



Подделка идентификатора

В случае утери идентификатора легальный пользователь системы должен сообщить об этом в службу безопасности, которая, в свою очередь, вводит в действие второй режим работы системы, при котором во время прохождения процедуры аутентификации необходимо вводить PIN-код.

Злоумышленник может украсть идентификатор и воспользоваться им при прохождении на объект, предоставив его системе. В данном случае, злоумышленник не знает о наличии на оборотной стороне идентификатора дополнительного невидимого QR-кода и не сможет попасть на контролируемую территорию.

Система, находясь во втором режиме работы, попросит субъект ввести PIN-код, который известен только законному пользователю. Нарушитель, попытавшись ввести его, получит отказ.

Возможности использования

Изготовление идентификаторов выполненных по данной технологии является несложным и быстрым процессом. Такие идентификаторы можно напечатать на любом принтере, лишь заменив в нем чернила на инфракрасные.

Перспективным решением является использование данных идентификаторов в качестве одноразовых пропусков на объектах с зонами ограниченного доступа. Контролер может выдавать одноразовые пропуска субъектам запросившим их. В данном случае, субъекту необходимо предоставить свои паспортные данные и сообщить цель визита на объект.

СКУД на основе двухфакторной графической аутентификации применимы во всех организациях, где присутствует необходимость контроля доступа на охраняемую территорию или в зону ограниченного доступа. К таким объектам можно отнести учреждения образования, здравоохранения, транспорта, бизнеса, культуры, жилищно-коммунального хозяйства.

Вывод

В рамках разработки системы двухфакторной графической аутентификации был предложен подход, заключающийся в использовании в качестве идентификатора субъекта технологии QR-кодов. Данная технология позволяет защитить пропуск от подделки, прилагая при этом минимум материальных, физических и финансовых затрат.

Отличительной особенностью подхода является применение на идентификаторе двух QR-кодов, нанесенных на разные стороны пропуска. Защитный QR-код, нанесенный на оборотную сторону является невидимым в обычном (видимом) диапазоне, что позволяет защитить идентификатор от подделки. Данный QR-код возможно считать только в инфракрасном диапазоне.

Предлагаемый подход позволяет не только повысить степень защищенности идентификатора, но и решить проблему стоимости внедрения СКУД, так как является более дешевым.



Литература

1. Ворона В. А. Системы контроля и управления доступом / Ворона В. А., Тихонов В. А. – М.: Горячая линия-Телеком, 2010. - 272 с.
2. Шелупанова А.А. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / А.А. Шелупанова [и др.]. – М.: Горячая линия-Телеком, 2012. – 550 с.
3. QR код [Электронный ресурс]. – Режим доступа: <http://www.qrcc.ru/qrcc.html>
4. Шаньгин В.Ф. Защита информации в компьютерных системах и сетях / В.Ф. Шаньгин. – М.: ДМК Пресс, 2012. – 592 с.
5. Громов Ю.Ю., Тихомирова А.А., Щербинин П.А, Яковлев А.В. Двумерный штрихкод как идентифицирующая метка в системах контроля и управления доступом // «Известия академии инженерных наук им. А.М. Прохорова»: ежеквартальный научно-технический журнал. – М.: Научтехлитиздат, 2013, №1

В.О. Рублевская, В.А. Акулов

ЗАЩИТА ИНФОРМАЦИИ НА ОСНОВЕ КЛАСТЕРИЗАЦИИ ОБЪЕКТОВ: АЛГОРИТМЫ И ПРОГРАММНЫЕ СРЕДСТВА

(Самарский государственный технический университет)

Актуальность и цели.

Объектом исследования являются алгоритмы кластеризации сложных объектов на геоинформационных картах, а так же ограничение доступа к ним [1],[2]. Предметом исследования являлась разработка новых алгоритмов на основе объединения объектов по расстоянию с использованием графов и окружностей.

Цель исследования: разработка программного средства, предназначенного для управления доступом к кластеризованным объектам.

Материалы и методы.

В качестве основного метода защиты информации применено имитационное моделирование. Предусмотрено отображение карт и кластеров на их поверхности с использованием средств библиотеки CesiumJS. Выполнена оценка быстродействия системы.

Результаты.

Решена задача кластеризации групп объектов с использованием графов и окружностей. Каждый из этих способов предусматривает наличие системы безопасности, которая отображает кластеризацию лишь на тех уровнях, которые доступны для просмотра пользователю. Уровень доступа напрямую связан с масштабированием ландшафтной сетки. В общей сложности предусмотрено 25 градаций, что, в свою очередь, обеспечивает высокую гибкость системы и адаптацию к конкретным условиям.



Выводы

1. Разработаны алгоритмы кластеризации объектов по расстоянию с использованием графов и окружностей. Система запускается на сервере, где хранятся необходимые объекты для кластеризации.
2. Предусмотрена защита данных посредством ограничения доступа к уровням для различных пользователей при помощи отображения кластеров лишь на разрешенных уровнях.
3. Решена задача по объединению отдельных объектов в кластеры с помощью графических и аналитических моделей. Построена экспериментальная модель зависимости разбиения кластеров от уровня высоты.
4. Система протестирована на реальной информации. Установлено, что система обладает высоким быстродействием при построении и отображении кластеров на трехмерной карте в Web-интерфейсе.
5. Сформулированы направления дальнейших исследований. В их числе, кластеризация групп объектов, вывод формул для группировки объектов в зависимости от высоты камеры, для расширения диапазона уровней доступа к объектам.

Литература

1. Котов А., Красильников Н. Кластеризация данных, 2006.
2. Воронцов К.В. Алгоритмы кластеризации и многомерного шкалирования. Курс лекций. МГУ, 2007.



В.П. Цветов

О ФАКТОРИЗАЦИИ БИНАРНЫХ ОТНОШЕНИЙ

(Самарский национальный исследовательский университет
имени академика С.П. Королёва)

Теория бинарных отношений, в частности, теория упорядоченных полугрупп бинарных отношений, представляет самостоятельный интерес, а также находит обширные применения, например, в теории графов, теории автоматов, теории кодирования и т.п. [1-2].

В докладе рассматривается представление произвольного бинарного отношения в виде произведения двух бинарных отношений, одно из которых функционально, а второе является обратным к функциональному, что может оказаться полезным при исследовании свойств бинарных отношений и разработке алгоритмов решения прикладных задач.

Введем следующие обозначения и определения.

\mathbb{N} - множество натуральных чисел;

$\mathbb{N}_0 = \mathbb{N} \cup \{0\}$ - множество натуральных чисел с нулем;

$m..n = \{m, m+1, \dots, n\} \subset \mathbb{N}_0$;

$|V|$ - мощность множества V ;

2^V - булеан над множеством V ;

$\chi_{V_1}(v) = \begin{cases} 1, & v \in V_1 \\ 0, & v \notin V_1 \end{cases}$ - индикатор множества $V_1 \in 2^V$;

$V \times U = \{e = (v, u) \mid v \in V, u \in U\}$ - декартово произведение множеств V и U ;

$2^{V \times U}$ - множество бинарных отношений из V в U ;

$I_V = \{(v, v) \mid v \in V\} \in 2^{V \times V}$ - тождественное бинарное отношение на множестве V ;

$R^{-1} = \{(u, v) \mid (v, u) \in R\} \in 2^{U \times V}$ - обратное к бинарному отношению $R \in 2^{V \times U}$;

$R_1 \circ R_2 = \{(v, w) \mid \exists u \in U (v, u) \in R_1 \wedge (u, w) \in R_2\} \in 2^{V \times W}$ - произведение бинарных отношений $R_1 \in 2^{V \times U}$ и $R_2 \in 2^{U \times W}$;

$D_R = \{v \mid \exists u \in U (v, u) \in R\} \in 2^V$ - область определения бинарного отношения $R \in 2^{V \times U}$;

$E_R = \{u \mid \exists v \in V (v, u) \in R\} \in 2^U$ - область значений бинарного отношения $R \in 2^{V \times U}$;

$R \in 2^{V \times U}$ - функционально (функция из V в U), если и только если $R^{-1} \circ R \subseteq I_U$;

$R \in 2^{V \times U}$ - инъективно, если и только если $R \circ R^{-1} \subseteq I_V$;

$R \in 2^{V \times U}$ - тотально, если и только если $D_R = V$;

$R \in 2^{V \times U}$ - сюръективно, если и только если $E_R = U$;

$U^V \in 2^{V \times U}$ - множество тотальных функций из V в U ;