РЕЗЮМЕТА
на научните публикации на доц. д-р Милена Николова Милева-Карова,

катедра "Компютърни науки и технологии", Технически университет - Варна, за участие в конкурс за заемане на академичната длъжност „Професор“, професионално направление 5.3. „Комуникационна и компютърна техника“, учебна дисциплина „Базово програмиране”

За рецензиране в този конкурс са представени **42** публикации (*за изпълнение на минималните национални изисквания по чл.2б, ал. 2 и 3, съответно на изискванията по чл. 2б, ал. 5 на ЗРАСРБ, определени в ППЗРАСРБ*), от които **10** равностойни на монография (хабилитационен труд) научни публикации (не по-малко от 10) в издания, които са реферирани и индексирани в световноизвестни бази данни с научна информация, **2** научни публикации в издания, които са реферирани и индексирани в световноизвестни бази данни с научна информация (Scopus) и **30** научни публикации в нереферирани списания с научно рецензиране или в редактирани колективни томове.
Тези публикации не повтарят представените за придобиване на ОНС „Доктор“ и АД „Доцент“.
Подредбата на публикациите и техните резюмета е направена според представения списък на публикациите (справка съгласно чл. 2б от ЗРАСРБ, чл. 60, ал.3 от ППЗРАСРБ и чл. 1, ал. 2 от ПУРЗАД в ТУ-Варна за изпълнение на минимални национални изисквания за заемане на академичната длъжност „ПРОФЕСОР“ по област на висше образование 5. Технически науки) по конкурса и номерацията в него.

В.4-1

Penev I., M. Karova, M. Todorova, D. Zhelyazkov. Robot Self-Detection System, Advances in Science, Technology and Engineering Systems Journal (ASTESJ), Vol. 3, Iss. 6, ISSN: 2415-6698, ASTES Publishers, USA, 2018, pp. 391-402. (https://astesj.com/v03/i06/p47/,
https://www.scopus.com/record/display.uri?eid=2-s2.0-85061769930&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=6a6a7ebdc623276acf21c2586370b124&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=13&citeCnt=0&searchTerm=)

Abstract:

The paper presents the design and implementation of a mobile robot, located in an accommodation. As opposed to other known solutions, the presented one is entirely based on standard, cheap and accessible devices and tools. An algorithm for transformation of the 2D coordinates of the robot into 3D coordinates is described. The presented approach provides a methodology for applying the robot orientation problem as follows: System overview, Robot recognition, Transformation of 2D coordinates to 3D, Analytic Geometry for Transformation, Transformation Algorithm Definition. The design and implementation of the system are presented. The robot used in this project is based on the Arduino platform. Programs for Arduino are written in either C, C++ or Processing. The board, used for assembling the robot, has the following parameters: Microcontroller: ATmega328, CPU: 8-bit AVR, Clock: 16MHz, Memory of 23KB flash, 2KB SRAM and 1KB EEPROM, 14 I/O pins, 6 Analog Input pins. Physical parameters: 68.6×53.4mm, 25g weight, Bluetooth module and Magnetometer. The Flowchart of the system's general design is done. The testing and evaluation are divided into 2 parts: Android Application (Robot recognition algorithm, Application Stability) and Robot behavior (Plane transformation algorithm, Turning accuracy). Experimental results are shown in tables.

Резюме:

Статията представя дизайн и реализация на мобилен робот, разположен в жилищно помещение. За разлика от други известни решения, представеното е изцяло базирано на стандартни, евтини и достъпни устройства и средства. Описан е алгоритъм за трансформиране на 2D координатите на робота в 3D координати. Представеният подход предоставя методология за прилагане на проблема с ориентацията на робота, както следва: Преглед на системата, Разпознаване на роботи, Трансформация на 2D координати в 3D, Аналитична геометрия за трансформация, Дефиниране на алгоритъм за трансформация. Представени са дизайнът и изпълнението на системата. Роботът, използван в този проект, е базиран на платформата Arduino. Програмите за Arduino са написани на C, C++ или Processing. Платката, използвана за сглобяване на робота, има следните параметри: Микроконтролер: ATmega328, CPU: 8-bit AVR, Clock: 16MHz, Памет 23kB flash, 2kB SRAM и 1kB EEPROM, 14 I/O пина, 6 аналогови входни пина; Физически параметри: 68.6×53.4mm, 25g тегло, Bluetooth модул и магнитометър. Представена е блок-схема на общия дизайн на системата. Тестването и оценката са разделени на 2 части: приложение за Android (алгоритъм за разпознаване на роботи, стабилност на приложението) и поведение на робота (алгоритъм за трансформация на равнина, точност на завъртане). Експерименталните резултати са показани в табличен вид.

B.4-2

Karova M., Penev I., Marinov D., Design and Implementation of Cryptocurrency Price Prediction System, Advances in Intelligent Systems and Computing 1230 AISC, Springer Nature, pp. 628-643, 2020, ISSN: 2194-5357. (https://www.scopus.com/record/display.uri?eid=2-s2.0-85088511005&origin=resultslist&sort=plf-f&src=s&st1=Penev&st2=Ivaylo&nlo=1&nlr=20&nls=count-f&sid=4f14e97b4d9bfb04e2b11bc2b95942b4&sot=anl&sdt=aut&sl=34&s=AU-ID%28%22Penev%2c+Ivaylo%22+34880589800%29&relpos=1&citeCnt=0&searchTerm=)

Abstract:

The paper presents conceptual design of a cryptocurrency price prediction system. The algorithm for data collection and a LSTM neural network for predicting future prices are presented. A brief explanation of the system implementation is shown. The structure of the neural network and the tuning of the hyper parameters are explained. The system consists of the following logical modules. 1) The collector collects data from remote sources (APIs). The data is then stored in a database for further usage by the machine learning algorithm; 2) the machine learning algorithm converts the stored in the database data to a suitable format for machine learning (CSV files). The data is then processed by a LSTM neural network, which outputs one day ahead predictions for the cryptocurrencies' close prices. The predictions are stored in the database. 3) REST API – exposes the predictions made by the machine learning algorithm to the end users. It gives permission only to authorized users to access the secured resources (predictions). 4) The security is implemented with JWT authentication. 5) The front end applications – Android and web application for displaying the predictions to the users.

The machine learning algorithm consists of two parts. The first one is loading the data and transforming it into a suitable format for training the neural network. This process is known as ETL (extract, transform, load). The second part is related to operations with the neural network. The crypto price prediction system consists of the following software modules: 1) Spring Boot application (back-end); 2) MongoDB database; 3) Angular web application (front-end); 4) Android mobile application (front-end). Finally, experimental results with predicted future price of Bitcoin cryptocurrency are presented. The results are compared to the prediction of the Bitcoin price for the same time periods obtained by Cryptomon system.

Резюме:

Докладът представя концептуален дизайн на система за прогнозиране на цената на криптовалута. Представени са алгоритъм за събиране на данни и LSTM невронна мрежа за прогнозиране на бъдещи цени. Показано е

кратко обяснение на реализацията на системата. Обяснява се структурата на невронната мрежа и настройката на хиперпараметрите. Системата се състои от следните логически модули. 1) Колекторът събира данни от отдалечени източници (API). След това данните се съхраняват в база данни за по-нататъшно използване от алгоритъма за машинно обучение. 2) Алгоритъмът за машинно обучение преобразува съхранените в базата данни в подходящ формат за машинно обучение (CSV файлове). След това данните се обработват от невронна мрежа LSTM, която извежда прогнози за един ден напред за цените на затваряне на криптовалутите. Прогнозите се съхраняват в базата данни. 3) REST API извежда към крайните потребители прогнозите, направени от алгоритъма за машинно обучение. Той дава разрешение само на оторизирани потребители за достъп до защитените ресурси (предсказания). 4) Сигурността е реализирана с JWT удостоверяване. 5) Приложенията: Android и уеб приложение за показване на прогнозите на потребителите.

Алгоритъмът за машинно обучение се състои от две части. Първият е зареждане на данните и трансформирането им в подходящ формат за обучение на невронната мрежа. Този процес е известен като ETL (извличане, трансформиране, зареждане). Втората част е свързана с операциите с невронната мрежа. Системата за прогнозиране на крипто-цените се състои от следните софтуерни модули: 1) Приложение Spring Boot (back-end); 2) MongoDB база данни; 3) Angular уеб приложение (front-end); 4) Мобилно приложение за Android (преден край). Накрая са представени експериментални резултати с прогнозирана бъдеща цена на биткойн криптовалутата. Резултатите се сравняват с прогнозата за цената на биткойн за същите периоди от време, получена от системата Cryptomon.

B.4-3

Kalcheva N., M. Karova, I. Penev. Comparison of the accuracy of SVM kernel functions in text classification, Proceedings of the International Conference on Biomedical Innovations and Applications, BIA 2020, ISBN: 978-172817073-2, Institute of Electrical and Electronics Engineers Inc., pp. 141-145, 2020. (https://www.scopus.com/record/display.uri?eid=2-s2.0-85096779803&origin=resultslist&sort=plf-f&s)

Abstract:

The objective of this paper is to compare the accuracy of different kernel functions of the SVM method for text classification. As a basis for the research film reviews are used. The authors try to detect the kernel functions and their parameters to achieve high accuracy in movie reviews classification. The studied kernel functions are: polynomial kernel of degree 2, a linear kernel and a radial base kernel. The achieved accuracy is higher than 83%. The experiments show that the sigmoid radial kernel is an inappropriate choice in text classification.

Резюме:

Целта на статията е да представи сравнение на точността на различни функции на ядрото на метода SVM при класификация на текст. Като база за изследването са използвани коментари за филми. Авторите се опитват да открият функции на ядрото и техните параметри за постигане на висока точност при класификация на филмови коментари. Изследвани са следните функции: полиномна функция от втора степен, линейна и радиално-базисна функция. Постигнатата точност надвишава 83%. Експериментите показват също, че сигмоидната радиална функция не е подходящ избор за класификация на текст.

B.4-4

Kalcheva N., M. Karova, I. Penev. Comparison of the accuracy and the execution time of classification algorithms for Bulgarian literary works, 2020 International Conference Automatics and Informatics (ICAI), ISBN:978-1-7281-9309-0, IEEE, 2020. (https://ieeexplore.ieee.org/document/9311373, https://www.scopus.com/record/display.uri?eid=2-s2.0-85100106110&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=6a6a7ebdc623276acf21c2586370b124&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=6&citeCnt=1&searchTerm=)

Abstract:

The purpose of this paper is to compare the accuracy and the execution time of machine learning algorithms for classification of texts, written by Bulgarian authors. The algorithms examined are: Multinomial Naive Bayes classifier, Support Vector Machines, Random Forest and AdaBoost. The results show that the Multinomial Naive Bayes classifier is the most accurate and fastest algorithm for classifying texts by two authors with an equal number of poems in Bulgarian language. The ensemble algorithm AdaBoost is the most accurate for unbalanced data classification. The Support Vector Classification has the highest accuracy. In a classification with an unbalanced set of data, the fastest algorithm is Bernoulli Naive Bayes classifier.

Резюме:

Целта на статията е да представи сравнение на точността и времето за изпълнение на алгоритми с машинно обучение при класификация на текст от произведения на български автори. Изследвани са следните алгоритми за класификация: Multinomial Naive Bayes, Support Vector Machines, Random Forest и AdaBoost. Резултатите показват, че Multinomial Naive Bayes класификаторът е най-точен и най-бърз алгоритъм при класификация на

текстове от двама автори при провеждане на експериментални тестове с еднакъв брой поеми на български език. Алгоритъмът AdaBoost е най-точен при класификация на небалансирани данни. Най-голяма точност се наблюдава при Support Vector Machines. При класификация на множества от небалансирани данни най-бърз е класификаторът Bernoulli Naive Bayes.

B.4-5

Karova M., Ivanov I, Penev I., Mitev K., A New Model of Logo Generator, International Conference Automatics and Informatics`2021, Proceedings, September 30 - October 02, 2021, Varna, Bulgaria (ICAI'21), DOI: 10.1109/ICAI52893.2021.9639860, IEEE, pp. 210-213, 2021, ISBN: 978-1-6654-2661-9. (https://www.scopus.com/record/display.uri?eid=2-s2.0-85123854966&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=d4ba1b66458e239078cdc737990499c1&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=1&citeCnt=0&searchTerm=&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1)

Abstract:

The paper presents a model of a logo generator. The proposed model uses extended StyleGAN neural network. The architecture of the StyleGAN network is presented with an emphasis on the additional components extending the classical GAN neural network. The configuration of the network parameters is also explained. Unlike the known logo generators, the proposed architecture achieves production of unique and original logos. The generator used in StyleGAN consists of two subnets - a mapping network and a synthesis network. The generator has the following parameters: 1) input latent vector Z; 2) input for the condition (i.e. categories); 3) input data for the truncation function (this function ensures the image areas for performing poorly during training, i.e. do not lead to a meaningful output).

Once the training data is available, several modifications are required to reach the stage where they are transformed into TF Records. The first step is to convert JPG format to PNG format, as the transformation of the output data into PNG is required and the model must be trained on this type of images. The next step of modification is to create pickles using the Python pickle library. It allows information of any kind to be serialized. Thus, the software transfers and processes the input data (in this case the images) faster, which will be in the form of bytes. NVIDIA offers a ready-made script for creating TF Records. This script takes as input bytes in pickle format and the directory where to save the file created by it. The data must meet the above requirements related to size, format, color space and others.

Experimental results are presented and discussed. The advantage of a logo generator (Logonator) over other similar applications is the way of generating the final results (i.e. the logos). The use of a neural network guarantees the uniqueness of each logo, and the ability of the user to edit the text dynamically while seeing the result of each change, contributes to better control of the result.

Резюме:

Статията представя модел на лого генератор. Предложеният модел използва разширена невронна мрежа StyleGAN. Архитектурата на мрежата StyleGAN е представена с акцент върху допълнителните компоненти, разширяващи класическата невронна мрежа GAN. Конфигурацията на мрежовите параметри също е обяснена. За разлика от известните генератори на лого, предложената архитектура постига производство на уникални и оригинални лога. Генераторът, използван в StyleGAN, се състои от две подмрежи - мрежа за картографиране и мрежа за синтез. Генераторът има следните параметри: 1) входен латентен вектор Z; 2) вход за условието (т.е. категории); 3) входни данни за функцията за съкращаване (тази функция гарантира, че областите на изображението се представят лошо по време на тренировка, т.е. не водят до смислен резултат).

След като данните за обучението са налични, са необходими няколко модификации, за да се достигне до етапа, в който те се трансформират в TF записи. Първата стъпка е да конвертирате JPG формат в PNG формат, тъй като е необходима трансформация на изходните данни в PNG и моделът трябва да бъде обучен на този тип изображения. Следващата стъпка на модификация е да се създадат т.н. pickles с помощта на библиотеката Python pickle. Тя позволява информация от всякакъв вид да бъде поставена серийно. Така софтуерът прехвърля и обработва по-бързо входните данни (в случая изображенията), които ще бъдат под формата на байтове. NVIDIA предлага готов скрипт за създаване на TF записи. Този скрипт приема като входни байтове във формат pickle и директорията, където да запише създадения от него файл. Данните трябва да отговарят на горните изисквания, свързани с размер, формат, цветово пространство и други.

Експерименталните резултати са представени и обсъдени. Предимството на генератора на лого (Logonator) пред други подобни приложения е начинът за генериране на крайните резултати (т.е. логата). Използването на невронна мрежа гарантира уникалността на всяко лого, а възможността потребителят да редактира текста динамично, докато вижда резултата от всяка промяна, допринася за по-добър контрол върху резултата.

B.4-6

Kalcheva N., Karova M., A Comparison of Machine Learning Classification Algorithms and Methods for English Author’s Works and their Translations into Bulgarian, Proceeding of 57th International Scientific Conference on Information,

Communication and Energy Systems and Technologies (ICEST 2022), Ohrid, North Macedonia, 16-18 June, 2022, pp.????, IEEE publisher, Electronic ISBN:978-1-6654-8500-5, DOI: 10.1109/ICEST55168.2022.9828579, https://ieeexplore.ieee.org/document/9828579, публикация: https://www.scopus.com/record/display.uri?eid=2-s2.0-85136143185&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=eb82b738bed1be2131d9d65b4799b0dd&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=2&citeCnt=0&searchTerm=)

Abstract:

The aim of the publication is to compare the accuracy, precision, sensitivity and F-measure of machine algorithms trained in the classification of authors of works by English authors and the classification of authors of the same works translated into Bulgarian. The algorithms examined are Multinomial Naive Bayes classifier, Bernoulli Naive Bayes classifier, Support Vector Machines, Random Forest, AdaBoost, Decision Tree and K-Nearest Neighbosr. In order to obtain a more stable assessment in classification, the method of cross-validation is applied. It guarantees an equal number of participations of each object in the training sample and exactly one participation in the test sample. In the cross-validation, the following parameters are calculated: Accuracy, Precision, Recall and the combined measure F-measure. The studied machine learning algorithms are implemented in Python. Two external libraries were used - nltk and scikit. 5-fold cross-validation and accuracy measure were used to evaluate the classification. The research results show that in the English author's classification with an equal number of works in English, Support Vector Machines and Multinomial Naive Bayes classifier receive the highest values of the studied indicators. In Bulgarian texts, the best results are obtained depending on specific authors.

Резюме:

Целта на публикацията е да се сравни точността, прецизността, чувствителността и F-мярката на машинни алгоритми, обучени в класификацията на авторите на произведения от английски автори и класификацията на авторите на същите произведения, преведени на български език. Изследваните алгоритми са Multinomial Naive Bayes classifier, Bernoulli Naive Bayes classifier, Support Vector Machines, Random Forest, AdaBoost, Decision Tree and K-Nearest Neighbosr. За да се получи по-стабилна оценка при класификацията, се прилага методът на кръстосано валидиране. Гарантира равен брой участия на всеки обект в обучителната извадка и точно едно участие в тестовата извадка. При кръстосаното валидиране се изчисляват следните параметри: точност, прецизност,

припомняне и комбинирана мярка F-мярка. Изследваните алгоритми за машинно обучение са реализирани на Python. Използвани са две външни библиотеки - nltk и scikit. За оценка на класификацията бяха използвани 5-кратно кръстосано валидиране и мярка за точност. Резултатите от изследването показват, че в класификацията на английския автор при равен брой произведения на английски език Support Vector Machines и Multinomial Naive Bayes classifier получават най-високи стойности на изследваните показатели. В българските текстове най-добри резултати се получават в зависимост от конкретни автори.

B.4-7

Todorov D., Karova M., Machine Secret Key Recognition in a Homogeneous Environment, 2021 International Conference Automatics and Informatics (ICAI), 2021, pp. 1-4, doi: 10.1109/ICAI52893.2021.9639544, ISBN:978-166542661-9
https://www.scopus.com/record/display.uri?eid=2-s2.0-85123857635&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=d4ba1b66458e239078cdc737990499c1&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=0&citeCnt=0&searchTerm=&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1

Abstract:

The most important characteristic of cryptographic systems is the management of a secret key and its resistance to brute force - attack with all possible variants of the key. The proposed article presents a scheme for recognizing secret keys using machine learning tools. Some of the most used and known symmetric encryption algorithms are used - AES, DES, TripleDES and RC2. It proposes a method for achieving encrypted communication without stipulating the encryption algorithm used. The secret key recognition methods and algorithms include: 1) Placing the generated key in a homogeneous environment; 2) Recognition with kNN algorithm. The kNN algorithm consists of three main steps: 1) calculation of distance between two points; 2) finding the nearest neighbors based on the calculated distances; 3) select a class based on the list of nearest neighbors. The presented modules were developed in the C # software environment, using the Accord.Net machine learning platform. The experiments are made with a total of 440 keys (by 110 for each encryption algorithm), recognized by each of the two machine learning algorithms - kNN and SVM, using basic data from 4000 known examples. The experimental staging has achieved good results, and with secret keys with significant differences, the recognition is about 100%.

Резюме:

Най-важната характеристика на криптографските системи е управлението на секретен ключ и неговата устойчивост на brute force - атака с всички възможни варианти на ключа. Предложената публикация представя схема за разпознаване на секретни ключове с помощта на инструменти за машинно обучение. Използват се едни от най-известните и познати алгоритми за симетрично криптиране - AES, DES, TripleDES и RC2. Предлага се метод за постигане на криптирана комуникация, без да се уточнява използвания алгоритъм за криптиране. Методите и алгоритмите за разпознаване на секретен ключ включват: 1) Поставяне на генерирания ключ в хомогенна среда; 2) Разпознаване с kNN алгоритъм. Алгоритъмът kNN се състои от три основни стъпки: 1) изчисляване на разстоянието между две точки; 2) намиране на най-близките съседи въз основа на изчислените разстояния; 3) избиране на клас въз основа на списъка на най-близките съседи. Представените модули са разработени в софтуерна среда C#, използвайки платформата за машинно обучение Accord.Net. Експериментите са направени с общо 440 ключа (по 110 за всеки алгоритъм за криптиране), разпознати от всеки от двата алгоритъма за машинно обучение - kNN и SVM, използвайки основни данни от 4000 известни примера. Експерименталната постановка е постигнала добри резултати, като при секретни ключове със значителни разлики разпознаването е около 100%.

B.4-8

Spasova Gergana, Karova Milena, An Algorithm for Detecting the Location and Parameters of the Iris in the Human Eye, Proceedings of 2022 International Conference on Communications, Information, Electronic and Energy Systems (CIEES), 24-26 November 2022, Veliko Tarnovo, Bulgaria, IEEE publisher, Electronic ISBN:978-1-6654-9149-5, DOI: 10.1109/CIEES55704.2022.9990831,
https://ieeexplore.ieee.org/document/9990831,
https://www.scopus.com/record/display.uri?eid=2-s2.0-85146488360&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=eb82b738bed1be2131d9d65b4799b0dd&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=0&citeCnt=0&searchTerm=)

Abstract:

In the present article, an algorithm for iris detecting in the human eye is proposed. The realization consists of two parts - opening the inner and outer edge of the iris. The Canny edge detection method is used to detect the inner edge, after

which the result is filtered and smoothed. The Daugman algorithm has been modified to detect the outer edge of the iris. The detection of an image with the human eye is for the purpose of establishing the presence of an iris in an image and determining its parameters, by which it can later be separated from the rest of the image. The requirements that must be met by the implementation are: 1)Detects the location and size of the pupil of the eye (inner edge of the iris); 2)Determining the location and size of the iris (outer edge); 3)Check the validity of the result - the outer and inner edges of the iris should be approximately concentric.The achieved results are better interception and localization of the two iris circles. The software product used for the image processing and the algorithm implementations is MATLAB.

Резюме:

В настоящата статия е предложен алгоритъм за откриване на ириса в човешкото око. Реализацията се състои от две части - отваряне на вътрешния и външния ръб на ириса. Методът Canny edge detection се използва за откриване на вътрешния ръб, след което резултатът се филтрира и изглажда. Алгоритъмът на Daugman е модифициран за откриване на външния ръб на ириса. Засичането на изображение с човешко око е с цел да се установи наличието на ирис в изображението и да се определят неговите параметри, чрез които той по-късно да бъде отделен от останалата част от изображението. Изискванията, които трябва да бъдат изпълнени при внедряването са: 1) Откриване на местоположението и размера на зеницата на окото (вътрешния ръб на ириса); 2)Определяне местоположението и размера на ириса (външен ръб); 3) Проверка валидността на резултата - външният и вътрешният ръб на ириса трябва да са приблизително концентрични. Постигнатите резултати са по-добро прихващане и локализиране на двата ирисови кръга. Софтуерният продукт, използван за обработка на изображенията и реализирането на алгоритъма е MATLAB.

B.4-9

Spasova G., Karova M., A New Secure Image Encryption Model Based on Symmetric Key, International Conference on Biomedical innovations and Applications BIA ‘2021, 2.06-4.06.2022, Technical University Varna, IEEE publisher, pp. 107-110, Electronic ISBN:978-1-6654-4581-8, DOI: 10.1109/BIA52594.2022.9831258,
https://ieeexplore.ieee.org/document/9831258,
https://www.scopus.com/record/display.uri?eid=2-s2.0-85136239884&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=eb82b738bed1be2131d9d65b4799b0dd&sot=anl&sdt=aut&sl=35&s=AU-

ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=3&citeCnt=0&searchTerm=)

Abstract:

This paper presents a new image encryption model with focus on symmetric key schemes. It discus 5 schemes: Random Generation Key (8B); Random Key Generation part A(4B) and part B(4B); Input User Key (4B), Encrypted key and Random Key generation (4B); Random Key Generate (4B) and Input User Encrypted Key (4B); Input User Key (8B). The proposed encryption model proposes an image encryption with symmetric key. Both the sender and the receiver know the same secret key. Messages are encrypted by the sender using the generated key (by 5 variants) and decrypted by the receiver using the same key. The symmetric cryptography largely depends on the symmetric key and key length. The input image is in .jpg format. After reading the image, it is encoded to obtain a byte stream in hexadecimal format, which is used for further processing of the image. Encrypted process contains 7 sequential activities. The key generation is the most important activity in the presented model. There are 5 generation ways (Key1, Key2, Key 3, Key 4 and Key 5). The process of Image encryption uses DES and AES algorithms with different generated keys. The process of Image encoding converts image from hexadecimal to binary format. The Picture Output Component in Cryptotool 2.0 (experimental software) does not work with hexadecimal format and needs binary format for Image visualization. A standard Header is placed for Image type determining. Experimental results are based on image encryption by DES algorithm (5 instances) and by AES algorithm (5 instances). A table with image quality values and a table with complex arithmetic mean error are done.

Резюме:

Тази статия представя нов модел за криптиране на изображения с фокус върху симетрични ключови схеми. Обсъждат се 5 схеми: Ключ за произволно генериране (8B); Генериране на случаен ключ част A(4B) и част B(4B); Въвеждане на потребителски ключ (4B), криптиран ключ и генериране на случаен ключ (4B); Генериране на случаен ключ (4B) и въвеждане на криптиран от потребителя ключ (4B); Въвеждане на потребителски ключ (8B). Предложеният модел за криптиране предлага криптиране на изображение със симетричен ключ. И подателят, и получателят знаят един и същ таен ключ. Съобщенията се криптират от подателя с помощта на генерирания ключ (по 5 варианта) и се дешифрират от получателя с помощта на същия ключ. Симетричната криптография до голяма степен зависи от симетричния ключ и дължината на ключа. Входното изображение е във формат .jpg. След прочитане на изображението, то се кодира, за да се получи поток от байтове в шестнадесетичен формат, който се използва за по-нататъшна обработка на

изображението. Криптираният процес съдържа 7 последователни операции. Генерирането на ключ е най-важната операция в представения модел. Показани са 5 начина за генериране (Ключ1, Ключ2, Ключ 3, Ключ 4 и Ключ 5). Процесът на криптиране на изображения използва DES и AES алгоритми с различни генерирани ключове. Процесът на кодиране на изображения преобразува изображението от шестнадесетичен в двоичен формат. Компонентът за извеждане на картина в Cryptotool 2.0 (използвания експериментален софтуер) не работи с шестнадесетичен формат и се нуждае от двоичен формат за визуализация на изображението. За определяне на типа на изображението се поставя стандартен колонтитул. Експерименталните резултати се основават на криптиране на изображение чрез DES алгоритъм (5 случая) и чрез AES алгоритъм (5 случая). Направена е таблица със стойности на качеството на изображението и таблица с комплексна средна аритметична грешка.

B.4-10

Mashkov V, Karova M., Penev I., State Of Charge Estimation in Lithium-Ion Batteries via Machine Learning, Proceeding of 2022 International Conference Automatics and Informatics (ICAI), 06-08 October 2022, Technical University Varna, Bulgaria, IEEE publisher, pp. 95-99, Electronic ISBN:978-1-6654-7625-6, DOI: 10.1109/ICAI55857.2022.9960064, https://ieeexplore.ieee.org/document/9960064, https://www.scopus.com/record/display.uri?eid=2-s2.0-85143748410&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=eb82b738bed1be2131d9d65b4799b0dd&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=1&citeCnt=0&searchTerm=)

Abstract:

Accurate State of Charge estimation is crucial for rationing the energy usage of lithium-ion batteries. The goal of this paper is to showcase different machine learning techniques for State of Charge modeling. Machine learning methods were trained and tested on the NASA lithium-ion battery dataset. The dataset includes data for charging, discharging and impedance testing for four, 18650 lithium-ion batteries. Different Support Vector Machine (SVM) and Deep Neural Network (DNN) models were trained and tested on this Battery dataset. The presented models take into account battery voltage, load voltage and battery temperature and can be applied for online State of Charge estimation. To evaluate the presented models' performance, the use of evaluation metrics is needed. In this paper, we use Root Mean Squared Error, Mean Absolute Error, and Mean Absolute Percentage Error to compare and optimize different machine learning

models. Mean Squared Error is used for model optimization, while MAE and MAPE are used for more human-readable and absolute evaluation. The conducted experiments show that Deep Neural Networks offer higher accuracy (MAPE - 1.2%), compared to SVM models (MAPE - 3.6%).

Резюме:

Точното определяне на състоянието на заряда е от решаващо значение за разпределяне на потреблението на енергия на литиево-йонните батерии. Целта на този документ е да покаже различни техники за машинно обучение за моделиране на състоянието на заряда. Методите за машинно обучение са обучени и тествани върху набора от данни за литиево-йонни батерии на НАСА. Наборът от данни включва данни за зареждане, разреждане и тестване на импеданса за четири литиево-йонни батерии 18650. Различни модели на Support Vector Machine (SVM) и Deep Neural Network (DNN) са обучени и тествани върху този набор от данни за батерията. Представените модели отчитат напрежението на батерията, напрежението на товара и температурата на батерията и могат да се прилагат за онлайн оценка на състоянието на заряда. За да се оцени ефективността на представените модели, е необходимо използването на метрики за оценка. В тази статия се използва средно-квадратична грешка, средна абсолютна грешка и средна абсолютна процентна грешка, за да се сравнят и оптимизират различни модели на машинно обучение. Средно-квадратичната грешка се използва за оптимизиране на модела, докато MAE и MAPE се използват за по-разбираемата от човека абсолютна оценка. Проведените експерименти показват, че Deep Neural Networks предлагат по-висока точност (MAPE - 1.2%), в сравнение със SVM моделите (MAPE - 3.6%).

Г.7-1

Karova M., Penev I., Algorithm for html preprocessing in email messages, Proceedings of the International Conference on Biomedical Innovations and Applications, BIA 2019, Institute of Electrical and Electronics Engineers Inc., 2019, ISBN: 978-172814754-3. (https://www.scopus.com/record/display.uri?eid=2-s2.0-85079270069&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=d4ba1b66458e239078cdc737990499c1&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=5&citeCnt=0&searchTerm=&featureToggles=FEATURE_NEW_DOC_DETAILS_EXPORT:1)

Abstract:

The paper presents an algorithm for preprocessing the HTML code of email messages; this is used in email client applications (such as Gmail App and Microsoft Outlook). The purpose is to create an easy-to-use tool, automatically inserting pre-declared styles from the <head> tag to <body> tag of the HTML document. The algorithm solves the following specific tasks, concerning the email preprocessing: 1) Extracts the styles, declared in the <head> tag of the HTML document, and to write them into the class attribute of the relevant element tag; 2) Recognizes the '__path__/' keyword, which stores the path to an image and to write the path into the src attribute of the image tag; 3) Recognizes the '<br height=" " />' tag and to transforms it into table <td> tag; 4) Recognizes the '<mobilebr height=" " />' tag and to add more paddings between the elements to provide responsive mobile design of the email content. In the lexical analysis step the algorithm recognizes the tokens from the HTML code. The token name is used in the next parsing step and the attribute value points to an entry into the symbol table. The parsing step of the preprocessing algorithm uses the tokens to produce parse tree of the HTML document. After the parse tree is created, the interpreter starts searching and replacing process.

The experimental results of running the algorithm are presented.

Резюме:

Статията представя алгоритъм за предварителна обработка на HTML кода на имейл съобщенията; това се използва в клиентски приложения за имейл (като приложението Gmail и Microsoft Outlook). Целта е да се създаде лесен за използване инструмент, автоматично вмъкващ предварително декларирани стилове от тага <head> към тага <body> на HTML документа. Алгоритъмът решава следните специфични задачи, свързани с предварителната обработка на имейла: 1) Извлича стиловете, декларирани в тага <head> на HTML документа, и ги записва в атрибута class на съответния таг на елемента; 2) Разпознава ключовата дума „__path__/", която съхранява пътя до изображение и за запис на пътя в атрибута src на тага на изображението; 3) Разпознава тага '<br height=" " />' и го трансформира в таг <td> за таблица; 4) Разпознава тага '<mobilebr height=" " />' и добавя повече подложки между елементите, за да осигури отзивчив мобилен дизайн на съдържанието на имейла. По време на лексикалния анализ, алгоритъмът разпознава токените от HTML кода. Името на токена се използва в следващата стъпка на анализ и стойността на атрибута сочи към запис в таблицата със символи. Стъпката анализ на алгоритъма за предварителна обработка използва токените, за да създаде дърво за анализ на HTML документа. След като дървото за разбор е създадено, интерпретаторът започва процеса на търсене и заместване.

Представени са експериментални резултати от изпълнението на алгоритъма.

Г.7-2

Penev I., M. Karova. Implementation of a Training Parser Using Explicit Abstract Syntax Tree, Proceedings of the 20th International Conference on Computer Systems and Technologies, CompSysTech'19, June 21-22, Ruse, Bulgaria, ACM International Conference Proceeding Series, ISBN: 978-1-4503-7149-0, ACM Inc., N.Y. USA, pp. 299-303, doi>10.1145/3345252.3345283, 2019, (https://dl.acm.org/citation.cfm?id=3345283, https://www.scopus.com/record/display.uri?eid=2-s2.0-85073051612&origin=resultslist&sort=plf-f&src=s&st1=Karova&st2=Milena&nlo=1&nlr=20&nls=count-f&sid=6a6a7ebdc623276acf21c2586370b124&sot=anl&sdt=aut&sl=35&s=AU-ID%28%22Karova%2c+Milena%22+24450850900%29&relpos=10&citeCnt=0&searchTerm=)

Abstract:

The presented report focuses on the use of a learning compiler to run a university course. The emphasis is on one of the modules of the compiler - the parser. The developed parser has the following two distinctive features compared to known parsers: 1) It contains the construction of an abstract syntactic tree (AST - Abstract Syntax Tree); 2) The abstract syntax tree is a structure that contains information about the program - variables, data types, operators. This structure is important because it is used to build the symbol table that is the basis of semantic analysis and code generation.

The well-known parsers used in most tutorials build this tree implicitly, i.e. it cannot be visualized and checked by the students. This makes the development of the parser easier, but makes it difficult to understand and work on the next stages - semantic analysis and code generation.

The parser is implemented as a completely self-contained module, making it convenient for testing by students. A programming language was created for compiler purposes that is procedurally oriented and is a subset of C and Java. A language grammar and a compiler code with parts of it removed is obtained.

The report shows a sample of the grammar that describes a variable definition. The syntax function for variable definition without building a tree is shown. It is proposed to extend the function with the construction of tree tops. The experiments were conducted in two school years.

Резюме:

Докладът е насочен към използването на учебен компилатор за провеждане на университетски курс. Акцентът е върху един от модулите на компилатора - синтактичния анализатор (parser). Разработеният синтактичен анализатор им следните две отличителни черти в сравнение с известните анализатори:

1) Съдържа построяване на абстрактно синтактично дърво (AST - Abstract Syntax Tree); 2) Абстрактното синтактично дърво е структура, която съдържа информация за програмата - променливи, типове данни, оператори. Тази структура е важна, защото се използва за построяване на символната таблица, която е в основата на семантичния анализ и генерирането на кода.

Известните синтактични анализатори, използвани в повечето учебни курсове, построяват това дърво неявно, т.е. то не може да се визуализира и да се проверява от студентите. Това прави разработването на синтактичния анализатор по-лесно, но затруднява разбирането и работата по следващите етапи - семантичен анализ и генериране на код.

Синтактичният анализатор е реализиран като изцяло самостоятелен модул, което го прави удобен за тестване от студенти. За целите на компилатора е създаден програмен език, който е процедурно ориентиран и е подмножество на C и Java. Получава се граматика на езика и кода на компилатора с премахнати части от него.

В доклада е показана извадка от граматиката, която описва дефиниция на променлива (variable_definition). Показана е синтактичната функция за variable_definition без построяване на дърво. Предлага се разширяване на функцията с построяване на върхове на дървото. Експериментите са проведени в две учебни години.

Г.8-1

Karova M., D. Zhelyazkov, M. Todorova, I. Penev, V. Nikolov, V. Petkov. Path Planning Algorithm for Mobile Robot. RECENT RESEARCHES in APPLIED COMPUTER SCIENCE, vol. 9, Proceedings of the 15th International Conference on Applied Computer Science (ACS'15), Konya, Turkey, pp. 26-30, ISBN: 978-1-61804-307-8, ISSN: 1790-5109, WSEAS Press, 2015,. (https://www.researchgate.net/publication/280622356_Path_Planning_Algorithm_for_Mobile_Robot#fullTextFileContent)

Abstract:

The paper presents an algorithm for planning the path of a mobile robot in a labyrinth. The algorithm uses an image, obtained by a camera. The algorithm processes the image to convert it into a matrix, presenting the labyrinth with obstacles and walls. Afterwards the algorithm, based on the Dijkstra's algorithm, finds the shortest path to a final target in the labyrinth. As opposed to the classical Dijkstra's algorithm, the presented algorithm compares the size of the robot to the size of the obstacles on the way. The algorithm consists of the following basic steps: 1) creation of a queue – a set of ordered points; 2) extraction of elements from the queue; 3) for each point all neighbor points are checked. The possible neighbors are in four directions – up, right, down, left. A neighbor point is free, if the following conditions are satisfied: 1) the point is not a part of an obstacle; 2) the point is not marked. A free point is marked and added to the queue. All free

points are marked by its neighbors. The order of marking forms the shortest path. A simulation of the algorithm is developed to visualize the movement of the robot. The algorithm is tested with labyrinths with varying sizes (different width and height in pixels). The following times are measured for each labyrinth: 1) time for labyrinth construction (i.e. converting the image into text format, suitable for processing); 2) time for obtaining a solution (i.e. finding a path to the target); 3) time for the movement of the robot to reach the target. The experimental results, obtained by the simulation, are presented.

Резюме:

В статията е представен алгоритъм за планиране на пътя на мобилен робот в лабиринт. Алгоритъмът използва изображение, получено от камера. Алгоритъмът обработва изображението, за да го преобразува в матрица, представяща лабиринта с препятствия и стени. След това алгоритъмът, базиран на алгоритъма на Дейкстра, намира най-краткия път до крайната цел в лабиринта. За разлика от класическия алгоритъм на Дейкстра, представеният алгоритъм сравнява размера на робота с размера на препятствията по пътя. Алгоритъмът се състои от следните основни стъпки: 1) създаване на опашка – набор от подредени точки; 2) извличане на елементи от опашката; 3) за всяка точка се проверяват всички съседни точки. Възможните съседи са в четири посоки – нагоре, надясно, долу, наляво. Съседна точка е свободна, ако са изпълнени следните условия: 1) точката не е част от препятствие; 2) точката не е отбелязана. Свободна точка се маркира и добавя към опашката. Всички свободни точки са маркирани от своите съседи. Редът на маркиране формира най-краткия път. Разработена е симулация на алгоритъма за визуализиране на движението на робота. Алгоритъмът е тестван с лабиринти с различни размери (различна ширина и височина в пиксели). За всеки лабиринт се измерват следните времена: 1) време за изграждане на лабиринта (т.е. конвертиране на изображението в текстов формат, подходящ за обработка); 2) време за получаване на решение (т.е. намиране на път към целта); 3) време за движение на робота до достигане на целта. Представени са експерименталните резултати, получени от симулацията.

Г.8-2

Karova M., I. Penev, V. Nikolov, D. Zhelyazkov. Path Planning Algorithm for a Robot in a Labyrinth. Proceedings of papers, L International Scientific Conference on Information, Communication and Energy Systems and Technologies, Publishing house TU-Sofia, 2015, pp. 228-231, ISBN: 978-619-167-182-3
(https://drive.google.com/file/d/1gRmyZBalf8f2zj1Q9NxjkKIvNPoijQBY/view)

Abstract:

The paper presents an algorithm for path planning for a robot in a labyrinth. The algorithm uses an image, obtained by a camera. The image is processed and converted to a matrix, presenting the labyrinth with obstacles and walls. Afterwards an algorithm, based on the Dijkstra`s algorithm, is applied to find the shortest path in the labyrinth. As opposed to the classical Dijkstra's algorithm, the presented algorithm compares the size of the robot to the size of an obstacle. The algorithm consists of the following basic steps: 1)Creation of a queue – a set of points; 2) Extraction of elements from the queue; 3) For each point all neighbor points are checked. The possible neighbors are in four directions – up, right, down, left. The application is implemented using the Java Swing technology for user interfaces. When the process is completed a maze monitor is shown as a panel in the main user window sharing the virtual labyrinth. A maze command executor is also used to move the robot according to the markers over which it is currently placed. If there are no markers in the robot position, then this means that the target is reached or there is no path in the labyrinth. The algorithm has been implemented in a real robot platform (in our case LEGO EV3 robot) and the obtained results are presented.

Резюме:

Докладът представя алгоритъм за планиране на пътя на робот в лабиринт. Алгоритъмът използва изображение, получено от камера. Изображението се обработва и преобразува в матрица, представяща лабиринта с препятствия и стени. След това се прилага алгоритъм, базиран на алгоритъма на Дейкстра, за намиране на най-краткия път в лабиринт. За разлика от класическия алгоритъм на Дейкстра, представеният алгоритъм сравнява размера на робота с размера на препятствието. Алгоритъмът се състои от следните основни стъпки: 1) Създаване на опашка – набор от точки; 2) Извличане на елементи от опашката; 3) За всяка точка се проверяват всички съседни точки. Възможните съседи са в четири посоки – нагоре, надясно, долу, наляво. Приложението е реализирано с помощта на технологията Java Swing за потребителски интерфейси. Когато процесът приключи, лабиринтът се показва като панел в главния потребителски прозорец, споделящ виртуалния лабиринт. Използва се команда за преместване на робота според маркерите, върху които е поставен в момента. Ако няма маркери в позицията на робота, това означава, че целта е достигната или няма пътека в лабиринта. Алгоритъмът е имплементиран в реална роботна платформа (в нашия случай LEGO EV3 робот) и са представени получените резултати.

Г.8-3

Karova M., Todorova G., Todorova M., Penev I., Nikolov V., Comparative Analysis of Algorithms for Communication Encryption. MATHEMATICS and

COMPUTERS in SCIENCES and INDUSTRY, Series: Mathematics and Computers in Science and Engineering Series - 50, INASE, 2015, pp. 38-42, ISBN: 978-1-61804-327-6, ISSN: 2227-4588 (http://www.inase.org/library/2015/books/MCSI.pdf)

Abstract:

A comparative analysis of the algorithms DES, Triple DES-128, Triple DES-192, AES-128, AES-192 and AES-256 is done. For this purpose an application for research of algorithms for cryptographic secure data transmission has been created. The application is developed in C#. It offers the user access to the transmitted data via password. The used resources and time required for encryption of groups of files with different lengths are studied with the help of the application. Two programs – server and client are developed. After starting the server passphrase and "salt" are set. They have to be strings with a length of at least 8 characters. From a security perspective, it is desirable for “salt” to contain uppercase and lowercase letters, numbers and symbols. There are built-in passphrases and “salt” that can be used for quick test of the application. To compare the algorithms groups of files with four different lengths (10,000 bytes; 100,000 bytes; 1,000,000 bytes and 10,000,000 bytes) is done. The tests were performed with minimal use of computer resources from other processes. The encryption is done by using each of the selected algorithms.The obtained results were compared and analyzed and corresponding conclusions are made.

Резюме:

Направен е сравнителен анализ на алгоритмите DES, Triple DES-128, Triple DES-192, AES-128, AES-192 и AES-256. За целта е създадено приложение за изследване на алгоритми за криптографско защитено предаване на данни. Приложението е разработено на C#. Той предлага на потребителя достъп до предаваните данни чрез парола. С помощта на приложението се изследват използваните ресурси и време, необходимо за криптиране на групи от файлове с различна дължина. Разработени са две програми – сървърна и клиентска. След стартиране на сървъра се задават парола и "сол". Те трябва да са низове с дължина най-малко 8 знака. От гледна точка на сигурността е желателно „солта“ да съдържа главни и малки букви, цифри и символи. Има вградена парола и „сол“, които могат да се използват за бърз тест на приложението. За сравняване на алгоритмите се правят групи от файлове с четири различни дължини (10 000 байта; 100 000 байта; 1 000 000 байта и 10 000 000 байта). Тестовете са проведени с минимално използване на компютърни ресурси от други процеси. Криптирането се извършва чрез използване на всеки един от избраните алгоритми. Получените резултати са сравнени и анализирани и са направени съответните изводи.

Г.8-4

Пенев И., Карова М., Николов В., Общ преглед на система за придвижване на робот в лабиринт, „Компютърни науки и технологии“, год. XIII, бр. 2/2015, ISSN: 1312-3335, 2015, pp. 55-60. (http://csejournal.cs.tu-varna.bg/cse_journal_2_2015.pdf

Abstract:

The paper presents a general structure of a system for moving a robot from a given starting position to a final goal in a maze. The system uses a photo of the maze taken in advance with an external camera. The captured image is sent to the robot, which converts it into a suitable format, finds the shortest path to the final destination, forms and executes commands to move the robot. In the presented implementation, the image is converted into a matrix in which the obstacles (walls), the starting position and the final goal in the maze are marked with appropriate symbols. An example maze matrix is presented in the experimental studies. In the present implementation, a modified Dijkstra algorithm is used. The change to the classic algorithm consists in the fact that when the robot moves, a check is made whether its dimensions correspond to the dimensions of the passages in the maze, i.e. whether the robot can pass through a given location. The path found is marked with appropriate symbols. As a result of the marking, movement commands (forward, backward, left, right) are formed, through which the robot moves from the initial position to the final position. The results of the system application for an idealized image of an example maze are presented.

Резюме:

Статията представя обща структура на система за придвижване на робот от зададена начална позиция до крайна цел в лабиринт. Системата използва снимка на лабиринта, направена предварително с външна камера. Направеното изображение се изпраща към робота, който го преобразува в подходящ формат, намира най-кратък път до крайната цел, формира и изпълнява команди за придвижване на робота. В представената реализация изображението се преобразува в матрица, в която с подходящи символи са маркирани препятствията (стените), началната позиция и крайната цел в лабиринта. Матрица на примерен лабиринт е представена в експерименталните изследвания. В настоящата реализация е използван модифициран алгоритъм на Дейкстра. Промяната на класическия алгоритъм се състои в това, че при придвижването на робота се прави проверка дали размерите му съответстват на размерите на проходите в лабиринта, т.е. дали роботът може да премине през дадено място. Намереният път се маркира с подходящи символи. В резултат от направената маркировка се формират команди за движение (напред, назад, наляво, надясно), чрез които роботът се придвижва от началната позиция до крайната Представени са резултати

от приложението на системата за идеализирано изображение на примерен лабиринт.

Г.8-5

Nikolov V., Penev I., Karova M. Processing of labyrinth images for moving of a mobile robot, journal "Computer Science and Technologies", year XIII, vol. 1/2015, ISSN: 1312-3335, 2015, pp. 121-125. (http://csejournal.cs.tu-varna.bg/cse_journal_1_2015.pdf)

Abstract:

This paper considers the stage of an image processing as a step of actions of moving of robot in a labyrinth. The image is received from a camera positioned above the labyrinth and after that it is analyzed in order to create a stylized image of the labyrinth in which the shortest path should be found from the mobile robot position to the labyrinth exit. A real image of a labyrinth is the scene contains perspective distortion. The image is first transformed into grayscale image and then so called edge detectors are used to traverse the image. Here appropriate gradient operators can be used, such as Sobel, Prewitt, Roberts operators, etc. or second derivative operators, Canny operator. Alternatively the image can be processed without transformation into grayscale by applying output fusion method or multidimensional gradient method. In order to find real edges in most cases additional actions are performed after their detection like thinning and connecting because of their false breakage. The sloped lines (edges) are analyzed and set up straight vertical or horizontal according to the smaller slope. The correction is performed by rotation of the sloped lines around the center in the middle between the critical points of the wall ends. The stylized image of the labyrinth is obtained by having the critical points and having preliminary information for the walls width.

Резюме:

Тази статия разглежда етапа на обработка на изображението като стъпка от действия на движение на робота в лабиринт. Изображението се получава от камера, разположена над лабиринта, след което се анализира, за да се създаде стилизирано изображение на лабиринта, в което трябва да се намери най-краткият път от позицията на мобилния робот до изхода на лабиринта. Реално изображение на лабиринт е сцената, която съдържа перспективно изкривяване. Изображението първо се трансформира в изображение в сива скала и след това се използват така наречените детектори за ръбове, за да се премине през изображението. Тук може да се използва подходящ оператор за градиент, като операторите на Sobel, Prewitt, Roberts и т.н. или оператори за втора производна, оператор Canny. Като алтернатива изображението може да бъде обработено без трансформация в скала на сивото чрез прилагане на метод на изходно сливане или метод на

многомерен градиент. За да се намерят реални ръбове в повечето случаи се извършват допълнителни действия след откриването им като изтъняване и свързване поради фалшивото им счупване. Наклонените линии (ръбове) се анализират и се настройват прави вертикално или хоризонтално според по-малкия наклон. Корекцията се извършва чрез завъртане на наклонените линии около центъра в средата между критичните точки на краищата на стената. Стилизираното изображение на лабиринта се получава чрез наличие на критичните точки и предварителна информация за ширината на стените.

Г.8-6

Karova M., Todorova G., Todorova M., Penev I., Nikolov V.. Research of Algorithms for Communication Encryption, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, vol. 10, NAUN, 2016, pp. 30-36, ISSN: 2074-1294 (http://www.naun.org/main/UPress/cc/2016/a122002-255.pdf)

Abstract:

An application for research of algorithms for cryptographic secure data transmission by using the algorithms DES, TripleDES-128, TripleDES-192, AES-128, AES-192 и AES-256 is developed in C#. It offers the user access to the transmitted data via password. Testing of the application is carried out to ensure trouble-free operation. The application is composed of two programs – server and client. On the basis of the passphrase and the "salt" are derived a key and an initialization vector to be used for decryption of the received data. Upon receipt of a connection request from the client, the server starts a thread in which the receiving and decryption of data is done. After completion of the exchange of data, or after a period of idle time (15 seconds), the connection with the client is closed. The example of Encrypted TCP server and the example of Encrypted TCP client are done. The used resources and time required for encryption of groups of files with different length are studied. A comparative analysis of the algorithms is presented in 31 figures and corresponding conclusions are made.

Резюме:

На C# е разработено приложение за изследване на алгоритми за криптографско защитено предаване на данни с помощта на алгоритмите DES, TripleDES-128, TripleDES-192, AES-128, AES-192 и AES-256. Той предлага на потребителя достъп до предаваните данни чрез парола. Извършено е тестване на приложението, за да се гарантира безпроблемна работа. Приложението се състои от две програми – сървърна и клиентска. На базата на паролата и "солта" се извличат ключ и инициализиращ вектор, които да се използват за дешифриране на получените данни. При получаване на заявка за връзка от клиента, сървърът стартира нишка, в която се извършва получаването и дешифрирането на данни. След приключване

на обмена на данни или след период на бездействие (15 секунди), връзката с клиента се затваря. Пример за шифрован TCP сървър и пример за шифрован TCP клиент са дадени. Изследвани са използваните ресурси и време, необходими за криптиране на групи от файлове с различна дължина. На общо 31 фигури е представен сравнителен анализ на алгоритмите и са направени съответните изводи.

Г.8-7

Karova M., Penev I., Todorova M., Bobev H., Kalcheva N. Graph Construction Algorithm for finding the Shortest Path in a Maze, Proceedings of Papers, 51st Scientific Conference on Information, Communication and Energy Systems and Technologies, Faculty of Technical Sciences, Bitola, Macedonia, 2016, pp. 225-228. ISBN: 978-9989-786-78-5, ISBN-10: 9989-786-78-X, ISBN-13: 978-9989-786-78-5. (https://drive.google.com/file/d/1eJR-L0t9xVQKaQWvuSapxDFzsIq0tqdV/view)

Abstract:

The paper presents implementation of an algorithm for movement of a robot from a start position to a final destination in a maze. The algorithm solves two main problems: transformation of the maze into a graph and finding the shortest path from an initial to a final position. The algorithm is implemented as a part of an application, using already generated text image, obtained by a picture of the maze from top. Walls (obstacles), empty spaces, starting position of the robot and the final destination are marked on the image. The maze is presented as a bit set to form a graph which vertexes are valid positions of the robot (i.e. the robot can rotate without touching a wall). The algorithm finds the shortest path, marks movement commands and saves them into a text file. The AlgoHris algorithm is compared to three other algorithms: Backtracking, A* and Genetic Algorithm GAPP. The most challenging problem in the implementation of the described algorithm is proper presentation of mazes with large dimensions (e.g. 1600x1013 pixels). Such images have to be quickly transformed to a graph, considering the limited memory and computing power in the selected robot platform. In the implementation of the AlgoHris algorithm the maze is presented as a set of bits. Each bit is a structure of elements with only 2 possible values: 0 (true) or 1 (false). The experiments are carried out in two directions: 1)Comparing the times for graph construction for mazes with various dimensions; 2)Comparing the algorithm with three other algorithms, using the same dimensions (height and width in pixels) of the maze.

Резюме:

В статията е представена реализация на алгоритъм за движение на робот от начална позиция до крайна дестинация в лабиринт. Алгоритъмът решава два основни проблема: трансформиране на лабиринта в графика и

намиране на най-краткия път от начална до крайна позиция. Алгоритъмът е реализиран като част от приложение, използвайки вече генерирано текстово изображение, получено от снимка на лабиринта отгоре. Стените (препятствията), празните пространства, началната позиция на робота и крайната дестинация са отбелязани на изображението. Лабиринтът е представен като бит, настроен да формира графика, чиито върхове са валидни позиции на робота (т.е. роботът може да се върти, без да докосва стена). Алгоритъмът намира най-краткия път, маркира командите за движение и ги записва в текстов файл. Алгоритъмът AlgoHris се сравнява с три други алгоритъма: Backtracking, A* и Genetic Algorithm GAPP. Най-предизвикателният проблем при прилагането на описания алгоритъм е правилното представяне на лабиринти с големи размери (например 1600x1013 пиксела). Такива изображения трябва бързо да се трансформират в графика, като се има предвид ограничената памет и изчислителна мощност в избраната платформа на робота. При реализацията на алгоритъма AlgoHris лабиринтът е представен като набор от битове. Всеки бит е структура от елементи само с 2 възможни стойности: 0 (вярно) или 1 (невярно). Експериментите се провеждат в две насоки: 1)Сравняване на времената за построяване на графи за лабиринти с различни размери; 2)Сравняване на алгоритъма с три други алгоритъма, като се използват същите размери (височина и ширина в пиксели) на лабиринта.

Г.8-8

Penev I., Karova M., Todorova M., Exploration of the K Parameter in Hand-Written Digit Recognition by K-Nearest Neighbor Algorithm, International Journal of Control Systems and Robotics, vol. 1, 2016, pp. 158-161, ISSN: 2367-8917. (http://www.iaras.org/iaras/filedownloads/ijcsr/2016/011-0022.pdf)

Abstract:

The paper presents the application of the k-nearest neighbor algorithm (kNN) for recognition of handwritten digits from 0 to 9. Typically the images of the digits are entered in some graphic format (e.g. BMP, JPG, PNG). The algorithm processes the digits as sets of characters 0 and 1. The character “1” presents availability of a pixel into the grey scale of the image, and the character “0” presents the lack of a pixel. The emphasis is on the choice of the number of the nearest neighbors (the k parameter), which has significant impact on the algorithm performance. The main steps of the algorithm are described. The function for distance calculation and the method for choosing a class of the recognized digit are explained. Experimental results are presented. According to the results recommendations for the choice of k are summarized. The aim is increasing the performance of the kNN algorithm for the hand-written digit recognition problem, regarding two criteria – percent of the correctly recognized input data and time for recognition. The tests are carried out with 946 examples of images of digits

from 0 to 9. The algorithm is run with a set of 946 digits for recognition. The tests are performed with different values of the k parameter. The good recognition time makes the algorithm proper to work in realtime systems, where large data sets should be processed quickly (for example in robots and controllers).

Резюме:

Статията представя приложението на алгоритъма на най-близкия съсед (kNN) за разпознаване на ръкописни цифри от 0 до 9. Обикновено изображенията на цифрите се въвеждат в някакъв графичен формат (напр. BMP, JPG, PNG). Алгоритъмът обработва цифрите като набори от знаци 0 и 1. Знакът "1" представя наличието на пиксел в сивата скала на изображението, а знакът "0" представя липсата на пиксел. Акцентът е върху избора на броя на най-близките съседи (параметър k), който има значително влияние върху производителността на алгоритъма. Описани са основните стъпки на алгоритъма. Разяснена е функцията за изчисляване на разстояние и методът за избор на клас на разпознатата цифра. Представени са експериментални резултати. Според резултатите са обобщени препоръки за избор на k. Целта е да се повиши производителността на kNN алгоритъма при задачата за разпознаване на ръкописни цифри по отношение на два критерия – процент на правилно разпознатите входни данни и време за разпознаване. Тестовете се провеждат с 946 примера на изображения на цифри от 0 до 9. Алгоритъмът се изпълнява с набор от 946 цифри за разпознаване. Тестовете се провеждат с различни стойности на параметъра k. Доброто време за разпознаване прави алгоритъма подходящ за работа в системи в реално време, където големи набори от данни трябва да се обработват бързо (например при роботи и контролери).

Г.8-9

Genchev P., Karova M., Analysis of some issues in risk assessment for information security., Computer Science and Technologies, TU-Varna, 2019, Vol. 1, p.p. 62-70, ISSN: 1312-3335. (http://csejournal.cs.tu-varna.bg/cse_journal_2019.pdf)

Abstract:

In the modern world, the importance of information security is growing. This is why many organizations are building information security management systems. The basis of these systems is risk management. This article discusses some issues related to risk assessment in building information security management systems. An attempt has been made to summarize and unify problems and to clarify the causes of these issues. A more detailed analysis of some of the problems has been made and tasks have been formulated to eliminate or to reduce the cause is impact of the causes of the problems. The problems with risk assessment methods, problems related to subjective factor, missed or

undervalued sources of risk and organizational problems are discussed. The problems associated with risk assessment methods, reduce the gaps and underestimate the sources of risk.

Резюме:

В съвременния свят значението на информационната сигурност нараства. Ето защо много организации изграждат системи за управление на информационната сигурност. Основата на тези системи е управлението на риска. Тази статия обсъжда някои въпроси, свързани с оценката на риска при изграждането на системи за управление на информационната сигурност. Направен е опит за обобщаване и унифициране на проблемите и изясняване на причините за тях. На някои от проблемите е направен по-детайлен анализ и са формулирани задачи за отстраняване или намаляване на причината е въздействието на причините за проблемите. Обсъждат се проблеми с методите за оценка на риска, проблеми, свързани със субективен фактор, пропуснати или подценени източници на риск и организационни проблеми. Проблемите, свързани с методите за оценка на риска, намаляват пропуските и подценяват източниците на риск.

Г.8-10

Karova M., Desktop Information System for Employee Management, Proceeding of XIX INTERNATIONAL SCIENTIFIC CONGRESS MACHINES, TECHNOLOGIES, MATERIALS 2022, vol. 4, 07-10.09.2022, pp. 290-293, VARNA, BULGARIA, PUBLISHER: SCIENTIFIC TECHNICAL UNION OF MECHANICAL ENGINEERING, INDUSTRY-4.0 ISSN 2535-0021 (Print), ISSN 2535-003X (Online). (https://stumejournals.com/journals/mtm/2022/9/318)

Abstract:

The report presents a developed Desktop Information System for Employee Management. The system includes database development and encryption using a special algorithm to create an encryption key. The main goal of the development is to provide two types of protection: at the entrance to the system and in the transmission and data storage.

The system must include the following safeguards: 1) Control of access to the system by filling in the personal identification number and password, individual for each employee; 2) Control over the number of failed login attempts; 3) Ensuring the possibility of secure communication between the application and the server; 4) Ensuring an input data protection through irreversible encryption of the password with a specially created system key and measures against SQL injections. The system includes four access levels: Employees, Executives or Managers, Directors and Administrators.

The information system provides the following functionalities, depending on the access levels: entering tasks, registering users, entering priorities for tasks,

entering the status of tasks, reviewing entered tasks, editing tasks and their status, deleting tasks, reviewing , add, edit and delete all users in the system; and others.

The database consists of five tables: Employees, Tasks, Task_Priorities, Task_States and Task_Archive.

The encryption algorithm is based on the PBKDF2 (Password-Based Key Derivation Function 2) function with 10000 iterations. The unique key is generated when a new user is registered in the system. It is formed from the current date and the time of registration in seconds and the last three digits of the EGN in reverse order. The date is a fractional number and the whole part is divided by the fractional part. The key is recorded in the database as a "unique identification key" to the respective user.

Резюме:

Докладът представя разработена настолна информационна система за управление на служителите. Системата включва разработване на база данни и криптиране с помощта на специален алгоритъм за създаване на ключ за криптиране. Основната цел на разработката е да осигури два вида защита: на входа на системата и при предаване и съхранение на данни.

Системата трябва да включва следните гаранции: 1) Контрол на достъпа до системата чрез попълване на ЕГН и парола, индивидуални за всеки служител; 2) Контрол върху броя неуспешни опити за влизане; 3) Осигуряване на възможност за сигурна комуникация между приложението и сървъра; 4) Осигуряване на защита на входните данни чрез необратимо криптиране на паролата със специално създаден системен ключ и мерки срещу SQL инжекции. Системата включва четири нива на достъп: служители, ръководители или мениджъри, директори и администратори.

Информационната система предоставя следните функционалности, в зависимост от нивата на достъп: въвеждане на задачи, регистриране на потребители, въвеждане на приоритети за задачи, въвеждане на статус на задачи, преглед на въведени задачи, редактиране на задачи и техния статус, изтриване на задачи, преглед, добавяне, редактиране и изтрийте всички потребители в системата; и други.

Базата данни се състои от пет таблици: Employees, Tasks, Task_Priorities, Task_States и Task_Archive.

Алгоритъмът за криптиране се основава на функцията PBKDF2 (функция за извличане на ключ, базирана на парола 2) с 10 000 итерации. Уникалният ключ се генерира при регистриране на нов потребител в системата. Формира се от текущата дата и час на регистрация в секунди и последните три цифри на ЕГН в обратен ред. Датата е дробно число и цялата част е разделена на дробната част. Ключът се записва в базата данни като "уникален идентификационен ключ" за съответния потребител.

Г.8-11

Todorov D., Zheynov Zh., Valchanov H., Karova M., Penev I., Investigation of the influence of a template matrix on the embedding of information in an image, Annual Journal of Technical University of Varna, vol, 5, No 2 (2021), Technical University of Varna, pp. 140-145, 2021, ISSN: 2603-316X. (https://aj-tuv.org/index.php/ajtuv/article/view/234/88)

Abstract:

Steganography is a modern approach to protect classified data against malicious attacks and misuse. Presented, accordingly, in this paper is a novel method for steganographic embedding of information. A template matrix is used for screening the original message embedded in an image. The efficiency of the steganographic embedding depends on the length of the message. The particular dependency is, therefore, the primary focus of the proposed work. Stego images or processed images are rela-tively small in size and are suitable for use in transporting messages in a communication environment. The processing times are within normal limits, but they are also highly dependent on the characteristics of the hardware host system. It can be seen that the retrieval time is less than the embedding time of the message, although the two operations are rather reversible and it is assumed that they are likely to have identical execution time in view of the fact that the use of the template is dependent on the length of the message, which is used in the retrieval, and practically everything outside it is ignored. The end results of the experiment were extremely satisfactory with the percentage of successfully retrieved messages being more than 90%, and the size of the processed images with embedded messages being fully acceptable and capable of being used in a communication environment.

Резюме:

Стеганографията е модерен подход за защита на класифицирани данни срещу злонамерени атаки и злоупотреба. Съответно в тази статия е представен нов метод за стеганографско вграждане на информация. Използва се шаблонна матрица за екраниране на оригиналното съобщение, вградено в изображение. Ефективността на стеганографското вграждане зависи от дължината на съобщението. Следователно конкретната зависимост е основният фокус на предложената работа. Стего изображенията или обработените изображения са относително малки по размер и са подходящи за използване при транспортиране на съобщения в комуникационна среда. Времената за обработка са в нормални граници, но също така силно зависят от характеристиките на хардуерната хост система. Може да се види, че времето за извличане е по-малко от времето за вграждане на съобщението, въпреки че двете операции са по-скоро обратими и се предполага, че е вероятно да имат идентично време за изпълнение с оглед на факта, че използването на шаблона е в зависимост от

дължината на съобщението, което се използва при извличането, и практически всичко извън него се игнорира. Крайните резултати от експеримента са изключително задоволителни, като процентът на успешно извлечените съобщения е над 90%, а размерът на обработените изображения с вградени съобщения е напълно приемлив и годен за използване в комуникационна среда.

Г.8-12

Жейнов Ж., Карова М., Приложение на генетичен алгоритъм при моделиране на оптично поле, Международна научно-практическа конференция „Математиката като приложна и фундаментална наука". ИУ-Варна, 2015, с.178-185. ISBN 978-954-21-0860-3, инф.сайт http://conference.ue-varna.bg/math/bg/srokove.html, публикация: . https://drive.google.com/drive/folders/1536GGj9vvT2dH2MoBmTM_SJX8r_U6Asl

Abstract:

The paper presents an application of a Genetic Algorithm (GA) to find the amplitude-phase distribution of an optical field at the open end of a multimode stepped optical fiber to produce a specified far-zone radiation field. The Genetic algorithm (GA) is applied as an optimization method for the synthesis of the aperture amplitude-phase distribution. The characteristic of the considered electrodynamic problem is the large number presence of parameters, which can be discrete, continuous, or both. The parameters are subject to implementation restrictions. In the GA program implementation, the chromosomes represent a one-dimensional array of P number of 32-bit genes, where P is the number of propagating modes. The initial amplitude and initial phase for each mode are coded in the gene, and the amplitudes and phases of the modes are represented by 16 bits each. An appropriate objective function is chosen depending on the total normalized field amplitude and the set field amplitude at a point number. The better chromosome has a smaller objective function. Genetic operators are applied, and the selection is important for faster convergence of the algorithm. The time to obtain a satisfactory solution of the considered problem is proportional to the number of analyzed modes and weakly depends on the number of considered points. The values of crossover and mutation coefficients have a weak influence on the final result.

Резюме:

Докладът представя едно приложение на Генетичен алгоритъм (ГА) за намиране на амплитудно-фазово разпределение на оптично поле в отворен край на многомодово стъпално оптично влакно за създаване на определено поле на излъчване в далечната зона. Генетичният алгоритъм (ГА) се прилага като метод за оптимизация на синтеза на апертурното амплитудно-фазово

разпределение. Характерно за разглежданата електродинамична задача е наличието на голям брой параметри, които могат да бъдат дискретни, непрекъснати или двата вида. Върху параметрите са наложени ограничения, свързани с реализацията. При програмната реализация на ГА хромозомите представляват едномерен масив от P на брой 32-битови гени, като P е броя на разпространяващите се моди. Началната амплитуда и началната фаза за всяка една мода се кодират в гена като амплитудите и фазите на модите се представят с по 16 бита. Избрана е подходяща целева функция, зависеща от сумарната нормирана амплитуда на полето и зададената амплитуда на полето в точка с определен номер. По-добрата хромозома има по-малка целева функция. Приложени са генетични оператори, като селекцията има важно значение за по-бърза сходимост на алгоритъма. Времето за получаване на задоволително решение на разглежданата задача е пропорционално на броя на анализираните моди и слабо зависи от броя на разглежданите точки. Слабо влияние на крайния резултат оказват стойностите на коефициентите на кръстосване и мутация.

Г.8-13

Todorov D., Karova M., Appropriate Conversion of Machine Learning Data, Annual Journal of Technical University of Varna, Vol. 6, No 2, 2022, ISSN 2603-316X (https://aj-tuv.org/index.php/ajtuv/article/view/262/97)

Abstract:

Data is an important part of computer technology and, as such, explains the strong dependence of machine learning algorithms on it. The data can be categorized into four main types: Numeric data, Categorized data, Time interval data and Text. The secret keys from the synchronous encryption algorithms AES, DES, TripleDES and RC2 are used as input data. The aim is to achieve recognition of the type of encryption algorithm of a secret key from machine learning algorithms. The second task is to determine the environment in which the data will exist during the implementation of the algorithm. It must be consistent with the data, in symbiosis with it and create sufficient contrast to the representation of the different data units. This contrast is of crucial importance for the learning machine learning algorithms. The term homogeneous environment is widespread in many fields of science. It can be determined that a homogeneous environment is an environment in which the data and their environment are presented with the same type, size and number of symbols of equal total length. The clearly defined individual data unit differences lead to more accurate operation of algorithms. The operation of any corresponding algorithm is directly dependent on the type of data and the proper data representation increases the productivity of these algorithms. Advanced in the present article is an algorithm for data pre-processing in a form that is most suitable for machine learning algorithms, with cryptographic secret keys being used as input data. The experimental results were satisfactory, and with

the utilization of secret keys with significant differences, the recognition obtained is about 100%.

Резюме:

Данните са важна част от компютърната технология и като такива обясняват силната зависимост на алгоритмите за машинно обучение от тях. Данните могат да бъдат категоризирани в четири основни типа: числови данни, категоризирани данни, данни за времеви интервал и текст. Като входни данни се използват секретните ключове от алгоритмите за синхронно криптиране AES, DES, TripleDES и RC2. Целта е да се постигне разпознаване на типа алгоритъм за криптиране на таен ключ от алгоритмите за машинно обучение. Втората задача е да се определи средата, в която ще съществуват данните по време на изпълнението на алгоритъма. Тя трябва да бъде в съответствие с данните, в симбиоза с тях и да създава достатъчен контраст с представянето на различните единици данни. Този контраст е от решаващо значение за алгоритмите за обучение на машината. Терминът хомогенна среда е широко разпространен в много области на науката. Може да се определи, че хомогенна среда е среда, в която данните и тяхната среда са представени с еднакъв тип, размер и брой символи с еднаква обща дължина. Ясно дефинираните разлики в отделните единици данни водят до по-точна работа на алгоритмите. Работата на всеки съответен алгоритъм зависи пряко от типа на данните и правилното представяне на данните, което увеличава производителността на тези алгоритми. Разширен и подобрен в настоящата статия е алгоритъм за предварителна обработка на данни във форма, която е най-подходяща за алгоритми за машинно обучение, като криптографските секретни ключове се използват като входни данни. Експерименталните резултати са добри и при използването на секретни ключове със значителни разлики, полученото разпознаване е около 100%.

Г.8-14

Генчев П., Карова М., Оценка на риска в системи за управление на сигурността на информацията – същност и насоки, сп. Компютърни науки и технологии, ТУ-Варна, 2018, бр. 2, pp. 96-104, ISSN: 1312-3335, (http://csejournal.cs.tu-varna.bg/cse_journal_2_2018.pdf)

Abstract:

In the modern world, the importance of information security is increasing more and more. This is why many organizations are building information security management systems. At the heart of these systems is the risk management. This article examines the main requirements of ISO standards in this area. The main attention is paid to the requirements for information security risk assessment activities. The material describes some of the problems associated with these

activities and described in cited articles on information security topics. The major emphasis is placed on risk identification, risk analysis, risk assessment, risk treatment, risk acceptance, risk communication and discussion, risk monitoring and review, risk assessment. The problems in risk assessment are shown: 1) lack of information on specific implementations; 2) campaignability; 3) uncertainty; 4) efficiency; 5) superficiality; 6) wrong choice; 7) multivariate; 8) complexity; 9) Subjectivity; 10) collection and processing of data. Conclusions related to overcoming these problems and increasing the effectiveness of risk assessment for information security have been made.

Резюме:

В съвременния свят все повече нараства значението на сигурността на информацията. Това е причина много организации да изграждат системи за управление на сигурността на информацията. В основата на тези системи е заложено управление на риска. В тази статия са разгледани основните изисквания на стандартите на ISO в тази сфера. Основно внимание е отделено на изискванията към дейностите по оценка на риска за сигурността на информацията. В материала са описани някои проблеми, свързани с тези дейности и описани в цитирани статии по теми за сигурността на информацията. Основен акцент е поставен върху идентифициране на риска, анализ на риска, преценяване на риска, третиране на риска, приемане на риска, съобщаване и обсъждане на риска, мониторинг и преглед на риска, оценяване на риска. Показани са проблемите при оценка на риска: 1)липсва информация за конкретни реализации; 2) кампанийност; 3) несигурност; 4) ефективност; 5) повърхностност; 6) грешен избор; 7) многовариантност; 8) сложност; 9) Субективност; 10) Събиране и обработване на данни. Направени са изводи, свързани с преодоляване на тези проблеми и повишаване на ефективността на оценката на риска за информационната сигурност.

Г.8-15

Penev I., Karova M., Todorova M., On the optimum choice of the K Parameter in Hand-Written Digit Recognition by kNN in comparison to SVM, INTERNATIONAL JOURNAL OF NEURAL NETWORKS and ADVANCED APPLICATIONS, vol. 3, NAUN, pp. 47-52, 2016, ISSN: 2313-0563. (http://www.naun.org/main/NAUN/neural/2016/a162016-082.pdf)

Abstract:

The paper concerns the application of two machine learning algorithms – k-nearest neighbor (kNN) and support vector machines (SVM) for solving the problem of hand-written digit recognition. The main goal of the work is to derive recommendations for the choice of the k parameter in kNN (number of the nearest neighbors) so that the performance of kNN to be the near (or even better than) the

performance of SVM – one of the most power machine learning known algorithms. The kNN distance function as well as the method for choosing a class of the recognized digit are explained. The presented experimental results show comparison of the kNN performance to SVM, regarding two criteria – percent of the correctly recognized digit images and run time for recognition. As a final result recommendations for the choice of the k value are summarized.

Резюме:

Докладът се отнася до приложението на два алгоритъма за машинно обучение – алгоритъма на най-близкия съсед (kNN) и Support Vector Mashine (SVM) за решаване на проблема с разпознаването на ръкописни цифри. Основната цел на работата е да се изведат препоръки за избора на параметъра k в kNN (броя на най-близките съседи), така че производителността на kNN да бъде близка (или дори по-добра от) производителността на SVM – един от повечето познати алгоритми за машинно обучение. Обяснена е функцията за разстояние kNN, както и методът за избор на клас на разпознатата цифра. Представените експериментални резултати показват сравнение на производителността на kNN спрямо SVM, по отношение на два критерия – процент на правилно разпознатите цифрови изображения и време за разпознаване. Като краен резултат са обобщени препоръки за избор на стойността на k.

Г.8-16

Genchev P., Mileva-Karova M., Determining the period for information security risk checks, Proceedings of International Scientific Conference CONFSEC 2021, pp.60-63, ISSN 2603-2945 (Print), ISSN 2603-2953 (Web). (https://confsec.eu/sbornik/2021.pdf)

Abstract:

Risk assessments are not a one-off action, but there are no formal guidelines on when and how often a risk assessment should be carried out. Changing factors affect the risk assessment parameters. The strongest influence of these changes is the probabil ity of an accident. The article describes the main parameters of a model that is built on the basis of an asset and the incident scenarios defined for it. An analysis of the changes in the probability of an accident has been made. Dependencies are derived to determine the appropr iate periods for checking the risk factors. These periods must ensure an acceptable level of risk, which is within acceptable levels for the organization.

Резюме:

Оценките на риска не са еднократно действие, но няма официални указания кога и колко често трябва да се извършва оценка на риска. Променящите се фактори влияят върху параметрите за оценка на риска. Най-силното влияние на тези промени е вероятността от инцидент. Статията

описва основните параметри на модел, който е изграден на базата на актив и сценариите на инциденти, дефинирани за него. Направен е анализ на промените във вероятността от злополука. Изведени са зависимости, за да се определят подходящите периоди за проверка на рисковите фактори. Тези периоди трябва да гарантират приемливо ниво на риск, което е в рамките на допустимите нива за организацията.

Г.8-17

Karova M. , Avramova N., Penev I., Petkova J. Management of Software Project using Genetic Algorithm, Procedings of ICEST 2012, pp.403-406, 28-30 June, 2012, Veliko Tarnovo, Bulgaria, ISBN: 978-619-167-002-4, (http://www.icestconf.org/wp-content/uploads/2016/proceedings/icest_2012_02.pdf, http://rcvt.tu-sofia.bg/ICEST2012_2_32.pdf)

Abstract:

This paper presents a heuristic method – genetic algorithm to solve the Project Management Problem. The problem is complex, NP complete. The objectives are to minimize the project duration and to minimize the project cost. The constraints are that each task must be performed by at least one person and every person must have a set of knowledge. The algorithm must define the degree of dedication of each employee. IGAPM (Implementation Genetic Algorithm for ProjectManagement) is a part of a group planning algorithms and it is defined as a tool for planning projects (in particular, and software projects). The application provides the ability to manage projects so that project will be completed at - short term and / or minimal cost and with minimal overlapping activities. IGAPM provides: an interface enabling the user to implementation of projects and their saving in format XML; GA management through its basic and additional parameters to obtain the optimal solution for each run of the GA (the decision to submit via charts) and removal of most – good fitness function. The Genetic Algorithm (IGAPM) proposes a binary chromosome encoding, single crossover, two types of selection and flip-bit mutation.

It analyzes and evaluates the Genetic Algorithm, changing the following parameters: number of generations, number of chromosomes in the population, crossover and mutation probability, type of selection and improvement of the initial population. For a finite number starts with a constant configuration of genetic parameters and genetic operators, the variations of the values of fitness function are relatively constant. The analysis is based on the different number of GA generations. The experiments were performed with common parameters: number of chromosomes in the population = 10, crossover rate Pc = 0.65, mutation rate Pm = 0.55, weight of the critical path ucr = 0.95, weight cost ucost = 0.15 and weight of overlapping activities upr = 0.5. Additional parameter is the type of selection - by rank. The fitness function finds its optimal solution for a

small number of generations and their further increase is not necessary. The role of mutation or other factors is important in order to escape the algorithm from local minimum.

Резюме:

Докладът представя евристичен метод – генетичен алгоритъм за решаване на проблема за управление на проекти. Проблемът е комплексен, NP-complete. Целите са да се сведе до минимум продължителността на проекта и да се сведат до минимум разходите по проекта. Ограниченията са, че всяка задача трябва да се изпълнява от поне един човек и всеки трябва да има набор от знания. Алгоритъмът трябва да определи степента на отдаденост на всеки служител. IGAPM (Implementation Genetic Algorithm for Project Management) е част от групови алгоритми за планиране и се определя като инструмент за планиране на проекти (по-специално и софтуерни проекти). Приложението предоставя възможност за управление на проекти, така че проектът да бъде завършен в - кратък срок и/или минимални разходи и с минимално припокриване на дейности. IGAPM предоставя: 1)интерфейс, позволяващ на потребителя изпълнение на проекти и записването им във формат XML; 2)управление на ГА чрез неговите основни и допълнителни параметри за получаване на оптималното решение за всяко изпълнение на ГА(решението за подаване чрез диаграми) и премахване на най-добрата фитнес функция. Генетичният алгоритъм (IGAPM) предлага бинарно хромозомно кодиране, единично кръстосване, два вида селекция и флип-битова мутация.

ГА се анализира и се оценява като се променят следните параметри: брой поколения, брой хромозоми в популацията, вероятност за кръстосване и мутация, тип селекция и подобряване на първоначалната популация. За ограничен брой стартирания се започва с постоянна конфигурация на генетични параметри и генетични оператори, вариациите на стойностите на фитнес функцията са относително постоянни. Анализът се основава на различния брой поколения на GA. Експериментите са проведени с общи параметри: брой хромозоми в популацията = 10, скорост на кръстосване Pc = 0,65, степен на мутация Pm = 0,55, тегло на критичния път ucr = 0,95, тегло на цената ucost = 0,15 и тегло на припокриващи се дейности upr = 0,5. Допълнителен параметър е типа на селекцията - по ранг. Фитнес функцията намира своето оптимално решение за малък брой поколения и не е необходимо по-нататъшното им увеличаване. Ролята на мутацията или други фактори е важна, за да се избегне попадането на алгоритъма в локален минимум.

Г.8-18

Karova M., Grigorova P. Catalogue System for Electronic Documents Management and Control, Proceeding of ICEST 2008, pp. 584-587, 25-27 June

2008, Nis, Serbia, ISBN: 978-86-85195-61-7, (http://rcvt.tu-sofia.bg/ICEST2008_141.pdf, http://www.icestconf.org/wp-content/uploads/2016/proceedings/icest_2008.pdf)

Abstract:

This paper introduces a desktop based catalogue system for managing and control of electronic documents. Electronic documents are wide spread and there is a need for a tool with witch to sort, search and store these files in easily accessible and convenient way. There are few other catalogue systems for managing this kind of data but they are somewhat limited. The currently described solution extends the data stored about the electronic document while preserving the initial file, using MS SQL powered database. The basic tasks performed by the application are: 1) input of additional data for the document; 2) searching a document, based on the input data. The electronic documents can be very different in format and contents that makes the automatic extracting of the aforementioned information nearly impossible. After input of all the needed data, the user can then easily search by random criteria.

One of the most important functions of the system is the possibility of searching files based on their additional data. It's independent from the selection and is invoked from the main menu. The user can search using criteria like filename, extension, genre, encoding and all the other data, stored in the database, also allowing multiple criteria selection.

Резюме:

Този документ представя десктоп базирана каталожна система за управление и контрол на електронни документи. Електронните документи са широко разпространени и има нужда от инструмент с който да се сортират, търсят и съхраняват тези файлове по лесно достъпен и удобен начин. Има малък брой други каталожни системи за управление на този вид данни, но те са донякъде ограничени. Описаното в момента решение разширява данните, съхранени за електронния документ, като същевременно запазва първоначалния файл, използвайки MS SQL база данни. Основните задачи, които изпълнява приложението са: 1) въвеждане на допълнителни данни за документа; 2) търсене в документ по входните данни. Електронните документи могат да бъдат много различни по формат и съдържание, което прави автоматичното извличане на горепосочената информация почти невъзможно. След въвеждане на всички необходими данни, потребителят може лесно да търси по произволен критерий.

Една от най-важните функции на системата е възможността за търсене на файлове въз основа на техните допълнителни данни. Тя е независима от избора и се извиква от главното меню. Потребителят може да търси, използвайки критерии като име на файл, разширение, жанр, кодиране и

всички други данни, съхранени в базата данни, което също позволява избор на множество критерии.

Г.8-19

Daskalov S., Karova M., Cryptographic Protocol With a Proposed Cipher and Aperiodic Key Replacement, Proceedings of ICEST 2015, pp.224-227, 24-26 June, Sofia, Bulgaria, ISBN: 978-619-167-182-3, (http://rcvt.tu-sofia.bg/ICEST2015_54.pdf)

Abstract:

The proposed cryptographic protocol implements a cipher with block and key length of 2n bits. For demonstration of the encryption algorithm and the majority of the experiments a length of 64 bits is chosen. The cipher uses a symmetrical key algorithm with key length equal to the block length. The encryption consists of n (n=log2blocklength) major phases and a final inversion phase. The block, with a length L equal to 64, the phases are 6+1. During the six major phases the ciphertext is divided into segments of length 2k-1, where k is the number of the current phase. In each phase the algorithm performs L/2k operations with neighboring segments. The result of each such operation forms a segment of greater rank, having the combined length of the two original segments and preserving their location in the ciphertext. The processing of each pair of segments is controlled by a predefined bit in the key and there are three possible outcomes of the operation: 1) The value of the control bit of the key is 0 – The two segments preserve their location and value; 2) The value of the control bit of the key is 1 and the two segments are not identical – In this case the segments preserve their value but swap their location; 3) The value of the control bit of the key is 1 and the two segments are identical – In this case each bit of the two segments is inverted. The last bit of the key is used for an inversion of the cipher text block if the bit's value is 1. Each key is used a seemingly random number of times between 0 and 15, afterwards the next generated key is encrypted and transmitted using the previous one. The initial key is established using Public key encryption. The results are separated in 4 categories: 1) Processing speed comparison with common encryption; 2) Analysis of the difference between plaintext and ciphertext algorithms; 3) Analysis of the randomness of key durability; 4) Performance analysis of the algorithm when using various block sizes.

Резюме:

Предложеният криптографски протокол реализира шифър с блок и дължина на ключа от 2n бита. За демонстрация на алгоритъма за криптиране и по-голямата част от експериментите е избрана дължина от 64 бита. Шифърът използва алгоритъм със симетричен ключ с дължина на ключа, равна на дължината на блока. Шифроването се състои от n

(n=log2blocklength) основни фази и крайна фаза на инверсия. Блокът е с дължина L равна на 64, фазите са 6+1. По време на шестте основни фази шифъртекстът се разделя на сегменти с дължина 2k-1, където k е номерът на текущата фаза. Във всяка фаза алгоритъмът извършва L/2k операции със съседни сегменти. Резултатът от всяка такава операция формира сегмент с по-висок ранг, имащ общата дължина на двата оригинални сегмента и запазвайки тяхното местоположение в шифрования текст. Обработката на всяка двойка сегменти се контролира от предварително дефиниран бит в ключа и има три възможни резултата от операцията: 1) Стойността на контролния бит на ключа е 0 – Двата сегмента запазват местоположението и стойността си; 2) Стойността на контролния бит на ключа е 1 и двата сегмента не са идентични – В този случай сегментите запазват стойността си, но разменят местоположението си; 3) Стойността на контролния бит на ключа е 1 и двата сегмента са идентични – В този случай всеки бит от двата сегмента е обърнат. Последният бит от ключа се използва за инверсия на блока за шифрован текст, ако стойността на бита е 1. Всеки ключ се използва привидно произволен брой пъти между 0 и 15, след което следващият генериран ключ се криптира и предава с помощта на предишния. Първоначалният ключ се установява чрез криптиране с публичен ключ. Резултатите са разделени в 4 категории: 1) Сравнение на скоростта на обработка с общо криптиране; 2) Анализ на разликата между алгоритмите за първоначален и шифрован текст; 3) Анализ на случайността на издръжливостта на ключовете; 4) Анализ на ефективността на алгоритъма при използване на различни размери блокове.

Г.8-20

Bojikova V., Karova M., An Approach to Measure the Cost of Program Restructuring, Proceedings of ICEST 2002, pp.669-671, 1-4 October,2002, Nis, Yugoslavia, ISBN: 86-80135-69-0. (http://rcvt.tu-sofia.bg/PO4.5.pdf)

Abstract:

The program restructuring tools make it easier to rewrite software, and so should be a key part of every software development environment. The problem is that software developers do not know how to restructure programs. This paper presents an approach for measuring the costs of program restructuring. The notion “distance” between the initial and the final software decisions was introduced.

Резюме:

Инструментите за преструктуриране на програмата улесняват пренаписване на софтуер и затова трябва да бъде ключова част от всяка софтуерна среда за развитие. Проблемът е, че използвайки този софтуер, разработчиците не знаят как да преструктурират програмите. Този доклад представя подход за измерване на разходите по дадена програма при

преструктуриране. Въведено е понятието „разстояние” между началния и крайния вариант на софтуерното решение.

Г.8-21

Николов В., Карова М., Подход за изграждане на концептуално описание на софтуерен проект, сп. Компютърни науки и технологии, год.XIII, бр.1/2015, pp.138-143, ТУ-Варна, България, ISSN: 1312-3335. (http://csejournal.cs.tu-varna.bg/cse_journal_1_2015.pdf)

Abstract:

The article presents and describes a detailed scheme of building a conceptual description of a software application. The correct description of the details in the development of the project, from its beginning to its completion, can not only lead to the clarification of its ideas and goals, but also it accelerates the development and it increases its quality.

The presented approach to conceptual description of software projects borrows fragments from different versions of the Project Management Body of Knowledge (PMBOK Guide), which presents a standard terminology and recommendations for general project management. The actions and steps of composing the description are considered as recommendations, resulting in a document that facilitates the development application process. As a result of the implementation of the schematically presented activities, a text document is compiled with a detailed preliminary description of the software project: 1)definition of goals; 2)WBS creation; 3)determination of the necessary resources (labor, material and cost resources); 4)determination of the project cost; 5)definition and visualization of the main activities; 6)planning the employment of team members; 7)software quality management; 8)risk management; 9)determining the probability of a certain event or risk factor occurring. When the Agile programming techniques are applyed, the time intervals for meetings between the development team and the customers/owners of the application are determined in advance.

Резюме:

В статията е представена и описана подробна схема на изграждане на концептуално описание на софтуерно приложение. Правилното и коректно описване на детайлите в развитието на проекта, от неговото начало до приключването му, може не само да доведе до изясняване на неговите идеи и цели, но също така да ускорят развитието и повишат качеството му.

В представения подход за концептуално описание на софтуерни проекти са заимствани фрагменти от различни версии на Project Management Body of Knowledge (PMBOK Guide), която представя стандартна терминология и препоръки за управление на проекти от общ характер. Действията и стъпките по съставяне на описанието се разглеждат като препоръки, в резултат на което се получава документ, който улеснява

процеса на разработка на приложението. В резултат от изпълнението на схематично представените дейности се съставя текстов документ с подробно предварително описание на софтуерния проект: 1)дефиниране на цели; 2)създаване на WBS структура; 3)определянето на необходимите ресурси (работни, материални и разходни ресурси); 4)определянето на цената на проекта; 5)дефинирането и визуализацията на основните дейности; 6)планирането на заетостта на участниците в екипа; 7)управлението на качеството на софтуера; 8)управлението на риска; 9)определяне на вероятността за сбъдване на определено събитие или рисков фактор. При прилагане на техники като Agile програмиране, предварително се определят интервалите от време, през които да се правят срещи между екипа за разработка и клиентите/собственици на приложението.

Г.8-22

Василев Н., Карова М., Анализ и изследване на алгоритми за намиране на път в среда, сп. Компютърни науки и технологии, бр.2/2016, pp.74-81, ТУ-Варна, България, ISSN: 1312-3335, (http://csejournal.cs.tu-varna.bg/cse_journal_2_2016.pdf)

Abstract:

The paper aims to discuss and compare three different robot orientation problems in a static environment. The robot is treated as a single point in a two-dimensional array. The environment is represented as a two-dimensional array, and the path (chromosome) as an array of points that are pairs of integer values. A standard DFS algorithm is used to create a "perfect maze" (which has only one possible path from the entry point to the exit point) and a simple obstacle clearing function to analyze the results. The method by which each chromosome is generated is based on the random generation of integers in the range 1 to 4, which are understood as four directions (forward, backward, up, down). A parameter of the method is the population size. The goal of the method is to find the shortest N paths from all chromosomes. At the beginning, two vectors are initialized that keep the sizes and the indexes of each chromosome. The size vector is sorted and the size of the vector is compared to the size of each chromosome. If they are identical, the index in the index vector is added, the desired chromosomes are swapped, and all others are cleared. It is recommended that a detach be done after the generation and not after the modification, because the execution time is extended up to ten times. To achieve the goal, modified genetic algorithms are used. In all cases, a path generation is random. The execution of the algorithms is completely dynamic. Genetic algorithms are fast, but they don't always give a good result. The Backtracking works best in the "perfect maze" case, and genetic algorithm - in any other environment. The larger the population, the better and better the solution. The crossover of the solutions is also used for the best solution.

In this case, the more chromosomes there are, the more generations will be formed.

Резюме:

Докладът има за цел да дискутира и сравни три различни проблема за ориентиране на робот в статична среда. Роботът се приема като една точка в двумерен масив. Средата се представя като двумерен масив, а пътят (хромозома), като масив от точки, които са чифт от целочислени стойности. Използва се стандартен DFS алгоритъм за създаване на „перфектен лабиринт“(който има само един възможен път от входната до изходната точка) и проста функция за изчистване на препятствия за анализ на резултатите. Методът, по който се генерира всяка една хромозома, е базиран на случайно генериране на цели числа в диапазона от 1 до 4, които се разбират като четири посоки (напред, назад, нагоре, надолу). Параметър на метода е размерът на популацията. Целта на метода е да се намерят най-кратките N пътища от всичките хромозоми. В началото се инициализират два вектора, които пазят размерите и индексите на всяка хромозома. Векторът с размерите се сортира и размерът на вектора се сравнява с размера на всяка хромозома. Ако са идентични, се добавя индексът във вектора за индекси, разменят се желаните хромозоми, а всички останали се изчистват. Препоръчително е отделянето да се извършва след генерацията, а не след модификацията, защото времето за изпълнение се удължава до десет пъти. За постигане на целта се използват модифицирани генетични алгоритми. Във всички случаи генерацията на път се получава на случаен принцип. Изпълнението на алгоритмите е напълно динамично. Генетичните алгоритми са бързи, но не винаги дават добър резултат. Връщането назад работи най-добре в случая „перфектен лабиринт“, а генетичният алгоритъм-във всякаква друга среда. Колкото е по-голяма популацията, толкова по-добро и качествено е решението. За най-добро решение се използва и кръстосване на решенията. В случая колкото повече хромозоми съществуват, толкова повече поколения ще се образуват.

Г.8-23

Naumov V., Karova M., Zhelyazkov D., Todorova M., Penev I., Nikolov V., Petkov V., Robot Path Planning Algorithm, INTERNATIONAL JOURNAL OF COMPUTERS AND COMMUNICATIONS, Volume 9, 2015, pp.96-99, ISSN: 2074-1294, (http://www.naun.org/main/UPress/cc/2015/a282012-148.pdf)

Abstract:

This paper presents an improvement of a classic Dijkstra algorithm to the domain of sampling-based motion. The algorithm uses an image, obtained by a camera. The algorithm processes the image to convert it into a matrix, presenting the labyrinth with obstacles and walls. Afterwards the algorithm finds the shortest

path to a final target in the labyrinth. In contrast to the classical Dijkstra's algorithm, the presented algorithm compares the size of the robot to the size of the obstacles on the way. A simulation of the algorithm is developed to visualize the movement of the robot. Experimental results, obtained by the simulation, are presented. The algorithm is tested by labyrinths with varying sizes (different width and height in pixels). The following times are measured for each labyrinth: 1)time for labyrinth construction (i.e. converting the image into text format, suitable for processing); 2)time for obtaining a solution (i.e. finding a path to the target); 3)time for the movement of the robot to reach the target. The potential of the proposed results is apparent both in terms of reliability and quality of solutions found.

Резюме:

Тази статия представя подобрение на класическия алгоритъм на Дейкстра в областта на движението, базирано на проба-грешка. Алгоритъмът използва изображение, получено от камера. Алгоритъмът обработва изображението, за да го преобразува в матрица, представяща лабиринта с препятствия и стени. След това алгоритъмът намира най-краткия път до крайната цел в лабиринта. За разлика от класическия алгоритъм на Дейкстра, представеният алгоритъм сравнява размера на робота с размера на препятствията по пътя. Разработена е симулация на алгоритъма за визуализиране на движението на робота. Представени са експериментални резултати, получени от симулацията. Алгоритъмът е тестван с лабиринти с различни размери (различна ширина и височина в пиксели). За всеки лабиринт се измерват следните времена: 1) време за изграждане на лабиринта (т.е. конвертиране на изображението в текстов формат, подходящ за обработка); 2) време за получаване на решение (т.е. намиране на път към целта); 3)време за движение на робота до достигане на целта. Потенциалът на предложените резултати е очевиден както по отношение на надеждността, така и по отношение на качеството на намерените решения.

Г.8-24

Karova M., Nikolova A., Zhekova D., Development of Air Traffic Controller Training Programming Model, Computer Science and Technologies, Publication of Computing and Automation Faculty Technical University of Varna, Vol.1, 2017, pp.106-113, TU-Varna, ISSN: 1312-3335, (http://csejournal.cs.tu-varna.bg/cse_journal_1_2017.pdf)

Abstract:

The article presents a programming model of simulator training for air traffic controllers (ATC). The objective of this research is to conceive, design, and implement an ATC system that can be easily used at schools, on courses or simply

manage an air traffic situation. The advanced simulators facilitate realistic training in the full-spectrum of ATC operations – from approach and departure phases to the enroot phase of flight, as well as ground movement at the airport.

The Mathematical Modeling of Aircraft Trajectory includes two constructors: one for usual trajectory change and one for landing. It is uses Bezier curves: parametric curves given by controlling points. Bezier curves, and more specifically cubic Bezier curves, are a standard tool in many computer-aided design applications such as PhotoShop, InDesign, GIMP, Scribus, etc. The cubic Bezier curves controlling polygon consists of 4 points: start point, end point and two intermediate ones. The advantage is that the curve passes through both of the endpoints while the two intermediate points act as magnets which can easily control the shape of the curve. Moreover, every given curve can be represented as a finite number of such four-point Bezier curves, connected to each other and its smoothness around the connection point can easily be controlled. Many practical problems require the approximation of circular arcs with Bezier curves. The development of the mathematical model includes approximation of arcs using cubic Bezier curves. The programming controllers contain action functions, performed by the user: 1) LoginController.java – controller, responsible for application initialization; 2) MainController.java and FlightController.java - controllers responsible for the main panel (manage the flights). Controller functions are used for airport drawing, runs runaways, the boundary of the flight range, course changing etc; 3) ReportController.java - controller for report writing.

The user interface of the desktop application is built by FXML. The elements of each screen in the application are vector-based controls and graphics resources. The appearance of the application describes using a software called JavaFX Scene Builder. There is a login panel with username and password given in advance by the administrator. Data storage is designed on Oracle 11g XE database, the connection is performed by Hibernate ORM.

The model simulates the control of aircraft landing and aircraft take off, the change of trajectory, the communication with flight control center and more. The presented simulator could extend simulators capabilities: tower simulator, radar simulation, putting dynamical environment and weather modelling, piloting and other advanced ATM tools.

Резюме:

Статията представя модел за програмиране на симулаторно обучение за ръководители на полети (АТС). Целта на това изследване е да се създаде, проектира и внедри система за АТС (КВД), която може лесно да се използва в училища, на курсове или просто да управлява ситуация на въздушно движение. Усъвършенстваните симулатори улесняват реалистично обучение в пълния спектър от операции на АТС (КВД) – от фазите на подход

и излитане до началната фаза на полета, както и движението по земята на летището.

Математическото моделиране на траекторията на самолета включва два конструктора: един за обичайна промяна на траекторията и един за кацане. Той използва криви на Безие: параметрични криви, дадени от контролни точки. Кривите на Безие, и по-специално кубичните криви на Безие, са стандартен инструмент в много приложения за компютърно проектиране като PhotoShop, InDesign, GIMP, Scribus и т.н. Кубичните криви на Безие, контролиращи полигона, се състоят от 4 точки: начална, крайна точка и две междинни. Предимството е, че кривата минава през двете крайни точки, докато двете междинни точки действат като магнити, които могат лесно да контролират формата на кривата. Всяка дадена крива може да бъде представена като краен брой такива четириточкови криви на Безие, свързани една с друга и нейната гладкост около точката на свързване може лесно да се контролира. Много практически проблеми изискват апроксимация на кръгови дъги с криви на Безие. Разработването на математическия модел включва апроксимация на дъги с помощта на кубични криви на Безие. Програмируемите контролери съдържат функции за действие, изпълнявани от потребителя: 1) LoginController.java – контролер, отговорен за инициализацията на приложението; 2) MainController.java и FlightController.java - контролери, отговорни за главния панел (управляват полетите). Функциите на контролера се използват за чертане на летището, границата на полета, промяна на курса и т.н.; 3) ReportController.java - контролер за писане на отчет.

Потребителският интерфейс на настолното приложение е изграден от FXML. Елементите на всеки екран в приложението са векторни контроли и графичен ресурс. Външният вид на приложението се описва с използването на софтуер, наречен JavaFX Scene Builder. Има панел за вход с потребителско име и парола, зададени предварително от администратора. Съхранението на данни е проектирано на Oracle 11g XE база данни, връзката се осъществява от Hibernate ORM.

Моделът, презентиран в доклада, симулира управлението на кацането и излитането на самолета, промяната на траекторията, комуникацията с центъра за управление на полета и др. Представеният симулатор може да разшири възможностите на симулаторите: симулатор на кула, радарна симулация, въвеждане на динамична среда и моделиране на времето, пилотиране и други усъвършенствани инструменти за АТМ (УВД).

Г.8-25

Karova M., Genchev L., Vasilev L., Penev I., The Application of Minimax Decision Rule in Games, Proceedings of ICEST 2011, Serbia, Niš, June 29 - July 1, 2011, ISBN: 978-86-6125-031-6, pp. 889-892, (http://www.icestconf.org/wp-content/uploads/2016/proceedings/icest_2011_03.pdf)

Abstract:

This paper demonstrates three different applications: Minimax algorithm, Alpha Beta pruning algorithm and Genetic Algorithm in games. They are used to evolve a Tic Tac Toe and Chess games. The Minimax decision rule is applied as a solution to twoplayer zero-sum games and in those cases is equal to the Nash equilibrium. Since in these types of games both players work towards the same mutual goal and one player's moves towards winning directly affect the chances of winning for the other player in a negative manner. The Minimax algorithm works by scanning the nodes (and all of its children) of a game tree from a given configuration and evaluates them based on the Minimax theory. The algorithm is in fact a form of depth-first search and on a programme level is normally implemented as a recursive algorithm. Two basic strategies exist for the Minimax algorithm: the first one consists of searching every child of every node of the whole tree and the second limits the depth of the search in order to save computational time.

Tic-tac-toe is a classic example of a game which can be played by a computer using the Minimax algorithm. In this case, Minimax is an ideal solution because the branching factor of the game is only 9, as opposed to more complex games such as Chess, which has a branching factor of 35. The algorithm will work in absolutely the same way as in its general form. The most negative feature of this algorithm is that it requires great computational time in more complex games if it runs in full depth.

The report presents a sort of improvement - the Alpha-beta pruning algorithm. The algorithm returns the same result as pure Minimax but in the best case it does it twice as fast. It literally prunes or cuts off some nodes that cannot lead to a better overall result. The algorithm calculates and keeps track of two variables: alpha and beta, one for each player. Alpha represents the value of the best possible move the current player has made so far. Beta, on the contrary, represents the value of the best possible move the opponent has made so far.

The size of strategies space is defined by the number of all possible game situations, which follows from the question of how many distinct matches can be played. The use of GA implementation improves the optimal paths and decreases the playing time. The encoding of chromosome depends on game problem. Each gene is defined by the corresponding move to be taken. The chromosome is a table with 827 genes to represent each game situation. The fitness function is important to create an efficient GA and it is formed as way:

f(n)=possible win configurations for current player – possible win configurations for opponent player. Once the parents are determined, the offspring is created by one-point crossover. The size of the population is 50 and the number of generations is 50. The optimal result of genetic algorithm for different games is not guaranteed because it depends on the length of the chromosome and the depth of the tree decision.

Резюме:

Този документ демонстрира три различни приложения: алгоритъм Minimax, алгоритъм Alpha Beta и Генетичен Алгоритъм в игрите. Те се използват за разработка на игрите Tic Tac Toe и шах. Правилото за решаване на Minimax се прилага като решение за игри с нулева сума за двама играчи и в тези случаи е равно на равновесието на Nash. Тъй като в тези типове игри и двамата играчи работят за една и съща обща цел и ходовете на един играч към победа директно влияят негативно на шансовете за печалба на другия играч. Алгоритъмът Minimax работи, като сканира възлите (и всички негови деца) на дърво на играта от дадена конфигурация и ги оценява въз основа на теорията на Minimax. Алгоритъмът всъщност е форма на търсене в дълбочина и на програмно ниво обикновено се прилага като рекурсивен алгоритъм. Съществуват две основни стратегии за алгоритъма Minimax: първата се състои в търсене на всички деца на всеки възел в цялото дърво, а втората ограничава дълбочината на търсенето, за да спести изчислително време.

Tic-tac-toe е класически пример за игра, която може да се играе от компютър с помощта на алгоритъма Minimax. В този случай Minimax е идеално решение, тъй като коефициентът на разклоняване на играта е само 9, за разлика от по-сложните игри като шаха, който има коефициент на разклоняване 35. Алгоритъмът ще работи по абсолютно същия начин, както при обща форма. Най-негативната характеристика на този алгоритъм е, че той изисква голямо изчислително време в по-сложни игри, ако работи в пълна дълбочина.

Докладът представя вид подобрение на алгоритъма Alpha-beta. Алгоритъмът връща същия резултат като чистия Minimax, но в най-добрия случай го прави два пъти по-бързо. Той буквално подрязва или отрязва някои възли на графа на играта, които не могат да доведат до по-добър общ резултат. Алгоритъмът изчислява и следи две променливи: алфа и бета, по една за всеки играч. Алфа представлява стойността на най-добрия възможен ход, който настоящият играч е направил досега. Бета, напротив, представлява стойността на най-добрия възможен ход, който противникът е направил досега.

Размерът на пространството за стратегии се определя от броя на всички възможни игрови ситуации, което следва от въпроса колко различни мача могат да се играят. Използването на внедряване на ГА подобрява оптималните пътища и намалява времето за игра. Кодирането на хромозомата зависи от проблема в играта. Всеки ген се определя от съответния ход, който трябва да се предприеме. Хромозомата е таблица с 827 гена, които представят всяка игрова ситуация. Фитнес функцията е важна за създаването на ефективен ГА и се формира по начин:

f(n)=възможни конфигурации за победа за текущия играч – възможни конфигурации за победа за противников играч. След като родителите са определени, потомството се създава чрез едноточково кръстосване. Размерът на популацията е 50, а броят на поколенията е 50. Оптималният резултат от генетичния алгоритъм за различните игри не е гарантиран, защото зависи от дължината на хромозомата и дълбочината на дървовидното решение.

Г.8-26

Penev I., Karova M., Graph-Based Neural Network for Handwritten Digit Recognition. Proceedings of 53-rd International Scientific Conference on Information, Communication and Energy Systems and Technologies (ICEST 2018), 28-30 June 2018, Sozopol, Bulgaria, Iss. 1, Publishing House, Technical University of Sofia, 2018, pp. 322-325, ISBN: 2603-3259. (http://icestconf.org/wp-content/uploads/2018/07/ICEST2018PROC.pdf)

Abstract:

The paper presents building and training of a neural network for handwritten digit recognition. As opposed to the known solutions this work uses computation graphs for building, training and estimating the neural network. This approach has two main advantages: reduces the time for network building and training and achieves relative independence of the constructed network model from the runtime environment. The forming of the computation graphs at each step of the neural network building, training and estimating is described. The structure of the neural network is designed using 2 calculation types: 1) Calculation of digit distance to a definite class; 2) Calculation of probability for belonging of the digit to a definite class. The NN training is performed by backpropagation and stochastic gradient descent algorithms. The results from experimental tests with standard data patterns for handwritten digits are discussed. The best training accuracy achieved is 99.5%. This result is close to the best known results for handwritten digit recognition by Neural Network.

Резюме:

Статията представя изграждането и обучението на невронна мрежа за разпознаване на ръкописни цифри. За разлика от известните решения, тази разработка използва изчислителни графики за изграждане, обучение и оценка на невронната мрежа. Този подход има две основни предимства: намалява времето за изграждане и обучение на мрежата и постига относителна независимост на изградения мрежов модел от средата за изпълнение. Описано е формирането на изчислителните графики на всяка стъпка от изграждането, обучението и оценката на невронната мрежа. Структурата на невронната мрежа е проектирана с помощта на 2 вида изчисления: 1) Изчисляване на цифровото разстояние до определен клас; 2)

Изчисляване на вероятността за принадлежност на цифрата към определен клас. Обучението на NN се извършва чрез алгоритми за обратно разпространение и стохастичен градиент. Обсъждат се резултатите от експериментални тестове със стандартни модели на данни за ръкописни цифри. Най-добрата постигната точност на обучение е 99,5%. Този резултат е близък до най-известните резултати за разпознаване на ръкописни цифри от невронна мрежа.

Г.8-27

Цеков Ц., Обретенов Н., Карова М., Прилагане на RSA алгоритъм при криптиране на съобщения в защитена комуникационна среда, сп. Компютърни науки и технологии, бр.2/2014, pp.98-106, ТУ-Варна, България, ISSN: 1312-3335, (http://csejournal.cs.tu-varna.bg/cse_journal_2_2014.pdf)

Abstract:

The report discusses a development representing a security system that serves to authenticate personal data in order to enter a secure virtual environment. In the developed system, the messages encryption is a part of ensuring the work in a "chat-room", which is hardware secured by a group of computers served by two servers - one main server and one backup server. The servers maintain the database with user records. These data serve to log into a chat room, which is a desktop application. Once registered, through their smartphones, the users use the smartphone-generated codes (passwords) to log in. After successfully entering data, the access to the system is provided. In this virtual environment, the communication takes place through encryption algorithms, ensuring secure correspondence between users. The security (in particular message encryption) is provided by a variant of the RSA algorithm for encrypting information. To facilitate possible access to a secure virtual environment by users, the secure structure includes a smartphone and a personal computer. The application provides a convenient and secure entry into the communication environment, increasing the security of the system. The server stores the login data for the desktop application, which comes from the smartphone used for registration. The information that is sent from the smartphone is the code of the computer from which the chat room will be entered and a user name for entering the chat room. The unique number of the device participating in the chat connection is also sent to the server.

The messages are encrypted is through an improved version of the RSA encryption algorithm.

The number of connection attempts (Maximum Attempts - MA) is a set as a parameter, and after reaching them, a block is loaded that opens a new connection with the selected chat participant. If the connection is established before "MA" is reached, the keys are generated, with which the secure communication between

the two parties will take place. The generated keys are private and public respectively. The public key is immediately sent to the interlocutor. This way, it will send encrypted messages with the same public key.

When a real communication takes place between the two parties, it is "listened" for the future user operation, i.e. whether to send or to receive a message. When it is a message receiving, it must be decrypted, and when it is a message sending, it must be encrypted and signed (to know who sent it).

The created application is very convenient and provides the necessary security for a confidential communication. It can cover any type of company or corporate activity where it is extremely important that the transfer of information is not disclosed to a third party.

Резюме:

Докладът дискутира разработка, представляваща система за сигурност, която служи за удостоверяване на лични данни, с цел навлизане в сигурна виртуална среда. В разработената системата криптирането на съобщения е част от обезпечаване на работата в „чат-стая“, която хардуерно се обезпечава от група компютри, обслужвани от два сървъра - един главен и един резервен (backup). Сървърите поддържат базата от данни, в която са записите на потребителите. Тези данни служат за вход в чат-стая, която е десктоп приложение. Веднъж регистрирани, чрез своите смартфони, потребителите използват за вход генерираните към смартфона кодове (пароли). След успешно въведени данни, достъпът до системата е осигурен. В тази виртуална среда комуникацията става чрез криптиращи алгоритми, осигуряващи сигурната кореспонденция между потребителите. Сигурността (по-специално криптиране на съобщения) се обезпечава от вариант на RSA алгоритъм за криптиране на информацията. За да се улесни възможния достъп до защитена виртуална среда от страна на потребителите, защитената структура включва в себе си смартфон и персонален компютър. Приложението осигурява удобен и сигурен вход в комуникационната среда като повишава сигурността на системата. В сървъра се съхраняват данните за вход в десктоп приложението, които постъпват от смартфона, служещ за регистрация. Информацията, която се изпраща от смартфона, е кодът на компютъра, от където ще се влиза в чат-стаята и потребителско име за вход в чат-стаята. Към сървъра се изпраща и уникалния номер на устройството, което участва в чат връзката.

Начинът на криптиране на съобщенията се осъществява чрез подобрен вариант на алгоритъма за криптиране RSA.

Като параметър се задава брой опити за свързване (Maximum Attempts – MA), като след достигането им се зарежда блок, който отваря нова връзка с избрания участник от чата. Ако връзката е установена преди достигане на “MA”, се генерират ключовете, с които ще се осъществи сигурната комуникация между двете страни. Генерираните ключове са съответно

личен и публичен. Публичният ключ веднага се изпраща към събеседника. По този начин той ще праща криптирани съобщения с един и същи публичен ключ.

При осъществена реална комуникация между двете страни се „слуша“ за операцията, която ще предприеме потребителят, т.е. дали ще се изпраща или ще се получава съобщение. При приемане на съобщение, то трябва да се декриптира, а при изпращане на съобщение то трябва да се криптира съответно и да се подпише (за да се знае от кого е изпратено).

Приложението, което е създадено е много удобно и осигурява нужната сигурност при конфиденциално общуване. Може да обхване всякакъв тип фирмена или корпоративна дейност, където изключително важно е преносът на информация да не бъде достояние на трета страна.

Г.8-28

Karova M., Desktop Information System for Employee Management, International Scientific Journals: Machines. Technologies. Materials, Vol. 16 (2022), Issue 9, pp. 318-320, Print ISSN: 1313-0226, Online ISSN: 1314-507X (https://stumejournals.com/journals/mtm/2022/9/318)

Abstract:

There are a number of software products that offer services related to personnel management. The workforce management systems provide managers with information about the available workforce and help them better plan and manage staff working hours. Thus, they could easily control labor costs and increase the productivity of the company.

The current development offers an information system with access control and different levels of access for each profile. It provides information security against some of the better-known cyber-attack methods. The software allows visualization of reports on registered employees and their tasks. A mechanism has been developed to add different priorities and states to tasks, which allows freedom to customize the system according to the needs of the owner.

The desktop information system development includes 2 phases: 1) creating a database and 2) design of an encryption algorithm using a special algorithm for creating a key. The main goal of the development is to ensure protection, both at the entrance to the system and in the transfer and storage of data. The designed information system uses database with 4 tables TASK_PRIORITIES, TASK_STATES, EMPLOYEES, TASKS_ARCHIVE.

The current development ensures data protection through the following methods: 1)Control of access to the system, by entering the personal identification number and password; 2)Control of entered data to protect against SQL injections; 3)Password length control; 4)Encryption of the access password; 5)Ability to maintain an encrypted connection between the application and the server;

6)Control of the number of attempts to enter the system; 7) The account blocking in case of three incorrectly entered passwords.

The access control to the system is achieved with the following steps:

1. When entering the employee's personal identification number and password, it is checked whether the personal identification number contains only numbers and it is 10 characters long, and whether the password is more than 8 characters.

2. If the validation from step 1 is successful, the system opens a connection to the database. It searches for an entry in the table for employees by entering a social security number. If it finds such a record, it reads it and loads it into the system memory.

3. If the record is successfully read, the status is checked to see if it is active.

4. If the status is active, the entered password is encrypted using the same algorithm and key that were used to encrypt the password stored in the database.

5. If the encryption is successful, the two encrypted strings are compared: the entered password and the one loaded into memory from step 2.

6. If there is a match, the employee enters the system. The counter for failed login attempts is reset. Its database ID and privilege level data remain loaded in memory until the application is closed.

In order to provide protection against Traffic Interception attacks, an encryption method has been developed with a key created uniquely for the system. A system-unique key is added to the encryption algorithm for the uniqueness of each user's encrypted password. This also adds an extra layer of security. It is 128 bits or 16 bytes long, and the recommended size is 32 bits or 4 bytes.

Резюме:

Съществува множество от софтуерни продукти, който предлагат услуги, свързани с управлението на персонал. Системите за управление на служители предоставя на мениджърите информация за наличната работна ръка и им помага да планират и управляват по-добре работното време на персонала. Така лесно биха могли да контролират разходите за труд и да увеличат производителността на фирмата

Настоящата разработка предлага информационна система с контрол на достъпа и различни нива на достъп за всеки профил. Той осигурява информационна сигурност срещу някои от по-известните методи за кибератаки. Софтуерът позволява визуализиране на справки за регистрирани служители и техните задачи. Разработен е механизъм за добавяне на различни приоритети и състояния към задачите, което позволява свобода за персонализиране на системата според нуждите на собственика.

Разработката на настолна информационна система включва 2 фази: 1) създаване на база данни и 2) проектиране на алгоритъм за криптиране с помощта на специален алгоритъм за създаване на ключ. Основната цел на

разработката е да осигури защита, както на входа на системата, така и при преноса и съхранението на данни. Проектираната информационна система използва база данни с 4 таблици TASK_PRIORITIES, TASK_STATES, EMPLOYEES, TASKS_ARCHIVE.

Текуща разработка осигурява защита на данните чрез следните методи: 1) Контрол на достъпа до системата, чрез въвеждане на ЕГН и парола; 2)Контрол на въведените данни за защита от SQL инжекции; 3)Контрол на дължината на паролата; 4) Криптиране на паролата за достъп; 5) Възможност за поддържане на криптирана връзка между приложението и сървъра; 6) Контрол на броя опити за влизане в системата; 7) Блокиране на акаунт при три неправилно въведени пароли.

Контролът на достъпа до системата се осъществява със следните стъпки:

1. При въвеждане на ЕГН и парола на служителя се проверява дали ЕГН съдържа само цифри и е 10 знака, както и дали паролата е повече от 8 знака.

2. Ако проверката от стъпка 1 е успешна, системата отваря връзка към базата данни. Търси се запис в таблицата за служители чрез въвеждане на социалноосигурителен номер. Ако системата открие такъв запис, той се прочита и се зарежда в системната памет.

3. Ако записът е прочетен успешно, статусът се проверява дали е активен.

4. Ако статусът е активен, въведената парола се криптира със същия алгоритъм и ключ, които са били използвани за криптиране на паролата, съхранена в базата данни.

5. Ако криптирането е успешно, се сравняват двата криптирани низа: въведената парола и тази, заредена в паметта от стъпка 2.

6. Ако има съвпадение, служителят влиза в системата. Броячът за неуспешни опити за влизане се нулира. Идентификационният номер на базата данни и данните за ниво на привилегия остават заредени в паметта, докато приложението не бъде затворено.

За да се осигури защита срещу атаки за прихващане на трафик, е разработен метод за криптиране с ключ, създаден уникално за системата. Към алгоритъма за криптиране се добавя уникален за системата ключ, който е отговорен за уникалността на криптираната парола на всеки потребител. Така се добавя допълнителен слой към сигурността на системата. Дължината на ключа е 128 бита или 16 байта, а препоръчителният размер е 32 бита или 4 байта.

Г.8-29

Карова М., Генчев П., Изследване на методи за оценка на риска за информационни активи, Сборник резюмета на проекти, финансирани от държавния бюджет, ТУ-Варна, 2019, pp. 55-56, ISSN: 2603-3208,

(https://drive.google.com/drive/folders/1536GGj9vvT2dH2MoBmTM_SJX8r_U6Asl)

Abstract:

In today's world, more and more organizations rely on information technology to help them achieve their business goals, such as a faster service response or better quality. This is why information security is of paramount importance for organizations. A systematic approach to information security risk management is needed to help define information security requirements and to establish an effective management system. The information security risk is often expressed as a combination of the consequences of an information security event and the probability that this event will occur. The subject of the risk assessment is called an information asset. These methods are differently effective for different information assets and most of them are based on the expert opinion of specialists and are purely subjective. The methods that are based on objective criteria and mathematical analysis are inapplicable to many of the assets. These features lead to the need to apply heterogeneous methodologies and to hard-to-comparable results.

The risk assessments for key information assets in exemplary information security management systems are analyzed and compared to the problems identified in the overview of risk assessment problems in scientific publications.

After the comparison, tasks are defined for analysis and overcoming problems related to the subjective factor influencing the level of risk for information security.

Based on the conclusions and findings, the main elements of a collecting methodology, an accumulating and updating information about the owner's behavior of the information assets are defined.

The various methods are considered for assessing the behavior risk of an information asset owner and the impact of that risk on the overall level of the asset risk.

The inter-influences of the risks of various information assets have been analyzed and measures to formalize these influences have been identified. In order to overcome the problems that are related to subjective factors, the collecting ways requirements and structuring the information related to the security of the information assets are derived. An attempt was made to structure a methodology for dynamic monitoring and updating the risk level related to the subjective behavior of the information assets owners.

Резюме:

В съвременния свят все повече организации разчитат на информационни технологии, за да им помогнат да постигнат своите бизнес цели, като по-бърз отговор на услугата или по-добро качество. Ето защо сигурността на информацията е от първостепенно значение за

организациите. Необходим е систематичен подход за управление на риска по отношение на сигурността на информацията, който да помогне да се определят изискванията за сигурност на информацията и да се създаде ефективна система за управление. Рискът за информационна сигурност често се изразява в комбинация от последствията от събитие за информационна сигурност и вероятността да възникване това събитие. Предметът на оценката на риска се нарича информационен актив. Тези методи са различно ефективни за различни информационни активи и повечето от тях са основани на експертно мнение на специалисти и са чисто субективни. Методите, които са основани на обективни критерии и математически анализ са неприложими за много от активите. Тези особености водят до необходимост от прилагане на разнородни методики и до трудно съпоставими резултати.

Анализирани са оценките на риска за ключови информационни активи в примерни системи за управление на информационната сигурност и са съпоставени с изведените проблеми при направения обзор на проблемите при оценка на риска в научни публикации.

След извършената съпоставка са дефинирани задачи за анализ и преодоляване на проблеми свързани със субективния фактор, влияещ на нивото на риска за информационната сигурност.

На базата на направените изводи и констатации са дефинирани основните елементи на методика за събиране, натрупване и актуализиране на информация за поведението на собствениците на информационни активи.

Разгледани са различни методи за оценка на риска от поведението на собственик на информационен актив и влиянието на този риск върху общото ниво на риска за актива.

Анализирани са взаимовлиянията на рисковете на различни информационни активи и са набелязани мерки за формализиране на тези влияния. За преодоляване на проблемите, които са свързани със субективни фактори са изведени изисквания за начините за събиране и структуриране на информацията свързана със сигурността на информационните активи. Направен е опит за структуриране на методика за динамично следене и актуализиране на нивото на риска свързано със субективното поведение на собствениците на информационни активи.

Г.8-30

Карова М., Тодоров Д., Изследване на методи за машинно обучение за криптиране на данни, Сборник резюмета на проекти, финансирани от държавния бюджет, ТУ-Варна, 2021, pp. 33-34, ISSN: 2603-3208, (https://drive.google.com/drive/folders/1536GGj9vvT2dH2MoBmTM_SJX8r_U6Asl).

Abstract:

Some of the most used and well-known symmetric encryption algorithms – AES, DES, TripleDES and RC2 – are reviewed. With their help, the secret keys were generated. AES algorithm with a key length of 256 bit, DES algorithm with a key length of 64 bit, TripleDES algorithm with a key length of 128 bit and RC2 algorithm with a key length of 128 bit were used for the experimental study purpose.

Each secret key is pre-processed and placed in a uniform environment. After that, the type of its encryption algorithm is recognized using two of the most used machine learning algorithms - kNN (k-Nearest Neighbors) and SVM (Support Vector Machines).

Selecting the input parameters, the different cryptographic algorithms were deliberately selected in this way - with different key lengths of 64, 128 and 256 bits. Expectedly, the results are best at both extremes at 64 and 256, because their footprint is more contrasting compared to the other two (with 128 bits) placed in a uniform environment. In TripleDES and RC2, in addition to inclusion to the set sample data, the competition of the given fingerprint with another similar one of the same length must be taken into account, but nevertheless, in both modules (kNN and SVM) the result is close to 50%.

A total of 440 keys, 110 for each encryption algorithm, were tested with each of the two machine learning algorithms, kNN and SVM, using a database of 4000 known examples. The results for kNN show that the execution time for one key recognition is under 1 s (about 200 ms on average), and the execution time for all 440 examples is just over 10 min. The percentage-wise, the results are very good for AES and DES, with the latter being even 100%. For TripleDES and RC2, the results are rather good, but definitely weaker compared to AES and DES.

Резюме:

Разгледани са едни от най-използваните и известни симетрични криптиращи алгоритми – AES, DES, TripleDES и RC2. С тяхна помощ са генерирани секретните ключове. За целта на опитната постановка са използвани AES алгоритъм с дължина на ключа от 256 bit, DES алгоритъм с дължина на ключа от 64 bit, TripleDES алгоритъм с дължина на ключа от 128 bit и RC2 алгоритъм с дължина на ключа от 128 bit.

Всеки секретен ключ се преработва предварително и се поставя в еднородна среда. След, което се разпознава вида на криптиращия му алгоритъм посредством два от най-използваните алгоритми от машинно обучение - kNN (k-Nearest Neighbors) и SVM (Support Vector Machines).

При подбиране на входните параметри умишлено са подбрани в този си вид различните криптографски алгоритми – с различна дължина на ключа 64, 128 и 256 бита. Очаквано резултатите са най-добри в двете крайности при 64 и 256, защото техния отпечатък е по-контрастиращ спрямо другите два (със 128 бита) поставени в еднородна среда. При TripleDES и RC2, освен

приобщаването към зададените примерни данни, трябва да се отчете и конкурирането на даденият отпечатък с друг себеподобен със същата дължина, но въпреки това и при двата модула (kNN и SVM) резултата е в близост до 50%.

Направен е опит с общо 440 ключа по 110 за всеки криптиращ алгоритъм, разпознавани с всеки един от двата алгоритми за машинно обучение – kNN и SVM, чрез базови данни от 4000 известни примера. Видно е, че времето за изпълнение на едно разпознаване на ключ е под 1 s (средно около 200 ms), а времето за изпълнение на всичките 440 примера – малко над 10 мин. Процентно резултатите са много добри при AES и DES, като при втория е дори 100%. За TripleDES и RC2 резултатите са по-скоро добри, но определено по-слаби в сравнение с AES и DES.

6.04.2023 г.

Изготвил:
доц. д-р Милена Карова