SUMMARIES

A. Misevičius, A. Blažinskas, A. Lenkevičius. Modified Local Search Heuristics for the Symmetric Travelling Salesman Problem. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 217–230.

In this paper, we investigate some modified local search (LS) heuristics for the solution of symmetric travelling salesman problem (TSP). These modifications are mainly due to the use of extended neighborhood structures. In addition, we are concerned with several new sets of the moves (transitions of solutions) based on the extended configurations of edge exchanges. We are also examining the performance of these extensions being used in an iterated local search (ILS) paradigm. The results from the experiments with the benchmark TSP instances from the TSP library (TSPLIB) demonstrate that the introduced improvements enable to seek solutions of higher quality without substantially increasing computational complexity.

Q. Xie, N. Dong, X. Tan, D. S. Wong, G. Wang. Improvement of a Three-Party Password-Based Key Exchange Protocol with Formal Verification. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 231–237.

A Three-party Password-based Authenticated Key Exchange (3PAKE) protocol allows two users to establish a secure session key over an insecure communication channel with the help of a third party, which is a trusted server. Recently, Lou and Huang proposed a 3PAKE which is efficient and suitable for running on resource-constrained devices such as smart cards and mobile phones. In this paper, we show that their scheme is vulnerable to off-line password guessing attack and partition attack. We then propose an efficient method to fix these problems. Additionally, the mutual authentication and session key secrecy of the proposed protocol are verified using a formal verification tool.

D. Birvinskas, V. Jusas, I. Martišius, R. Damaševičius. Data Compression of EEG Signals for Artificial Neural Network Classification. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 238–241.

Brain – Computer interface (BCI) systems require intensive signal processing in order to form control signals for electronic devices. The majority of BCI systems work by reading and interpreting cortically evoked electro-potentials across the scalp via an electro-encephalogram (EEG). Feature extraction and classification are the main tasks in EEG signal processing. In this paper, we propose a method to compress EEG data using discrete cosine transform (DCT). DCT takes correlated input data and concentrates its energy in just first few transform coefficients. This method is used as feature extraction step and allows reducing data size without losing important information. For classification we use feed forward artificial neural network. Experimental results show that our proposed method does not lose the important information. We conclude that the method can be successfully used for the feature extraction.

J. Woo, S. Nadarajah. On the Maximum and Minimum of Multivariate Pareto Random Variables. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 242-246.

Aksomaitis and Burauskaite-Harju *[Information Technology and Control*, 38, 2009, 301-302] studied the distribution of $\max(X_1, X_2,..., X_p)$ when $(X_1, X_2,..., X_p)$ follows the multivariate normal distribution. Here, we study the moments of $\min(X_1, X_2,..., X_p)$ and $\max(X_1, X_2, ..., X_p)$ when $(X_1, X_2, ..., X_p)$ follows the most commonly known multivariate Pareto distribution. Multivariate Pareto distributions are most relevant for modeling extreme values.

C.-C. Lee, Y.-M. Lai, C.-L. Chen, L. A. Chen. A Novel Designated Verifier Signature Scheme Based on Bilinear Pairing. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 247-252.

A designated verifier scheme can protect information from uncertainty. Only the designated verifier can verify the signature and make sure that the information is correct. In addition, a strong designated verifier scheme allows the verifier to maintain a transcript signature of the verifier's secret key. Recently, Yoon proposed an identity-based strong designated verifier signature scheme to solve the problems of some previously proposed schemes. Unfortunately, Yoon's scheme still has some weaknesses, such as inefficiency in the verifying phase and being vulnerable to replay-attack. To overcome these, we propose a novel designated verifier signature scheme in this paper.

R. Pacevič, A. Kačeniauskas, R. Kutas, D. Markauskas, L. Radvilavičius. Cell Attribute-Based Algorithm for Crack Visualization. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 252-259.

The paper presents the development of the visualization algorithm for propagating cracks. The novel algorithm is based on the cell attribute obtained from the damaged lattice connections employed for discrete element computations of mono-dispersed particulate media. Generation of the cells is efficiently performed by using the positions of particles and the lattice connections. The developed visualization algorithm is implemented in the distributed visualization software VisPartDEM. The efficiency of the software is tested visualizing the datasets resulting from computations of the lattice-based discrete element method. The performance of the developed algorithm is compared with that of the visualization algorithms based on the Voronoi diagrams and the inscribed spheres.

N. Morkevičius, G. Petraitis, A. Venčkauskas, J. Čeponis. Covert Channel for Cluster-based File Systems Using Multiple Cover Files. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 260-267.

Problems of sensitive information hiding in disk drives using cluster-based file systems are analyzed in this study. A new covert channel method for information hiding in disk drives is proposed and discussed. The method uses multiple cover files and is based on relative allocation of clusters of cover files in relation to one another. The experimental results presented in this paper show that the proposed method is easy to implement, provides good (for the covert channel) storage capacity and has the property of two-fold plausible deniability. The proposed covert channel method can be used for the storage of small and very sensitive information (such as passwords or encryption keys) on removable disk drives.

Han-Yu Lin. Secure Universal Designated Verifier Signature and its Variant for Privacy Protection. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 268–276.

Based on the bilinear inverse Diffie-Hellman problem (BIDHP), we first propose a provably secure probabilistic signature scheme. Furthermore, we extend it into two universal designated verifier signature (UDVS) schemes under the same computational assumption. The first one is a conventional UDVS scheme for one designated verifier while the other is designed for cooperative multi-verifier. UDVS schemes aim at protecting the privacy of signature holders and have practical benefits to the applications, e.g., the certificate for medical records and income summary, etc. The comparison results demonstrate that the signature generation and designation of our scheme are both pairing-free, which could benefit the application of devices with constrained computation. We also give formal security proofs of unforgeability against existential forgery under adaptive chosen-message attacks (EF-CMA) in the random oracle model.

Z. Perić, J. Lukić, J. Nikolić, D. Denić. Application of Mean-Square Approximation for Piecewise Linear Optimal Compander Design for Gaussian Source and Gaussian Mixture Model. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 277–285.

This paper proposes a novel piecewise linear optimal compander design method based on the mean-square approximation of the first derivative of the optimal compressor function. Designing of the piecewise linear optimal compander is conducted for signals modeled with the Gaussian probability density function (PDF) and signals modeled with the Gaussian mixture model (GMM). The slopes of the piecewise linear optimal compressor function are optimized for each quantization segment from the support region. The optimization is performed with a goal of obtaining minimal mean-squared error introduced with the proposed approximation, in this manner affecting the number of the uniform cells within each segment. The obtained numerical results show that signal to quantization noise ratio (SQNR) of so obtained piecewise linear optimal compander overreaches SQNR of the uniform quantizer, whereas approaches to the SQNR of the nonlinear optimal compander for higher number of quantization segments. Features of the proposed quantizer indicate great possibilities for its widespread application in quantization of signals modeled by Gaussian PDF and GMM.

M. Sigmund. Statistical Analysis of Fundamental Frequency Based Features in Speech Under Stress. *Information Technology and Control, Kaunas, Technologija,* 2013, Vol. 42, No. 3, 285–291.

A significant part of the non-linguistic information carried in speech refers to the speaker and his/her internal state. This study investigates sixteen features based on fundamental frequency of speech F_0 in order to detect stress in speakers. The most effective features resulting from experiments are presented here. The total frequency ranges of F_0 across specific short-time speech segments created by two or three frames having stable F_0 values were evaluated as the best features for speaker-independent stress detection. F_0 contours were computed frame-by-frame using an optimized autocorrelation function. In our experiments, we used utterances spoken by 14 male speakers and taken from own database of speech under real psychological stress.

SANTRAUKOS

A. Misevičius, A. Blažinskas, A. Lenkevičius. Modifikuoti euristiniai lokaliosios paieškos algoritmai sprendžiant simetrinio tipo komivojažieriaus uždavinį. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 217-230.

Šiame straipsnyje yra tiriamos kai kurios euristinių lokaliosios paieškos (LP) algoritmų modifikacijos (patobulinimai), sprendžiant simetrinio tipo komivojažieriaus uždavinį (KU). Patobulinimai daugiausia susiję su išplėstinių sprendinių aplinkų panaudojimu. Be to, yra nagrinėjamos naujos sprendinių perėjimų aibės, kurios remiasi išplėstinėmis perėjimų formavimo taisyklėmis. Taip pat yra išbandytas sudarytų išplėstinių algoritmų veikimas, taikant vadinamąją iteratyviosios lokaliosios paieškos (ILP) metodiką. Kompiuterinių eksperimentų, atliktų taikant testinius pavyzdžius („gairėmis“), paimtus iš viešosios elektroninės KU pavyzdžių saugyklos (TSPLIB), rezultatai rodo, kad pasiūlyti išplėstiniai LP algoritmai, palyginti su įprastomis LP procedūromis, leidžia gauti geresnės kokybės sprendinius nelabai padidėjus skaičiavimų laikui.

Q. Xie, N. Dong, X. Tan, D. S. Wong, G. Wang. Trišalio slaptažodžiu grindžiamo raktų apsikeitimo protokolo patobulinimas ir oficialus patvirtinimas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 231-237.

Naudojant trišalį slaptažodžiu grindžiamą autentifikuotą raktų apsikeitimo (3PAKE) protokolą, du vartotojai, padedant trečiajai šaliai – patikimam serveriui, gali užtikrinti saugų sesijos raktą, jei ryšio kanalas yra neapsaugotas. Lou ir Huang pasiūlė efektyvų ir tinkamą 3PAKE, naudojantis ribotų galimybių įrenginiais: pvz., lustinėmis kortelėmis ir mobiliaisiais telefonais. Straipsnyje pateikta, kad šių įrenginių sistemą gali pažeisti atakos, siekiant atspėti slaptažodį neprisijungus, ir atakos, siekiant pažeisti vientisumą. Taigi šioms problemoms spręsti siūlomas efektyvus metodas. Be to, siūlomo protokolo abipusis autentiškumo patvirtinimas ir sesijos rakto slaptumas yra patvirtinami oficialia patikrinimo priemone.

D. Birvinskas, V. Jusas, I. Martišius, R. Damaševičius. EEG signalų duomenų glaudinimas, klasifikuojant dirbtinius neuroninius tinklus. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 238–241.

Smegenų sąsajų su kompiuteriu (BCI) sistemose signalai turi būti apdorojami intensyviai, kad būtų sugeneruoti elektroninių prietaisų valdymo signalai. Dauguma BCI sistemų veikia skaitydamos ir aiškindamos smegenų žievėje sukeltą elektrinį potencialą per paviršinius ant galvos odos esančius jutiklius, žinomus kaip EEG (elektroencefalograma). Išskirti ir klasifikuoti atvaizdo požymius – tai pagrindiniai uždaviniai siekiant perdirbti EEG signalus. Straipsnyje pateikiamas EEG duomenų glaudinimo metodas, naudojant diskretinę kosinuso transformaciją (DCT). DCT naudoja koreliuotus įvesties duomenis ir skiria dėmesį tik pirmiems keliems transformacijos koeficientams. Šis metodas yra taikomas atvaizdo požymiams išskirti, taip pat leidžia sumažinti duomenų dydį neprarandant svarbios informacijos. Tiesioginio sklidimo dirbtiniai neuroniniai tinklai naudojami klasifikuojant. Bandymais gauti rezultatai rodo, kad siūlomas metodas neleidžia prarasti svarbios informacijos. Apibendrinant teigiama, kad šis metodas gali būti sėkmingai taikomas atvaizdo požymiams išskirti.

J. Woo, S. Nadarajah. Pareto daugiamačių atsitiktinių dydžių maksimumo ir minimumo tyrimas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 242–246.

Aksomaitis ir Burauskaitė-Harju [Informacinės technologijos ir valdymas, 2009, T. 38, 301–302] nagrinėjo maksimumų (X_1, X_2,..., X_p) pasiskirstymą, kai (X_1, X_2,..., X_p) išvedami iš daugiamačio normaliojo skirstinio. Straipsnyje analizuojamos minimumų (X_1, X_2,..., X_p) ir maksimumų (X_1, X_2,..., X_p) reikšmės, kai (X_1, X_2,..., X_p) gaunami iš labiausiai žinomo daugiamačio Pareto skirstinio. Daugiamačiai Pareto skirstiniai yra tinkamiausi modeliuojant ekstremumus.

C.-C. Lee, Y.-M. Lai, C.-L. Chen, L. A. Chen. Dvikanaliu poravimu pagrįsta neįprasta paskirtojo verifikatoriaus parašo schema. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 247–252.

Paskirtojo verifikatoriaus schema gali apsaugoti informaciją nuo netikrumo. Tik paskirtasis verifikatorius gali patikrinti parašą ir užtikrinti, kad informacija yra teisinga. Taip pat stipri paskirtojo verifikatoriaus schema leidžia verifikatoriui išlaikyti verifikatoriaus slaptojo rakto iššifruotos stenogramos parašą. Neseniai Yoon pasiūlė tapatybe grįstą stipraus paskirtojo verifikatoriaus parašo schemą kelių jau pasiūlytų schemų problemoms spręsti. Deja, Yoono schema turi keletą trūkumų: verifikuojant neužtikrinama efektyvi veikla, taip pat šią schemą gali pažeisti pakartotinės atakos. Siekiant šiuos trūkumus išspręsti, siūloma nauja paskirtojo verifikatoriaus schema.

R. Pacevič, A. Kačeniauskas, R. Kutas, D. Markauskas, L. Radvilavičius. Langelių atributais grįstas plyšių vaizdavimo algoritmas. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 253–259.

Straipsnyje aprašomas langelių atributais grįstas algoritmas, skirtas plintantiems plyšiams vaizduoti. Naujas algoritmo pagrindas yra langelio atributas, kuris apskaičiuojamas remiantis monodispersinių dalelių sistemos, modeliuojamos taikant diskretinį elementų metodą, nutrūkusiomis jungtimis. Langeliai efektyviai generuojami iš dalelių pozicijų ir jungčių topologijos. Sukurtas vaizdavimo algoritmas įdiegtas paskirstytojoje vaizdavimo programinėje įrangoje VisPartDEM. Programos

efektyvumas ištirtas vaizduojant duomenų rinkinius, kuriuose saugomi diskretinių elementų metodo skaičiavimų rezultatai. Algoritmo greitaveika lyginama su alternatyvių algoritmų, pagrįstų Voronojaus diagramomis ir įbrėžtomis sferomis, greitaveika.

N. Morkevičius, G. Petraitis, A. Venčkauskas, J. Čeponis. Slaptas kanalas klasterinėms failų sistemoms aptarti naudojant kelis dengiamuosius failus. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 260–267.

Darbe analizuojama slaptos informacijos slėpimo diskiniuose kaupikliuose problema. Straipsnyje pasiūlytas ir išanalizuotas naujas metodas skirtas informacijai slėpti klasterinėse failų sistemose. Taikant metodą naudojami keli dengiamieji failai, ir informacija saugoma keičiant šių failų klasterių tarpusavio padėtį. Eksperimento rezultatai rodo, kad pasiūlytam metodui būdinga dvigubo pagrįsto išsigynimo savybė.

Han-Yu Lin. Saugus paskirtojo verifikatoriaus parašas ir jo atmaina privatumo apsaugai. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 268–276.

Pirmiausia straipsnyje siūloma pagrįstai saugi tikimybinė parašo schema, atsižvelgiant į dvitiesę atvirkštinę Diffie-Hellman problemą (BIDHP). Be to, remiantis ta pačia skaičiavimo prielaida, ši schema išplėčiama į dvi universalaus paskirtojo verifikatoriaus parašo (UDVS) schemas. Pirmoji yra standartinė UDVS schema, skirta paskirtajam verifikatoriui, o kita schema sumodeliuota kooperaciniam nuodugniam verifikatoriui. UDVS schemos skirtos parašo savininkų privatumui apsaugoti ir yra naudingos praktiniam pritaikymui, pvz., sertifikatui medicininiams įrašams, pajamų reziumė ir t. t. Palyginimo rezultatai rodo, kad tiek parašas generuojamas, tiek nagrinjėma schema paskirstoma ne kartu, o tai gali būti naudinga pritaikant riboto skaičiavimo prietaisus. Taip pat pateikiami nustatytos formos parašo nesuklastojamumo saugumo įrodymai prieš klastojimą pagal prisitaikančias pasirinktų žinučių atakas (EF-CMA) atsitiktiniame ORACLE modelyje.

Z. Perić, J. Lukić, J. Nikolić, D. Denić. Vidutinės kvadratinės aproksimacijos pritaikymas tolydinės tiesinės funkcijos optimalaus kompresoriaus-plėstuvo modelio Gauso pluošto šaltiniui ir Gauso mišinių modeliui. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 277–285.

Straipsnyje siūlomas naujas tolydinės tiesinės funkcijos optimalaus kompresoriausprojektavimo metodas, pagrįstas pirmosios optimalios kompresoriaus funkcijos išvestinės vidutine kvadratine aproksimacija. Tolydinės tiesinės funkcijos optimalaus kompresoriaus projektavimas yra skirtas signalams, kuriuos sukuria Gauso tikimybinė tankio funkcija (PDF), ir signalams, generuojamiems Gauso mišinių modeliu (GMM). Tolydinės optimalaus kompresoriaus tiesinės funkcijos posvyriai yra optimizuojami kiekvienam atraminės srities kvantavimo segmentui. Optimizuojama norint gauti minimalią vidutinę kvadratinę paklaidą, kurią rodo siūloma aproksimacija. Taip daroma įtaka kiekvieno segmento tolygių langelių skaičiui. Skaičiais išreikšti gauti rezultatai rodo, kad taip gauto tolydinės tiesinės funkcijos optimalaus kompresoriaus signalo-kvantizacijos triukšmo santykis (SQNR) viršija pastovaus kvantizatoriaus SQNR, tačiau yra susijęs su netiesinės funkcijos optimalaus kompresoriaus SQNR, norint padidinti kvantizacijos segmentų skaičių. Siūlomo kvantizatoriaus savybės rodo, kad jis gali būti plačiai taikomas kvantizuojant signalus, kuriuos modeliuoja Gauso PDF ir GMM.

M. Sigmund. Pagrindiniu dažniu pagrįstų kalbos bruožų stresinėse situacijose statistinė analizė. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2013, T. 42, Nr. 3, 286–291.

Reikšminga kalboje aptinkama nelingvistinės informacijos dalis susijusi su kalbančiuoju ir jo vidine būsena. Siekiant atskleisti kalbančiųjų patiriamą stresą, šiame straipsnyje analizuojama šešiolika požymių, pagrįstų pagrindiniu kalbos dažniu F_0. Straipsnyje pateikiami eksperimentų metu nustatyti patys akivaizdžiausi požymiai. Konkrečių trumpalaikių kalbos segmentų pagrindinio dažnio F_0 intervalai, kuriuos sukelia dvi ar trys pastoviomis F_0 reikšmėmis pasižyminčios sistemos, buvo pripažinti geriausiais požymiais, leidžiančiais atskleisti stresą, kuriam kalbantysis neturi galios. F_0 kontūrams apskaičiuoti analizuojant struktūrą po struktūros buvo taikoma optimizuota autokoreliacijos funkcija. Eksperimentuose buvo panaudota 14 iš kalbos duomenų bazės paimtų vyriškos lyties kalbėtojų kalbų, sakytų patiriant tikrą psichologinį stresą.