SUMMARIES

D. Brodić, D. R. Milivojević. An Algorithm for the Estimation of the Initial Text Skew. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 211 – 219.

The paper presents a methodology for the estimation of the initial skew rate of text lines. Firstly, it splits text into groups according to the bounding boxes. Linked bounding boxes establish the bigger objects called connected components. After applying mathematical morphology operations, the enlarged group of the connected components is formed. The longest connected component is extracted by the longest common subsequence method. Inside the longest connected component, the gravity centers are determined for each bounding box. They represent the reference points, which are used for the calculation of the initial skew rate. Calculation is made by the moment based method. The comparative analysis of the origin and estimated skew rate is used to evaluate the algorithm. Hence, the proposed algorithm is examined with different printed text samples. It showed robustness for the skew estimation in the wide range of resolutions.

C.-L. Chen, Y.-C. Huang, T.-F. Shih. A Novel Mutual Authentication Scheme for RFID conforming EPCglobal Class 1 Generation 2 Standards. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 220 – 228.

Radio-frequency identification (RFID) is an automatic identification technology. In recent years, more and more applications have been found for its use. However, there are still many security issues worth discussing. In this paper, we propose a mutual authentication scheme, which can solve problems such as privacy, replay attack, forward security, and user location privacy. In our scheme, we only use the tag for the purposes of being a storage media based on EPCglobal Class 1 Generation 2 (C1G2) standards. Analysis shows that the proposed scheme can resist known attacks and can be used in light-weight RFID systems of the current low-cost tags.

F. Jin, Q.-Q. Liu. Quantized Feedback Control Over Packet Dropout Communication Channels. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 229 – 238.

This paper investigates quantized feedback control problems for linear time-invariant control systems, where the sensors and controllers are geographically separated and connected via noisy, bandwidth-limited digital communication channels. The packet dropout process of the channel is modeled as a time-homogeneous Markov process. An adaptive differential coding strategy and a predictive control policy are implemented to achieve the minimum data rate of the channel for mean square stabilization of the unstable plant. In particular, it is shown that a sufficient condition on mean square stabilization of the system with disturbances is that the data rate is more than the lower bound given in our results. The sufficient condition decomposes into two terms: a condition on the data rate and a condition on the transition probabilities of the Markov chain. An illustrative example is given to demonstrate the effectiveness of the proposed method.

D. Kančelkis, J. Valantinas. A New Le Gall Wavelet-Based Approach to Progressive Encoding and Transmission of Image Blocks. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 239 – 247.

In this paper, a modified version of the discrete reversible (integer-to-integer) Le Gall wavelet transform (DLGT), distinguishing itself by apparently improved space localization properties and visibly extended potential capabilities, is proposed. The key point of the proposal – ensuring full decorrelation of Le Gall wavelet coefficients across the lower scales. Based on the latter circumstance, a novel exceptionally fast procedure for computing the integer DLGT spectra of the selected image blocks (regions of interest - ROI) is presented. It is shown that the new developments can be efficiently applied to progressive encoding and transmission of image blocks. Progressive encoding and transmission of image blocks is achieved by first transmitting a "rough" estimate of the original image, then sending further details related to one or another image block (ROI). To translate the idea into action, the zero-tree-based encoder SPIHT (Set Partitioning in Hierarchical Trees) with an improved quad-tree analysis scheme is employed.

K. Kazlauskas, R. Pupeikis. On Speedy Recognition of Non-Aliased Realization after Multifold Downsampling of an Oversampled Bandlimited Signal. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 248 – 257.

The aim of the given paper is the development of the criterion and some expressions for recognizing a nonaliased realization in the set of realizations obtained by multifold decimation (filtering and downsampling) of any oversampled bandlimited signal that has been obtained at the beginning by periodic sampling of a continuous-time signal. For each nondecimated as well as decimated realization discrete-time Fourier series coefficient values, located at Nyquist frequency are calculated, using speedy recursive expressions based on reverse order processing of the given realizations. In such a case, the summing calculation amount has been significantly reduced by applying the expressions that use, in each iteration, the respective values obtained by processing samples of a previously downsampled realization and some samples of the currently downsampled one. We formulate definitions and prove the corollaries that refer to the recursive Fourier coefficient calculation and present here an example. Finally, the simulation results for the bandlimited signal with a triangularshaped spectrum are presented.

C.-C. Lee, R.-X. Chang, T.-Y. Chen, L. A. Chen. An Improved Delegation-Based Authentication Protocol for PCSs. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 258 – 267.

Portable Communication Systems (PCS) can provide mobile users with an opportunity to enjoy global roaming services. A lot of researchers have previously proposed their secure protocols for protecting the mobile privacy of the users in PCS. Most protocols pointed out that Lee-Yeh's protocol and Lee et al.'s protocol are vulnerable to some attacks. Then they proposed their improved protocols to remedy these shortcomings. Unfortunately, we found out that the Lee et al.'s protocol still cannot achieve user anonymity and does not provide perfect forward secrecy. In this paper, we also propose an improved protocol to solve these security problems. Compared with other protocols, our proposed protocol not only achieves all security requirements and functionality requirements but also is more efficient.

R. Lileikytė, L. Telksnys. Quality Estimation of Speech Recognition Features for Dynamic Time Warping Classifier. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 268 – 273.

The choice of the quality features set remains the main issue for the successful speech recognition system. In the literature, quality of features is estimated by calculating the classification error. So that, it is needed to run classification process with each explored feature system in order to choose the highest quality one. Therefore, a major issue of this paper is to propose a methodology for quality establishment of speech features without running the classification process. The proposed methodology is based on metrics that do not need parameters setting, thus the results can be uniformly interpreted across the different problems. The methodology consists of the following parts: 1) establishment of the best metric in combination with used classifier, 2) making a decision regarding the highest quality feature system. In the experiment, we use Dynamic Time Warping (DTW) classifier. The metric of intra/inter class nearest neighbor distances (Q3) is identified as the best one. Employing our proposed methodology, we established Perceptual Linear Prediction analyses to be the highest quality feature system within the explored feature systems. The correctness of the results is confirmed by DTW classification error.

H.-T. Yau, Y.-C. Pu, S. C. Li. Application of a Chaotic Synchronization System to Secure Communication. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 274 – 282.

This work describes a novel scheme that applies a Sprott master/slave chaotic synchronization system to secure transmission. A sliding plane is chosen to design a sliding mode controller to ensure robustness. In the presence of an external disturbance and system uncertainty, the slave chaotic circuit system is then synchronized with the master. The Lyapunov theorem verifies that the proposed controller is stable and robust. Simulation results indicate that the synchronization error state asymptotically converges to the origin of the phase plane, implying that the master/slave chaotic system synchronization is achieved while the sliding mode controller is in operation. While consisting of operational amplifiers, resistors, capacitors and diodes, the chaotic circuit system together with a sliding mode controller is subsequently implemented to validate the system synchronization. Finally, the chaotic system combined with cryptography is embedded into a chaotic synchronization cryptosystem to resolve secure communications-related problems.

Y. Zheng, L. Jia, H. Cao. Multi-Objective Gene Expression Programming for Clustering. *Information Technology and Control, Kaunas, Technologija,* 2012, Vol. 41, No. 3, 283 – 294.

This paper proposes a multi-objective gene expression programming for clustering (MGEPC), which could automatically determine the number of clusters and the appropriate partitioning from the data set. The clustering algebraic operations of gene expression programming are extended first. Then based on the framework of the Non-dominated Sorting Genetic Algorithm-II, two enhancements are proposed in MGEPC. First, a multi-objective k-means clustering is proposed for local search, where the total symmetrical compactness and the cluster connectivity are used as two complementary objectives and the point symmetry based distance is adopted as the distance metric. Second, the power-law distribution based selection strategy is proposed for the parent population generation. In addition, the external archive and the archive truncation are used to keep a historical record of the non-dominated solutions found along the search process. Experiments are performed on five artificial and three real-life data sets. Results show that the proposed algorithm outperforms the PESA-II based clustering method (MOCK), the archived multiobjective simulated annealing based clustering technique with point symmetry based distance (VAMOSA) and the single-objective version of gene expression programming based clustering technique (GEP-Cluster).

SANTRAUKOS

D. Brodić, D. R. Milivojević. Algoritmas pradinio teksto pasvirimui apytikriai apskaičiuoti. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 211 – 219.

Pristatoma pradinio teksto linijų pasvirimo normos apytikslio apskaičiavimo metodologija. Pirma, ji suskirsto tekstą į grupes pagal apribojimo laukelius. Sujungti apribojimo laukeliai nustato didesnius objektus, vadinamus sujungtaisiais komponentais. Atlikus matematinės morfologijos operacijas, suformuojama padidinta susijusių komponentų grupė. Ilgiausias susietas komponentas išskiriamas ilgiausiu bendru sekos metodu. Ilgiausiame susijusiame komponente nustatomi kiekvieno apribojimo laukelio svorio centrai. Jie vaizduoja atskaitos taškus, kurie yra naudojami pradinio pasvirimo normai apskaičiuoti. Skaičiavimas atliekamas momentu paremtu metodu. Lyginamoji pradžios ir apskaičiuoto pasvirimo normos analizė yra panaudota algoritmui įvertinti. Vadinasi, pasiūlytasis algoritmas yra nagrinėtas naudojant skirtingus išspausdinto teksto pavyzdžius. Tai rodo, kad pasvirimo įvertinimas tinka plačiam sprendimų diapazonui.

C.-L. Chen, Y.-C. Huang, T.-F. Shih. Naujoviška abipusio tapatumo nustatymo schema RFID, patvirtinanti EPCglobal klasės 1 kartos du standartus. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 220 – 228.

Atpažinimas radijo dažniu (RFID) yra automatinė tapatumo nustatymo technologija. Pastaraisiais metais šiuo tikslu vis daugiau programų buvo sukurta. Tačiau vis dar daug yra saugumo spragų, kurias vertėtų apsvarstyti. Šiame straipsnyje siūloma abipusė tapatumo nustatymo schema, kuri gali padėti išspręsti tokias problemas kaip privatumas, atsakymo atakos, persiuntimo saugumas ir vartotojo adreso privatumas. Schemoje naudojama tiktai kortelė siekiant, kad saugojimo terpė būtų pagrįsta EPCglobal klasės 1 kartos dviem (K1K2) standartais. Analizė rodo, kad pasiūlyta schema gali pasipriešinti žinomoms atakoms ir gali būti naudojama supaprastintose einamųjų pigių kortelių RFID sistemose.

F. Jin, Q.-Q. Liu. Kvantuota komunikacijos kanalų paketų pradingimo grįžtamojo ryšio kontrolė. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 229 – 238.

Tiriamas kvantuoto grįžtamojo ryšio kontrolės problemos tiesinėse laikui bėgant nekintančiose kontrolės sistemose, kai jutikliai ir valdikliai yra geografiškai atskirti ir sujunti triukšmingais, riboto pralaidumo skaitmeniniais komunikacijos kanalais. Paketų pradingimo kanale procesas yra sumodeliuotas kaip laikui bėgant homogeninis Markovo procesas. Siekiant minimalaus kanalo duomenų dažnio nestabilaus augimo, vidurkio kvadratui stabilizuoti, yra įdiegta adaptyvi diferencialinė kodavimo strategija ir profilaktinės kontrolės taisyklės. Pastebėta, kad pakankama sistemos su trukdžiais vidurkio kvadrato stabilizavimo sąlyga yra ta, kad duomenų dažnis yra didesnis už žemesniąją ribą, pateiktą mūsų rezultatuose. Pakankama sąlyga skaidoma į dvi sąlygas: sąlygą duomenų dažniui ir sąlygą Markovo grandinės perėjimo tikimybėms. Pasiūlyto metodo efektyvumui parodyti pateiktas pavyzdys.

D. Kančelkis, J. Valantinas. Naujas Le Gall bangelėmis grindžiamas požiūris į progresyvųjį vaizdo blokų kodavimą ir perdavimą. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 239 – 247.

Straipsnyje siūloma modifikuota diskrečiosios atvirkštinės Le Gall bangelių transformacijos (DLGT) versija, pasižyminti geresnėmis lokalizavimo erdvėje savybėmis bei akivaizdžiai praplėstomis jos praktinio taikymo galimybėmis. Kertinis pasiūlymo momentas – užtikrinama visiška Le Gall spektrinių koeficientų dekoreliacija žemesniame lygmenyje. Remiantis šia aplinkybe, sudaryta nauja išskirtinai greita (modifikuoto) DLGT spektro apskaičiavimo pasirinktiems skaitmeninio vaizdo fragmentams (blokams) procedūra. Parodoma, jog sudarytoji procedūra gali būti sėkmingai pritaikyta skaitmeninio vaizdo blokų progresyviojo kodavimo ir perdavimo idėjai įgyvendinti. Šios idėjos esmė tokia: pirmiausia vartotojui mažo pralaidumo ryšio kanalu perduodamas netikslus apdorojamo vaizdo įvertis, paskui siunčiama (nedideliais kiekiais) papildoma bitinė informacija, išryškinanti detales vartotojo pasirinktuose vaizdo fragmentuose. Idėjai įgyvendinti panaudotas skaitmeninių vaizdų glaudinimo algoritmas SPIHT su pagerinta kvadmedžių paieškos vaizdo DLGT spektre schema.

K. Kazlauskas, R. Pupeikis. Optimalus erdvėlaivio sandaros pertvarkymas susidūrimui išvengti optimizuojant dalelių spiečių. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 248 – 257.

Straipsnyje nagrinėjamas nesutampančios dažnių srityje realizacijos iš realizacijų rinkinio, gauto po daugkartinės perdiskretizuoto baigtinės juostos signalo decimacijos (vienkartinio filtravimo ir daugkartinio atskaitų išrinkimo), greito atpažinimo uždavinys. Kiekvienai gauto rinkinio realizacijai skaičiuojamos diskrečiosios Furjė transformacijos koeficiento, atitinkančio Naikvisto dažnį, reikšmės. Koeficientui skaičiuoti taikomos skaičiavimų prasme greitos rekurentinės išraiškos ir atvirkštinis duotų realizacijų apdorojimas. Pasiūlytas kriterijus paskutinei realizacijų rinkinio realizacijai, dar nesutampančiai dažnių srityje, nustatyti. Šitaip gerokai sumažinama sudėties operacijų apimtis, nes, taikant rekurentines išraiškas ir atvirkštinį duotų realizacijų apdorojimą, Furjė koeficiento reikšmės gaunamos apdorojus tam tikrus ankstesnės realizacijos dydžius bei

trūkstamas esamos realizacijos atskaitas. Pateikti perdiskretizuoto baigtinės juostos signalo su trikampiu spektru modeliavimo bei jo paskutinės realizacijos, dar nesutampančios dažnių srityje, rekurentinio išrinkimo rezultatai (1–6 pav.).

C.-C. Lee, R.-X. Chang, T.-Y. Chen, L. A. Chen. Patobulintas delegacija grindžiamas tapatumo nustatymo protokolas PKS-oms. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 258 – 267.

Portatyviosios komunikacijos sistemos (PKS) mobiliesiems vartotojams leidžia naudotis visuotinėmis tarptinklinio ryšio paslaugomis. Nemaža tyrėjų anksčiau siūlė saugius protokolus tam, kad apsaugotų vartotojų mobilų privatumą PKS. Dauguma protokolų parodė, kad Lee-Yeh protokolas ir Lee ir kitų protokolas yra menkai apsaugoti nuo kai kurių atakų. Tada jie pasiūlė savo patobulintus protokolus, kad ištaisytų šiuos trūkumus. Deja, išsiaiškinome, kad Lee ir kitų protokolas vis dar neužtikrina vartotojų anonimiškumo ir visiško persiuntimo slaptumo. Šiame straipsnyje taip pat siūlomas patobulintas protokolas šioms saugumo problemoms išspręsti. Palyginti su kitais protokolais, pasiūlytasis protokolas ne tiktai tenkina visus saugumo ir funkcionalumo reikalavimus, bet ir yra efektyvesnis.

R. Lileikytė, L. Telksnys. Šnekos atpažinimo požymių kokybės vertinimas, kai naudojamas dinaminio laiko skalės kraipymo klasifikatorius. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 268 – 273.

Kuriant atpažinimo sistemą svarbu parinkti kokybišką požymių sistemą. Literatūroje požymių kokybė yra vertinama apskaičiuojant klasifikavimo klaidą. Tačiau tokiu atveju klasifikavimo eksperimentai turi būti atliekami su kiekviena tiriama požymių sistema. Šio straipsnio tikslas - sukurti šnekos atpažinimo požymių kokybės vertinimo metodologiją, kurią taikant nereikėtų apskaičiuoti klasifikavimo klaidos. Sukurta metodologija yra grindžiama metrikų naudojimu. Naudojant metrikas nereikia nustatyti parametrų ir skirtingų uždavinių rezultatai interpretuojami vienodai. Metodologija sudaryta iš dviejų etapų: 1) geriausios metrikos nustatymas, kai naudojamas tam tikras klasifikatorius, 2) kokybiškos požymių sistemos nustatymas. Eksperimente naudojamas dinaminio laiko skalės kraipymo (DTW) klasifikatorius. Geriausiąja metrika laikoma metrika, nurodanti klasių artimiausiųjų kaimynų atstumų santykį. Taikant sukurtąją metodologiją, tiesinio suvokimo prognozės kepstro koeficientų požymių sistema pripažinta kokybiškąja požymių sistema. Rezultatų teisingumas patvirtintas naudojant DTW klasifikatoriaus klaidą.

H.-T. Yau, Y.-C. Pu, S. C. Li. Chaotiškos sinchronizacijos sistemos pritaikymas saugiai komunikacijai. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 274 – 282.

Šiame darbe apibūdinama naujoviška schema, kurioje naudojama chaotiška Sprott pavaldumo sinchronizacijos sistema, kad apsaugotų perdavimą. Slankumo būsenos valdikliui, užtikrinančiam gyvybingumą, suprojektuoti pasirinkta slankioji plokštuma. Kai yra išorinių trikdžių ir sistema nepastovi, pavaldi chaotiška kontūro sistema sinchronizuojama su valdančiąja. Liapunovo teorema patvirtina, kad pasiūlytasis valdiklis yra stabilus ir veiksmingas. Modeliavimo rezultatai rodo, kad sinchronizacijos klaidos būklė asimptotiškai sueina į fazinės plokštumos pradžią, o tai reiškia, kad pavaldumo chaotiškos sistemos sinchronizacija yra atlikta, kol veikia slankumo būsenos valdiklis. Kol sutampa su operaciniais stiprintuvais, rezistoriais, kondensatoriais ir diodais, chaotiška kontūro sistema diegiama kartu su slankumo būsenos valdikliu, kad patvirtintų sistemos sinchronizaciją. Pabaigoje chaotiška sistema, sujungta su kriptografija, yra įterpiama į chaotiškos sinchronizacijos kriptosistemą, kad išspręstų problemas, susijusias su saugia komunikacija.

Zheng, L. Jia, H. Cao. Multiobjektyvus genų išraiškos programavimas sankaupoms formuoti. *Informacinės technologijos ir valdymas, Kaunas, Technologija,* 2012, T. 41, Nr. 3, 283 – 294.

Siūlomas multiobjektyvus genų išraiškos programavimas sankaupų formavimui (MGEPC), kuris įgalintų automatiškai nustatyti sankaupų skaičių ir tinkamą atskyrimą iš duomenų aibės. Genų išraiškos programavimo sankaupų formavimo algebrinės operacijos iš pradžių yra išplečiamos. Tada, priklausomai nuo nedominuojančio rūšiavimo genetinio algoritmo II struktūros, siūlomi du MGEPC-o patobulinimai. Pirma, siūlomas multiobjektyvus k-priemonių sankaupų formavimas vietinei paieškai, kur visas simetriškas suglaudinimas ir sankaupų jungiamumas yra naudojami kaip du vienas kitą papildantys tikslai, ir taško simetrija grįstas atstumas yra priimtas kaip atstumo metrika. Antra, galios teisių paskirstymu besiremianti atrinkimo strategija yra siūloma tėvinės populiacijos sudarymui. Be to, išorinis archyvas ir archyvo atmetimas naudojami tam, kad nedominuojančių sprendimų istorinį įrašą būtų galima rasti atliekant paiešką. Atlikti bandymai su penkiais dirbtiniais ir trimis tikroviškais duomenų rinkiniais. Rezultatai parodė, kad pasiūlytasis algoritmas veikia geriau už PESA-II, grįstą sankaupų formavimu metodą (MOCK), archyvuotą daug tikslų modeliuojantį atkaitinimu paremtą sankaupų formavimo metodą su taško simetrija paremtu atstumu (VAMOSA) ir viena tikslia genų išraiškos programavimu paremta sankaupų formavimo metodo (GEP-sankaupa) versija.