Ana Lucila Sandoval Orozco

List of Publications by Year
in descending order

84	1,026	516215 16	476904 29
papers	citations	h-index	g-index

85	85	85	843
all docs	docs citations	times ranked	citing authors

#	Article	IF	Citations
1	A survey of artificial intelligence strategies for automatic detection of sexually explicit videos. Multimedia Tools and Applications, 2022, 81, 3205-3222.	2.6	5
2	Digital Video Manipulation Detection Technique Based on Compression Algorithms. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 2596-2605.	4.7	6
3	Analysis of MP4 Videos in 5G Using SDN. IEEE Transactions on Intelligent Transportation Systems, 2022, 23, 2668-2677.	4.7	1
4	A Model for the Definition, Prioritization and Optimization of Indicators. Electronics (Switzerland), 2022, 11, 967.	1.8	0
5	FASSVid: Fast and Accurate Semantic Segmentation for Video Sequences. Entropy, 2022, 24, 942.	1.1	1
6	Copy-move forgery detection technique based on discrete cosine transform blocks features. Neural Computing and Applications, 2021, 33, 4713-4727.	3.2	17
7	A security framework for Ethereum smart contracts. Computer Communications, 2021, 172, 119-129.	3.1	25
8	Compression effects and scene details on the source camera identification of digital videos. Expert Systems With Applications, 2021, 170, 114515.	4.4	6
9	IoT-based security service for the documentary chain of custody. Sustainable Cities and Society, 2021, 71, 102940.	5.1	2
10	The 51% Attack on Blockchains: A Mining Behavior Study. IEEE Access, 2021, 9, 140549-140564.	2.6	41
11	Development and Evaluation of an Intelligence and Learning System in Jurisprudence Text Mining in the Field of Competition Defense. Applied Sciences (Switzerland), 2021, 11, 11365.	1.3	1
12	Passive Image Forgery Detection Based on the Demosaicing Algorithm and JPEG Compression. IEEE Access, 2020, 8, 11815-11823.	2.6	14
13	Methodology for Forensics Data Reconstruction on Mobile Devices with Android Operating System Applying In-System Programming and Combination Firmware. Applied Sciences (Switzerland), 2020, 10, 4231.	1.3	8
14	Securing Instant Messages With Hardware-Based Cryptography and Authentication in Browser Extension. IEEE Access, 2020, 8, 95137-95152.	2.6	2
15	Authentication and integrity of smartphone videos through multimedia container structure analysis. Future Generation Computer Systems, 2020, 108, 15-33.	4.9	11
16	Digital Video Source Identification Based on Containerâ€™s Structure Analysis. IEEE Access, 2020, 8, 36363-36375.	2.6	16
17	Image tampering detection by estimating interpolation patterns. Future Generation Computer Systems, 2020, 107, 229-237.	4.9	8
18	Mirror saturation in amplified reflection Distributed Denial of Service: A case of study using SNMP, SSDP, NTP and DNS protocols. Future Generation Computer Systems, 2020, 108, 68-81.	4.9	15

#	Article	IF	Citations
19	A machine learning forensics technique to detect post-processing in digital videos. Future Generation Computer Systems, 2020, 111, 199-212.	4.9	13
20	Synthetic Minority Oversampling Technique for Optimizing Classification Tasks in Botnet and Intrusion-Detection-System Datasets. Applied Sciences (Switzerland), 2020, 10, 794.	1.3	46
21	An Analysis of Smart Contracts Security Threats Alongside Existing Solutions. Entropy, 2020, 22, 203.	1.1	20
22	Locating similar names through locality sensitive hashing and graph theory. Multimedia Tools and Applications, 2019, 78, 29853-29866.	2.6	0
23	Early Fire Detection on Video Using LBP and Spread Ascending of Smoke. Sustainability, 2019, 11, 3261.	1.6	9
24	Vehicle Counting in Video Sequences: An Incremental Subspace Learning Approach. Sensors, 2019, 19, 2848.	2.1	12
25	Hy-SAIL: Hyper-Scalability, Availability and Integrity Layer for Cloud Storage Systems. IEEE Access, 2019, 7, 90082-90093.	2.6	4
26	EBVBF: Energy Balanced Vector Based Forwarding Protocol. IEEE Access, 2019, 7, 54273-54284.	2.6	10
27	Outdoor Location of Mobile Devices Using Trilateration Algorithms for Emergency Services. IEEE Access, 2019, 7, 52052-52059.	2.6	15
28	Analysis of the GPS Spoofing Vulnerability in the Drone 3DR Solo. IEEE Access, 2019, 7, 51782-51789.	2.6	60
29	Digital Video Source Acquisition Forgery Technique Based on Pattern Sensor Noise Extraction. IEEE Access, 2019, 7, 157363-157373.	2.6	4
30	A traffic analysis attack to compute social network measures. Multimedia Tools and Applications, 2019, 78, 29731-29745.	2.6	3
31	A comparison of learning methods over raw data: forecasting cab services market share in New York City. Multimedia Tools and Applications, 2019, 78, 29783-29804.	2.6	5
32	Adaptive artificial immune networks for mitigating DoS flooding attacks. Swarm and Evolutionary Computation, 2018, 38, 94-108.	4.5	69
33	Distributed One Time Password Infrastructure for Linux Environments. Entropy, 2018, 20, 319.	1.1	1
34	Digital Image Tamper Detection Technique Based on Spectrum Analysis of CFA Artifacts. Sensors, 2018, 18, 2804.	2.1	17
35	Ransomware Automatic Data Acquisition Tool. IEEE Access, 2018, 6, 55043-55052.	2.6	10
36	Digital Images Authentication Technique Based on DWT, DCT and Local Binary Patterns. Sensors, 2018, 18, 3372.	2.1	17

#	Article	IF	Citations
37	Alert correlation framework for malware detection by anomaly-based packet payload analysis. Journal of Network and Computer Applications, 2017, 97, 11-22.	5.8	17
38	Advanced Payload Analyzer Preprocessor. Future Generation Computer Systems, 2017, 76, 474-485.	4.9	8
39	A PRNU-based counter-forensic method to manipulate smartphone image source identification techniques. Future Generation Computer Systems, 2017, 76, 418-427.	4.9	25
40	A Family of ACO Routing Protocols for Mobile Ad Hoc Networks. Sensors, 2017, 17, 1179.	2.1	7
41	Endpoint Security in Networks: An OpenMP Approach for Increasing Malware Detection Speed. Symmetry, 2017, 9, 172.	1.1	2
42	Estimation of Anonymous Email Network Characteristics through Statistical Disclosure Attacks. Sensors, 2016, 16, 1832.	2.1	5
43	Theia: a tool for the forensic analysis of mobile devices pictures. Computing (Vienna/New York), 2016, 98, 1251-1286.	3.2	0
44	Online masquerade detection resistant to mimicry. Expert Systems With Applications, 2016, 61, 162-180.	4.4	18
45	Advances on Software Defined Sensor, Mobile, and Fixed Networks. International Journal of Distributed Sensor Networks, 2016, 12, 5153718.	1.3	1
46	Disclosing user relationships in email networks. Journal of Supercomputing, 2016, 72, 3787-3800.	2.4	4
47	Image source acquisition identification of mobile devices based on the use of features. Multimedia Tools and Applications, 2016, 75, 7087-7111.	2.6	10
48	Dynamic IEEE 802.21 information server mesh architecture for heterogeneous networks. International Journal of Ad Hoc and Ubiquitous Computing, 2016, 21, 207.	0.3	0
49	Identification of smartphone brand and model via forensic video analysis. Expert Systems With Applications, 2016, 55, 59-69.	4.4	20
50	Leveraging information security and computational trust for cybersecurity. Journal of Supercomputing, 2016, 72, 3729-3763.	2.4	15
51	On multiple burst-correcting MDS codes. Journal of Computational and Applied Mathematics, 2016, 295, 170-174.	1.1	2
52	Quantitative Criteria for Alert Correlation of Anomalies-based NIDS. IEEE Latin America Transactions, 2015, 13, 3461-3466.	1.2	2
53	Extracting Association Patterns in Network Communications. Sensors, 2015, 15, 4052-4071.	2.1	3
54	Malware Detection System by Payload Analysis of Network Traffic. IEEE Latin America Transactions, 2015, 13, 850-855.	1.2	15

#	Article	IF	Citations
55	Smartphone image acquisition forensics using sensor fingerprint. IET Computer Vision, 2015, 9, 723-731.	1.3	8
56	Analysis of errors in exif metadata on mobile devices. Multimedia Tools and Applications, 2015, 74, 4735-4763.	2.6	10
57	Smartphone image clustering. Expert Systems With Applications, 2015, 42, 1927-1940.	4.4	33
58	Monitoring of Data Centers using Wireless Sensor Networks. , 2015, , 1171-1183.		2
59	Network Intrusion Detection Systems in Data Centers. , 2015, , 1185-1207.		0
60	Some new bounds for binary multiple burstâ€correcting codes. Electronics Letters, 2014, 50, 756-758.	0.5	1
61	A Layered Trust Information Security Architecture. Sensors, 2014, 14, 22754-22772.	2.1	6
62	Source identification for mobile devices, based on wavelet transforms combined with sensor imperfections. Computing (Vienna/New York), 2014, 96, 829-841.	3.2	10
63	E-D2HCP: enhanced distributed dynamic host configuration protocol. Computing (Vienna/New York), 2014, 96, 777-791.	3.2	7
64	Adaptive routing protocol for mobile ad hoc networks. Computing (Vienna/New York), 2014, 96, 817-827.	3.2	4
65	A Zone-Based Media Independent Information Service for IEEE 802.21 Networks. International Journal of Distributed Sensor Networks, 2014, 10, 737218.	1.3	2
66	Routing Techniques Based on Swarm Intelligence. Advances in Intelligent Systems and Computing, 2014, , 515-519.	0.5	0
67	Parallel approach of a bioinspired routing protocol for MANETs. International Journal of Ad Hoc and Ubiquitous Computing, 2013, 12, 141.	0.3	1
68	Hybrid ACO Routing Protocol for Mobile Ad Hoc Networks. International Journal of Distributed Sensor Networks, 2013, 9, 265485.	1.3	9
69	Multiple Interface Parallel Approach of Bioinspired Routing Protocol for Mobile Ad Hoc Networks. International Journal of Distributed Sensor Networks, 2012, 8, 532572.	1.3	1
70	Security Issues in Mobile Ad Hoc Networks. International Journal of Distributed Sensor Networks, 2012, 8, 818054.	1.3	6
71	Restrictive Disjoint-Link-Based Bioinspired Routing Protocol for Mobile Ad Hoc Networks. International Journal of Distributed Sensor Networks, 2012, 8, 956146.	1.3	1
72	A distributed QoS mechanism for ad hoc network. International Journal of Ad Hoc and Ubiquitous Computing, 2012, 11, 25.	0.3	4

#	Article	IF	Citations
73	Malware Detection System by Payload Analysis of Network Traffic (Poster Abstract). Lecture Notes in Computer Science, 2012, , 397-398.	1.0	5
74	An Efficient Algorithm for Searching Optimal Shortened Cyclic Single-Burst-Correcting Codes. IEEE Communications Letters, 2012, 16, 89-91.	2.5	5
75	Technique to Neutralize Link Failures for an ACO-Based Routing Algorithm. Lecture Notes in Computer Science, 2012, , 251-260.	1.0	0
76	Efficient Shortened Cyclic Codes Correcting Either Random Errors or Bursts. IEEE Communications Letters, 2011, 15, 749-751.	2.5	1
77	Secure extension to the optimised link state routing protocol. IET Information Security, 2011, 5, 163.	1.1	5
78	Use of Gray codes for optimizing the search of (shortened) cyclic single burst-correcting codes. , 2011, , .		1
79	Auto-Configuration Protocols in Mobile Ad Hoc Networks. Sensors, 2011, 11, 3652-3666.	2.1	28
80	Distributed Dynamic Host Configuration Protocol (D2HCP). Sensors, 2011, 11, 4438-4461.	2.1	26
81	A Comparison Study between AntOR-Disjoint Node Routing and AntOR-Disjoint Link Routing for Mobile Ad Hoc Networks. Communications in Computer and Information Science, 2011, , 300-304.	0.4	2
82	Comparing AntOR-Disjoint Node Routing Protocol with Its Parallel Extension. Communications in Computer and Information Science, 2011, , 305-309.	0.4	2
83	Bio-inspired routing protocol for mobile ad hoc networks. IET Communications, 2010, 4, 2187.	1.5	27
84	Routing Protocols in Wireless Sensor Networks. Sensors, 2009, 9, 8399-8421.	2.1	171