Література

1. Терейковский И.А. Использование искусственных нейронных сетей в задачах распознавания атак на компьютерные системы. // Захист інформації, 2006, №3. – С.57-65 .
2. Терейковський І.А. Концепція визначення оптимального режиму контролю захищеності програмного забезпечення комп'ютерних систем // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – Київ, 2006. – Випуск 1(12) – С.88-96
3. Терейковський І.А. Концепція використання марківських процесів для контролю атак на програмне забезпечення комп'ютерних систем та мереж. Науковоий журнал "Захист інфорації" №3 2005, с.37-49.
4. Терейковский И.А. Моделирование профилей нормального поведения компьютерных систем. // Защита информации, Сб. н. тр. К.: НАУ. –2006. – С. 103-108.
5. Терейковський І.А. Нейронні мережі в засобах захисту комп'ютерної інформації.– К.: ТОВ ПоліграфКонсалтинг, 2007. – 209 с.

УДК681.3

БАРАНОВ А.Н., БАРАНОВ Н.А.

Севастопольський военно морской ордена Красной Звезды институт им. П.С. Нахимова

НОВЫЙ СПОСОБ И АЛГОРИТМ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА ПО КЛАВИАТУРНОМУ ПОЧЕРКУ

В статье рассматривается новый способ аутентификации пользователя персонального компьютера по клавиатурному почерку и мультипликативный алгоритм для его реализации. Показано, что набранная ключевая фраза по сути своей является кодовой последовательностью и при работе с клавиатурой разных пользователей будут наблюдаться деформации временного масштаба (растяжение-сжатие) формируемых кодовых последовательностей. С учётом такого типа искажений во временной области при известном времени начала комбинации модель клавиатурного почерка назовём идеальной системой деформации временного масштаба (ИСДВМ). Новая модель уже характеризует совокупность кодовых комбинаций как мультипликативно стационарный процесс.

Библ.-5.

Большинство описанных в литературе биометрических систем [1-3] сориентировано на анализ клавиатурного почерка. Все известные существующие способы аутентификации по клавиатурному почерку основаны на расчете временных числовых параметров пользователя, сравнении их с эталонными по статистическим критериям и принятии решения о легальности пользователя.

В работе предлагается новый способ аутентификации по клавиатурному почерку и мультипликативный алгоритм для его реализации.

Отличительной способностью систем цифровой связи вообще является то, что за конечный промежуток времени посылается сигнал, состоящий из конечного набора элементарных сигналов – идеальных двоичных цифровых импульсов. При аутентификации набранная ключевая фраза также по сути своей является кодовой последовательностью нулей и единиц. Очевидно, что кодовые последовательности пользователей ПЭВМ будут иметь разный масштаб времени в силу разницы в стиле работы с клавиатурой этих пользователей (временные интервалы между нажатием клавиш и время удержания-нажатия клавиш характеризуют стиль работы пользователя с клавиатурой). Таким образом, при работе с клавиатурой разных пользователей будут наблюдаться деформации временного масштаба (растяжение-сжатие) формируемых кодовых последовательно-

стей. С учётом такого типа искажений во временной области при известном времени начала комбинации такую модель клавиатурного почерка назовём идеальной системой деформации временного масштаба (ИСДВМ). Новая модель уже характеризует совокупность кодовых комбинаций как мультипликативно стационарный процесс. Для такой модели применима концепция мультипликативной свёртки, как операции над переданным и принятым сигналами, которая естественным образом приводит к интегральним уравнениям с ядром, зависящим от произведения (частного) аргументов.

В данном случае представляется целесообразным применение алгоритма первичной обработки кодовых последовательностей, имеющих разный масштаб аргументов - корреляционное сравнение текущих кодовых последовательностей с эталонной кодовой последовательностью. Для оценки деформации временного масштаба в радио- и гидролокации используется мультипликативный интеграл Меллина [4,5]:

$$MKF(\alpha)=\frac{1}{T}\int_0^{\infty}s_1(t)\cdot s_2(\alpha\cdot t)\cdot\frac{dt}{t}=\int_0^{\infty}s_1(\varepsilon)\cdot s_2(\alpha\cdot\varepsilon)\cdot\frac{d\varepsilon}{\varepsilon} \quad (1)$$

Из (1) видно, что сигналы $s_1(\varepsilon);\ s_2(\alpha\cdot\varepsilon)$ должны быть выравнены по фронту кодовых последовательностей с условием $\eta_{12}=\tau_{12}\cdot f_{dk}=0$. Очевидно, что это жесткое условие в системах аутентификации выполняется. Если его невозможно выполнить, то оценку коэффициента сжатия α осуществляют через спектры, независящие от временной задержки. Это могут быть амплитудный и производный спектры:

$$A(k)=\sqrt{S_d^2(k)+S_m^2(k)}:\ P(k)=\frac{1}{A^2(k)}\cdot arctg\left(\frac{S_m(k)}{S_d(k)}\right)=\left[S_d(k+1)\cdot S_m(k)-S_d(k)\cdot S_m(k+1)\right] \quad (2)$$

В мультипликативном интеграле (1) время $\frac{dt}{t}=\frac{d\varepsilon}{\varepsilon}$ изменяется по логарифмическому закону. Рассмотрим для сигнала $s(\varepsilon)=s\left(\frac{t}{T}\right)$ преобразование Меллина:

$$S(\nu)=\int_0^{\infty}s(\varepsilon)\cdot\varepsilon^{-j\cdot\nu}\cdot\frac{d\varepsilon}{\varepsilon}=\int_0^{\infty}s\left(e^{\ln(\varepsilon)}\right)\cdot e^{-j\cdot\nu\cdot\ln(\varepsilon)}\cdot d[\ln(\varepsilon)]=\int_{-\infty}^{\infty}S(x)\cdot e^{-j\cdot\nu\cdot x}\cdot dx \quad (3)$$

Преобразование Меллина с логарифмическим масштабом времени $x=\ln(\varepsilon)$ приводится к преобразованию Фурье. В общем случае основание логарифма может быть произвольным. Сигнал $s(\varepsilon)$ существует на интервале времени $\varepsilon=\overline{0,1}$. Для представления интеграла Меллина в цифровом виде произведем на интервале наблюдения $t=\overline{0,T}$ замену аргумента $\varepsilon=\frac{t}{T}=q^{\frac{\theta}{T}};\ \frac{\theta}{T}=\log_q(\varepsilon)$:

$$S(\nu)=\frac{1}{\ln(q)}\cdot\int_{-\infty}^{0}s\left(q^{\frac{\theta}{T}}\right)\cdot q^{-j\nu\cdot\frac{\theta}{T}}\cdot\frac{d\theta}{T}=\frac{1}{\ln(q)}\cdot\int_{-\infty}^{0}S\left(\frac{\theta}{T}\right)\cdot e^{-j\cdot\nu\cdot\frac{\theta}{T\cdot\ln(q)}}\cdot d\left(\frac{\theta}{T}\right) \quad (4)$$

Основание логарифма q целесообразно определять из условия равенства логарифмического масштаба времени $d\theta$ масштабу равномерного времени dt при $t = T$. Тогда имеем соотношение: $\frac{d\theta}{T} = \frac{dt}{T \cdot \ln(q)}$; $\ln(q) = 1$; $q = e$, а соотношение (4) принимает следующий вид:

$$S(\nu) = \int_{-\infty}^{\infty} s(e^x) \cdot e^{-j \cdot \nu \cdot x} \cdot dx; \quad S(m) = \sum_{m=-\infty}^{-\infty} s\left[(q)^{\frac{m}{N}}\right] \cdot e^{-j \cdot \frac{2\pi}{N} \cdot \nu \cdot m}. \qquad (5)$$

В дискретном преобразовании Меллина $S(m)$ приняты следующие условия: дискретизация логарифмического масштаба времени производится в моменты $\theta_m = m \cdot \Delta t = \frac{m}{f_{dk}}$; параметр ν соответствует частотным составляющим $f_\nu = \frac{\nu}{N} \cdot f_{dk}$. Осталось определить моменты дискретизации сигнала $s(n)$ с равномерным масштабом времени $\varepsilon_n = \frac{n}{N}$ для целочисленных значений $m = -(0, 1, 2, 3, \ldots)$ логарифмического масштаба времени $\theta_m = e^{\frac{m}{N}} = \left(1 + \frac{1}{N}\right)^m = \left(1 - \frac{1}{N}\right)^{-m}$; $\theta_0 = 1$. Меняя знак параметра m на обратное состояние, получим алгоритм экспоненциального сжатия цифрового сигнала:

$$n(m) = N - \sum_{\mu=0}^{m-1}\left(\rho^\mu\right) = N - \sum_{\mu=0}^{m-1}\left(1 - \frac{1}{N}\right)^\mu = N \cdot \rho^m; \quad n(N-1) = N \cdot \left(1 - \frac{1}{N}\right)^N = \frac{N}{e} = 0{,}368 \cdot N \qquad (6)$$

Сигнал $s(n)$ наблюдается на интервале значений аргумента $n = \overline{0, N-1}$, поэтому интерполирование значений отсчетов $s(n)$ для аргумента $n(m)$ при $m = 0, 1, 2, 3, \ldots$ выполняется по соотношению:

$$n(m) = [n(m-1) - \rho^m] = [N \cdot \rho^m - \rho^m] = N \cdot \rho^{m+1}; \quad m = \overline{0, N-1} \qquad (7)$$

Интервалы дискретизации логарифмического масштаба времени $\frac{n(m)}{N}$ уменьшаются по экспоненциальному закону $\Delta n(m) = \frac{1}{N} \cdot \rho^m$. Из вещественного числа $n(m)$ выделяется целая $k = Trunc(n(m))$ и дробная $q = Frac(n(m))$ части стандартными функциями языка программирования. По индексу k выбираются отсчеты для интерполирования функции $s(n)$ с параметром q. Интерполирование можно достаточно эффективно выполнить по формуле Бесселя для отсчетов $y_{-1} = s(k-1)$; $y_0 = s(k)$; $y_1 = s(k+1)$; $y_2 = s(k+2)$ по формуле:

$$y(q) = y_0 + q_1 \cdot (y_1 - y_0) + q_2 \cdot (y_{=1} - y_0 - y_1 + y_2) + q_3 \cdot (y_{-1} - 3 \cdot y_0 + 3 \cdot y_1 - y_2);$$

$$q_1 = q; \quad q_2 = \frac{q \cdot (q-1)}{4}; \quad q_3 = \frac{(q-0{,}5) \cdot q \cdot (q-1)}{6} \qquad (8)$$

Корреляционный интеграл Меллина легко приводится к обычному корреляционному интегралу путем замены равномерного масштаба времени $\varepsilon = \frac{t}{T}$ на логарифмический масштаб $\frac{\theta}{T} = \ln(\varepsilon)$. Для этого достаточно выполнить экспоненциальное сжатие сигналов $s_1(\varepsilon);\ s_2(\alpha \cdot \varepsilon)$ в цифровом виде по соотношению (7) с использованием интерполяционной формулы (8) Бесселя:

$$\int_{-\infty}^{\infty} S_1\left(e^{\frac{\theta}{N}}\right) \cdot S_2\left(e^{\frac{\theta+\beta}{N}}\right) \cdot d\left(\frac{\theta}{N}\right) = \frac{1}{T}\int_{-\infty}^{\infty} S_1(\theta) \cdot S_2(\theta+\beta) \cdot d\theta \qquad (9)$$

Если сигналы $s_1(\varepsilon);\ s_2(\alpha \cdot \varepsilon)$ выравнивать по фронту волны не представляется возможным, то коэффициент α оценивается через независящие от временной задержки спектры (2), которые всегда начинаются с частоты $\omega = 0$:

$$MKF(\alpha) = \int_{0}^{\infty} S_1(\omega) \cdot S_2\left(\frac{\omega}{\alpha}\right) \cdot \frac{d\omega}{\omega} \qquad (10)$$

В предлагаемой работе показана целесообразность использования безразмерного времени и частоты, приведены алгоритмы цифровой обработки случайных сигналов.

Литература:

1. *Тумоян Е.П.* Биометрическая аутентификация мобильных пользователей// Информационное противодействие угрозам терроризма: Научно-информационный журнал.-2005, №5.-с.79-91.
2. *Широчин В.П., Кулик А.В., Марченко В.В.* Динамическая аутентификация на основе анализа клавиатурного почерка// Официальный сайт Донецкого Национального технического университета (http://donntu.edu.ua/2002/fvti/aslamov/files/bio_autentification.htm).
3. *Гайша О.О.* Аналіз можливих методів ідентифікації особи в системах дистанційної освіти//Методологічні засади дистанційного дистанційного навчання: Матер. міжн. наук.-техн. конф. – Дніпропетрівськ:ДНУ, 2005.-с.16-19.
4. *Гельфанд И.И., Граев М.И., Пятецкий-Шапиро И.И.* Теория представлений и автоморфные функции / М.:"Наука", Гл. ред ФМЛ. —1966. — 512 с.
5. *Тихонов А.Н., Арсенин В.Я.* Методы решения некорректных задач. Гл. ред. ФМЛ, Наука, М., 1974.-223с.

УДК 681.3.004

Петров А.А
Восточноукраинский национальный университет имени Владимира Даля

ОПРЕДЕЛЕНИЯ ОПЕРАТИВНО-ТЕХНИЧЕСКИХ ХАРАКТЕРИСТИК СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

Под оперативно-техническими характеристиками (ОТХ) систем активной защиты будем понимать ряд важнейших качеств данной системы, определяющих эффективность ее применения как средства защиты информации от утечки за счет ПЭМИН. К числу таких характеристик могут быть отнесены:

1) маскировочная способность;