Динамические методы биометрической аутентификации личности

Черкезов Роман

11 апреля 2006 г.

Эссе по курсу "Защита информации", кафедра радиотехники, Московский физико-технический институт (ГУ МФТИ), http://www.re.mipt.ru/infsec

В наше время всеобщей информатизации особую важность и значимость приобретают задачи защиты информации. Постоянно разрабатываются новые методы защиты, которые позволяют увеличивать надежность и стойкость систем, предназначенных для решения такого рода задач.

Среди задач защиты выделяются задачи аутентификации (установление подлинности). И одними из наиболее перспективных и активно развивающихся сейчас методов являются методы биометрической аутентификации.

Что дает нам биометрия? Среди явных плюсов то, что биометрические характеристики каждого человека уникальны. У каждого свое неповторимое лицо, отпечатки пальцев, походка и пр. Не возникает проблема содержания в секрете пароля. Кроме того, биометрические характеристики всегда при человеке, он не может их «забыть» или потерять. Их можно в любой момент измерить (естественно, при наличии соответствующего оборудования).

При рассмотрении любых систем распознавания важнейшими показателями таких систем являются вероятности ошибок системы. Если она (система) предназначена для разделения всех объектов на два класса (а именно такое разделение осуществляют системы аутентификации пользователей — они всех, кто пытается авторизоваться, должны разделить на два класса — «своих» и «чужих»), то для нее могут существовать две ошибки. Это так называемые ошибка первого рода (когда «своего» мы принимаем за «чужого») и ошибка второго рода (когда, наоборот, мы «чужого» принимаем за «своего»). Наиболее значимой считается вероятность пропуска «чужого», т.е вероятность ошибки второго рода. Действительно, если, скажем, вероятность ложной тревоги (ошибки первого рода) равна 1%, а вероятность пропуска - 10^{-6} %, то это значит, что из сотни «своих» одного система не пропустит. Но ведь он может пройти процедуру распознавания еще раз. Зато для того, чтобы система допустила ошибку и пропустила «чужого», по статистике требуется 100 миллионов попыток (в данном гипотетическом случае). Гораздо хуже будет, если вероятность ошибки второго рода станет равной 1%. Тогда из ста злоумышленников одного система наверняка пропустит. Такая ситуация недопустима.

Вероятности ошибок первого и второго рода являются очень значимыми для систем распознавания. Именно значения вероятностей этих ошибок и определяют (в основном) качество функционирования системы.

В настоящее время активно развиваются методы биометрической аутентификации по статическим (неизменяемым) данным личности, как то: по двумерному изображению лица, трехмерному изображению лица, отпечаткам пальцев, радужной оболочке глаза, рисунку сосудов глазного дна, геометрии кисти руки, термографической картине лицевых артерий и вен, венам руки и пр.

Преимуществом таких методов является относительная простота организации процесса аутентификации потока людей (т.к. измерение статических характеристик не требует больших усилий от пользователей и, кроме того, не зависит от их психологического состояния).

К сожалению, есть у статических методов и недостатки, причем весьма существенные. Один из серьезнейших — неизменяемость и открытость статических биометрических характеристик человека, что означает возможность для злоумышленника тем или иным образом их подделывать. К примеру, для систем аутентификации, работающих с отпечатками пальцев, возможно изготовление муляжей из парафина, с высокой точностью имитирующих папиллярный рисунок пальцев руки. И пока что неизвестны способы бороться с такого рода атаками.

Кроме того, технологии, существующие сегодня на рынке, достаточно дороги и обладают вероятностями ошибки второго рода на уровне 10^{-7} — 10^{-12} (дальнейшему увеличению точности мешают физические ограничения уникальности статических образов личности), что довольно неплохо, но недостаточно для широкомасштабного применения.

Такие недостатки можно преодолеть с помощью динамических методов биометрической аутентификации (аутентификация по особенностям голоса человека, по динамике рукописной подписи, по походке, по клавиатурному почерку, по работе с компьютерной мышкой, по характеру взаимодействия кисти руки и пистолета(см. [4]) и многое другое). Эти методы, во-первых, дают возможность изменять измеряемый образ. Так, человек может изменить контрольное слово, которое он использует при аутентификации в системе распознавания личности по особенностям голоса. Или может изменить контрольную фразу, которую вводит при аутентификации по клавиатурному почерку. Это делает такие системы предпочтительными при аутентификации личности по открытому каналу.

Далее. Большинство динамических методов достаточно дешевы в реализации, т.к. для них не нужно специализированное оборудования для измерения характеристик. Обычно такие системы можно реализовать с помощью стандартных средств мультимедиа. Поэтому стоимость системы определяется в основном стоимостью программного обеспечения.

Еще одним преимуществом динамических систем заключается в возможности (для некоторых систем) сделать биометрические образы тайными. В этом случае злоумышленник уже не сможет использовать заранее подготовленный муляж. При этом утверждается, что для системы аутентификации по клавиатурному почерку при использовании слова из 5 букв вероятности ошибок второго рода достигают величин порядка 10^{-33}. При увеличении длины слова вероятность еще уменьшается.

Основным недостатком же динамических биометрических систем является то, что на их функционирование влияет психофизиологическое состояние человека. Он может волноваться или быть спокойным, усталым или бодрым, здоровым или больным, и т.п. Возьмем, например, систему распознавания личности по голосу. Если в базе данных хранится голос здорового человека, а он (этот человек) простудится, и его голос станет хриплым, то системе будет сложнее (возможно, намного) его узнать.

Итак, рассмотрим некоторые биометрические системы аутентификации личности динамическими методами и некоторые вопросы и проблемы, возникающие для таких систем.

Начнем с аутентификации личности по рукописной подписи (и динамике ее воспроизведения). Такой способ является одним из старейших способов аутентификации личности. Уже несколько веков назад стали использовать подпись для подтверждения подлинности тех или иных ценных бумаг.

Некоторые авторы считают целесообразным разделение проблемы аутентификации личности по факсимильной подписи на две независимые задачи:

- аутентификация только по статической подписи, которая поставлена заранее на проверяемом документе:

- аутентификация по динамике воспроизведения, т.е. в момент подписания, с возможностью наблюдения индивидуальных особенностей процесса;

Обе задачи можно решать параллельно и независимо. Первая задача – статическая, нужно просто сравнивать полученное изображение с тем, которое имеется в базе. Такие задачи сейчас активно пытаются решать. При этом для современных технологий она достаточно сложная. И качество ее решения все еще оставляет желать лучшего, хотя и достигнуты некоторые серьезные результаты на сегодняшний день.

Во второй задаче мы должны обрабатывать данные о колебаниях пера автора. Возьмем декартову систему координат (X,Y,Z). Данные о динамике воспроизведения – две функции времени колебаний пера в плоскости графического планшета X(t), Y(t) плюс функция вариации давления пера на планшет Z(t).

Современные системы могут быть одно-, двух-, и трехкоординатные в зависимости от того, анализируют ли они одну кривую, две или все три X,Y и Z.

Некоторые системы используют не сами функции X,Y,Z, а их производные (или даже вторые производные). Использование производных обусловлено только типом используемого датчика. Впрочем, корреляция данных, полученных из производных, с данными, полученными из самих функций, обычно близка к единице. Поэтому это не дает ощутимого улучшения функционирования системы.

Сейчас изготавливаются системы с вероятностями ошибки второго рода порядка $10^{-6}\ldots10^{-8}$.

Для того, чтобы аутентифицировать динамические параметры вычисляются некоторые линейные функционалы. Обычно в качестве линейных функционалов выбирают ортогональные функционалы Фурье, Уолша, Хаара. Их считают либо по всей реализации (глобальные функционалы), либо по некоторой части (локальные функционалы — например, по разным буквам слова) или частям.

При этом нужно помнить, что глобальные параметры показывают, насколько похожа подпись на образец в целом. Локальные же показывают схожесть некоторых динамических особенностей.

Одной из основных сложностей для систем аутентификации личности по динамическим характеристикам подписи является проблема выбора разметки подписи. Разметка – это разделение подписи на части, где вычисляются локальные функционалы. Сложность же заключается в том, что при каждом подписывании автором могут добавляться некоторые фрагменты подписи, так же как некоторые фрагменты могут сливаться там, где в образце этого нет. Поэтому если выбрать слишком частую разметку, то многие части подписи могут не совпадать, что не позволить аутентифицировать данного пользователя. При этом и вычислительная сложность задачи, и время ее решения, увеличиваются.

Если выбрать слишком редкую разметку (в этом случае число локальных параметров будет меньшим), могут быть не учтены многие динамические особенности подписи. Как следствие, увеличится величина вероятности ошибки второго рода.

Также серьезной проблемой является сильная зависимость параметров системы от психологического состояния людей и стабильности их почерка.

Рассмотрим теперь систему аутентификации личности по клавиатурному почерку.

В свое время для идентификации телеграфистов, работавших с кодом Морзе, использовалось то обстоятельство, что у каждого телеграфиста при такой передаче информации вырабатывался свой собственный индивидуальный почерк.

Аналогично и для людей, постоянно набирающих тексты с клавиатуры. Каждый по-своему набирает текст. При этом можно идентифицировать пользователей по скорости набора, по ритмическим характеристикам набора; можно учитывать количество ошибок, их характер и т.п.

Возможность аутентифицировать клавиатурный почерк человека появляется при вводе в качестве пароля фразы, состоящей из достаточно большого количества букв. Система фиксирует времена нажатия клавиш и интервалы между нажатиями и отпусканиями клавиш (контрольные параметры).

Скорость набора и контрольные параметры значительно зависят от того, сколько пальцев используется при наборе. При наборе одним пальцем одной руки клавиатурный почерк теряет свою уникальность. Это происходит из-за того, что при наборе несколькими пальцами интервалы между нажатиями зависят от характерных для каждого пользователя сочетаний движения пальцев рук и самих рук тоже. При наборе одним пальцем интервалы становятся пропорциональными временам нажатия клавиш.

При совершенствовании навыков работы с клавиатурой растет и индивидуальность набора каждого пользователя.

Установлено, что парольная фраза должна быть по длине не менее 20 символов. Причем при наборе этой фразы допустимы ошибки в 1-2 символах. Это ухудшает стойкость системы, но зато сильно уменьшает вероятность «ложной тревоги».

Одним из серьезнейших вопросов для такого рода систем является вопрос о наличии у конкретного пользователя собственного характерного для него клавиатурного почерка. В настоящее время предлагаются специальные процедуры, предназначенные для ответа на этот вопрос[5]. Существуют также процедуры для измерения уровня стабильности и индивидуальности клавиатурного почерка.

В настоящее время популярностью в России и за рубежом пользуется задача аутентификации личности по голосовым особенностям. Интерес к задаче возник уже более 30 лет назад. И до сих пор не утихает. Предложено несколько подходов к ее решению.

Общие принципы работы строятся на особенностях тембральной окраски голосов. При этом обычно учитываются и неравномерности распределения мощности по частотному спектру.

Особую популярность в последнее время заслужил метод линейного предсказания речи. Он основан на аппроксимации соседних волн в звуковой пачке переходным процессом некоторого линейного цифрового фильтра. Исходный сигнал разбивается на отдельный интервалы анализа. Определяется тип звука внутри интервала анализа (шум или тон). Если внутри интервала присутствует шум, определяются его энергетические параметры. В противном случае сигналу дополнительно задают коэффициенты линейного предсказания (цифрового фильтра) и период импульсов основного тона, возбуждающих переходные процессы на выходе предсказателя. Методы нахождения коэффициентов могут быть разными. Каждый подход имеет свои преимущества и недостатки. После этого фраза дробится на последовательные интервалы. Обработав данные на каждом интервале, получают систему функций коэффициентов линейного предсказателя $\{a_1(t), a_2(t), ..., a_n(t)\}$.

Система анализирует несколько произношений контрольной фразы, на основе чего создается биометрический эталон, который, по сути, предсказывает наиболее вероятные значения характерных функций.

Недостатком системы (причем серьезным) служит невозможность сохранения контрольной фразы в тайне. Поэтому современные ожидания эффективности систем аутентификации по голосу базируются на предположении о возможности такой аутентификации при произнесении произвольной фразы.

По данным некоторых исследований ошибки первого и второго рода для систем распознавания голоса составляют величины порядка процента.

Итак, мы рассмотрели современное состояние и возможности биометрических систем аутентификации личности на основе динамических методов. Направление это актуально и бурно развивается в настоящее время. Многочисленные фирмы предлагают

свои разработки такого рода систем (можно заглянуть на сайт Биометрического Консорциума http://www.biometrics.org и убедиться в огромном количестве предлагаемых сегодня систем). Многие страны сегодня вводят или собираются вводить биометрические паспорта (правда, там используются только статические параметры), в которых будут храниться биометрические образы, а автоматические системы будут аутентифицировать владельца паспорта. Имеется и много других приложений.

Так что тема биометрической аутентификации требует, как минимум, ознакомления. Данное эссе может послужить неплохим введением в динамические методы биометрической аутентификации.

Источники, использованные при подготовке эссе

1. *Иванов А.И. Нейросетевые алгоритмы биометрической идентификации личности.— Серия «Нейрокомпьютеры и их применение». Кн. 15. — М.: Радиотехника, 2004. – с. 22-50.*
2. *http://www.biometric.ru*
3. *http://www.biometrics.org*
4. *http://daily.sec.ru/dailypblshow.cfm?rid=19&pid=14342*
5. *Рыбченко Д.Е., Критерии устойчивости и индивидуальности компьютерного почерка при вводе ключевых фраз.— Специальная техника средств связи. Серия «Системы, сети и технические средства конфиденциальной связи».— Пенза, ПНИЭИ, 1997, вып.№2 – с. 104-107.*
6. *Обзор технологий биометрической идентификации – 16.11.03. http://center.forever.kz/hard/other/f0003.htm*
7. Иванов А.И. "Биометрические и нейросетевые механизмы связи с криптографическими механизмами информационной безопасности". Труды научно-технической конференции "Безопасность информационных технологий". Том 4, Секция 9. Стр. 3-6, Пенза, 2003 (http://beda.stup.ac.ru/RV-conf/v04/001/)
8. *http://www.aladdin.com/*
9. *Бочкарев С.Л. Система голосовой аутентификации по динамическим параметрам акустического тракта человека.— Специальная техника средств связи. Серия «Системы, сети и технические средства конфиденциальной связи».— Пенза, ПНИЭИ, 1996, вып.№1 – с. 93-96*
10. *Ю.А. Брюхомицкий, М.Н. Казарин. Учебные биометрические системы контроля доступа по рукописному и клавиатурному почеркам.— Таганрог, ТРГУ, 2004*
    (http://www.library.mephi.ru/data/scientific-sessions/2006/vnk13/0-1-12.doc)