Интеллектуальные системы

УДК 004.056.53

ПРИМЕНЕНИЕ ЦИФРОВЫХ ВОДЯНЫХ ЗНАКОВ ДЛЯ РАЗРАБОТКИ СИСТЕМ ГРАФИЧЕСКОГО ПАРОЛЯ

Шокарев Алексей Владимирович,
канд. техн. наук, доцент кафедры информационных технологий
Юргинского технологического института (филиала) Томского
политехнического университета, Россия, 652055,
г. Юрга, ул. Ленинградская, д. 26. E-mail: Shokarev_av@mail.ru

Актуальность работы состоит в повышении безопасности защищаемых ресурсов при прохождении идентификации/аутентификации пользователей средствами систем графического пароля, которую можно обеспечить с помощью применения методов стеганографии.

***Цель работы** заключается в повышении достоверности идентификации/аутентификации пользователей за счет применения системы графического пароля с использованием цифровых водяных знаков. Применение методов стеганографии повышает стойкость систем к большинству известных методов взлома систем с парольной аутентификацией пользователей.*

***Методы исследования:** методы теории вероятности, математического анализа, стеганографии и экспериментальных исследований. Программная реализация метода выполнена с использованием среды программирования Borland C++.*

***Результаты:** показана возможность создания системы графических паролей с использованием методов стеганографии, в частности цифровых водяных знаков, которые применяются в данных системах идентификации/аутентификации как одноразовые пароли для авторизации и доступа пользователя к защищаемым ресурсам. Также представлены основные блок-схемы реализации двух систем графического пароля, первая – на основе пиктограмм, вторая использует графический файл с множеством деталей. Опытным путем доказана эффективность применения приведенных систем паролей по отношению к привычным парольным методам аутентификации пользователей, в частности, пользователю не требуется запоминать сложные парольные последовательности – достаточно запомнить последовательность пиктограмм или последовательность нажатий на области графического файла, система самостоятельно меняет пароли без вмешательства пользователя в процесс, но по желанию пользователь самостоятельно может изменить последовательность пиктограмм или областей нажатий на графическом файле для входа в систему. Использование предложенных алгоритмов позволяет создать стойкие системы идентификации/аутентификации, а также уменьшить время запоминания паролей и авторизацию пользователей в системах, требующих ввода логина и пароля.*

Ключевые слова:
Системы графических паролей, цифровой водяной знак, методы реализации систем графических паролей, стеганография, идентификация/аутентификация пользователей.

Пользователи имеют определенную трудность заучивания сложных, псевдослучайных паролей в течение определенного времени [1]. Большинство из них забывают пароль, который не используется регулярно, а также могут или смешать элементы различных паролей, или помнить пароль, но путать, какой системе он соответствует.

Пользователи часто уменьшают сложность и число символов в паролях, тем самым снижая безопасность систем для взлома. Безопасный пароль должен содержать не менее 8 символов, его желательно создавать генератором случайных последовательностей из символов с верхним регистром, символов с нижним регистром, цифр, а также использовать специальные символы. С такими паролями у людей возникает проблема в запоминании, и большинство пользователей игнорируют данные рекомендации. Практика показывает, что пользователи часто выбирают короткие пароли, состоящие из имен, фамилий семьи или друзей, названия домашних животных, и даже не редко встречается слово «пароль». Чтобы не забывать пароли записывают их на бумагу либо используют тот же самый пароль для различных систем, иногда с единственной цифрой в конце [2, 3].

В связи с этими факторами и появлением мониторов и различных устройств с сенсорными экранами ведутся разработки систем графических паролей [4–6], которые создаются, чтобы избавить пользователя от сложных паролей и упростить авторизацию. Одним из недостатков этих систем является то, что большинство из них основаны на присвоении определенных символов изображению и/или координат нажатий, выбранных пользова-

телем для авторизации. Предлагаемые далее системы графических паролей на основе цифровых водяных знаков (ЦВЗ) избавлены от этого недостатка путем встраивания в графические файлы случайных символов, выработанных встроенным генератором случайных последовательностей. Пароли в приведенных системах являются одноразовыми. То есть после каждой успешной авторизации автоматически меняется последовательность символов цифровых водяных знаков, используемых в качестве паролей.

Предлагаемая модель системы ЦВЗ для разграничения доступа пользователей к защищенным ресурсам, применяемая в построении системы графического пароля [7, 8], показана на рис. 1.

Системой пользователю предлагается выбрать последовательность графических файлов, далее на все предложенные графические файлы система накладывает цифровой водяной знак W, индивидуальный для каждого графического объекта, который преобразовывается в кодере к удобному виду для встраивания в заверяемое сообщение. Алгоритм формирования такой конструкции водяного знака A представим в виде: $A=F(I,W)$, где F – функция, зависящая от I – контейнера (графический файл) и W – водяного знака [9, 10].

Затем в формирователе заверенных сообщений конструкция водяного знака A встраивается с помощью функции Z в графический контейнер, используя конфиденциальный ключ K: $Z=\Psi(A,I,K)$, где Ψ – функция, зависящая от A – конструкции водяного знака, I – контейнера (графического файла) и K – секретного ключа [11, 12].

После выбора пользователем последовательности графических объектов для своей аутентификации система передает ее по каналу связи. В канале связи на заверенное сообщение Y воздействуют нарушитель, а также случайные и преднамеренные помехи. В результате этого воздействия на приеме в устройство проверки водяных знаков поступает модифицированное сообщение Y. По алгоритму обнаружения водяного знака [13] формируется оценка водяного знака W' вида: $W'=G(Y,W,K)$, где G – функция с зависимостями от Y – модифицированное сообщение, W – водяной знак, K – секретный ключ.

Подлинность пользователя определяется в соответствии с этой оценкой [14]. Возможны решения вида $W'=1$ (подлинность сообщения подтверждена) или $W'=0$ (подлинность сообщения не подтверждена). Также возможны и другие решения вида $0{,}5\le W_j'\le 1$ (j-й фрагмент, скорее всего, подлинный) или $0\le W_j'<0{,}5$ (j-й фрагмент, скорее всего, навязан или искажен помехами передачи). При формировании оценки водяных знаков могут возникнуть ошибки их обнаружения получателем сообщения [15, 16].

По сравнению с криптографическими системами аутентификации система аутентификации пользователей на основе ЦВЗ имеет следующие особенности [9]:

- заверяемое сообщение и встроенный в него ЦВЗ взаимозависимы, то есть при разрушении первого разрушается и второй, а если водяной знак сохранил свою целостность, то и принятое сообщение ее не потеряло;
- при приеме искаженного фрагмента сообщения получатель может, не отказываясь от всего сообщения в целом, отказаться лишь от данного фрагмента.

В отличие от сравнительных методов методы контроля подлинности на основе водяных знаков обладают существенными достоинствами:

- высокой устойчивостью к удалению аутентификатора заверенного сообщения без разрушения самого сообщения;
- обнаружением несанкционированного копирования заверенных сообщений;
- согласованностью с источниками сообщений, обладающими существенными статистическими зависимостью и памятью, такими как изображение и звуковой сигнал.

Взяв во внимание все вышесказанное [10], можно получить несколько различных систем графического пароля, использующих стеганографические методы, которые повышают безопасность всей системы аутентификации. Первая из таких систем – система графического пароля на основе пиктограмм, вторая – система графического пароля на основе графического файла с множеством деталей. Блок-схемы работы сервера и клиентской части системы графического пароля на основе пик-

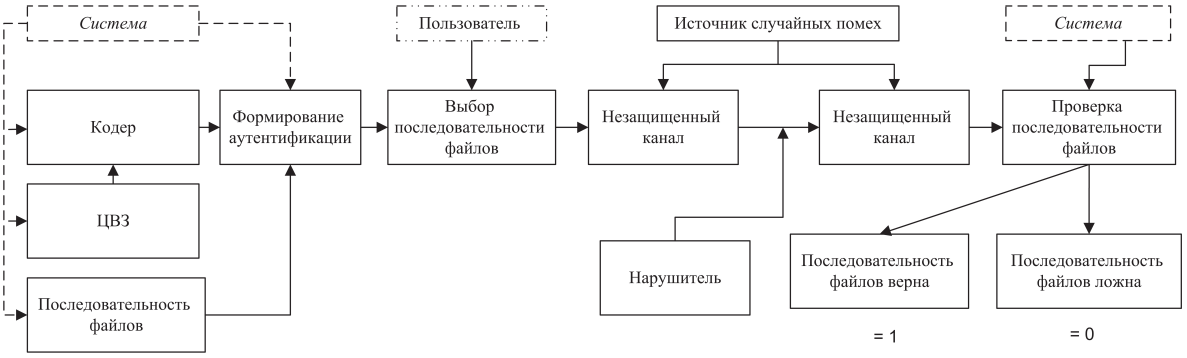


Рис. 1. *Модель системы ЦВЗ для аутентификации*

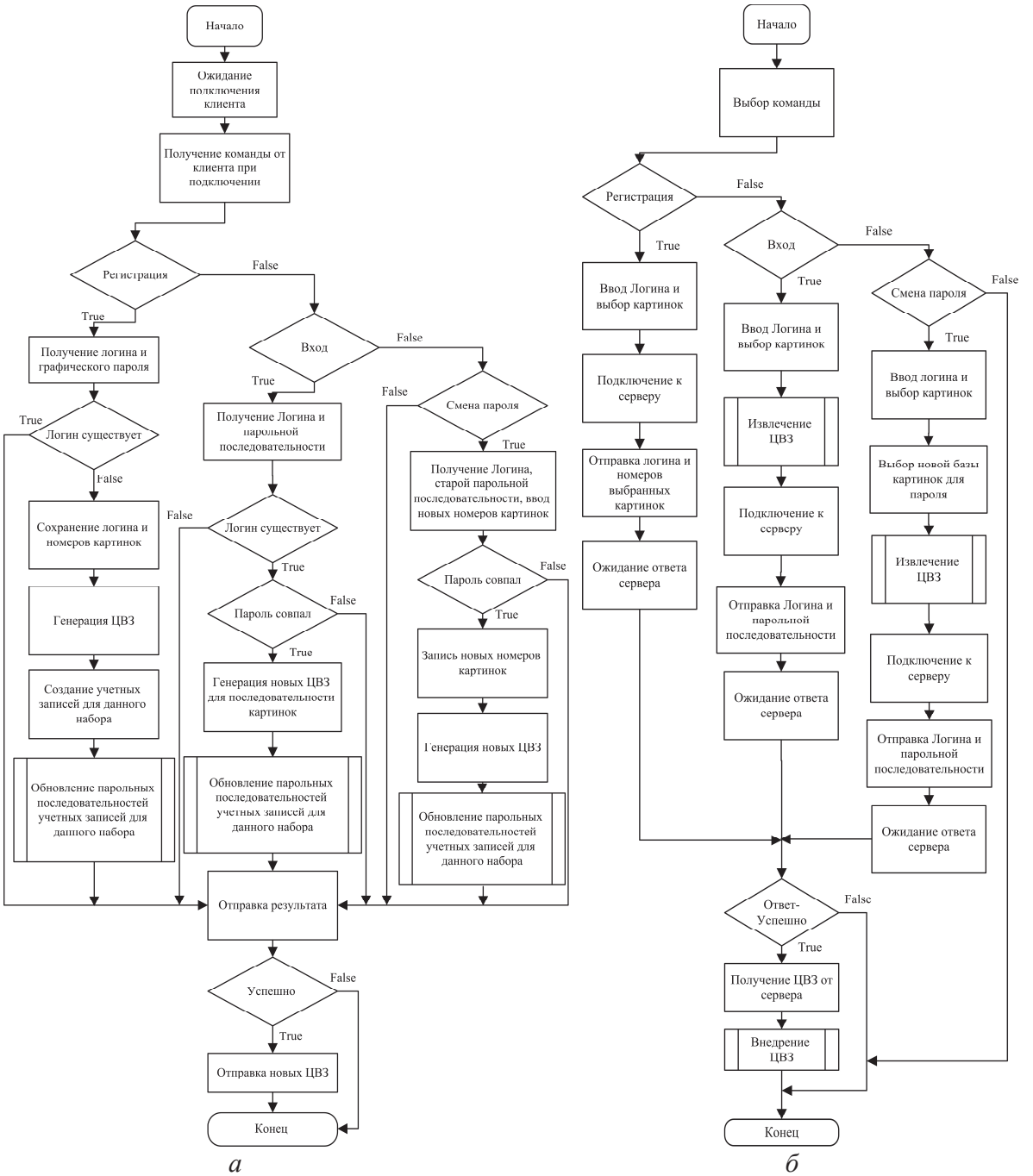


Рис. 2. *Блок-схема алгоритма работы системы графического пароля на основе пиктограмм: а) сервер; б) клиент*

тограмм при авторизации пользователя показаны на рис. 2.

Описание алгоритма работы сервера графического пароля на основе пиктограмм:

1. При запуске программа находится в режиме ожидания подключения клиента.
2. При подключении клиента к серверу сервер ожидает команду от клиента.
3. Действия на предъявленную клиентом команду.

Регистрация. Сервер считывает присланные клиентом логин и номера картинок. Далее сервер сравнивает логин, предложенный клиентом, с имеющимися в базе данных учетными записями пользователей. Если такой логин уже существует, то сервер не регистрирует нового пользователя. Если учетной записи с таким логином не существует, то сервер заносит в базу данных новую запись с данным логином и предложенными номерами картинок:

- генерирует последовательность, которая будет являться ЦВЗ;
- выбирает список учетных записей, которые базируются на том же наборе картинок;

- последовательно проходит все эти записи в базе данных, меняя парольную последовательность на новую в соответствии со сгенерированными ЦВЗ и номерами картинок.

Авторизация. Сервер считывает присланные клиентом логин и парольную последовательность. Далее сервер ищет в базе данных аккаунтов учетную запись с таким логином, и если такая учетная запись существует, то сравнивает присланный пароль с хранящимся в базе данных. Если проверка прошла успешно, то сервер:

- генерирует последовательность, которая будет являться ЦВЗ;
- выбирает список учетных записей, которые базируются на том же наборе картинок;
- последовательно проходит все эти записи в базе данных, меняя парольную последовательность на новую в соответствии со сгенерированными ЦВЗ и номерами картинок.

Смена пароля. Сервер считывает присланные клиентом логин, парольную последовательность и номера картинок, соответствующих новому паролю. Далее сервер ищет в базе данных аккаунтов учетную запись с таким логином и, если такая учетная запись существует, сравнивает присланный пароль с хранящимся в базе данных. Если проверка прошла успешно, то сервер:

- заменяет в базе данных у данной учетной записи номера картинок на новые;
- генерирует последовательность, которая будет являться ЦВЗ;
- выбирает список учетных записей, которые базируются на том же наборе картинок;
- последовательно проходит все эти записи в базе данных, меняя парольную последовательность на новую в соответствии со сгенерированными ЦВЗ и номерами картинок.

4. Сервер отправляет клиенту ответ на его команду. Если запрашиваемая команда прошла успешно, то сервер отправляет сгенерированную на предыдущем этапе последовательность ЦВЗ.

Алгоритм работы клиента заключается в следующем:

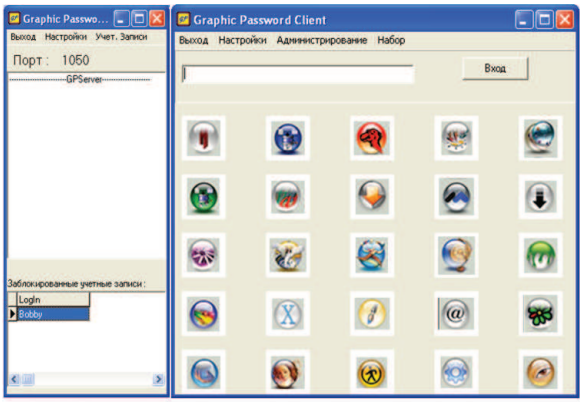
1. Клиент определяет команду для отправки серверу.
2. Действия клиента в соответствии с выбранной командой.

Регистрация. На данном этапе происходит ввод пользователем желаемого логина и картинок. Далее клиент подключается к серверу и передает ему введенный логин и номера картинок, после чего ожидает ответа сервера.

Авторизация. На клиенте вводится логин и выбираются картинки. По нажатию на соответствующую картинку формируется пароль на основе извлеченных из картинок скрытых данных. Клиент подключается к серверу и передает ему логин и пароль, после чего ожидает ответа от сервера.

Смена пароля. На клиенте вводится логин и формируется пароль на основе выбранных картинок. Далее клиент просит ввести новый пароль и регистрирует уже номера введенных картинок. Клиент подключается к серверу и передает ему логин, пароль и номера картинок, после чего ожидает ответа от сервера.

3) При получении ответа от сервера регистрируется результат выполнения команды, и в случае успешного выполнения команды клиент принимает от сервера новую последовательность ЦВЗ. Клиент внедряет в используемый набор картинок присланную последовательность.



а *б*

Рис. 3. *Программа: а) сервер; б) программа-клиент перед началом работы*

Внешний вид полученной системы графического пароля на основе пиктограмм представлен на рис. 3.

Следующей реализацией системы графического пароля является реализация с применением графического файла с множеством деталей.

Обобщенная блок-схема алгоритма работы представлена на рис. 4.

Описание алгоритма:

1. При запуске программа находится в режиме ожидания подключения клиента.
2. При подключении клиента к серверу сервер ожидает команду от клиента.
3. Действия на предъявленную клиентом команду.

Регистрация. Сервер считывает присланные клиентом логин и координаты по осям X и Y. Далее сервер сравнивает логин, предложенный клиентом, с имеющимися в базе данных учетными записями пользователей. Если такой логин уже существует, то сервер не регистрирует нового пользователя. Если учетной записи с таким логином не существует, то сервер

- заносит в базу данных новую запись с данным логином и последовательностями X и Y;
- генерирует последовательность, которая будет являться ЦВЗ;
- заносит сгенерированный ЦВЗ в базу данных.

Авторизация. Сервер считывает присланные клиентом логин и парольные последовательности X и Y. Далее сервер ищет в базе данных аккаунтов учетную запись с таким логином и, если такая учетная запись существует, сравнивает присланный пароль с

хранящимся в базе данных. В случае успешной проверки сервер выполняет следующие действия:

- генерирует последовательность, которая будет являться ЦВЗ;
- заменяет у данной учетной записи в базе данных строку, соответствующую ЦВЗ на сгенерированную.

Смена пароля. Сервер считывает присланные клиентом логин, старые и новые парольные последовательности X и Y. Далее сервер ищет в базе данных аккаунтов учетную запись с таким логином и если такая учетная запись существует, то сравнивает присланный пароль с хранящимся в базе данных. Если проверка прошла успешно, то сервер:

- заменяет в базе данных у данной учетной записи старые последовательности, соответствующие X и Y, на новые;
- генерирует последовательность, которая будет являться ЦВЗ;
- заменяет у данной учетной записи в базе данных строку, соответствующую ЦВЗ, на сгенерированную.

Рис. 4. *Блок-схема алгоритма работы системы графического пароля на основе графического файла со множеством деталей: а) сервер; б) клиент*

4. Сервер отправляет клиенту ответ на его команду. Если запрашиваемая команда прошла успешно, то сервер отправляет сгенерированную на предыдущем этапе ЦВЗ.

Данную версию графического пароля можно усилить путем применения алгоритмов теории распознавания образов. Так как в данной реализации используются картинки, то можно сравнивать эталон с предъявляемой картинкой по составляющим rgb каждого пикселя картинки. Тогда на третьем этапе работы сервера появятся дополнительные блоки, соответствующие сравнению rgb-составляющих, а в базе данных аккаунтов необходимо создать BLOB-поле для хранения эталона.

Алгоритм работы клиента:

1. Клиент определяет, какую команду необходимо отправить серверу.
2. Действия клиента в соответствии с выбранной командой.

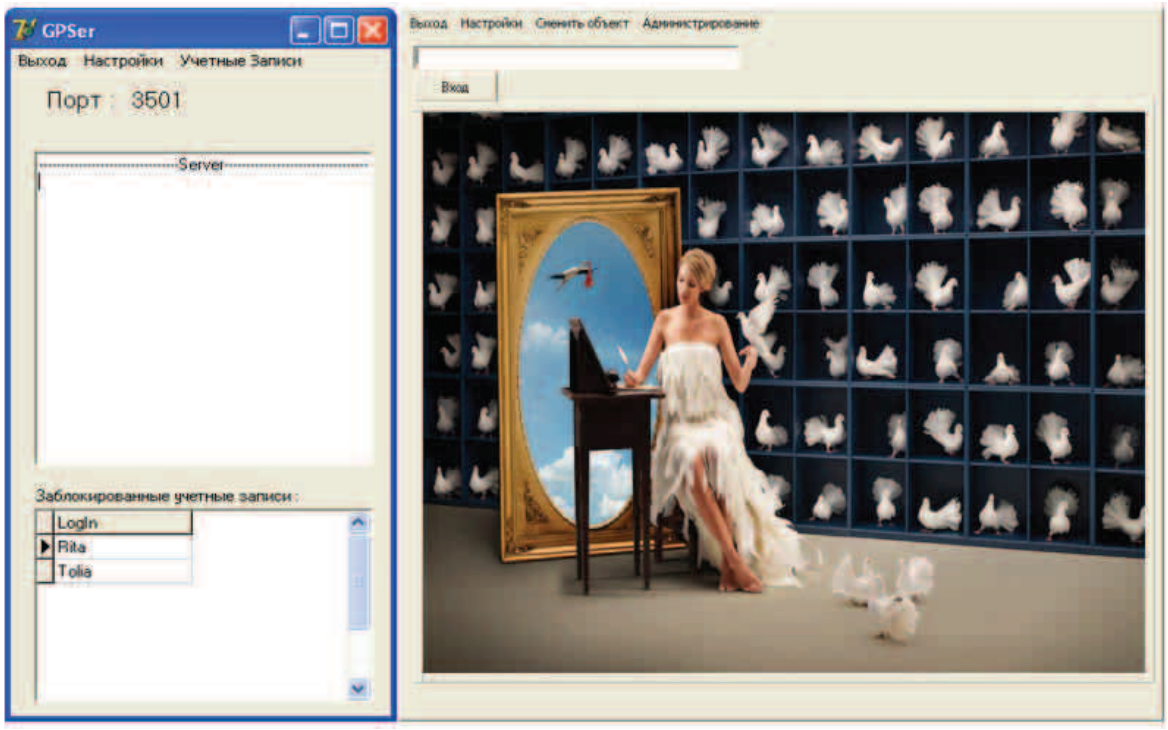
Регистрация. На данном этапе происходит ввод пользователем желаемого логина и точек на изображении. Далее клиент подключается к серверу и передает ему введенный логин и последовательности X и Y, после чего ожидает ответа сервера.

Авторизация. На клиенте вводится логин и точки на изображении. По нажатию на соответствующую точку формируется двойной пароль на основе координат точек, указанных пользователем, также из изображения извлекаются скрытые данные. Клиент подключается к серверу и передает ему логин, пароль и ЦВЗ, после чего ожидает ответа от сервера.

Таблица. *Данные, полученные опытным путем в реализациях систем графического пароля*

Показатель	Пиктограммы	Изображение	Изображение с распознаванием образа
Мощность по графическим данным	минимальная: 421900 максимальная: $1{,}335 \cdot 10^{13}$	минимальная: $3{,}034 \cdot 10^{16}$ максимальная: $2{,}846 \cdot 10^{38}$	минимальная: $3{,}034 \cdot 10^{16}$ максимальная: $2{,}846 \cdot 10^{38}$
Мощность пространства паролей по ЦВЗ	минимальная: $7{,}602 \cdot 10^{17}$ максимальная: $5{,}275 \cdot 10^{41}$	$8{,}587 \cdot 10^{19}$	$8{,}587 \cdot 10^{19}$
Время авторизации (часы:минуты:секунды)	00:00:00,466	00:00:00,48	00:02:29,771
Среднее и максимальное время набора пароля в мин	00:00:02,505 00:00:06,199	00:00:03,129 00:00:06,029	00:00:03,129 00:00:06,029
Хранение пароля	64-битное кодирование		
Ограничения на количество попыток ввода пароля	3	3	3
Блокирование учетной записи	Да		

Смена пароля. На клиенте вводится логин и формируется пароль на основе указанных пользователем точек. Далее клиент просит ввести новый пароль и регистрирует новые точки на картинке.



а *б*

Рис. 5. *Реализация системы графического пароля с применением графического файла с множеством деталей: а) сервер; б) программа-клиент*

Клиент подключается к серверу и передает ему логин, ЦВЗ и парольные последовательности, после чего ожидает ответа от сервера;

3. При получении ответа от сервера регистрируется результат выполнения команды, и в случае успешного выполнения команды клиент принимает от сервера новую последовательность ЦВЗ. Клиент внедряет в используемое изображение присланную последовательность.

При усилении данной реализации графического пароля с применением распознавания образов на клиентской части алгоритм работы будет заключаться в загрузке изображения в память, последовательном переборе всех пикселей и отправке rgb-составляющих каждого пикселя на сервер.

При тестировании реализаций систем графического пароля были получены опытным путем данные, представленные в таблице.

В приведенных реализациях систем графических паролей использована защита пароля стеганографическим методом – встраивание ЦВЗ, который генерируется случайным образом из алфавита мощностью 97 символов латинского, русского алфавита, цифровых и специальных символов. Внедряемые данные имеют небольшой объем, а предъявляемые к ним требования минимальны [17, 18]: заголовки вносят незначительные искажения и устойчивы к основным геометрическим преобразованиям; парольная последовательность, состоящая из набора ЦВЗ, хранится в базе данных аккаунтов в зашифрованном виде по алгоритму 64-битного кодирования, а для варианта графического пароля на основе изображения со множеством деталей зашифровываются также последовательности, соответствующие точкам входа пользователя [19].

Использование ЦВЗ в системах графических паролей показывает, что атаки на данные системы более сложные в реализации [20] и совершенно отличаются от атак на привычные и часто используемые символьные системы. Следовательно, системы графического пароля с использованием ЦВЗ имеют ряд преимуществ, таких как увеличение стойкости систем идентификации/аутентификации к взломам злоумышленниками, быстрое запоминание пароля пользователем, а также уменьшение времени авторизации в системах разграничения доступа.

СПИСОК ЛИТЕРАТУРЫ

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др. / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.
2. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.
3. Основы информационной безопасности / А.А. Шелупанов, В.П. Лось, Р.В. Мещеряков, Е.Б. Белов. – М.: Горячая линия – Телеком, 2006. – 544 с.
4. Sobrado L., Birget J.C. Graphical passwords // The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research. – 2002. – V. 4. – P. 152–158.
5. Davis D., Monrose F., Reiter M.K. On user choice in graphical password schemes. Thirteenth Usenix Security Symposium. – San Diego, CA, USA, Aug. 9–13, 2004. URL: http://www.usenix.org/events/sec04/tech/davis.html (дата обращения: 21.02.2006).
6. Authentication using graphical passwords: Effects of tolerance and image choice / S. Wiedenbeck, J. Waters, J.C. Birget, A. Broditskiy, N. Memon. URL: http://clam.rutgers.edu/birget/grPssw/index.html (дата обращения: 15.10.2006).
7. Шокарев А.В. Использование цифровых водяных знаков для аутентификации передаваемых сообщений // Вестник СибГАУ «Системная интеграция и безопасность». – 2006. – Спец. выпуск. – С. 123–127
8. Шокарев А.В., Шелупанов А.А. Использование компьютерной стеганографии для аутентификации пользователей // Научная сессия ТУСУР – 2006: Материалы докладов Всеросс. научно-техн. конф. студентов, аспирантов и молодых ученых. – Томск: ТУСУР, 2006. – С. 173–176
9. Шокарев А.В., Шелупанов А.А. Аутентификация пользователей в защищенном документообороте на основе цифровых водяных знаков // Прогрессивные технологии и экономика в машиностроении: Труды IV Всеросс. научно-практ. конф. – Томск: Изд. ТПУ, 2006. – Т. 2 – С. 20–22.
10. Шокарев А.В. Графические пароли с использованием методов стеганографии // Инновационные технологии и экономика в машиностроении: Труды VII Всеросс. научно-практ. конф. с междунар. участием. – Томск: Изд-во Томского политехнического университета, 2009. – С. 293–299.
11. Стеганография, цифровые водяные знаки и стеганоанализ / А.В. Аграновский, А.В. Балакин, В.Г. Грибунин, С. Сапожников. – М.: Вузовская книга, 2009. – 220 с.
12. Fridrich J. Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes // Information Hiding: VI International Workshop, LNCS. – Berlin, Heidelberg: Springer-Verlag, 2004. – V. 3200. – P. 67–81.
13. Шелупанов А.А., Шокарев А.В. Теоретико-информационный и теоретико-сложностный подходы для оценки стойкости стеганографических систем // Вестник СибГАУ «Системная интеграция и безопасность». – Красноярск, 2006. – Спец. выпуск. – С. 121–123.
14. Cachin C. An information-theoretic model for steganography // Information Hiding. II International Workshop, LNCS. – Berlin, Heidelberg: Springer-Verlag, 1998. – V. 1525. – P. 306–318.
15. Ker A. General Framework for Structural Steganalysis of LSB Replacement // VII International Workshop on Information Hiding. – Berlin, Springer-Verlag, 2005. – V. 3727. – P. 296–311.
16. Барсуков В.С. Стеганографические технологии защиты документов, авторских прав и информации // Обзор специальной техники. – 2000. – № 2. – С. 31–40.
17. Craver S. On public-key steganography in the presence of an active warden // Information Hiding, II International Workshop. – Portland, Oregon: Springer, 1998. – V. 1525. – P. 355–368.
18. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. – М.: Солон-Пресс, 2002. – 272 с.
19. Основы компьютерной стеганографии / А.В. Аграновский, П.Н. Девянин, Р.А. Хади, А.В. Черемушкин. – М.: Радио и связь, 2003. – 152 с.
20. Коханович Г.Ф., Пузыренко А.Ю. Компьютерная стеганография. Теория и практика. – К.: МК-Пресс, 2006. – 288 с.

Поступила 18.12.2013 г.

UDC 004.056.53

APPLICATION OF DIGITAL WATER MARKS FOR DEVELOPING GRAPHICAL PASSWORD SYSTEMS

Aleksey V. Shokarev,
Cand. Sc., Yurga Institute of Technology (Affiliate) of Tomsk Polytechnic University, 26, Leningradskaya street, Yurga, 652055, Russia.
E-mail: Shokarev_AV@mail.ru

The relevance of the work consists in increasing the security of protected resources with the passage of identification/authentication of users by means of graphic password, which can be achieved through the application of methods of steganography.
The main aim of the study *is to improve the reliability of user identification/authentication applying a graphical password system using digital watermarking. Application of steganography methods increases system resistance to the majority of known methods of hacking systems with password authentication.*
The methods used in the study: *the methods of probability theory, mathematical analysis and experimental studies of steganography. Software implementation of the method was performed using a programming environment Borland C + +.*
The results: *The paper introduces the possibility of creating a system of graphical passwords using steganography techniques, in particular digital watermarks, which are used in the systems of identification/authentication as one-time passwords for authentication and user access to protected resources. The author also introduces the basic block diagrams for implementing two graphical password systems, the first one is icon-based, the second uses an image file with many details. The author has proved empirically the effectiveness of applying the given password systems with respect to the common password authentication methods. A user just remembers the sequence of icons or sequence of keystrokes on a graphic file, but not the complex password sequences. The system changes automatically the passwords without user intervention in the process. But as an option a user can change the order of icons or areas of clicks on an image file to login. The use of the proposed algorithms allows you to create a stable system identification/authentication, and reduce time-remember passwords and authorization of users in systems that require login and password.*

Key words:
Graphical password system, digital watermark, implementation techniques of graphical password systems, steganography, identification/authentication of users.

REFERENCES

1. Afanasev A.A., Vedenev L.T., Vorontsov A.A. *Autentifikatsiya. Teoriya i praktika obespecheniya bezopasnogo dostupa k informatsionnym resursam* [Authentication. Theory and practice of providing secure access to information resources]. Ed. A.A. Shelupanov, S.L. Gruzdev, Yu.S. Nakhaev. Moscow, Goryachaya liniya – Telekom Publ., 2009. 552 p.
2. Zegzhda D.P., Ivashko A.M. *Osnovy bezopasnosti informatsionnykh system* [Fundamentals of Information Systems Security]. Moscow, Goryachaya liniya – Telekom Publ., 2000. 452 p.
3. Shelupanov A.A., Los V.P., Meshcheryakov R.V., Belov E.B. *Osnovy informatsionnoy bezopasnosti* [Fundamentals of Information Security]. Moscow, Goryachaya liniya – Telekom Publ., 2006. 544 p.
4. Sobrado L., Birget J.C. Graphical passwords. *The Rutgers Scholar, an Electronic Bulletin for Undergraduate Research*, 2002, vol. 4, pp. 152–158.
5. Davis D., Monrose F., Reiter M.K. On user choice in graphical password schemes. *Thirteenth Usenix Security Symposium*. San Diego, CA, USA, Aug. 9–13, 2004. Available at: http://www.usenix.org/events/sec04/tech/davis.html (accessed 21 February 2006).
6. Wiedenbeck S., Waters J., Birget J.C., Broditskiy A., Memon N. *Authentication using graphical passwords: Effects of tolerance and image choice*. Available at: http://clam.rutgers.edu/birget/grPssw/index.html (accessed 15 October 2006).
7. Shokarev A.V. Ispolzovanie tsifrovykh vodyanykh znakov dlya autentifikatsii peredavaemykh soobshcheniy [The use of digital watermarking for authentication of messages transmitted]. *Vestnik SibGAU. Sistemnaya integratsiya i bezopastnost – Herald of SibSAU. System integration and security*, 2006, Spec. Iss., pp. 123–127.
8. Shokarev A.V., Shelupanov A.A. Ispolzovanie kompyuternoy steganografii dlya autentifikatsii polzovateley [Using computer steganography for user authentication]. *Naucnaya sessiya TUSUR. Materialy dokladov Vserossiyskoy nauchno-technikheskoy konferentsii studentov, aspirantov i molodykh uchenykh* [Scientific session TUSUR-2006 Proceedings of the Russian scientific and technical conference of students and young scientists]. Tomsk, 2006, pp. 173–176.
9. Shokarev A.V., Shelupanov A.A. Autentifikatsiya polzovateley v zashchishchennom dokumentooborote na osnove tsifrovykh vodyanykh znakov [User authentication in a secure workflow based on digital watermarking]. *Progressivnye tekhnologii i ekonomika v mashinostroenii. Trudy IV Vserossiyskoy nauchno-prakticheskoy konferentsii* [Progressive Technologies in Mechanical Engineering and Economics. Proc. IV All-Russian scientific-practical conference]. Tomsk, 2006, vol. 2, pp. 20–22.
10. Shokarev A.V. Graficheskie paroli s ispolzovaniem metodov steganografii [Graphical passwords using steganography methods]. *Innovatsionnye tekhnologii i ekonomika v mashinostroenii. VII Vserossiyskaya nauchno-prakticheskaya konferentsiya s mezhdunarodnym uchastiem* [Innovative technologies in mechanical engineering and economics. Proc. VII All-Russian scientific and practical conference with international participation]. Tomsk, 2009. pp. 293–299.
11. Agranovskiy A.V., Balakin A.V., Gribunin V.G., Sapozhnikov S. *Steganografiya, tsifrovye vodyanye znaki i steganoanaliz* [Steganography, digital watermarks, steganalysis]. Moscow, Vuzovskaya kniga Publ., 2009. 220 p.
12. Fridrich J. Feature-Based Steganalysis for JPEG Images and its Implications for Future Design of Steganographic Schemes. *Information Hiding. VI International Workshop, LNCS*. Berlin, Heidelberg, Springer-Verlag 2004. Vol. 3200, pp. 67–81.
13. Shelupanov A.A., Shokarev A.V. Teoretiko-informatsionny i teoretiko-slozhnostny podkhody dlya otsenki stoykosti steganograficheskikh system [Information-theoretic and complexity-theoretic approaches for assessing resistance of steganographic systems]. *Vestnik SibGAU. Sistemnaya integratsiya i bezopastnost – Herald of SibSAU. System integration and security*, 2006, Spec. Iss., pp. 121–123.
14. Cachin C. An information-theoretic model for steganography. *Information Hiding. II International Workshop, LNCS*. Berlin, Heidelberg, Springer-Verlag, 1998. Vol. 1525, pp. 306–318.

15. Ker A. General Framework for Structural Steganalysis of LSB Replacement. *VII International Workshop on Information Hiding*. Berlin, Springer-Verlag, 2005. Vol. 3727, pp. 296–311.
16. Barsukov V.S. Steganograficheskie tekhnologii zashchity dokumentov, avtorskikh prav i informatsii [Steganographic security technology for documents, copyrights and information]. *Obzor spetsialnoy tekhniki*, 2000, no. 2, pp. 31–40.
17. Craver S. On public-key steganography in the presence of an active warden. *Information Hiding, II International Workshop*. Portland, Oregon, 1998, vol. 1525, pp. 355–368.
18. Gribunin V.G., Okov I.N., Turintsev I.V. *Tsifrovaya steganografiya* [Digital steganography]. Moscow, Solon-Press Publ., 2002. 272 p.
19. Agranovskiy A.V., Devyanin P.N., Khadi R.A., Cheremushkin A.V. *Osnovy kompyuternoy steganografii* [Fundamentals of computer steganography]. Moscow, Radio i svyaz Publ., 2003. 152 p.
20. Kokhanovich G.F., Puzyrenko A.Yu. *Kompyuternaya steganografiya. Teoriya i praktika* [Computer steganography. Theory and practice]. Kiev, MK-Press Publ., 2006. 288 p.

УДК 004.4::004.85[3+5]

АВТОМАТИЧЕСКАЯ СИСТЕМА МЕТА-ОБУЧЕНИЯ С ПОДДЕРЖКОЙ ВЫБОРА ОПТИМАЛЬНОГО АЛГОРИТМА РЕШЕНИЯ ЗАДАЧИ И ВЫЧИСЛЕНИЯ ОПТИМАЛЬНЫХ ПАРАМЕТРОВ ЕГО ФУНКЦИОНИРОВАНИЯ

Орлов Андрей Александрович,
ассистент каф. промышленной электроники Томского Государственного Университета Систем Управления и Радиоэлектроники,
634050, Россия, Томск, пр. Ленина, д. 40. Email: d1scnc@gmail.com

Актуальность исследования *обусловлена необходимостью повышения эффективности работы автоматических систем интеллектуального анализа данных, основанных на мета-обучении.*
Цель исследования *состоит в разработке автоматической системы мета-обучения с поддержкой выбора оптимального алгоритма решения задачи и вычисления оптимальных параметров его функционирования.*
Методы исследования: *индуктивное моделирование, методы статистической обработки результатов.*
В результате исследования *проведена систематизация известных систем мета-обучения на основании выработанных классификационных признаков, учитывающих внутреннюю организацию систем. Сформулированы требования к реализации автоматической системы мета-обучения. Предложен способ построения системы мета-обучения, удовлетворяющей всем сформулированным требованиям и производящей накопление мета-знаний, построение на их основе мета-моделей, выбор оптимального алгоритма из набора доступных и вычисление оптимальных параметров его функционирования. Разработана объектно-ориентированная архитектура программной платформы для реализации любой из систем мета-обучения, представленных в систематизации. Эффективность реализованной автоматической системы мета-обучения с использованием алгоритмов методов группового учета аргументов проверена экспериментально при решении набора задач, относящихся к классу задач прогнозирования временных последовательностей (1428 временных последовательностей из тестового набора, известного под названием «M3 Competition»).*

Ключевые слова:
Мета-обучение, мета-характеристики данных, мета-модель, программная платформа, объектно-ориентированный анализ и проектирование, прогнозирование временных последовательностей, метод группового учета аргументов.

Введение

Задачей Интеллектуального Анализа Данных (ИАД, в англоязычной литературе используется термин «Data Mining») является обнаружение (извлечение) в доступных исследователю исходных данных ранее неизвестных, неочевидных, но практически полезных знаний [1]. В настоящее время существует большое количество алгоритмов искусственного интеллекта (включая машинное обучение), математической статистики, оптимизации и прогнозирования и пр., применяемых для решения задачи ИАД: искусственные нейронные сети, генетические алгоритмы, деревья решений, алгоритмы нечеткой логики, корреляционный и регрессионный анализ и т. д. Каждый из существующих алгоритмов показал свою эффективность при решении разнообразных практических задач. Однако в работе [2] было показано, что не существует единственного алгоритма, способного максимально эффективно решать задачу ИАД во всех возможных практических применениях, поэтому решение каждой новой практической задачи требует привлечения некоторых экспертных знаний для выбора наиболее подходящего алгоритма из числа доступных.

В работе [3] был формализован подход к проблеме выбора алгоритма (рис. 1): на основании набора мета-характеристик (meta-features, MF) $f(x) \in F$ (F – пространство мета-характеристик) для выборки данных x из пространства проблем (задач) X функция $S(f(x))$ («selection mapping») производит выбор такого алгоритма a из пространства доступных алгоритмов A таким образом, что его эффективность $p(a,x)$ («performance mapping») на