваются обработанные измерения биометрического параметра с указанной совокупностью ранее введенных эталонов и принимается решение о наиболее близком их соответствии.

Из биометрических технологий в компьютерных системах уже около десяти лет используют системы аутентификации личности по динамике написания подписи, так как данный метод сочетает в себе приемлемую стоимость и надежность. Особенно широко данная технология применяется в банковской сфере, электронной коммерции и документообороте. Все коммерческие системы данного класса работают в режиме верификации [2].

Авторами разработана технология, позволяющая проводить идентификацию пользователей по динамике написания слов. Подпись является частным случаем. Экспериментально было доказано, что динамика написания любого выбранного слова из четырех-пяти букв у пользователей становится стабильной после примерно тридцати повторов. Процесс идентификации личности по динамике написания слова (подписи) можно разделить на следующие этапы:

1) Ввод рукописного слова в компьютер с помощью графического планшета (см. рис. 1). На стадии регистрации пользователя (создания эталона) данная процедура повторяется несколько раз.

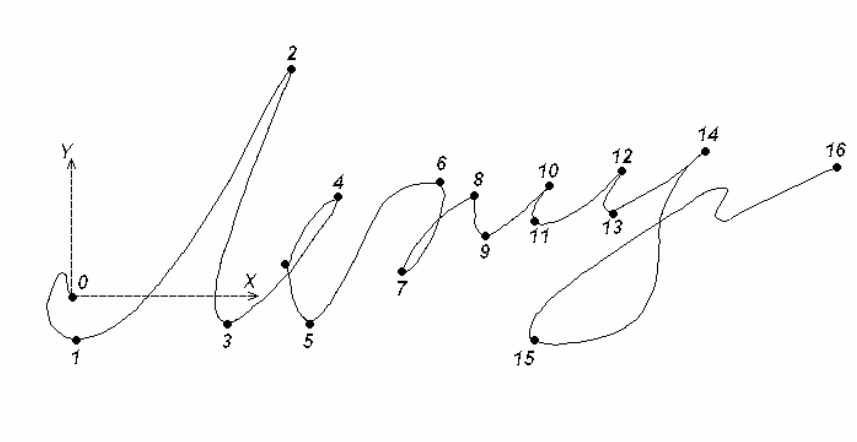

Рис 1. Введенная в компьютер с помощью графического планшета подпись

2) Предварительная обработка полученных сигналов.
3) Выделение набора признаков, характеризующих динамику рукописного слова (подписи). Первичные данные о динамике написания слова получают в виде двух функций времени изменения положения светового пера в плоскости планшета $x(t)$ и $y(t)$, а также в виде вариаций давления чувствительного к нажатию кончика пера на поверхность планшета: $z(t)$. (см. рис. 2)

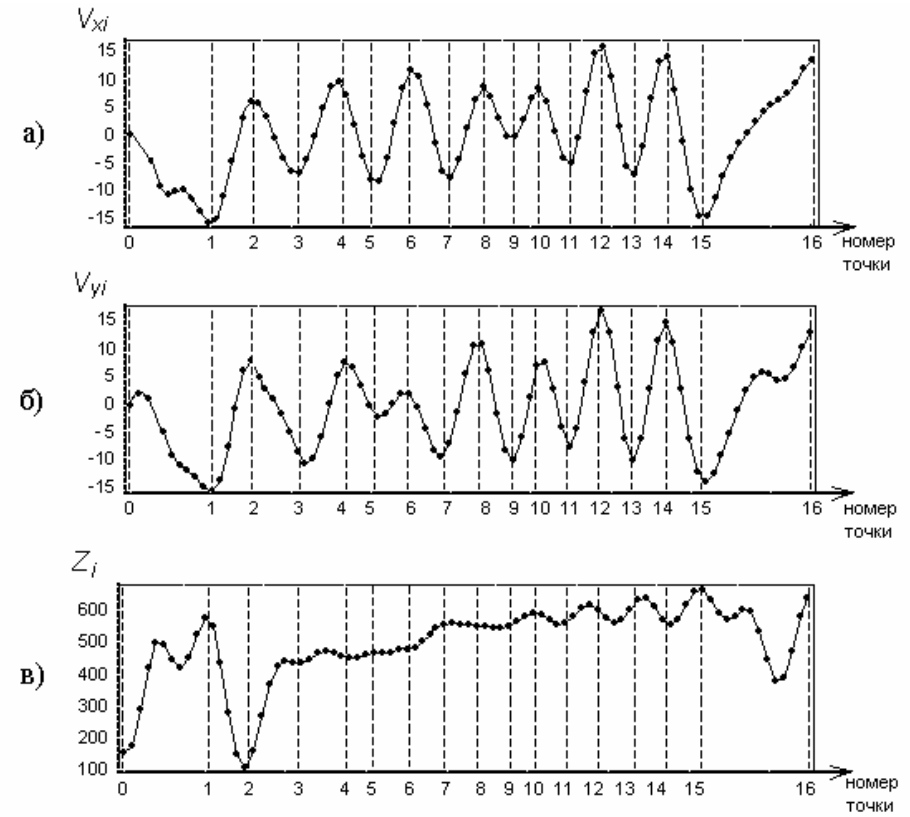

Рис. 2.Кривые, отражающие динамику написания подписи на рис 1.

4) Нахождение наиболее вероятной гипотезы о предъявленном рукописном слове (подписи). Количество зарегистрированных пользователей соответствует количеству первоначально выдвигаемых гипотез о принадлежности предъявленного образца подписи к какому-либо эталону. Разработанный метод идентификации пользователя по динамике написания слов основан на последовательном применении стратегии выбора гипотез Байеса.

У представленной технологии идентификации пользователей по динамике написания слов есть ограничение по количеству зарегистрированных пользователей (т.е. эталонов рукописных слов или подписей). Она обеспечивает уровни ошибок первого и второго рода примерно 1-2% (как и у систем верификации данного класса) при условии, что число пользователей не превышает 30. Если же данный порог превышается, предусматривается регистрация второго рукописного слова, таким образом, пользователям необходимо будет последовательно вводить два слова.

Преимущество данной технологии над системами верификации подписи в том, что она позволяет осуществлять скрытую идентификацию пользователей. Здесь имеется ввиду, что пользователи просто могут не знать, как их идентифицируют. Это возможно, например, если пользовательский интерфейс соответствующего программного обеспечения поддерживает ввод рукописных команд (слов) или в электронном документе имеется возможность ставить подпись с графического планшета. При вводе рукописного слова или попытке подделки подписи посторонним (незарегистрированным) пользователем, предусмотрен алгоритм, который позволяет его идентифицировать как «чужого» с вероятностью 0,98.

В первую очередь, данная технология рассчитана на использование в компьютерных системах по ограничению несанкционированного доступа лиц к конфиденциальной информации.

Литература

1. BioAPI Specification Version 1.1 March 16th, 2001 developed by The BioAPI Consortium, http://www.bioapi.com/BIOAPI1.1.pdf.
2. Евангели А. Технологии биоидентификации и биометрический рынок. // PC WEEK/RE №7 2003, -с. 24.