УДК 621.391

ОЦЕНКА УРОВНЯ ЗАЩИЩЕННОСТИ СРЕДСТВА АУТЕНТИФИКАЦИИ ПО РАДУЖНОЙ ОБОЛОЧКЕ ГЛАЗА

П.М. БУЙ, М.В. ЛАСТОВСКАЯ

Белорусский государственный университет транспорта
ул. Кирова, 34, Гомель 246653, Беларусь

Поступила в редакцию 9 октября 2010

Рассматривается алгоритм работы средства аутентификации по радужной оболочке глаза. Производится вывод аналитической формулы для расчета вероятности пропуска «чужого» субъекта данным средством аутентификации с первой попытки. Приводится пример расчета вероятности пропуска «чужого» с первой попытки при заданных значениях порога меры близости.

Ключевые слова: средство аутентификации, радужная оболочка глаза, вероятность пропуска «чужого» субъекта.

Введение

Средство аутентификации – это программный модуль или аппаратно-программное устройство, которое обеспечивает проверку подлинности субъекта, т.е. устанавливает, является ли он тем, за кого себя выдает.

Процесс проверки подлинности субъекта зависит от метода, который используется в средстве аутентификации. Известные методы опознания объединены в три класса, которые базируются на:

а) условных, заранее присваиваемых признаках (сведениях), известных субъекту (что знает субъект);

б) физических средствах, действующих аналогично физическому ключу (что имеет субъект);

в) индивидуальных характеристиках субъекта, его физических данных, позволяющих выделить его среди других лиц (что присуще субъекту) [1].

В средствах аутентификации, относящихся к первым двум классам, проверка подлинности субъекта осуществляется на основании предоставляемого им пароля или ключа. В средствах аутентификации третьего класса, проверка подлинности субъекта осуществляется на основании предоставляемого им биометрического признака.

В процессе проверки субъекта предоставляемый им пароль или ключ либо идентичен эталонному, хранящемуся в базе данных средства аутентификации, в результате чего субъект считается подлинным, либо не идентичен, в результате чего субъект считается ложным.

Биометрические средства аутентификации отличаются тем, что предоставляемый субъектом биометрический признак никогда не будет полностью идентичен эталонному признаку. Для данного класса средств аутентификации вводится понятие меры близости предоставляемого признака с эталонным [2]. Для принятия решения об аутентичности субъекта используется понятие порога меры близости. Порог меры близости – это критическое значение меры близости предоставляемого субъектом признака с эталонным, которое разделяет субъектов на «своих» и «чужих».

Алгоритм сканирования радужной оболочки глаза

Алгоритм сканирования радужной оболочки глаза состоит из следующих этапов.

Этап 1. Автоматический захват изображения. Средство аутентификации оснащено неподвижной камерой, поэтому субъект сам позиционируется в пространстве. Он устанавливается в положение для регистрации при помощи фиксатора взгляда – элемента, который видим только при определенном положении глаза. Субъект помещает свой глаз на дистанцию распознавания, которая составляет 45–55 см от камеры.

Роговица глаза отражает окружающие предметы и, тем самым, перекрывает картину радужки, создавая сильные вариации яркости изображения. Поэтому необходимо использовать собственную подсветку, которая дает в области регистрации радужки освещенность в несколько раз превышающую ту, что создается посторонними источниками. Видимый свет с такой интенсивностью вызывает большое неудобство. Поэтому используется инфракрасная подсветка.

Далее происходит процесс фотографирования захваченного изображения.

Этап 2. Выделение радужной оболочки глаза на изображении. На этом этапе осуществляется поиск на изображении относительно темного объекта, близкого по форме к кругу, содержащего внутри себя концентрический еще более темный объект, зрачок.

На процесс получения изображения в минимальной степени влияет угол освещения. На полученные результаты не оказывают воздействия такие характеристики, как расовые различия, выражающиеся в очень темных глазах или их узком разрезе. Аутентификация успешно проводится сквозь очки или контактные линзы, а также в темноте с использованием инфракрасной подсветки.

Этап 3. Нормирование размеров изображения радужной оболочки глаза. Нормирование размеров изображения радужки производится по двум причинам: различие масштабов снимков и изменение относительного размера и формы зрачка. Нормирование к единому масштабу производится исходя из полученного на предыдущем этапе эллипса – внешнего контура радужки. Задача решается аффинным преобразованием этого эллипса к некоторой заданной окружности. Значительно сложнее устранить вариации, вызванные изменением размеров и формы зрачка. Это производится перемещением элементов радужной оболочки глаза при изменении радиуса зрачка.

Этап 4. Наложение на зрачок фиксированной маски полярной системы координат. На нормированное по масштабу изображение радужной оболочки глаза накладывается фиксированная маска полярной системы координат. Преобразование системы координат происходит путем вычисления дифференциальных признаков вдоль концентрических окружностей.

Этап 5. Бинаризация изображения и запись его в матрицу. Значение каждого пикселя радужной оболочки глаза в точке, соответствующей координатам маски, сравнивается с некоторым заданным порогом и в зависимости от результата сравнения записывается как «0» или «1» в определенное место матрицы.

Этап 6. Сопоставление бинарных матриц. Образ-эталон радужной оболочки, то есть радужной оболочки глаза «своего» субъекта, записывается в память системы в виде файла фиксированного размера. На этапе аутентификации очередного клиента системы, сравнение каждой новой матрицы, полученной по отсканированному изображению, с матрицей-эталоном производится побитно.

Этап 7. Выбор из базы нескольких бинарных матриц, для которых коэффициент взаимной корреляции превышает некоторый заданный порог. В задаче аутентификации субъекта процесс надо повторять для всех образов-эталонов радужной оболочки глаза. В некоторых системах аутентификации из базы выбирают несколько образов-эталонов, которым соответствуют максимальные коэффициенты взаимной корреляции с бинарной матрицей радужной оболочки аутентификатора, превышающие некоторый заданный порог. Так же могут выбираться несколько образов-эталонов, которым соответствуют минимальное расстояние между бинарными матрицами радужных оболочек аутентификатора и каждого образа-эталона, не превышающие некоторый заданный порог.

Этап 8. Выбор бинарной матрицы с максимальным коэффициентом взаимной корреляции. За окончательный результат принимается тот вариант аутентификации, для эталона которого получено максимальное значение коэффициента взаимной корреляции бинарных

матриц или минимальное расстояние между бинарными матрицами среди нескольких выбранных.

На рис. 1 показан алгоритм функционирования средства аутентификации по радужной оболочке глаза.

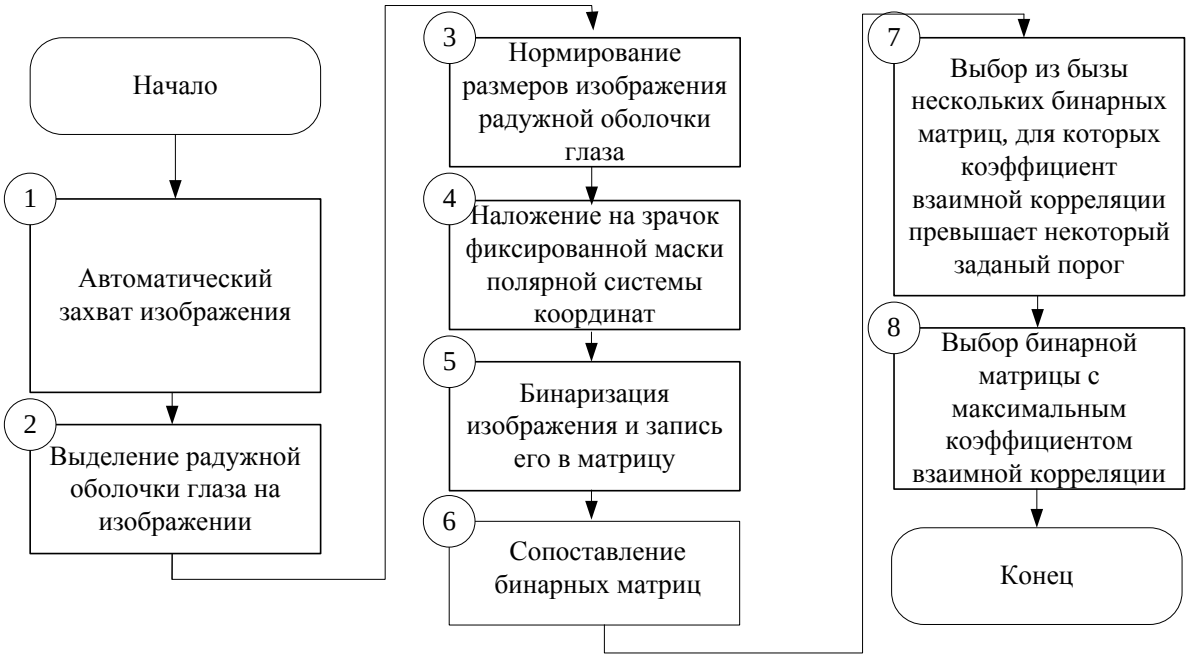

Рис. 1. Алгоритм функционирования средства аутентификации по радужной оболочке глаза

Определение вероятности пропуска «чужого» субъекта

Вероятность пропуска «чужого» субъекта данным средством аутентификации рассчитывается как вероятность совпадения матрицы-эталона радужной оболочки глаза с матрицей радужной оболочки глаза, предоставленной субъектом.

Изображение радужной оболочки глаза в процессе оцифровки формируется в матрицу, которую можно представить в виде бинарной последовательности размером B байт.

Для установления совпадения изображений радужной оболочки глаза используют порог меры близости D, который может принимать значения от 0 до 1 (от 0 до 100 %).

Изображения радужной оболочки глаза будут считаться идентичными, если матрица-эталон радужной оболочки глаза будет совпадать побитно с матрицей радужной оболочки глаза, представленной субъектом, с долей совпавших битов, большей или равной заданному порогу меры близости.

Вероятность того, что одна пара бит в матрицах совпадет будет определяться по следующей формуле:

$$p = P_{00} + P_{11}, \quad (1)$$

где P_{00} – вероятность появления двух нулей в одной паре бит в матрицах; P_{11} – вероятность появления двух единиц в одной паре бит в матрицах.

Тогда, вероятность того, что одна пара бит в матрицах не совпадет будет определяться по следующей формуле:

$$q = P_{01} + P_{10}, \quad (2)$$

где P_{01} – вероятность появления нуля и единицы в одной паре бит в матрицах; P_{10} – вероятность появления единицы и нуля в одной паре бит в матрицах.

Так как бинарные элементы могут принимать значения только нуля и единицы и эти события не являются зависимыми друг от друга, то вероятность появления единицы или нуля в бите будут равны между собой и примут значение, равное 0,5.

Тогда вероятности P_{00}, P_{11}, P_{01}, P_{10} будут равны между собой и примут значение, равное $0{,}5^2 = 0{,}25$.

В связи с этим, вероятности p и q, согласно формулам (1) и (2), примут следующие значения:

$$p = q = 0{,}25 + 0{,}25 = 0{,}5.$$

Используя формулу комбинаторики [3], вероятность совпадения двух матриц с долей совпавших битов, равной заданному порогу меры близости, будет определяться по следующей формуле:

$$P_C = \frac{A!}{(\text{int}(A \cdot D)+1)! \cdot (A - (\text{int}(A \cdot D)+1))!} \cdot p^{\text{int}(A \cdot D)+1} \cdot q^{(A-(\text{int}(A \cdot D)+1))}, \quad (3)$$

где A – размер матрицы в битах, $A = B \cdot 8$; $\text{int}(A \cdot D)+1$ – доля совпавших бит в матрицах; $A - (\text{int}(A \cdot D)+1)$ – доля не совпавших бит в матрицах.

В связи с тем, что данный биометрический аутентификатор будет считаться подобранным, если матрицы совпадут с долей совпавших битов, большей или равной заданному порогу меры близости, вероятность подбора аутентификатора будет вычисляться как сумма вероятностей P_c для числа совпавших бит от $\text{int}(A \cdot D)+1$ до A:

$$P_{\text{ПА1}} = \sum_{i=\text{int}(A \cdot D)+1}^{A} \frac{A!}{i! \cdot (A-i)!} \cdot p^i \cdot q^{A-i}. \quad (4)$$

Анализ вероятности пропуска «чужого» субъекта

Рассмотрим на примерах оценку вероятности подбора биометрического образа средством аутентификации по радужной оболочке глаза. Для этого выберем следующие исходные параметры:

1. Объем данных, хранящихся в базе данных для одного человека B примем равным 128, 256, 512 и 1024 байт/глаз или A – 1024, 2048, 4096 и 8192 бит/глаз соответственно.

2. Значение порога меры близости D – равным 0,1, 0,3, 0,4, 0,45, 0,5, 0,55, 0,6, 0,7 и 0,9.

3. Вероятность совпадения одного бита в матрице радужной оболочки, представленной субъектом, с матрицей-эталоном, хранящимся в базе данных средства аутентификации p – равной 0,5.

4. Вероятность несовпадения одного бита в матрице радужной оболочки, представленной субъектом, с матрицей-эталоном, хранящимся в базе данных средства аутентификации q – равной 0,5.

Используя формулу (4) найдем значения вероятности пропуска средством аутентификации по радужной оболочке глаза «чужого» субъекта в результате подбора последним биометрического аутентификатора с первой попытки.

Для порога меры близости (D), равного 0,55, бинарная последовательность размером 512 байт будет состоять из:

$$512 \cdot 8 = 4096 \text{ бит } (A).$$

Минимальная доля совпавших бит в матрицах, которая необходима для пропуска данным средством аутентификации «чужого» субъекта будет равна:

$$N_1 = \text{int}(4096 \cdot 0{,}55) + 1 = 2253.$$

Тогда вероятность подбора аутентификатора с первой попытки, согласно формуле (4), будет равна:

$$P_{\text{ПА1}} = \sum_{i=2253}^{4096} \frac{4096!}{i! \cdot (4096-i)!} \cdot p^i \cdot q^{4096-i} = 7{,}457 \cdot 10^{-11}.$$

Полученные данные, соответствующие заданным параметрам, представлены в таблице.

Значения вероятности пропуска средством аутентификации по радужной оболочке глаза «чужого» субъекта в результате подбора последним биометрического аутентификатора с первой попытки

B, байт/глаз	*D*	$P_{ПА1}$	*B*, байт/глаз	*D*	$P_{ПА1}$
128	0,1	1	512	0,1	1
	0,3	1		0,3	1
	0,4	1		0,4	1
	0,45	0,999		0,45	1
	0,5	0,5		0,5	0,5
	0,55	$7{,}175 \cdot 10^{-4}$		0,55	$7{,}457 \cdot 10^{-11}$
	0,6	$9{,}148 \cdot 10^{-11}$		0,6	0
	0,7	0		0,7	0
	0,9	0		0,9	0
256	0,1	1	1024	0,1	1
	0,3	1		0,3	1
	0,4	1		0,4	1
	0,45	0,999		0,45	1
	0,5	0,5		0,5	0,5
	0,55	$3{,}275 \cdot 10^{-6}$		0,55	0
	0,6	0		0,6	0
	0,7	0		0,7	0
	0,9	0		0,9	0

Зависимость вероятности подбора биометрического аутентификатора от значения порога меры близости представлена на рис. 2.

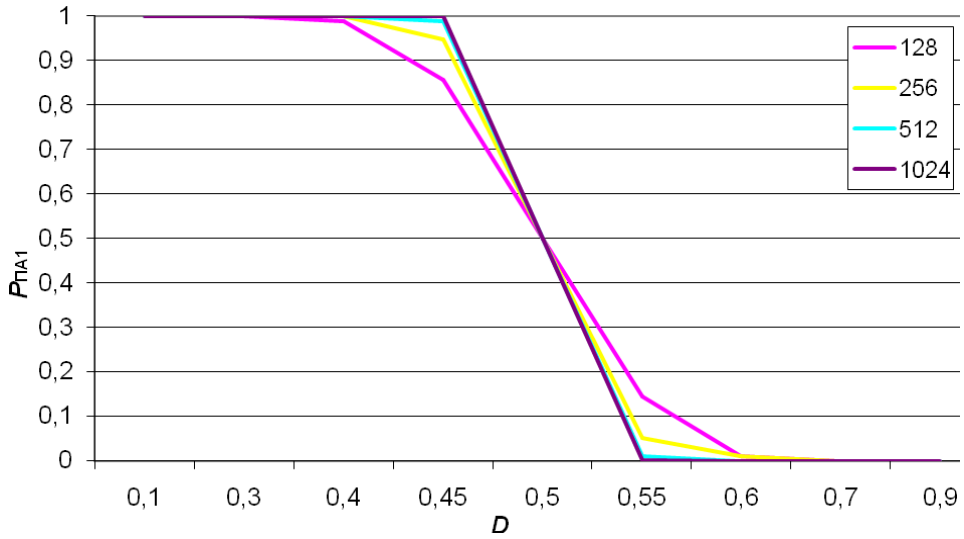

Рис. 2. График зависимости вероятности подбора биометрического аутентификатора от значения порога меры близости

Выводы

Полученная аналитическая формула для расчета вероятности пропуска «чужого» субъекта средством аутентификации по радужной оболочке глаза с первой попытки позволяет произвести анализ эффективности данного средства аутентификации по сравнению с прочими биометрическими и не биометрическими средствами аутентификации.

С увеличением порога меры близости резко уменьшается вероятность пропуска «чужого» субъекта данным средством аутентификации. Для всех исследованных размеров файлов совпадение 50–55% бит матрицы-эталона радужной оболочки глаза с матрицей радужной оболочки глаза, представленной субъектом, будет достаточно для надёжной аутентификации субъектов.

THE LEVEL OF SECURITY ESTIMATION OF THE AUTHENTIFICATION'S MEANS ON THE IRIDESCENT ENVIRONMENT OF THE EYE

P.M. BUI, M.V. LASTOVSKAJA

Abstract

The algorithm of work of the authentification's mean on the iridescent environment of the eye is considered. The conclusion of the analytical formula for account of probability of the «another's» subject passing by the given authentification's mean from the first attempt is made. The example of account of probability of the «another's» passing from the first attempt is resulted at the given importance of the threshold of the affinity measure.

Литература

1. *Бобов М.Н., Конопелько В.К.* Обеспечение безопасности информации в телекоммуникационных системах Минск. 2002.
2. *Кухарев, Г.А.* Биометрические системы: Методы и средства идентификации личности человека. СПб. 2001.
3. *Пугачев В.С.* Введение в теорию вероятностей. Минск. 1968.