JAYWANTI HAKSAR GOVT. PG COLLEGE, BETUL

Office: Civil Lines, Betul (M.P.) 460001 Tel: 07141- 234244
E-mail: hegjhpgcbet@mp.gov.in Website: www.jhgovtbetul.com

3RD CYCLE
ASSESSMENT AND ACCREDITATION BY NAAC

Criterion – 3

Research, Innovations and Extension

3.3: Research Publications and Awards

3.3.1: Number of research papers published per teacher in the Journals notified on UGC care list during the last five years

Signature Not Verified
RAKESH KUMAR TIWARI
e verified
Principal JH Govt. PG College
Betul, MP
09.08.2023 12:19:32

जयवन्ती हॉक्सर शासकीय स्नातकोत्तर महाविद्यालय, बैतूल (मप्र)
Jaywanti Haksar Government Post Graduate College, Betul (MP)
Office: Civil Lines, Betul- 460001 Tel: 07141- 234244
E-mail : hegjhpgcbet@mp.gov.inWebsite: www.jhgovtbetul.com

Ref. No. 701/2023

Betul, Date 07/07/2023

DECLARATION

The information, reports, true copies of the supporting documents, numerical data etc. furnished in this file are verified by IQAC and found correct.

Hence this certificate.

Dr Meenakshi Choubey
Coordinator, IQAC

COORDINATOR
INTERNAL QUALITY ASSURANCE CELL
JH GOVT. PG COLLEGE, BETUL, (M.P.)

Dr Rakesh Tiwari
Principal

PRINCIPAL
J.H. GOVT.PG.COLLEGE
BETUL(M.P)

Signature Not Verified
RAKESH KUMAR TIWARI
e verified
Principal JH Govt. PG College
Betul, MP
09.08.2023 12:19:32

Table of Contents

3.3.1.1. Number of research papers in the Journals notified on UGC CARE year wise during the last five years.

At a Glance

Year	2021 -2022	2020-2021	2019-2020	2018-2019	2017-2018
Number	22	28	11	00	00

Signature Not Verified
RAKESH KUMAR TIWARI
e verified
Principal JH Govt. PG College
Betul, MP
09.08.2023 12:19:32

Index

SN	Title of paper	Name of the author/s	Department of the teacher	Name of journal	Year of publication	ISSN number	Page No.
	Academic Session 2021-2022						
1	Morphometric Deterministic Model for Prediction of Sediment Yield Index for Selected Watersheds in Upper Narmada Basin	Chandrashekhar Meshram	Mathematics	Applied Water Science	2022	2190-5495	8
2	Conformal Chebyshev Chaotic Maps based Remote User Password Authentication Protocol using Smart Card	Chandrashekhar Meshram	Mathematics	Complex & Intelligent Systems	2022	2198-6053	9
3	Assessing Erosion Prone Areas in a Watershed Using Interval Rough-Analytical Hierarchy Process (IR-AHP) and Fuzzy Logic (FL)	Chandrashekhar Meshram	Mathematics	Stochastic Environmental Research and Risk Assessment	2022	1436-3259	10
4	An Efficient Authentication with Key Agreement Procedure using Mittag-Leffler-Chebyshev Summation Chaotic Map under the Multi-Server Architecture	Chandrashekhar Meshram	Mathematics	The Journal of Supercomputing	2022	1573-0484	11-12
5	A Multi-Layer Perceptron (MLP)-Fire Fly Algorithm (FFA)-based model for sediment prediction	Chandrashekhar Meshram	Mathematics	Soft Computing	2022	1433-7479	13
6	Barriers of Managing Cloud Outsource Software Development Projects: A Multivocal Study	Chandrashekhar Meshram	Mathematics	Multimedia Tools and Applications	2022	1573-7721	14
7	An Efficient Remote User Authentication with Key Agreement Procedure based on Convolution-Chebyshev Chaotic Maps using Biometric	Chandrashekhar Meshram	Mathematics	The Journal of Supercomputing	2022	1573-0484	15-17
8	SBOOSP for Massive Devices in 5G WSNs Using Conformable Chaotic Maps	Chandrashekhar Meshram	Mathematics	CMC-Computers, Materials & Continua	2022	1546-2218	18
9	Prioritization of soil erosion–prone sub-watersheds using Fuzzy based Multi Criteria Decision Making Methods in Narmada basin watershed, India	Chandrashekhar Meshram	Mathematics	International Journal of Environmental Science and Technology	2022	1735-2630	19
10	Assessing vulnerability to soil erosion based on fuzzy best worse multi-criteria decision-making method	Chandrashekhar Meshram	Mathematics	Applied Water Science	2022	2190-5495	20
11	Prioritization of watersheds based on a picture fuzzy analytic hierarchy process and linear assignment model	Chandrashekhar Meshram	Mathematics	Stochastic Environmental Research and Risk Assessment	2022	1436-3259	21
12	Development and evaluation of a water quality index for groundwater quality assessment in parts of Jabalpur District, Madhya Pradesh, India	Chandrashekhar Meshram	Mathematics	Water Supply	2022	1606-9749	22
13	CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps	Chandrashekhar Meshram	Mathematics	IEEE Access	2022	2169-3536	23
14	An Efficient Conformable Fractional Chaotic Map-Based Online/Offline IBSS Scheme for Provable Security in ROM	Chandrashekhar Meshram	Mathematics	Complexity	2022	1076-2787	24
15	Fixed Point Results for Rational Type Contraction in A-Metric Spaces	Manoj Ughade	Mathematics	Advances and Applications in Mathematical Sciences	2022	0974-6803	25
16	An Efficient Three-Factor Authenticated Key Agreement Technique Using FCM Under HC-IoT Architectures	Chandrashekhar Meshram	Mathematics	CMC-Computers, Materials & Continua	2022	1546-2218	26
17	Streamflow Prediction Based on Artificial Intelligence Techniques	Chandrashekhar Meshram	Mathematics	Iranian Journal of Science and Technology, Transactions of Civil Engineering	2022	2364-1843	27-28

Signature Not Verified
RAKESH KUMAR TIWARI
e verified
Principal JH Govt. PG College
Betul, MP
09.08.2023 12:19:32

18	Ecological niche of Cryptococcus neoformans species complex from Betul city of Madhya Pradesh	Mahendra Nawange, Alka Pandey	Microbiology	Journal of Engineering, Computing & Architecture	2022	1934-7197	29
19	Globalization and Marketism in Indian Media (Analytical Studies)	Mousmi Rai	Commerce	ShodhKosh: Journal of Visual and Performing Arts	2022	2582-7472	30
20	व्यवसायिक जगत में महिलाओं की सहभागिता (चुनौतियां एवं समाधान)	Mousmi Rai	Commerce	Mukt Shabd Journal	2022	2347-3150	31
21	Phytochemical screening and quanitative analysis of active phytocontents of Guizotia abyssinica seed to knows of their therapeutic values	Manoj Kumar Ghorase,	Chemistry	International Journal of Health Sciences	2022	2550-6978	32
22	Extracellular phospholipase activity in the environmental strains of Cryptococcus neoformans and Cryptococcus gattii isolated from Betul city of Madhya Pradesh	Mahendra Nawange, Alka Pandey	Microbiology	The International journal of analytical and experimental modal analysis	2022	0886-9367	33
	Academic Session 2020-2021						
23	Fractional Chaotic Maps based Short Signature Scheme under Human-Centred IoT Environments	Chandrashekhar Meshram	Mathematics	Journal of Advanced Research	2021	2090-1232	34
24	Simplified Sediment Yield Index Incorporating Parameter Stream Length	Chandrashekhar Meshram	Mathematics	Environmental Earth Sciences	2021	1866-6299	35
25	An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps	Chandrashekhar Meshram	Mathematics	Sensors	2021	1424-8220	36
26	A Provably Secure IBE Transformation Model for PKC Using Conformable Chebyshev Chaotic Maps Under Human-Centered IoT Environments	Chandrashekhar Meshram	Mathematics	Sensors	2021	1424-8220	37
27	Performance Measurement System and Quality Management in Data-Driven Industry 4.0: A Review	Chandrashekhar Meshram	Mathematics	Sensors	2021	1424-8220	38
28	IBOOST: A Lightweight Provably Secure Identity-Based Online/Offline Signature Technique Based on FCM for Massive Devices in 5G Wireless Sensor Networks	Chandrashekhar Meshram	Mathematics	IEEE Access	2021	2169-3536	39
29	An Efficient Provably Secure Verifier-Based Three-Factor Authentication Technique Using PDL for Data Exchange in TMIS	Chandrashekhar Meshram	Mathematics	IEEE Access	2021	2169-3536	40
30	An Efficient, Robust and Lightweight Subtree-based Three-Factor Authentication Procedure for Large-Scale DWSN in Random Oracle	Chandrashekhar Meshram	Mathematics	IEEE Systems Journal	2021	1932-8184	41
31	A Lightweight Provably Secure Digital Short Signature Technique using Extended Chaotic Maps for Human-Centered IoT Systems	Chandrashekhar Meshram	Mathematics	IEEE Systems Journal	2021	1932-8185	42
32	Provably Secure Lightweight Client Authentication Scheme with Anonymity for TMIS using Chaotic Hash Function	Chandrashekhar Meshram	Mathematics	The Journal of Supercomputing	2021	0920-8542	43-45
33	A Provably Secure Lightweight Subtree-based Short Signature Scheme with Fuzzy User Data Sharing for Human-Centered IoT	Chandrashekhar Meshram	Mathematics	IEEE Access	2021	2169-3536	46
34	An Effective Mobile-Healthcare Emerging Emergency Medical System using Conformable Chaotic Maps	Chandrashekhar Meshram	Mathematics	Soft Computing	2021	1432-7643	47
35	A Comparative Study between Dynamic and Soft Computing Models for Sediment Forecasting	Chandrashekhar Meshram	Mathematics	Soft Computing	2021	1432-7644	48
36	Soil Erosion Modelling of Watershed using Cubic, Quadratic and Quintic Splines	Chandrashekhar Meshram	Mathematics	Natural Hazards	2021	0921-030X	49
37	Iterative classifier optimizer-based pace regression and random forest hybrid models for suspended sediment load prediction	Chandrashekhar Meshram	Mathematics	Environmental Science and Pollution Research	2021	0944-1344	50
38	An Efficient Key Exchange Scheme using Santilli's Isofields Second-Kind for Secure Communication	Chandrashekhar Meshram	Mathematics	Advances in Mathematics: Scientific Journal	2021	1857-8365	51-52
39	A New Remote Fuzzy User Password Authentication Scheme Using Sub-tree for Cloud Computing	Chandrashekhar Meshram	Mathematics	International Journal of Circuits, Systems and Signal Processing	2021	1998-4464	53
40	Identification of Critical Watershed for Soil	Chandrashekhar	Mathematics	Water Resources	2021	0[illegible]4741	54-56

	Conservation Using Game Theory-Based Approaches	Meshram		Management			
41	Coincidence Points and Common Fixed Points of Expansive Mappings in Ab-Metric Spaces	Manoj Ughade	Mathematics	South East Asian J. of Mathematics and Mathematical Sciences	2021	0972-7752	57
42	Rational Type Contraction in Controlled Metric Spaces	Manoj Ughade	Mathematics	Journal of Mathematical and Computational Science	2021	1927-5307	58
43	Study of all subgroups of the symmetric group S6	Manoj Ughade	Mathematics	Zeichen Journal	2021	0932-4747	59
44	Coincidence Points and Common Fixed Points of Expansive Mappings in A-Metric Spaces	Manoj Ughade	Mathematics	Zeichen Journal	2021	0932-4747	60
45	Fixed Point for Rational Type Contraction in S-Metric Spaces	Manoj Ughade	Mathematics	Journal of Xidian University	2021	1001-2400	61
46	SIFK based Isobeta Cryptosystem	Chandrashekhar Meshram	Mathematics	International Journal of Engineering Trends and Technology	2021	2231-5381	62
47	New decomposition of soft supra locally α - closed sets applied to soft supra continuity	Chandrashekhar Meshram	Mathematics	Journal of Interdisciplinary Mathematics	2021	2169-012X	63-64
48	Common Fixed-Point Theorem For a Sequence of Fuzzy Mappings Satisfying a Rational Contractive Condition Involving Non-Expansive Mapping	Manoj Ughade,	Mathematics	Malaya Journal of Matematik	2021	2319-3786	65
49	Dass and Gupta Rational Type Contraction in Controlled Metric Spaces	Manoj Ughade,	Mathematics	The International Journal of analytical and experimental modal analysis	2021	0886-9367	66
50	Screening of Phytochemical Contants of Linum Usitatissimum Plant Extracted by Different Solvent	Manoj Kumar Ghorase	Chemistry	Journal of Cardiovascular Disease Research	2021	0975-3583	67
	Academic Session 2019-2020						
51	Application of Artificial Neural Networks, Support Vector Machine and Multiple Model-ANN to Sediment Yield Prediction	Chandrashekhar Meshram	Mathematics	Water Resources Management	2020	0920-4741	68-69
52	The feasibility of Multi-Criteria Decision-Making Approach for Prioritization of Sensitive Area at Risk of Water Erosion	Chandrashekhar Meshram	Mathematics	Water Resources Management	2020	0920-4742	70-71
53	Application of SAW and TOPSIS in Prioritizing Watersheds	Chandrashekhar Meshram	Mathematics	Water Resources Management	2020	0920-4743	72-73
54	An Effective Dynamic Runoff-Sediment Yield Modelling for Shakkar Watershed, Central India	Chandrashekhar Meshram	Mathematics	Arabian Journal of Geoscience	2020	1866-7511	74
55	Long-term temperature trend analysis associated with agriculture crops	Chandrashekhar Meshram	Mathematics	Theoretical and Applied Climatology	2020	1434-4483	75
56	Common Fixed Points of Fuzzy Maps Under Nonexpansive Type Condition	Manoj Ughade	Mathematics	Journal of Mathematical and Computational Science	2020	1927-5307	76
57	Fixed Point Theorems for Dualistic Contractions of Rational Type in Partially Ordered Dualistic Partial Metric Spaces	Manoj Ughade	Mathematics	Journal of Mathematical and Computational Science	2020	1927-5308	77
58	Numerical Treatment of Fourth-order Self-Adjoint Singulalrly Perturbed Boundary Value Problems via Septic B-Spline Method	Sonali Saini Sahu	Mathematics	Solid State Technology	2020	0038-111X	78
59	Multicriteria Decision Making Taxonomy of Cloud-based Global Software Development Motivators	Chandrashekhar Meshram	Mathematics	IEEE Access	2020	2169-3536	79
60	An Efficient ID-based Cryptographic Technique using IFP and GDLP	Chandrashekhar Meshram	Mathematics	Security and Privacy	2020	2475-6725	80
61	RIPIC based Key Exchange Protocol	Chandrashekhar Meshram	Mathematics	Advances in Mathematics: Scientific Journal	2020	1857-8365	81-82
	Academic Session 2018-2019						
	Academic Session 2017-2018						

Applied Water Science (2022) 12:153
https://doi.org/10.1007/s13201-022-01644-0

ORIGINAL ARTICLE

Morphometric deterministic model for prediction of sediment yield index for selected watersheds in upper Narmada Basin

Sarita Gajbhiye Meshram[1] · Chandrashekhar Meshram[2] · Mohd Abul Hasan[3] · Muhammad Arshad Khan[4] · Saiful Islam[3]

Received: 13 July 2021 / Accepted: 8 March 2022

Abstract
Soil erosion is common and has a wide range of spatiotemporal variability. It is crucial in determining sediment output, which is essential for proper watershed management. In this research, we propose morphometric deterministic models (MDM) for prediction of sediment yield index using morphometric parameters of 49 watersheds from Upper Narmada Basin of Madhya Pradesh state, India. For this purpose, Shuttle Radar Topography Mission generated Digital Elevation Model was used to extract and analyze 12 morphometric parameters including linear, aerial, and relief parameters. Principle Component Analysis has been applied for the most effective parameter estimation. The linear and nonlinear MDM were discovered to be suitable for the field of sediment research due to the high value of R^2 (over 70%). The sediment yield forecasting is critical for taking the appropriate management measures in the watershed to reduce the sediment load in the reservoir and extend the life of the structure.

Keywords Unguaged watersheds · Morphological parameters · Sediment yield index · PCA

Abbreviations

AISLUS	All India soil and land use survey
Ba	Bamhan
C_c	Compactness coefficient
D_d	Drainage density
DEM	Digital elevation model
F_s	Drainage frequency
GIS	Geographic information system
HI	Hypsometric index
km	Kilometers
km^2	Square kilometer
L_o	Length of overland flow
MDM	Morphometric deterministic models
Ma	Manot
Mo	Mohgaon
MAE	Mean absolute error
NSE	Nash–Sutcliffe efficiency
PCA	Principle component analysis
R^2	Correlation coefficient
RS	Remote sensing
R_e	Elongation ratio
R_f	Form factor
R_h	Relief ratio
R_r	Relative ratio
R_N	Ruggedness number
R_c	Circularity ratio
R_b	Bifurcation ratio
SYI	Sediment yield index
SRTM	Shuttle radar topography mission
SPR	Sediment production rate

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Mohd Abul Hasan
mohad@kku.edu.sa

Muhammad Arshad Khan
moakhan@kku.edu.sa

Saiful Islam
sfakrul@kku.edu.sa

[1] Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India

[2] Department of Mathematics, Jaywanti Haksar Government P. G. College, Chhindwara University, Betul, M.P., India

[3] Civil Engineering Department, College of Engineering, King Khalid University, P.O. Box 394, Abha 61321, Saudi Arabia

[4] Department of Chemical Engineering, College of Engineering, King Khalid University, P.O. Box 394, Abha 61321, Saudi Arabia

Published online: 09 May 2022

Name of Faculty: Dr. Chandrashekhar Meshram

Complex & Intelligent Systems (2022) 8:973–987
https://doi.org/10.1007/s40747-021-00555-y

ORIGINAL ARTICLE

Conformal Chebyshev chaotic map-based remote user password authentication protocol using smart card

Chandrashekhar Meshram[1] · Sarita Gajbhiye Meshram[2] · Rabha W. Ibrahim[3] · Hamid A. Jalab[4] · Sajjad Shaukat Jamal[5] · Sharad Kumar Barve[2]

Received: 25 October 2020 / Accepted: 21 September 2021 / Published online: 29 October 2021

Abstract
With the rapid advancement and growth of computer networks, there have been greater and greater demands for remote user password authentication protocols. In current ages, smartcard-based authentication protocol has formed the standard with their incredibly insubstantial, user-friendly equipment and low-cost apps. In this study, we proposed an effective robust authentication protocol using the conformable chaotic map, where a conformable calculus is a branch of newly appearing fractional calculus. It has a magnificent property, because it formulates using a controller term. We shall also offer formal proof of smooth execution of the proposed authenticated protocol. Our new protocol is more secure as compared to several comparable protocols.

Keywords Mutual authentication · Smart card · Session key · Conformable chaotic map · Fractional calculus · Conformable calculus · Perfect forward secrecy · Hash function · Cryptography

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Hamid A. Jalab
hamidjalab@um.edu.my

Sajjad Shaukat Jamal
shussain@kku.edu.sa

Sharad Kumar Barve
drsharadbarve@gmail.com

1 Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul 480001, India

2 Water Resources & Applied Mathematics Research Lab, Nagpur, India

3 IEEE: 94086547, Kuala Lumpur 59200, Malaysia

4 Department of Computer System and Technology -Multimedia Unit, Faculty of Computer Science and Information Technology, University of Malaya, 50603 Kuala Lumpur, Malaysia

5 Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

Introduction

In recent years, research in chaotic maps and their applications within the field of cryptography has acquired significant attention Chaotic frameworks are defined by subtle need on initial situations and proximity to random behavior; features that appear to be fundamentally analogous to those needed by certain cryptographic primitives [1, 2]. In his doctoral thesis in 1993, Hwu [3] introduced the idea of chaos theory to public-key cryptography (PKC). He defined his chaotic development of a PKC with a quadratic equation of difference and a one-dimensional equation of difference (1DDE), which is a well-qualified one-way function. In contrast, Hwu's scheme uses ElGmal's method [4] to execute the cycle of encryption. The security of this scheme is based on the infeasibility of resolving the given discrete logarithm over finite fields. Nonetheless, it is possible to work out a trapdoor by letting the true owner know the reiteration times of the distinguishing condition.

The smartcard-founded remote client authentication system allows a device to authenticate a remote client through open, unsafe networks. In general, one of the two approaches next is used by a system to identify a client such as (a) use something that is accessible only to the client, like a password, (b) single client has permitted admission to

Name of Faculty: Dr. Chandrashekhar Meshram

Stochastic Environmental Research and Risk Assessment (2022) 36:297–312
https://doi.org/10.1007/s00477-021-02134-6

ORIGINAL PAPER

Assessing erosion prone areas in a watershed using interval rough-analytical hierarchy process (IR-AHP) and fuzzy logic (FL)

Sarita Gajbhiye Meshram[1] · Vijay P. Singh[2] · Ercan Kahya[3,4] · Mehdi Sepehri[5] · Chandrashekhar Meshram[6] · Mohd Abul Hasan[7] · Saiful Islam[7] · Pham Anh Duc[8]

Accepted: 23 October 2021 / Published online: 29 November 2021

Abstract
Soil erosion is one of the major land loss problems in agricultural land and is regarded as a serious environmental hazard worldwide. This study focused on watershed prioritization using morphometric parameters using Fuzzy Logic (FL), Interval Rough-Analytical Hierarchy Process (IR-AHP) and Geographic Information Systems (GIS) integration for Gusru Watershed, India. Fourteen morphometric parameters, including circulatory ratio (R_c), form factor (R_f), elongation ratio (R_e), compactness coefficient (C_c), drainage density (D_d), stream frequency (F_s), texture ratio (T), relief ratio (R_h), relative relief (R_r), ruggedness number (R_N), bifurcation ratio (R_b), average slope (S_a), length of overland flow (L_o), and hypsometric integral (HI) were evaluated to determine the erosion susceptibility. Each morphometric parameter was assigned a weight value by the FL and IR-AHP methods, and mapping and analysis were then carried out in the GIS environment. Our results showed that the sub-watersheds (SW) 9, 2, and 11 were most susceptible to soil erosion and the sub-watershed 1 was the least from the viewpoint of soil erosion ranking.

Keywords Watershed · Morphometric parameter · Soil erosion · AHP · Fuzzy logic

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

[1] Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India

[2] Department of Biological and Agricultural Engineering, Zachry Department of Civil & Environmental Engineering, Texas A&M University, College Station, TX, USA

[3] Department of Civil Engineering, Istanbul Technical University (ITU), 34469 Istanbul, Turkey

[4] Tashkent Institute of Architecture and Civil Engineering, Tashkent, Uzbekistan

[5] Department of Watershed Management, Faculty of Natural Resources, Yazd University, Yazd, Iran

[6] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Chhindwara University, Betul 460001, India

[7] Civil Engineering Department, College of Engineering, King Khalid University, PO Box 394, Abha 61421, Kingdom of Saudi Arabia

[8] Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam

1 Introduction

Soil erosion is an environmental, economic and social problem that affects all countries. For sustainable development of natural resources to diminish the impacts of natural calamities, a watershed could be taken as developmental unit (UNEP 1997). Although a number of factors are involved in soil erosion, a major agent is the water in the problem of land deterioration in most parts of the world. India's lands are not resistant to this type of natural hazards, since a total of 147 M ha soil loss were estimated in the country (Bhattacharyya et al. 2015).

Soil erosion, excess water flow or runoff, changes in river geometry, degradation of streams, sediment accumulation in river and stream characters are, to some extent, all water borne natural processes, which are related with morphometry (Meshram and Meshram, 2020). This clearly suggests that the morphometry of a basin is fundamental to the basin hydrology. Nowadays the latest technologies such as remote sensing (RS) and geographic information systems (GIS) have been so effectively utilized in the morphometric analyses as the old practices of measuring

Name of Faculty: Dr. Chandrashekhar Meshram

The Journal of Supercomputing (2022) 78:4938–4959
https://doi.org/10.1007/s11227-021-04039-1

An efficient authentication with key agreement procedure using Mittag–Leffler–Chebyshev summation chaotic map under the multi-server architecture

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Sarita Gajbhiye Meshram[3] · Sajjad Shaukat Jamal[4] · Agbotiname Lucky Imoize[5,6]

Accepted: 19 August 2021 / Published online: 14 September 2021

Abstract

The recent technological advancement and rapid development of computer networks have increased the popularity of remote password authentication protocols. Toward this end, the emphasis has shifted to protocols that apply to smart cards-empowered multi-server environments. In order to defend against the replay attack, these protocols usually depend on the nonce or timestamp. In this paper, an efficient Mittag–Leffler–Chebyshev Summation Chaotic Map (MLCSCM)-enabled multi-server authentication protocol with the key agreement is proposed and generalized to address this peculiarity in multi-server-oriented applications. The security proof and efficiency analysis of the presented MLCSCM authenticated key agreement protocol is rigorously derived and validated. Compared to the recently published literature, the proposed protocol presents high efficiency with unique features, and it is highly resistant to sophisticated attacks and achieves perfect forward secrecy.

Keywords Mittag–Leffler–Chebyshev Summation Chaotic Map (MLCSCM) · Computer networks · Mutual authentication · Multi-server architecture · Key exchange · Smart card

1 Introduction

The widespread adoption of the Internet globally is attributed to its numerous benefits and usefulness in government parastatals, non-governmental agencies, educational institutions, smart cities, industries, private sectors, and others [1]. There are various applications in which clients can access various services from multiple networks remotely, such as healthcare, banking, smart grid, smart agriculture, home

✉ Chandrashekhar Meshram
csmeshram84pdf@gmail.com

Extended author information available on the last page of the article

Name of Faculty: Dr. Chandrashekhar Meshram

42. He D, Ma M, Zhang Y, Chen C, Bu J (2011) A strong user authentication scheme with smart cards for wireless communications. Comput Commun 34(3):367–374. https://doi.org/10.1016/j.comcom.2010.02.031
43. Meshram C, Powar PL (2016) An efficient identity-based QER cryptographic scheme. Complex Intell Syst 2(4):285–291. https://doi.org/10.1007/s40747-016-0030-8

Authors and Affiliations

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Sarita Gajbhiye Meshram[3] · Sajjad Shaukat Jamal[4] · Agbotiname Lucky Imoize[5,6]

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Sajjad Shaukat Jamal
shussain@kku.edu.sa

Agbotiname Lucky Imoize
aimoize@unilag.edu.ng

1 Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, M.P. 460001, India

2 IEEE: 94086547, 59200 Kuala Lumpur, Malaysia

3 Department for Management of Science and Technology Development, Ton DucThang University, Ho Chi Minh City, Vietnam

4 Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

5 Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka 100213, Lagos, Nigeria

6 Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany

Soft Computing (2022) 26:911–920
https://doi.org/10.1007/s00500-021-06281-4

APPLICATION OF SOFT COMPUTING

A Multi-Layer Perceptron (MLP)-Fire Fly Algorithm (FFA)-based model for sediment prediction

Sarita Gajbhiye Meshram[1] · Chandrashekhar Meshram[2] · Fateme Akhoni Pourhosseini[3] · Mohd Abul Hasan[4] · Saiful Islam[4]

Accepted: 9 September 2021 / Published online: 7 October 2021

Abstract
The prediction of river sediment load is an essential issue in water resource engineering problems. In this study, artificial neural network employed in order to estimate the daily sediment load on rivers. Two different algorithms, multi-layer perceptron (MLP) and hybrid MLP-FFA (MLP integrated with the FFA) were used for this purpose in the Lake Mahabad, Iran. For this purpose, nine different scenarios are considered as inputs of the models. Performance of selected models was evaluated on basis of performance criterion namely root mean square error (RMSE), mean absolute error (MAE), coefficient of determination (R^2) for choosing best fit model. The results indicated that the new hybrid model MLP-FFA is successful in estimating sediment load with high accuracy as compared with its alternatives with RMSE = 2018 ton/day, MAE = 1698 and R^2 = 0.95, which were much lower than those of MLP-based model with RMSE = 3044 ton/day, MAE = 2481 and R^2 = 0.90. The results of the present study confirmed the suitability of proposed methodology for precise modeling of suspended sediment load.

Keywords Firefly algorithm · Mahabad River · Multi-layer perceptron · Prediction · Sediment

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Fateme Akhoni Pourhosseini
fateme.pourhosseini@yahoo.com

Mohd Abul Hasan
mohad@kku.edu.sa

Saiful Islam
sfakrul@kku.edu.sa

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh 460001, India

[3] Water Resources Engineering, University of Tehran, Karaj, Iran

[4] Civil Engineering Department, College of Engineering, King Khalid University, PO Box 394, Abha 61421, Kingdom of Saudi Arabia

1 Introduction

Sediment load information is useful for problems in the design of reservoirs and dams, transport of sediment and pollutants in rivers, lakes and estuaries, design of stable channels and dams, protection of fish and wildlife habitats, determination of the effects of watershed management and environmental impact assessment (Cigizoglu 2004). Water quality and sediment modeling have been a challenging task in the field of computational hydrology (Kişi 2009). Traditionally used methods (e.g., Ahmad et al. 2009, 2010) to determine runoff often do not take into account sediment load. Estimation of sediment load has been approached through empirical relationships, numerical simulations, physically-based models and using remote sensing and Geographic Information Systems (GIS) techniques.

Precise simulation of sediment load is important for sustainable water supplies and environmental systems, because it plays a major role in any decision-making process on water availability. In recent years (Lohani et al. 2007; Boukhrissa et al. 2013; Yadav et al. 2018; Ampomah

Name of Faculty: Dr. Chandrashekhar Meshram

Multimedia Tools and Applications
https://doi.org/10.1007/s11042-021-11245-9

1179: MULTIMEDIA SOFTWARE ENGINEERING: CHALLENGES AND OPPORTUNITIES

Check for updates

Barriers of managing cloud outsource software development projects: a multivocal study

Muhammad Azeem Akbar[1] · Sajjad Mahmood[2] · Chandrashekhar Meshram[3] · Ahmed Alsanad[4] · Abdu Gumaei[4] · Salman A. AlQahtani[5]

Received: 11 July 2020 / Revised: 22 May 2021 / Accepted: 8 July 2021

Abstract
Management of COSD projects is a challenging task due to number of distant development locations in different time zones, client and vendor organizations, different cloud deployment models and range of different service level agreements. The objective of this study is to identify the barriers associated with managing COSD projects. We implemented a Multivocal Literature Review to identify barriers that influence management of COSD projects. We identified 21 COSD management barriers from 165 primary studies. The comparison between the barriers identified from formal and grey literature indicate that there are similarities between the barriers investigated from both types of literature. Moreover, client-vendor analysis shows that there is no significant difference between COSD management barriers associated with both types of organizations. We believe that the study findings will assist both research and industry community to better understand and manage COSD projects.

Keywords Cloud outsource software development · Software outsourcing · Cloud computing · Barriers · Multivocal literature review

✉ Muhammad Azeem Akbar
azeem.akbar@lut.fi

✉ Ahmed Alsanad
aasanad@ksu.edu.sa

[1] Department of Information Technology, Lappeenranta-Lahti University of Technology (LUT), Lappeenranta 53851, Finland

[2] Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia

[3] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduation College, College of Chhindwara University, Betul, MP 460001, India

[4] STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia

[5] Computer Engineering Department, College of Computer and Information Sciences, King Saud University, Riyadh, Saudi Arabia

Published online: 15 September 2021

Name of Faculty: Dr. Chandrashekhar Meshram

The Journal of Supercomputing
https://doi.org/10.1007/s11227-021-04280-8

An efficient remote user authentication with key agreement procedure based on convolution-Chebyshev chaotic maps using biometric

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Sarita Gajbhiye Meshram[3] · Agbotiname Lucky Imoize[4,5] · Sajjad Shaukat Jamal[6] · Sharad Kumar Barve[3]

Accepted: 21 December 2021

Abstract

The study of chaotic constructions and their associated cryptographic frameworks has sparked a lot of research interest in recent years. Latest advances in wireless technology and the proliferating limitations posed by open communication channels, biometric-enabled remote client authentication procedures with passwords have recently gained traction. In order to address this problem, this paper proposes a secure biometric-based remote user authentication procedure using convolution-Chebyshev chaotic maps with a key agreement procedure. The extended convolution-Chebyshev chaotic maps-based scheme was developed over the interval $(-\infty, +\infty)$, and the required properties for the procedure were verified rigorously. The proposed procedure provides a secure client authentication mechanism using biometrics. Additionally, the projected procedure provides a good key agreement feature with perfect forward secrecy while reducing the computation loads for smart cards. As a result, the proposed procedure outperforms related authentication procedures in terms of security and computational performance.

Keywords Mutual authentication · Convolution-Chebyshev chaotic maps · Biometric · Anonymity · Smart cards

1 Introduction

There has been a lot of research interest in analyzing chaotic systems and their possible cryptographic structures in recent years [1–3]. Specific cryptographic primitives behave in a way that is fundamentally similar to chaotic frameworks, which are described by their sensitivity to random operations and initial conditions in the

✉ Chandrashekhar Meshram
csmeshram84pdf@gmail.com

Extended author information available on the last page of the article

Published online: 12 March 2022

Name of Faculty: Dr. Chandrashekhar Meshram

54. Gaikwad VP, Tembhurne JV, Meshram C, Lee C-C (2021) Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function. J Supercomput. https://doi.org/10.1007/s11227-020-03553-y
55. Mason JC, Handscomb DC (2002) Chebyshev polynomials. CRC Press
56. Bergamo P, D'Arco P, De Santis A, Kocarev L (2005) Security of public-key cryptosystems based on Chebyshev polynomials. IEEE Trans Circuits Syst I Regul Pap 52(7):1382–1393. https://doi.org/10.1109/TCSI.2005.851701
57. Han S, Chang E (2009) Chaotic map based key agreement with/out clock synchronization. Chaos Solitons Fract 39(3):1283–1289. https://doi.org/10.1016/j.chaos.2007.06.030
58. Zhang L (2008) Cryptanalysis of the public key encryption based on multiple chaotic systems. Chaos Solitons Fract 37(3):669–674. https://doi.org/10.1016/j.chaos.2006.09.047
59. Chen F, Liao X, Wong K, Han Q, Li Y (2012) Period distribution analysis of some linear maps. Commun Nonlinear Sci Numer Simul 17(10):3848–3856
60. Laine TP (1980) The product formula and convolution structure for the generalized Chebyshev polynomials. SIAM J Math Anal 11(1):133–146
61. He D, Chen Y, Chen J (2012) Cryptanalysis and improvement of an extended chaotic maps-based key agreement protocol. Nonlinear Dyn 69(3):1149–1157. https://doi.org/10.1007/s11071-012-0335-0
62. He D, Ma M, Zhang Y, Chen C, Bu J (2011) A strong user authentication scheme with smart cards for wireless communications. Comput Commun 34(3):367–374. https://doi.org/10.1016/j.comcom.2010.02.031
63. Kocher P, Jaffe J, Jun B (1999) Differential power analysis. In: Annual International Cryptology Conference, pp 388–397
64. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
65. Lee C-C, Chen C-L, Wu C-Y, Huang S-Y (2012) An extended chaotic maps-based key agreement protocol with user anonymity. Nonlinear Dyn 69(1):79–87. https://doi.org/10.1007/s11071-011-0247-4
66. Lee C-C, Hsu C-W (2013) A secure biometric-based remote user authentication with key agreement scheme using extended chaotic maps. Nonlinear Dyn 71(1):201–211. https://doi.org/10.1007/s11071-012-0652-3
67. Wu F, Xu L, Kumari S, Li X (2015) A novel and provably secure biometrics-based three-factor remote authentication scheme for mobile client–server networks. Comput Electr Eng 45:274–285
68. Secure Hash Standard, National Institute of Standards and Technology (NIST), Federal Information Processing Standards Publication. FIPS 180-4, 2015
69. Ibrahim MH, Kumari S, Das AK, Wazid M, Odelu V (2016) Secure anonymous mutual authentication for star two-tier wireless body area networks. Comput Methods Programs Biomed 135:37–50
70. Park Y, Park K, Lee K, Song H, Park Y (2017) Security analysis and enhancements of an improved multi-factor biometric authentication scheme. Int J Distrib Sens Netw 13(8):1–12

Authors and Affiliations

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Sarita Gajbhiye Meshram[3] · Agbotiname Lucky Imoize[4,5] · Sajjad Shaukat Jamal[6] · Sharad Kumar Barve[3]

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Name of Faculty: Dr. Chandrashekhar Meshram

An efficient remote user authentication with key agreement...

Agbotiname Lucky Imoize
aimoize@unilag.edu.ng

Sajjad Shaukat Jamal
shussain@kku.edu.sa

Sharad Kumar Barve
drsharadbarve@gmail.com

1 Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, M.P. 460001, India

2 IEEE: 94086547, 59200 Kuala Lumpur, Malaysia

3 Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India

4 Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka 100213, Lagos, Nigeria

5 Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany

6 Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia

Name of Faculty: Dr. Chandrashekhar Meshram

Computers, Materials & Continua
DOI:10.32604/cmc.2022.022642
Article

Tech Science Press

SBOOSP for Massive Devices in 5G WSNs Using Conformable Chaotic Maps

Chandrashekhar Meshram[1,*], Agbotiname Lucky Imoize[2,3], Sajjad Shaukat Jamal[4], Amer Aljaedi[5] and Adel R. Alharbi[5]

[1]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, 460001, M.P., India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, 100213, Lagos, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801, Bochum, Germany
[4]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
[5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
*Corresponding Author: Chandrashekhar Meshram. Email: cs_meshram@rediffmail.com
Received: 13 August 2021; Accepted: 15 October 2021

Abstract: The commercialization of the fifth-generation (5G) wireless network has begun. Massive devices are being integrated into 5G-enabled wireless sensor networks (5G WSNs) to deliver a variety of valuable services to network users. However, there are rising fears that 5G WSNs will expose sensitive user data to new security vulnerabilities. For secure end-to-end communication, key agreement and user authentication have been proposed. However, when billions of massive devices are networked to collect and analyze complex user data, more stringent security approaches are required. Data integrity, non-repudiation, and authentication necessitate special-purpose subtree-based signature mechanisms that are pretty difficult to create in practice. To address this issue, this work provides an efficient, provably secure, lightweight subtree-based online/offline signature procedure (SBOOSP) and its aggregation (Agg-SBOOSP) for massive devices in 5G WSNs using conformable chaotic maps. The SBOOSP enables multi-time offline storage access while reducing processing time. As a result, the signer can utilize the pre-stored offline information in polynomial time. This feature distinguishes our presented SBOOSP from previous online/offline-signing procedures that only allow for one signature. Furthermore, the new procedure supports a secret key during the pre-registration process, but no secret key is necessary during the offline stage. The suggested SBOOSP is secure in the logic of unforgeability on the chosen message attack in the random oracle. Additionally, SBOOSP and Agg-SBOOSP had the lowest computing costs compared to other contending schemes. Overall, the suggested SBOOSP outperforms several preliminary security schemes in terms of performance and computational overhead.

Keywords: Subtree-based online/offline signature procedure (SBOOSP); 5G WSNs; provably secure scheme; massive devices; conformable chaotic maps

Name of Faculty: Dr. Chandrashekhar Meshram

International Journal of Environmental Science and Technology
https://doi.org/10.1007/s13762-022-04044-8

ORIGINAL PAPER

Prioritization of soil erosion-prone sub-watersheds using fuzzy-based multi-criteria decision-making methods in Narmada basin watershed, India

S. G. Meshram[1] · S. Tirivarombo[2] · C. Meshram[3] · E. Alvandi[4]

Received: 23 August 2021 / Revised: 12 February 2022 / Accepted: 17 February 2022

Abstract
Every year, soil erosion causes significant damage to humans by reducing soil productivity and filling reservoirs from sediment deposition in the Manot watershed in the Narmada basin, India. Hence, it is important in this basin to recognize soil erosion-prone areas for preventive steps. In this research, prioritization of sub-watersheds of the Manot watershed has been done using fuzzy MCDM approaches such as Fuzzy-SAW, Fuzzy-VIKOR and Fuzzy-TOPSIS methods. For this purpose, the Shuttle Radar Topography Mission (SRTM)-generated Digital Elevation Model (DEM) was used to extract and analyze 12 morphometric parameters, including linear, aerial, and relief parameters. A fuzzy MCDM was successfully implemented for prioritizing watersheds in terms of soil erosion. Overall, the descending order in terms of susceptibility to erosion is found to be MN8 > MN7 > MN2 > MN10 > MN1 > MN9 > MN12 > MN4 > MN5 > MN6 > MN14 > MN3 > MN13 > MN11. The findings showed that morphometric parameters and the fuzzy MCDM approach have high efficiency in recognizing areas that are vulnerable to erosion.

Keywords MCDM · Prioritization technique · Soil conservation · Watershed management · Fuzzy MCDM

Introduction

Soil erosion is one of the major land loss problems on agricultural land and is regarded in modern times worldwide as a serious environmental hazard (Lu et al. 2003; Kim et al. 2005; Srinivasan et al. 2019; Meshram et al. 2021a, b, c; Silakhori et al. 2022; Benzougagh et al. 2022). Water erosion risk is an environmental, economic, and social issue that affects all countries. Soil degradation in India is estimated to be occurring on 147 million hectares (Mha) of land, including 94 Mha from water erosion, 16 Mha from acidification, 14 Mha from flooding, 9 Mha from wind erosion, 6 Mha from salinity, and 7 Mha from a combination of factors (Bhattacharyya et al. 2015). Therefore, the problem needs to be addressed prudently and a systematic solution to reduce the extent of the problem needs to be pursued. To exploit land and water resources efficiently and sustainably, one needs to try to find a sustainable unit so that such resources can be effectively handled and controlled.

Soil attrition or erosion, excess water flow or runoff, changes in rivers geometry, degradation of streams, and sediment accumulation in river and stream characteristics are related to morphometry (UNEP 1997). This suggests that the morphology of a basin's is fundamental to the basin hydrology. At present, geo-morphometric analysis using a new technique, i.e., RS and GIS is being utilized as this tool gives flexibility to analyze spatial data in new manner (Gajbhiye et al. 2014; Meshram and Sharma 2017).

In today's world, the majority of researchers use RS and GIS to evaluate natural disasters, prioritize watersheds, and

Editorial responsibility: Chenxi Li.

✉ S. G. Meshram
gajbhiyesarita@gmail.com

[1] Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India

[2] Botswana International University of Science and Technology, P. Bag 16, Palapye, Botswana

[3] Department of Mathematics, Jaywanti Haksar Government P. G. College, College of Chhindwara University, Betul, M.P., India

[4] Department of Watershed Management, Gorgan University of Agricultural Sciences and Natural Resources, Gorgan, Iran

Published online: 10 May 2022

Name of Faculty: Dr. Chandrashekhar Meshram

Applied Water Science (2022) 12: 219
https://doi.org/10.1007/s13201-022-01714-3

ORIGINAL ARTICLE

Assessing vulnerability to soil erosion based on fuzzy best worse multi-criteria decision-making method

Sarita Gajbhiye Meshram[1] · Mohd Abul Hasan[2] · Chandrashekhar Meshram[3] · Ali Reza Ilderomi[4] · Sithabile Tirivarombo[5] · Saiful Islam[2]

Received: 12 July 2021 / Accepted: 1 June 2022 / Published online: 2 August 2022

Abstract
Soil wearing away or erosion is a chief agent of land loss in agricultural land and is regarded worldwide as a serious environmental hazard. This study performed watershed prioritization using morphometric parameters based on fuzzy best worse method (F-BWM) and GIS integration for Gusru Watershed, India. This study prioritizes sub-watersheds of the study area from viewpoint of soil erosion using five major parameters i.e., stream frequency (F_s), relative relief (R_r), length of overland flow (L_o), relief ratio (R_h) and drainage density (D_d). Fuzzy based Best Worse Multi-Criteria Decision-Making (F-BWM) Method was used to assigning weights to used criteria and combining them to achieve erosion susceptibility for each sub-watershed. Results showed that sub-watersheds 9, 14, and 5 were most susceptible to soil erosion and sub-watershed 3 was the least from the viewpoint of soil erosion ranking.

Keywords Soil erosion · Prioritization · Best worse method · Fuzzy logic · Multi-criteria decision-making method

List of symbols

F-BWM	Fuzzy best worse method
GIS	Geographical information system
AHP	Analytic hierarchy process
MCDM	Multi criteria decision making
PCA	Principal component analysis
DEM	Digital elevation model
SRTM	Shutter radar topography mission
TFN	Triangular fuzzy number
F_s	Stream frequency
R_r	Relative relief
L_o	Length of overland flow
R_h	Relief ratio
R_c	Circulatory ratio
D_d	Drainage density
l, m, u	Lower, median and upper numbers of $\tilde{A}$
$\tilde{A}$	Relative importance of criterion
c_B	Best criterion
c_W	Worst criterion
$\tilde{w}_1^*, \tilde{w}_2^*, \ldots, \tilde{w}_n^*$	Optimal fuzzy weight
ξ	Consistency ratio
$c_1, c_1, \ldots, c_j, \ldots, c_n$	Criteria
C_c	Compactness coefficient
R_e	Elongation ratio
R_f	Farm factor

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Mohd Abul Hasan
mohad@kku.edu.sa

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Ali Reza Ilderomi
a.ildoromi@yahoo.com

Sithabile Tirivarombo
tirivarombos@biust.ac.bw

Saiful Islam
sfakrul@kku.edu.sa

[1] Water Resources and Applied Mathematics Research Lab, Nagpur, Maharashtra 440027, India

[2] Civil Engineering Department, College of Engineering, King Khalid University, Abha, Kingdom of Saudi Arabia

[3] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, Chhindwara University, Betul, Madhya Pradesh, India

[4] Department of Nature Engineering, Faculty of Natural Resources, Malayer University, Hamadan, Iran

[5] Botswana International University of Science and Technology, P. Bag 16, Palapye, Botswana

Name of Faculty: Dr. Chandrashekhar Meshram

Stochastic Environmental Research and Risk Assessment
https://doi.org/10.1007/s00477-022-02280-5

ORIGINAL PAPER

Prioritization of watersheds based on a picture fuzzy analytic hierarchy process and linear assignment model

Sarita Gajbhiye Meshram[1] · Mehdi Sepheri[2] · Chandrashekhar Meshram[3] · Adel Moatamed[4,5,6] · Brahim Benzougagh[7] · Sara Parvizi[2] · Ehsan Bazrafshan[2] · Yegane Rahimi[8]

Accepted: 6 July 2022

Abstract
Soil erosion is one of the most dangerous natural dangers, causing a great deal of harm in many parts of the world. In the presented study, the Gusru river watershed in Indi was divided into 14 sub-watersheds, and then 14 morphometric parameters were calculated, including drainage density (D_d), bifurcation ratio (R_b), streams frequency (F_s), average slope (S_a), form factor (R_f), circulatory ratio (R_C), elongation ratio (R_e), relative relief (R_h), ruggedness number (R_N), bifurcation ratio (R_b), texture ratio (T), length of the overland flow (L_o) compactness coefficient (C_C) and hypsometric integral (HI) were derived for each sub- watershed. Afterward, the combination of picture fuzzy-analytic hierarchy process and picture fuzzy-linear assignment model were used to assign weights to selected morphometric criteria and to rank the sub-watersheds based on the level of soil erosion susceptibility. The results of the study showed that sub-watersheds 11 and 2 were the most susceptible sub watersheds, while sub-watersheds 13 and 14 had the lowest susceptibility to soil erosion. Prioritization and ranking of sub-watersheds from the perspective of soil erosion susceptibility can be used as a powerful tool for prevention and mitigation measures.

Keywords Erosion susceptibility · Picture fuzzy · Analytic hierarchy process · Linear assignment model · Watershed prioritization

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Mehdi Sepheri
sepehri_mehdi@ymail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Adel Moatamed
amuatmed@kku.edu.sa

Brahim Benzougagh
benzougaghbrahim@gmail.com

Sara Parvizi
saraparvizi90@yahoo.com

Ehsan Bazrafshan
ehsan.bazrafshan71@gmail.com

Yegane Rahimi
yeganeh.rahimi70@gmail.com

[1] WRAM Research Lab, Pvt. Ltd., Nagpur, Maharashtra 440027, India

[2] Department of Watershed Management, Faculty of Natural Resources, Yazd University, Yazd, Iran

[3] Department of Mathematics, Jaywanti Haksar Government P. G. College, College of Chhindwara University, Betul, M.P., India

[4] Department of Geography, College of Humanities, King Khalid University, Abha, Saudi Arabia

[5] Department of Geography, Faculty of Arts, Assiut University, Assiut, Egypt

[6] Prince Sultan Bin Abdul-Aziz Center for Environment and Tourism Research and Studies, King Khalid University, Abha, Saudi Arabia

[7] Geophysics and Natural Hazards Laboratory, Department of Geomorphology and Geomatics, Scientific Institute, Mohammed V University in Rabat, Avenue Ibn Batouta, Agdal, PO Box 703, 10106 Rabat-City, Morocco

[8] Department of Pure Mathematics, Faculty of Mathematical Sciences, Yazd University, Yazd, Iran

Published online: 23 September 2022

Name of Faculty: Dr. Chandrashekhar Meshram

Water Supply

IWA PUBLISHING

Water Supply Vol 22 No 6, 6002 doi: 10.2166/ws.2022.174

Development and evaluation of a water quality index for groundwater quality assessment in parts of Jabalpur District, Madhya Pradesh, India

Sudesh Bhaskar Ghoderao[a], Sarita Gajbhiye Meshram[b,*] and Chandrashekhar Meshram[c]
[a] Department of Chemistry, RNC Arts, JDB Commerce and NSC Science College, Nasik Road, Nasik, Maharashtra 422101, India
[b] Water Resources and Applied Mathematics Research Lab, Nagpur, Maharashtra 440027, India
[c] Department of Mathematics, Jaywanti Haksar Government PG College, College of Chhindwara University, Betul, MP, India
*Corresponding author. E-mail: gajbhiyesarita@gmail.com

SGM, 0000-0001-5453-3791

ABSTRACT

Groundwater is an important source for drinking water supply in Jabalpur District, Madhya Pradesh, India. An attempt has been made in this work to understand the suitability of groundwater for human consumption. The parameters of pH, Electrical Conductivity (EC), Copper (Cu), Chromium (Cr), Sulphate (SO_4), Iron (Fe), Nitrate (NO_3), Chloride (Cl), Total Hardness (TH), Total Alkalinity (TA), and Sodium (Na) were analyzed to estimate the groundwater quality. The water quality index (WQI) has been applied to categorize the water quality, which is quite useful to infer the quality of water for the people and policy makers in the concerned area. The WQI in the study area ranges from 17.90 to 176.88. According to the WQI rating, sites 1, 3, and 4 are not appropriate for drinking water or have low water quality and site 2 has moderate drinking condition, whereas site 5 has excellent drinking condition. The current study suggests that the groundwater of the area with deteriorated water quality needs treatment before consumption.

Key words: groundwater, principal component analysis (PCA), water quality, WQI

HIGHLIGHTS

- WQI values in sites 1, 3 and 4 are 106.99, 176.88, 161.25, showing that the groundwater is not suitable for drinking purposes.
- WQI value in site 5 is 17.90, showing that water is fit for drinking purposes.
- Principal component analysis reveals that four parameters are responsible for the high values of WQI.
- The outcome of the study will be helpful in formulating effective drinking water management measures for residents in the Jabalpur region, India.

Name of Faculty: Dr. Chandrashekhar Meshram

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2022, accepted April 2, 2022, date of publication April 7, 2022, date of current version April 18, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3165565

CGST: Provably Secure Lightweight Certificateless Group Signcryption Technique Based on Fractional Chaotic Maps

CHANDRASHEKHAR MESHRAM[1], AGBOTINAME LUCKY IMOIZE[2,3], (Member, IEEE), SAJJAD SHAUKAT JAMAL[4], ADEL R. ALHARBI[5], SARITA GAJBHIYE MESHRAM[6], AND IQTADAR HUSSAIN[7,8]

[1]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, Chhindwara University, Betul, Madhya Pradesh 460001, India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University Bochum, 44801 Bochum, Germany
[4]Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia
[5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[6]Water Resources and Applied Mathematics Research Laboratory, Nagpur 440027, India
[7]Mathematics Program, Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, Doha, Qatar
[8]Statistical Consulting Unit, College of Arts and Science, Qatar University, Doha, Qatar

Corresponding authors: Chandrashekhar Meshram (cs_meshram@rediffmail.com), Sajjad Shaukat Jamal (shussain@kku.edu.sa), and Agbotiname Lucky Imoize (aimoize@unilag.edu.ng)

This work was supported in part by the Deanship of Scientific Research, King Khalid University, through the Research Groups Program under Grant R. G. P. 1/399/42. The work of Agbotiname Lucky Imoize was supported in part by the Nigerian Petroleum Technology Development Fund (PTDF), and in part by the German Academic Exchange Service (DAAD) through the Nigerian–German Postgraduate Program under Grant 57473408.

ABSTRACT In recent years, there has been a lot of research interest in analyzing chaotic constructions and their associated cryptographic structures. Compared with the essential combination of encryption and signature, the signcryption scheme has a more realistic solution for achieving message confidentiality and authentication simultaneously. However, the security of a signcryption scheme is questionable when deployed in modern safety-critical systems, especially as billions of sensitive user information is transmitted over open communication channels. In order to address this problem, a lightweight, provably secure certificateless technique that uses Fractional Chaotic Maps (FCM) for group-oriented signcryption (CGST) is proposed. The main feature of the CGST-FCM technique is that any group signcrypter may encrypt data/information with the group manager (GM) and have it sent to the verifier seamlessly. This implies the legitimacy of the signcrypted information/data is verifiable using the public conditions of the group, but they cannot link it to the conforming signcrypter. In this scenario, valid signcrypted information/data cannot be produced by the GM or any signcrypter in that category alone. However, the GM is allowed to reveal the identity of the signcrypter when there is a legal conflict to restrict repudiation of the signature. Generally, the CGST-FCM technique is protected from the indistinguishably chosen ciphertext attack (IND-CCA). Additionally, the computationally difficult Diffie-Hellman (DH) problems have been used to build unlinkability, untraceability, unforgeability, and robustness of the projected CGST-FCM scheme. Finally, the security investigation of the presented CGST-FCM technique shows appreciable consistency and high efficiency when applied in real-time security applications.

INDEX TERMS Certificateless group signcryption scheme (CGSS), fractional chaotic maps (FCM), provably secure scheme, authentication, Diffie-Hellman (DH) problem, wireless security networks.

I. INTRODUCTION

The study of chaotic structures and their potential cryptographic designs has sparked much research interest in recent years [1]–[3]. The behaviours of certain cryptographic primitives are fundamentally similar to that of chaotic frameworks, which are represented by their sensitive reliance on random operations and initial operations in the vicinity [4]–[6]. In modern wireless communication systems, information security is essential to protect critical user information/data

The associate editor coordinating the review of this manuscript and approving it for publication was Tawfik Al-Hadhrami.

Hindawi
Complexity
Volume 2022, Article ID 6302328, 11 pages
https://doi.org/10.1155/2022/6302328

WILEY | Hindawi

Research Article

An Efficient Conformable Fractional Chaotic Map-Based Online/Offline IBSS Scheme for Provable Security in ROM

Chandrashekhar Meshram,[1] **Rabha W. Ibrahim**,[2] **and Rafida M. Elobaid**[3]

[1]*Department of Post Graduate Studies and Research, Mathematics, Jaywanti Haksar Government Post Graduation College, College of Chhindwara University, Betul 480001, India*
[2]*The Institute of Electrical and Electronics Engineers (IEEE) 94086547, Portland, USA*
[3]*Deanship of Educational Service, Price Sultan University, Riyadh, Saudi Arabia*

Correspondence should be addressed to Rafida M. Elobaid; robaid@psu.edu.sa

Received 11 February 2020; Revised 19 November 2021; Accepted 25 January 2022; Published 31 March 2022

Academic Editor: Honglei Xu

Chaos distributes with a covert method to condense the dynamic of complexity and satisfies the security requirements of a cryptographic system. This study gives an ability online/offline (O/O) ID-based short signature (IBSS) scheme using conformable fractional chaotic maps. Furthermore, we establish its security under IBSS existential unforgeability of identity-based short signature (IBSS) under chosen message attack (EUF-IBSS-CMA) in the random oracle model (ROM). Some of the stimulating preparations of obtainable processes are that they give a multiperiod application of the offline storage, which licenses the agent to recycle the offline pre-registered data in time series (especially the polynomial time), rather than one-period usage in all past IBSS processes.

1. Introduction

Newly, the time-fractional difference [1] provides a robust concept for discrete (not continuous) fractional display. It has a limited fractional alteration formula, which rests on the change consequences of all the past figurines. This attribute can show the disconnected arrangements long historical properties or long interactions. In the meantime, chaos definitions, formulas, ideas, and chaos synchronization have wide uses [2–5]. Discrete maps can produce chaotic signatures. Therefore, they rewarded much care in all areas of mathematical sciences. The logistic map idea (is a well-known repeated record founded on the first-order nonlinear alteration equation) and other types of maps have converted straightforward representations. Nevertheless, fewer works utilized the fractional discrete arrangements, which clamp compound chaotic dynamics. This action presents the disconnected memory, which occurs in the chaotic records. Then, chaos and harmonization of the fractional logistic record are specified. The diverse fractional powers yield different chaotic ranges so that the chaotic activities will take extra problematical [6, 7]. Discrete maps are used regularly in disconnected natural phenomena. The standing fractional disconnected arrangements (equations, inequalities, and inclusions) are typically joined with two techniques: mathematical discretization (the process of changing continuous functions, simulations, variables, and equations into discrete complements) of time-fractional differential equations and fractional time-difference equations. The former one is a numerical formulation of fractional continuous simulations and the Grünwald–Letnikov difference usually accepted in the numerical action. In this study, we shall use the fractional Caputo difference operator. Our aim is to use a new fractional calculus, called fractional conformable calculus, to generalize the Chebyshev polynomials [8].

The inquiry into chaotic constructions and their possible cryptographic structures has been the subject of considerable interest in research over the past few years. Chaotic systems are clearly characterized by their delicate reliance on the initial conditions and random surrounding operations, both

Name of Faculty: Dr. Manoj Ughade

Advances and Applications in Mathematical Sciences
Volume 21, Issue 3, January 2022, Pages 1589-1600

FIXED POINT RESULTS FOR RATIONAL TYPE CONTRACTION IN A-METRIC SPACES

JYOTI VARMA, MANOJ UGHADE and AMIT KUMAR PANDEY

Department of Mathematics
Government College Shahpur
College of Chhindawara University
Shahpur 460440, India

Department of Post Graduate Studies
and Research in Mathematics
Jaywanti Haksar Government Post Graduate
College, College of Chhindawara University
Betul, 460001, India

Department of Engineering Mathematics
and Research Center
Sarvepalli Radhakrishanan University
Bhopal 462026, India

Abstract

The goal of this paper is to define rational contraction in the context of A-metric spaces and develop various fixed point theorems in order to elaborate, generalize, and synthesize a number of previously published results. Finally, to illustrate the new theorem, an example is given.

1. Introduction

Fixed point theory is crucial in science and mathematics. This topic has drawn a lot of interest from academics in the last two decades due to its wide range of applications in disciplines such as nonlinear analysis, topology, and engineering difficulties. The Banach contraction principle [2] is the starting

2020 Mathematics Subject Classification: Primary 47H10; Secondary 54H25.
Keywords: A-metric space; rational contraction; fixed point.
*Corresponding author; E-mail: jyoti.varma2504@gmail.com
Received October 10, 2021; Accepted December 11, 2021

Name of Faculty: Dr. Chandrashekhar Meshram

Computers, Materials & Continua
DOI: 10.32604/cmc.2022.024996
Article

Tech Science Press

An Efficient Three-Factor Authenticated Key Agreement Technique Using FCM Under HC-IoT Architectures

Chandrashekhar Meshram[1,*], Agbotiname Lucky Imoize[2,3], Sajjad Shaukat Jamal[4], Parkash Tambare[5], Adel R. Alharbi[6] and Iqtadar Hussain[7]

[1]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, 460001, M.P., India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos, 100213, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801, Bochum, Germany
[4]Department of Mathematics, College of Science, King Khalid University, Abha, Saudi Arabia
[5]Water Resources & Applied Mathematics Research Lab, Nagpur, 440027, India
[6]College of Computing and Information Technology, University of Tabuk, Tabuk, 71491, Saudi Arabia
[7]Mathematics Program, Department of Mathematics, Statistics and Physics, College of Arts and Sciences, Qatar University, 2713, Doha, Qatar
*Corresponding Author: Chandrashekhar Meshram. Email: cs_meshram@rediffmail.com
Received: 07 November 2021; Accepted: 31 December 2021

Abstract: The Human-Centered Internet of Things (HC-IoT) is fast becoming a hotbed of security and privacy concerns. Two users can establish a common session key through a trusted server over an open communication channel using a three-party authenticated key agreement. Most of the early authenticated key agreement systems relied on pairing, hashing, or modular exponentiation processes that are computationally intensive and cost-prohibitive. In order to address this problem, this paper offers a new three-party authenticated key agreement technique based on fractional chaotic maps. The new scheme uses fractional chaotic maps and supports the dynamic sensing of HC-IoT devices in the network architecture without a password table. The projected security scheme utilized a hash function, which works well for the resource-limited HC-IoT architectures. Test results show that our new technique is resistant to password guessing attacks since it does not use a password. Furthermore, our approach provides users with comprehensive privacy protection, ensuring that a user forgery attack causes no harm. Finally, our new technique offers better security features than the techniques currently available in the literature.

Keywords: Three-party authenticated key agreement; anonymity; fractional chaotic maps; Chebyshev polynomial; password table; human-centered internet of things (HC-IoT)

Name of Faculty: Dr. Chandrashekhar Meshram

Iranian Journal of Science and Technology, Transactions of Civil Engineering
https://doi.org/10.1007/s40996-021-00696-7

RESEARCH PAPER

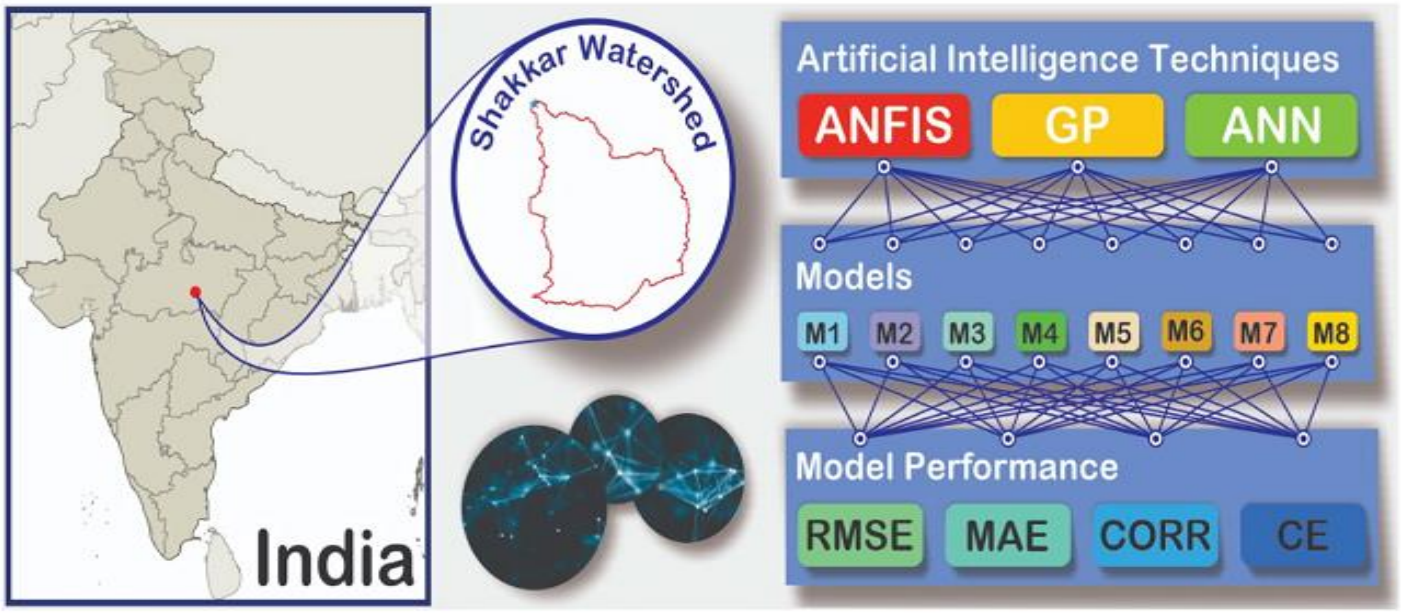
Streamflow Prediction Based on Artificial Intelligence Techniques

Sarita Gajbhiye Meshram[1] · Chandrashekhar Meshram[2] · Celso Augusto Guimarães Santos[3] · Brahim Benzougagh[4] · Khaled Mohamed Khedher[5,6]

Received: 31 May 2020 / Accepted: 19 June 2021

Abstract
The application of Artificial Intelligence (AI) techniques has become popular in science and engineering applications since the middle of the twentieth century. In this present study, three AI techniques (ANFIS, GP and ANN) have been used for forecasting streamflow into Shakkar watershed (Narmada Basin), India. The models have been used considering previous streamflow and cyclic terms in the input vector to provide a suitable time series model for streamflow forecasting. To evaluate the model performance, RMSE, MAE, CORR and CE were employed. Results showed that the ANFIS has the best performance in forecasting streamflow time series for Shakkar watershed. The GP and ANN are in the 2nd and 3rd ranks, respectively. According to the results, in all the AI methods (ANFIS, GP and ANN), the model with cyclic terms had better performance compared to those models not considering periodic nature and being applied by only considering the previous streamflow.

Graphical Abstract



Keywords Artificial Intelligence models · Cyclic Term · Streamflow · Forecasting · Artificial Neural Network

Extended author information available on the last page of the article

Published online: 30 June 2021

Name of Faculty: Dr. Chandrashekhar Meshram

Londhe S, Charhate S (2010) Comparison of data-driven modelling techniques for river flow forecasting. Hydrol Sci J 55(7):1163–1174. https://doi.org/10.1080/02626667.2010.512867
Meshram SG, Ghorbani MA, Deo RC, Kashani MH, Meshram C, Karimi V (2019a) New approach for sediment yield forecasting with a two-phase feedforward neuron network-particle swarm optimization model integrated with the gravitational search algorithm. Water Res Manag 33(7):2335–2356
Meshram SG, Ghorbani MA, Shamshirband S, Karimi V, Meshram C (2019b) River flow prediction using hybrid PSOGSA algorithm based on feed-forward neural network. Soft Comput 23(20):10429–10438
Meshram SG, Safari MJS, Khosravi K, Meshram C (2021a). Iterative classifier optimizer-based pace regression and random forest hybrid models for suspended sediment load prediction. Environmental Science and Pollution Research 28 (1):11637–11649
Meshram SG, Pourghasemi HR, Abba SI, Alvandi E, Meshram C, Khedher KM (2021b) A comparative study between dynamic and soft computing models for sediment forecasting. Soft Comput, https://doi.org/10.1007/s00500-021-05834-x.
Mugumo M (2012) A simple operating model of the Van der Kloof Reservoir using ANN streamflow forecasts. MSc Dissertation. University of the Witwatersrand, South Africa
Nash JE, Sutcliffe JV (1970) River flow forecasting through conceptual models part I - A discussion of principles. J Hydrol 10(3):282–290
Nayak PC, Sudheer KP, Rangan DM, Ramasastri KS (2004) A neuro fuzzy computing technique for modeling hydrological time series. Jhydrol 29:52–66
Nourani V, Komasi M, Alami MT (2012) Hybrid wavelet–genetic programming approach to optimize ANN modelling of rainfall–runoff process. J Hydrol Eng 17(6):724–741
Rasouli K, Hsieh WW, Cannon AJ (2012) Daily streamflow forecasting by machine learning methods with weather and climate inputs. J Hydrol 414–415:284–293
Reddy MJ (2006) Swarm intelligence and evolutionary computation for single and multi-objective optimation in water resource systems. A Thesis Submitted for the Degree of Doctor of Philosophy in the Faculty of Engineering, Department of Civil Engineering Indian Institute of Science Bangalore -560012, India, September 2006.
Salas JD (1993) Analysis and modeling of hydrologic time series. In: Maidment DR (ed) Handbook of Hydrology. The McGraw Hill, New York, pp 19.5-19.9
Santos CAG, Silva GBL (2013) Daily streamflow forecasting using a wavelet transform and artificial neural network hybrid models. Hydrol Sci J 59(2):312–324
Santos CAG, Freire PKMM, Silva RM, Akrami SA (2019) Hybrid wavelet neural network approach for daily inflow forecasting using tropical rainfall measuring mission data. J Hydrol Eng 24(2):04018062
Saraiva SV, Carvalho FO, Santos CAG, B LC, Freire, PKMM, (2021) Daily streamflow forecasting in Sobradinho Reservoir using machine learning models coupled with wavelet transform and bootstrapping. Appl Soft Comput. https://doi.org/10.1016/j.asoc.2021.107081
Shiri J, Kisi O (2010) Short-term and long-term streamflow forecasting using a wavelet and neuro-fuzzy conjunction model. J Hydrol 394(3–4):486–493
Sreekanth J, Datta B (2011) Coupled simulation–optimization model for coastal aquifer management using genetic programming-based ensemble surrogate models and multiple-realization optimization. Water Resour Res 47:W04516
Srikanthan R, McMahon TA (2001) Stochastic generation of annual, monthly and daily climate data: a review. Hydrol Earth Syst Sci 5(4):653–670
Toth E, Brath A, Montanari A (2000) Comparison of short-term rainfall prediction models for real-time flood forecasting. J Hydrol 239(1–4):132–147
Valipour M, Banihabib ME, Behbahani SMR (2013) Comparison of the ARMA, ARIMA, and the autoregressive artificial neural network models in forecasting the monthly inflow of Dez dam reservoir. J Hydrol 476:433–441
Wang WC, Chau KW, Cheng CT, Qiu L (2009) A comparison of performance of several artificial intelligence methods for forecasting monthly discharge time series. J Hydrol 374:294–306
Zadeh LA (1965) Fuzzy Sets. Inf Control 8:338–353
Zimmermann HJ (1996) Fuzzy Set Theory and Its Applications, 3rd edn. Kluwer Academic Publishers, Boston, MA

Authors and Affiliations

Sarita Gajbhiye Meshram[1] · Chandrashekhar Meshram[2] · Celso Augusto Guimarães Santos[3] · Brahim Benzougagh[4] · Khaled Mohamed Khedher[5,6]

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Celso Augusto Guimarães Santos
celso@ct.ufpb.br

Brahim Benzougagh
benzougaghbrahim@gmail.com

Khaled Mohamed Khedher
kkhedher@kku.edu.sa

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India

[3] Department of Civil and Environmental Engineering, Federal University of Paraíba, João Pessoa, Paraíba 58051-900, Brazil

[4] Department of Geomorphology and Geomatics, Scientific Institute, Mohammed V University, Avenue Ibn Batouta, P.O. Box 703, 10106 Rabat City, Morocco

[5] Department of Civil Engineering, College of Engineering, King Khalid University, Abha 61421, Saudi Arabia

[6] Department of Civil Engineering, High Institute of Technological Studies, Mrezgua University Campus, 8000 Nabeul, Tunisia

JOURNAL OF ENGINEERING, COMPUTING & ARCHITECTURE ISSN NO:1934-7197

Ecological niche of *Cryptococcus neoformans* species complex from Betul city of Madhya Pradesh

Mahendra Nawange[1,2,3], Alka Pandey[1], Anil Prakash [2], Shesh Rao Nawange[3,4], Richa Gumasta[3,5], Jitendra Nawange[1,3]

1. *Department of Microbiology, J.H. GOVT. P.G. College, Betul (M.P.) India*
2. *Department of Microbiology Barkatullah University, Bhopal (M.P.) India*
3. *Centre for Medical Mycology, Fungal Disease Diagnostic and Research Center, Jabalpur, (M.P.) India*
4. *Department of Botany and Zoology, NSCB Government Girls College, Seoni, Madhya Pradesh, India*

5.Government Science College, Jabalpur, (M.P.) India

Abstract

Globally the risk of outbreaks has been increasing with the expansion of environmental *Cryptococcus neoformans* and *Cryptococcus gattii* pathogens. In this prospective study we analyzed the isolation of *C. neoformans* - *C. gattii* strains from a total of 500 tree samples and *C. neoformans* from 194 pigeon samples collected from different sites of Betul and Bhopal city of Madhya Pradesh (India). Selective isolation of *C. neoformans* sp. complex was done by swabbing and Direct Plating Method. As per the data, out of total 500 tree samples 30 were found positive for *Cryptococcus neoformans* and 36 samples positive for *C. gattii*. Highest cfu was obtained from *Tamarindus indica* ($19x10^4$). Total 35 pigeon samples were found positive for *C. neoformans* and the highest frequency was observed from the pigeon sample collected from Bablu Talab Kothin Bazar (12.08%), Betul city of Madhya Pradesh (India). This study suggested the living tree trunk hollows and pigeon excreta as a possible ecologic niche for *C. neoformans* species complex, hence it gains more attention in the environmental occurrence and role in cryptococcosis.

Keywords: *C. neoformans* species complex, living tree trunk hollows, pigeon excreta

Corresponding author: nawange1990@gmail.com

Introduction

Cryptococcosis is caused by both the varieties of *C.neoformans* species complex, *i.e., Cryptococcus neoformans* and *Cryptococcus gattii* that affects lungs and central nervous system predominantly and is the commonest fungal meningitis (Meyer *et al.,* 2009).

Over the past 2 decades, the case of deadly disease has increased worldwide dramatically in the number of immunocompromised individuals with HIV infection, cancer

Name of Faculty: Dr. Mousmi Rai

Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2022 3(1), 409–414

GLOBALIZATION AND MARKETISM IN INDIAN MEDIA (ANALYTICAL STUDIES)
भारतीय मीडिया में वैश्वीकरण और बाजारवाद (विश्लेषणात्मक अध्ययन)

Dr. Mousmi Rai [1]

[1,2] Assistant Professor, Government. J.H. P.G. College, Betul, Madhya Pradesh, India

Received 26 March 2022
Accepted 30 May 2022
Published 10 June 2022

Corresponding Author
Dr. Mousmi Rai,
mousmi.pramod@gmail.com

DOI
10.29121/shodhkosh.v3.i1.2022.110

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

ABSTRACT

English: There is a famous saying- good things should always be accepted and bad things should always be discarded. But in the context of Indian media, this proverb has a different meaning. In the present era Indian media especially broadcasting media is following western and European countries. This is a worrying situation, which is very important to get control in time. But the way the current media is moving towards digital platforms, the boundaries of news are shrinking. In the case of media convergence, the condition of broadcast journalism cannot be said to be very good. Not everything is negative though. In the era of globalization, the Internet has also served to enrich broadcast journalism. This is the reason that now along with traditional media, digital media has increased penetration among the people. Monopoly has also ended with the news. The truth is reaching the public fast.

Hindi: एक प्रसिद्ध कहावत है- अच्छी चीजों को हमेशा ग्रहण करना चाहिए और बुरी चीजों को हमेशा छोड़ देना चाहिए। लेकिन भारतीय मीडिया के परिप्रेक्ष्य में यह कहावत कुछ अलग अर्थ लिए हुए है। वर्तमान दौर में भारतीय मीडिया खासकर प्रसारण मीडिया पश्चिमी और यूरोपीय देशों का अनुसरण कर रहा है। यह एक चिंताजनक स्थिति है, जिसपर समय रहते नियंत्रण पाना बेहद जरूरी है। Prasad (1989) लेकिन जिस तरह से वर्तमान मीडिया डिजिटल प्लेटफॉर्म की तरफ बढ़ रहा है, वैसे-वैसे खबरों की सीमाएं सिमटती जा रही हैं। मीडिया कंजवर्जेंस की स्थिति में प्रसारण पत्रकारिता की स्थिति बहुत अच्छी नहीं कही जा सकती। हालांकि सबकुछ नकारात्मक भी नहीं है। वैश्वीकरण के दौर में इंटरनेट ने प्रसारण पत्रकारिता को समृद्ध करने का भी कार्य किया है। यही कारण है कि अब पारंपरिक मीडिया के साथ-साथ डिजिटल मीडिया ने लोगों के बीच पैठ बढ़ाई है। खबरों से एकाधिकार भी खत्म हुआ है। जनता तक सच तेजी से पहुंच रहा है।

Keywords: Broadcast, Journalism, Western, Digital, Monopoly, प्रसारण, पत्रकारिता, पश्चिमी, डिजिटल, एकाधिकार।

1. प्रस्तावना

ऐसी मान्यता है कि ऋषि नारद एक लोक से दूसरे लोक तक संचार प्रतिनिधि के रूप में भूमिका अदा करते थे। उन्हें दुनिया के पहले पत्रकार के रूप में भी मान्यता मिली हुई है। उस युग में नारद मुनि एक सूचना को अन्य स्थान तक पहुंचाते थे। वह जस की तस सूचना दूसरे स्थान तक पहुंचती थी। लेकिन वर्तमान समय में मीडिया की छवि में बदलाव आया है। भारतीय मीडिया पर वैश्वीकरण का प्रभाव पड़ा है। Pataanjali (1997) इसके बाद से पत्रकारिता के सिद्धांतों में आमूल-चूल परिवर्तन देखने को मिल रहे हैं। वर्ष 2019 में केंद्र सरकार ने डिजिटल मीडिया में 26 फीसद प्रत्यक्ष विदेशी निवेश (एफडीआई) को मंजूरी प्रदान की है। कई लोग इस फैसले का स्वागत कर रहे हैं। उनका कहना है कि देश में चल रहे तमाम

Name of Faculty: Dr. Mousmi Rai

Mukt Shabd Journal **ISSN NO : 2347-3150**

व्यावसायिक जगत में महिलाओं की सहभागिता (चुनौतियां एवं समाधान)

- डॉ. मौसमी राय

सहायक प्राध्यापक, वाणिज्य विभाग, शासकीय जे.एच. पी. जी. कॉलेज बैतूल, मध्यप्रदेश

सारांश :

'यत्र नार्यस्तु पूज्यन्ते रमन्ते तत्र देवताः', अर्थात् जहाँ महिला की पूजा होती है वहाँ देवता निवास करते हैं। जहाँ महिला की पूजा नहीं होती है, उनका सम्मान नहीं होता, वहाँ किये गये समस्त कर्म निष्फल हो जाते हैं। हमारे वेद, पुराणों में लिखी यह बातें हमें गौरव की अनुभूति कराते हैं। हमारी सनातन भारतीय परंपरा में महिलाओं को देवी का दर्जा दिया गया है। यह बात शास्त्रों तक ही सीमित नहीं है। किसी भी देश को तब तक लोकतांत्रिक नहीं माना जा सकता, जब तक वहां महिलाओं का बराबर का दर्जा न दिया जाये। वैश्विक परिदृश्य में देखा जाये तो आज हर क्षेत्र में महिलाओं ने परचम लहराया है। व्यवासायिक जगत में अपनी पैठ जमाई है। दुनियाभर के देशों में महिलाओं के प्रति अलग–अलग वर्ताव की खबरें हमेशा आती हैं। कहीं महिलाएं विकास के पथ पर आगे बढ़ रही हैं, तो कहीं महिलाओं को घर के उपभोग की वस्तु बनाकर सीमित कर दिया गया है। लोकतांत्रिक देश भारत की स्थिति संतोषजनक कहीं जा सकती है, लेकिन इसे पूर्ण विकास नहीं कहा जा सकता। देश के व्यावसायिक तंत्र में भी महिलाओं की स्थिति सुदृढ़ हो रही है, लेकिन पूर्ण सशक्त कहने की बात अभी बेमानी होगी।

मुख्य शब्द :

महिला, भारतीय, शास्त्र, व्यावसायिक, सशक्त

प्रस्तावना :

भारत जैसे लोकतंत्र की स्थिति थोड़ा उलट है। आदिकाल से ही महिलाओं का वर्चस्व रहा है। हिन्दू धर्म के शास्त्रों में देवियों की स्थिति देखकर हम सहर्ष अंदाजा लगा लेते हैं कि यहां महिलाएं, बराबरी का दर्जा पाती रही हैं। दुर्गा शक्ति का रूप रही हैं तो लक्ष्मी धन की देवी कहलाईं, सरस्वती ने जगत को शिक्षा से सराबोर कर दिया। भारत माता के पैरों से गुलामी की जंजीर को तोड़ फेंकने वाली महिलाओं की शौर्य गाधा से तो इतिहास भरा पड़ा है। आजादी के बाद राजनीतिक नेृतत्व में भी हमने महिलाओं की पैठ देखी है।अब व्यावसायिक जगत में कहानी हम सभी के सामने है।व्यवसाय हो या अन्य कोई भी क्षेत्र। महिलाएं तभी आगे बढ़ सकती हैं जबकि वे शिक्षित हो। जब भी महिला के सशक्त होने की बात की जाएगी तो शिक्षा ही पहली सीढ़ी मानी जाएगी। परिवार, समाज और देश के विकास में शिक्षित महिला महत्वपूर्ण भूमिका निभा सकती है। शिक्षित महिलाएं समाज में बदलाव ला सकती हैं। पढ़ी–लिखी महिलाओं को बैंक से लेकर सार्वजनिक स्थलों पर कोई गुमराह नहीं कर सकता है। शिक्षित महिला समाज की रीढ़ होती है। शिक्षित महिला मां, पत्नी, बेटी के रूप में एक सभ्य और संस्कारी समाज की शिल्पकार होती है। शिक्षित महिलाएं अपने अधिकारों के साथ ही कर्तव्यों के प्रति भी जागरूक हैं। एक पढ़ी–लिखी महिला अपने परिवार को सभ्य और प्रगतिशील तो बनाती ही है, इसके साथ ही समाज और देश के विकास में अप्रत्यक्ष व परोक्ष रूप से कई भूमिकाएं निभाती है। समाज और देश का सही, सच्चे अर्थों में तभी विकास हो सकता है, जब देश की नारी शिक्षित हो। आज पढ़ी–लिखी महिला घर से लेकर व्यवसाय और अन्य कार्य क्षेत्रों में मुकाम हासिल कर रही है।

अध्ययन के उद्देश्य :

1. वैश्विक स्तर पर महिलाओं की स्थिति का अध्ययन करना?

Name of Faculty: Mr. Manoj Kumar Ghorase

How to Cite:
Ghorase, M. K., Bele, P., & Udaipure, S. K. (2022). Phytochemical screening and quanitative analysis of active phytocontents of Guizotia abyssinica seed to knows of their therapeutic values . *International Journal of Health Sciences*, *6*(S2), 2880–2892.
https://doi.org/10.53730/ijhs.v6nS2.5794

Phytochemical screening and quanitative analysis of active phytocontents of Guizotia abyssinica seed to knows of their therapeutic values

Manoj Kumar Ghorase
Govt. J.H. P.G. College, Betul

Parasnath Bele
Govt. N.M.V, Hohashangabad

S. K. Udaipure
Govt. N.M.V, Hohashangabad

Abstract---*Guizotia abyssinica Cass.* belonging to the family Asteraceae is a vegetable plant with many industrial and medicinal value. Current research describes a simple, effective and reproducible G-in-vitro propagation protocol. *G. abyssinica* and comparative phytochemical analysis of natural seeds, leaf (mature and in vitro regenerated) and *G. abyssinica* Different annotations namely. apical and axilllary buds, leaves and internode were selected for the in vitro regeneration study to assess the effect of differential concentrations on TDZ. Different parts of the plant such as seeds, natural leaf, in vitro leaf and callus were dried and extracted from different solvents and tested with various phytochemical analyzes. Of all the four annotations used, the apical shoot appeared to be the best in terms of shoot reproduction and reproduction. In vitro renewed callus has shown the presence of phenol. It may be concluded that additional suspension of hormonal compounds may be helpful in the widespread distribution and release of drugs for commercial use. The findings provide potential support for tissue tissue techniques in the production of bioactive compounds but further studies are needed as well.

Keywords---phytochemicals, guizotiaabyssinica, callus, in vitro regeneration, TPC, TFC

Name of Faculties: Dr. Mahendra Nawange, Dr. Alka Pandey

The International journal of analytical and experimental modal analysis ISSN NO: 0886-9367

Extracellular phospholipase activity in the environmental strains of *Cryptococcus neoformans* and *Cryptococcus gattii* isolated from Betul city of Madhya Pradesh

Mahendra Nawange[1,2,3], Alka Pandey[1], Anil Prakash [2], Shesh Rao Nawange[3,4], Richa Gumasta[3,5], Jitendra Nawange[1,3]

1. Department of Microbiology, J.H. GOVT. P.G. College, Betul (M.P.) India
2. Department of Microbiology Barkatullah University, Bhopal (M.P.) India
3. Centre for Medical Mycology, Fungal Disease Diagnostic and Research Center, Jabalpur, (M.P.) India
4. Department of Botany and Zoology, NSCB Government Girls College, Seoni, Madhya Pradesh, India
5.Government Science College, Jabalpur, (M.P.) India

Abstract

Cryptococcosis accounts for significantly life-threatening diseases in healthy and immunocompromised individuals by the production of extracellular enzymes in host cell. In the present study we focused on the extracellular phospholipase (PLP) activity which contributes to the most widely concerned issue of these enzymes as prominent virulence factors. For the screening of phospholipase producing strains, 45 environmental isolates of both *Cryptococcus neoformans* and *C. gattii* strains were point inoculated on egg yolk agar. In reference to *C. neoformans* and *C. gattii* isolated from tree samples, 17 (62.9%) strains showed high phospholipase production on 5th day and 18 (66.66 %) on 8th day of incubation with low Pz value (Pz $\leq$ 0.6). However, in case of yeast strains obtained from pigeon samples showed high phospholipase production that is 10 (55.55 %) and 11 (61.11 %) on 5th and 8th day of incubation. As per the statistical analysis using Independent "t" test, no significant difference was observed between phospholipase production by *C. neoformans and C. gattii* strains.

Keywords: *Cryptococcus neoformans*, *C. gattii,* phospholipase activity, virulence factors

Corresponding author: nawange1990@gmail.com

Introduction

The potential *Cryptococcus* virulence determinants play crucial roles in the fungal pathogenesis, these include extracellular enzymes production, the release of polyol metabolites, interaction with hormones, adherence, and production of mannoproteins (Kronstad *et al.,* 2011).

Cryptococcus neoformans species complex produces phospholipase enzyme which is pathogenic and the mechanism to decline its activity *in-vivo* is a subject less explored.

Academic Session 2020-2021

Name of Faculty: Dr. Chandrashekhar Meshram

Journal of Advanced Research 32 (2021) 139–148

Contents lists available at ScienceDirect

Journal of Advanced Research

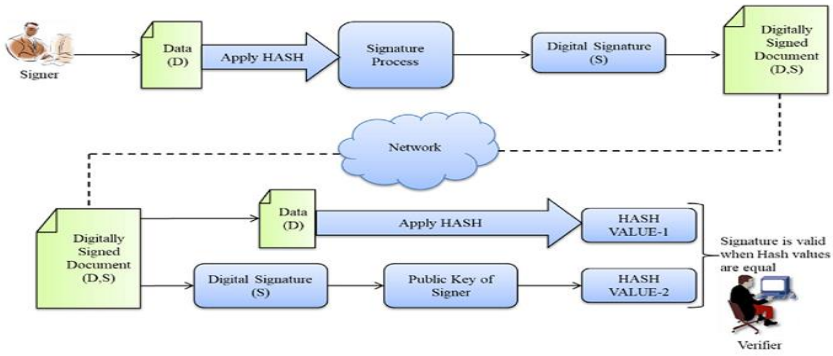
journal homepage: www.elsevier.com/locate/jare

Fractional chaotic maps based short signature scheme under human-centered IoT environments

Chandrashekhar Meshram [a,*], Rabha W. Ibrahim [b,c], Ahmed J. Obaid [d], Sarita Gajbhiye Meshram [e,f], Akshaykumar Meshram [g], Alaa Mohamed Abd El-Latif [h,i]

[a] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Barkatullah Vishwavidyalaya, Betul, M.P. 460001, India
[b] Informetrics Research Group, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
[c] Faculty of Mathematics & Statistics, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
[d] Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Iraq
[e] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
[f] Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Viet Nam
[g] Department of Applied Mathematics, Yeshwantrao Chavan College of Engineering, Nagpur, M.S., India
[h] Department of Mathematics, Faculty of Education, Ain Shams University, Roxy, Cairo, Egypt
[i] Department of Mathematics, Faculty of Arts and Science, Northern Border University, Rafha, Saudi Arabia

GRAPHICAL ABSTRACT



ARTICLE INFO

Article history:
Received 30 May 2020
Revised 19 August 2020
Accepted 22 August 2020
Available online 9 September 2020

ABSTRACT

Introduction: The Internet of Things (IoT) comprises of various smart devices for the sharing of sensed data through online services. People will be directly contacted to check their health parameters and the reports will be collected centrally through smart devices. The requirement is protection of messages during the exchange of data between sender and receiver in order to tackle human malicious attacks. Various signature-based schemes are discussed in the literature to provide secure communication.

Peer review under responsibility of Cairo University.
* Corresponding author.
E-mail addresses: cs_meshram@rediffmail.com (C. Meshram), rabhaibrahim@tdtu.edu.vn (R.W. Ibrahim), ahmedj.aljanaby@uokufa.edu.iq (A.J. Obaid), saritagmeshram@tdtu.edu.vn (S.G. Meshram), alaa.Ali@nbu.edu.sa (A.M.A. El-Latif).

https://doi.org/10.1016/j.jare.2020.08.015

Name of Faculty: Dr. Chandrashekhar Meshram

Environmental Earth Sciences (2021) 80:631
https://doi.org/10.1007/s12665-021-09919-6

ORIGINAL ARTICLE

Simplified sediment yield index incorporating parameter stream length

Sarita Gajbhiye Meshram[1] · Vijay P. Singh[2,3] · Chandrashekhar Meshram[4] · Mohd Abul Hasan[5] · Saiful Islam[5]

Received: 20 November 2020 / Accepted: 27 August 2021

Abstract
Sediment-Runoff process is highly variable and nonlinear in nature. In the present study an attempt has been made to develop a relationship between watershed stream length and Sediment Yield Index (SYI) and test it on Narmada watersheds, Madhya Pradesh, India. Area (A), Curve Number (CN) and stream length (SL) were utilized as input for model development. The three models (A model, CN model and simplified All India Soil and Land Use Survey (AISLUS) model including parameter SL) performed differently, with the coefficient of R^2 equal to 0.01, 0.02 and 0.71 (Shakkar watershed), 0.11, 0.23 and 0.91 (Bamhani watershed), 0.06, 0.001 and 0.80 (Manot watershed) and 0.40, 0.05 and 0.66 (Mohgaon watershed), respectively. The logarithmic simplified AISLUS model incorporating parameter SL resulted with the coefficient of R^2 as 0.76 (Shakkar watershed), 0.93 (Bamhani watershed), 0.84 (Manot watershed) and 0.66 (Mohgaon watershed). Therefore, the logarithm simplified AISLUS model was chosen as the best regression model for this study. It is observed that the simplified AISLUS model (logarithm form) incorporating parameter SL had a satisfactory efficiency as 76.35% (Shakkar watershed), 66.05% (Mohgaon watershed), 93.36% (Bamhani watershed), and 83.83% (Manot watershed) by Nash efficiency scale. The resulting higher Nash efficiency values support the versatility of the derived relationship and invoke assessment of SYI from the watershed stream length value. The prediction of SYI is important when adopting a suitable soil conservation measure in the watershed for minimizing soil erosion.

Keywords Sediment yield · Runoff · Narmada river · Modeling · Stream length

Introduction

Accurate estimation of the amount of runoff and sediment is important for management of the water resources (Gajbhiye et al. 2014). Surface runoff and sediment yield are two major hydrological response caused by precipitation (Gajbhiye et al. 2014). Water is the major agent responsible for soil erosion may be defined as detachment and then movement of soil particles from one place to another place. At many locations, wind and glacial runoff may also be the agent of soil erosion. To control soil erosion in any area by various soil and water management measures the developmental unit

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Vijay P. Singh
v.singh@tamu.edu

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Mohd Abul Hasan
mohad@kku.edu.sa

Saiful Islam
sfakrul@kku.edu.sa

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Department of Biological and Agricultural Engineering, Texas A and M University, College Station, TX 77843-2117, USA

[3] Zachry Department of Civil Engineering, Texas A and M University, College Station, TX 77843-2117, USA

[4] Department of Mathematics, Jaywanti Haksar Government P. G. College, College of Chhindwara University, Betul, Madhaya Pradesh, India

[5] Civil Engineering Department, College of Engineering, King Khalid University, Abha, Saudi Arabia

Published online: 14 September 2021

sensors
MDPI

Article

An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps

Chandrashekhar Meshram [1], Agbotiname Lucky Imoize [2,3,*], Amer Aljaedi [4], Adel R. Alharbi [4], Sajjad Shaukat Jamal [5] and Sharad Kumar Barve [6]

[1] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul 460001, India; cs_meshram@rediffmail.com
[2] Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[3] Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany
[4] College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia; aaljaedi@ut.edu.sa (A.A.); aalharbi@ut.edu.sa (A.R.A.)
[5] Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia; shussain@kku.edu.sa
[6] Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India; drshardbarve@rediffmail.com
* Correspondence: aimoize@unilag.edu.ng

Citation: Meshram, C.; Imoize, A.L.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S.; Barve, S.K. An Efficient Electronic Cash System Based on Certificateless Group Signcryption Scheme Using Conformable Chaotic Maps. *Sensors* **2021**, *21*, 7039. https://doi.org/10.3390/s21217039

Academic Editor: Jiankun Hu

Received: 17 September 2021
Accepted: 21 October 2021
Published: 23 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: Signcryption schemes leveraging chaotic constructions have garnered significant research interest in recent years. These schemes have proffered practical solutions towards addressing the vast security vulnerabilities in Electronic Cash Systems (ECS). The schemes can seamlessly perform message confidentiality and authentication simultaneously. Still, their applications in emerging electronic cash platforms require a higher degree of complexity in design and robustness, especially as billions of online transactions are conducted globally. Consequently, several security issues arise from using open wireless channels for online business transactions. In order to guarantee the security of user information over these safety-limited channels, sophisticated security schemes are solely desired. However, the existing signcryption schemes cannot provide the required confidentiality and authentication for user information on these online platforms. Therefore, the need for certificateless group signcryption schemes (CGSS) becomes imperative. This paper presents an efficient electronic cash system based on CGSS using conformable chaotic maps (CCM). In our design, any group signcrypter would encrypt information/data with the group manager (GM) and send it to the verifier, who confirms the authenticity of the signcrypted information/data using the public criteria of the group. Additionally, the traceability, unforgeability, unlinkability, and robust security of the proposed CGSS-CCM ECS scheme have been built leveraging computationally difficult problems. Performance evaluation of the proposed CGSS-CCM ECS scheme shows that it is secure from the Indistinguishably Chosen Ciphertext Attack. Finally, the security analysis of the proposed technique shows high efficiency in security-vulnerable applications. Overall, the scheme gave superior security features compared to the existing methods in the preliminaries.

Keywords: certificateless group signcryption scheme (CGSS); conformable chaotic maps (CCM); electronic cash system (ECS); signcrypter; provably secure schemes; authentication; E-commerce channels

1. Introduction

In modern electronic commerce, digital signatures play a significant role due to integrity and authentication requirements. Integrity is a vital property that helps to monitor

sensors
MDPI

Article

A Provably Secure IBE Transformation Model for PKC Using Conformable Chebyshev Chaotic Maps under Human-Centered IoT Environments

Chandrashekhar Meshram [1], Agbotiname Lucky Imoize [2,3,*], Amer Aljaedi [4], Adel R. Alharbi [4], Sajjad Shaukat Jamal [5] and Sharad Kumar Barve [6]

[1] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul 460001, Madhya Pradesh, India; cs_meshram@rediffmail.com
[2] Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[3] Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany
[4] College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia; aaljaedi@ut.edu.sa (A.A.); aalharbi@ut.edu.sa (A.R.A.)
[5] Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia; shussain@kku.edu.sa
[6] Water Resources and Applied Mathematics Research Lab, Nagpur 440027, India; drshardbarve@rediffmail.com
* Correspondence: aimoize@unilag.edu.ng

Citation: Meshram, C.; Imoize, A.L.; Aljaedi, A.; Alharbi, A.R.; Jamal, S.S.; Barve, S.K. A Provably Secure IBE Transformation Model for PKC Using Conformable Chebyshev Chaotic Maps under Human-Centered IoT Environments. *Sensors* **2021**, *21*, 7227. https://doi.org/10.3390/s21217227

Academic Editor: Andrei Gurtov

Received: 29 September 2021
Accepted: 27 October 2021
Published: 30 October 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: The place of public key cryptography (PKC) in guaranteeing the security of wireless networks under human-centered IoT environments cannot be overemphasized. PKC uses the idea of paired keys that are mathematically dependent but independent in practice. In PKC, each communicating party needs the public key and the authorized digital certificate of the other party to achieve encryption and decryption. In this circumstance, a directory is required to store the public keys of the participating parties. However, the design of such a directory can be cost-prohibitive and time-consuming. Recently, identity-based encryption (IBE) schemes have been introduced to address the vast limitations of PKC schemes. In a typical IBE system, a third-party server can distribute the public credentials to all parties involved in the system. Thus, the private key can be harvested from the arbitrary public key. As a result, the sender could use the public key of the receiver to encrypt the message, and the receiver could use the extracted private key to decrypt the message. In order to improve systems security, new IBE schemes are solely desired. However, the complexity and cost of designing an entirely new IBE technique remain. In order to address this problem, this paper presents a provably secure IBE transformation model for PKC using conformable Chebyshev chaotic maps under the human-centered IoT environment. In particular, we offer a robust and secure IBE transformation model and provide extensive performance analysis and security proofs of the model. Finally, we demonstrate the superiority of the proposed IBE transformation model over the existing IBE schemes. Overall, results indicate that the proposed scheme posed excellent security capabilities compared to the preliminary IBE-based schemes.

Keywords: public key cryptography; identity-based encryption schemes; Chebyshev polynomial; conformable Chebyshev chaotic maps; human-centered Internet of Things

1. Introduction

Human-centered Internet of Things (IoT) enables seamless processing of electronic transactions, healthcare information systems, efficient operation of intelligent devices,

Name of Faculty: Dr. Chandrashekhar Meshram

sensors

MDPI

Review

Performance Measurement System and Quality Management in Data-Driven Industry 4.0: A Review

Parkash Tambare [1], Chandrashekhar Meshram [2,*], Cheng-Chi Lee [3,4,*], Rakesh Jagdish Ramteke [5] and Agbotiname Lucky Imoize [6,7]

[1] Water Resources & Applied Mathematics Research Lab, Nagpur 440027, India; prakash.tambare058@gmail.com
[2] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul 460001, Madhya Pradesh, India
[3] Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei 24205, Taiwan
[4] Department of Computer Science and Information Engineering, Asia University, Wufeng Shiang, Taichung 41354, Taiwan
[5] School of Computer Sciences, KBC North Maharashtra University, P.B. No.80, Umavinagar, Jalgaon 425001, Maharashtra, India; rakeshramteke@yahoo.co.in
[6] Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria; aimoize@unilag.edu.ng
[7] Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University, 44801 Bochum, Germany
* Correspondence: cs_meshram@rediffmail.com (C.M.); cclee@mail.fju.edu.tw (C.-C.L.)

Citation: Tambare, P.; Meshram, C.; Lee, C.-C.; Ramteke, R.J.; Imoize, A.L. Performance Measurement System and Quality Management in Data-Driven Industry 4.0: A Review. *Sensors* **2022**, *22*, 224. https://doi.org/10.3390/s22010224

Academic Editors: Aris Leivadeas, Vasileios Karyotis and Dimitrios Dechouniotis

Received: 30 November 2021
Accepted: 21 December 2021
Published: 29 December 2021

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Abstract: The birth of mass production started in the early 1900s. The manufacturing industries were transformed from mechanization to digitalization with the help of Information and Communication Technology (ICT). Now, the advancement of ICT and the Internet of Things has enabled smart manufacturing or Industry 4.0. Industry 4.0 refers to the various technologies that are transforming the way we work in manufacturing industries such as Internet of Things, cloud, big data, AI, robotics, blockchain, autonomous vehicles, enterprise software, etc. Additionally, the Industry 4.0 concept refers to new production patterns involving new technologies, manufacturing factors, and workforce organization. It changes the production process and creates a highly efficient production system that reduces production costs and improves product quality. The concept of Industry 4.0 is relatively new; there is high uncertainty, lack of knowledge and limited publication about the performance measurement and quality management with respect to Industry 4.0. Conversely, manufacturing companies are still struggling to understand the variety of Industry 4.0 technologies. Industrial standards are used to measure performance and manage the quality of the product and services. In order to fill this gap, our study focuses on how the manufacturing industries use different industrial standards to measure performance and manage the quality of the product and services. This paper reviews the current methods, industrial standards, key performance indicators (KPIs) used for performance measurement systems in data-driven Industry 4.0, and the case studies to understand how smart manufacturing companies are taking advantage of Industry 4.0. Furthermore, this article discusses the digitalization of quality called Quality 4.0, research challenges and opportunities in data-driven Industry 4.0 are discussed.

Keywords: Industry 4.0; Internet of Things; Quality 4.0; performance measurement system; cyber–physical production system

Name of Faculty: Dr. Chandrashekhar Meshram

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 1, 2021, accepted September 18, 2021, date of publication September 20, 2021,
date of current version September 30, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3114287

IBOOST: A Lightweight Provably Secure Identity-Based Online/Offline Signature Technique Based on FCM for Massive Devices in 5G Wireless Sensor Networks

CHANDRASHEKHAR MESHRAM[1], AGBOTINAME LUCKY IMOIZE[2,3], (Member, IEEE), AZEDDINE ELHASSOUNY[4], AMER ALJAEDI[5], ADEL R. ALHARBI[5], AND SAJJAD SHAUKAT JAMAL[6]

[1]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, Chhindwara University, Betul, Madhya Pradesh 460001, India
[2]Department of Electrical and Electronics Engineering, Faculty of Engineering, University of Lagos, Akoka, Lagos 100213, Nigeria
[3]Department of Electrical Engineering and Information Technology, Institute of Digital Communication, Ruhr University Bochum, 44801 Bochum, Germany
[4]ENSIAS, Mohammed V University in Rabat, Rabat 10000, Morocco
[5]College of Computing and Information Technology, University of Tabuk, Tabuk 71491, Saudi Arabia
[6]Department of Mathematics, College of Science, King Khalid University, Abha 61413, Saudi Arabia

Corresponding authors: Chandrashekhar Meshram (cs_meshram@rediffmail.com), Sajjad Shaukat Jamal (shussain@kku.edu.sa), and Agbotiname Lucky Imoize (aimoize@unilag.edu.ng)

This work was supported by the Deanship of Scientific Research at King Khalid University through the Research Groups Program under Grant R. G. P. 1/72/42. The work of Agbotiname Lucky Imoize was supported by the Nigerian Petroleum Technology Development Fund (PTDF) and the German Academic Exchange Service (DAAD) through the Nigerian-German Postgraduate Program under Grant 57473408.

ABSTRACT The fifth-generation (5G) wireless network is commercialized. The need to integrate massive devices in 5G and wireless sensor networks (WSN) to provide several convenient services for network users becomes imperative. However, there are growing concerns that 5G-WSNs pose new security threats to sensitive user information. User authentication and key agreement have been provided for secure end-to-end communication. However, stricter security techniques are required as billions of massive devices are being networked to collect and process complex user data in real-time. Therefore, anonymous authentication and authorization are highly coveted for privacy preservation and prevention of unlawful exploitation of user data. However, guaranteeing data integrity, authentication, and non-repudiation require special-purpose identity-based signature techniques that are quite difficult to design in practice. In order to address this problem, this paper proposes a lightweight, provably secure identity-based online/offline signature technique (IBOOST) and its extension for massive devices in 5G-WSNs using fractional chaotic maps. The IBOOST scheme achieves multi-time use of offline storage at a lower processing time. Therefore, the signer can reuse the offline pre-stored information in a polynomial time. This makes our IBOOST superior to the existing online/offline signature techniques that allow only a single signature. Additionally, the new technique enables the pre-registration process with a secret key, and no secret key is required in the offline stage. Also, the proposed IBOOST proves to be secure in the random oracle unforgeability under the chosen message attack (UF-IBS-CMA). Finally, the IBOOST and its enhanced version (A-IBOOST) give the lowest computational costs compared to several contending techniques. Therefore, the proposed IBOOST shows superior security and performance with better computational overhead than the preliminary techniques.

INDEX TERMS 5G wireless sensor network systems, fractional chaotic maps, identity-based signature scheme, provably secure.

I. INTRODUCTION

The fifth-generation (5G) wireless networks that are rapidly deployed worldwide have ushered in great relief to the proliferating issues inherent in the ubiquitous 4G wireless networks [1]. 5G wireless networks support the application of blockchain technology [2], holographic communication [3], Industrial Internet of Things (IIoT) [4], wireless security networks [5], and more. Wireless sensor nodes are spatially

The associate editor coordinating the review of this manuscript and approving it for publication was Luyu Zhao.

Name of Faculty: Dr. Chandrashekhar Meshram

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 8, 2021, accepted July 19, 2021, date of publication July 28, 2021, date of current version August 10, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3101111

An Efficient Provably Secure Verifier-Based Three-Factor Authentication Technique Using PDL for Data Exchange in TMIS

VISHESH P. GAIKWAD[1], JITENDRA V. TEMBHURNE[1], CHANDRASHEKHAR MESHRAM[2], CHENG-CHI LEE[3,4], (Member, IEEE), AND CHUN-TA LI[5], (Member, IEEE)

[1]Department of Computer Science and Engineering, Indian Institute of Information Technology at Nagpur, Nagpur 440006, India
[2]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh 460001, India
[3]Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei City 24205, Taiwan
[4]Department of Computer Science and Information Engineering, Asia University, Wufeng Shiang, Taichung 41354, Taiwan
[5]Department of Information Management, Tainan University of Technology, Tainan 710302, Taiwan

Corresponding authors: Cheng-Chi Lee (cclee@mail.fju.edu.tw), Chandrashekhar Meshram (cs_meshram@rediffmail.com), and Chun-Ta Li (th0040@mail.tut.edu.tw)

This work was supported in part by Visvesvaraya Ph.D. Scheme through the Ministry of Electronics and Information Technology (MeitY) by the Government of India under Grant MEITY-PHD-3039, and in part by the Ministry of Science and Technology, Taiwan, under Contract MOST 109-2410-H-165-001 and Contract MOST 110-2410-H-165-001-MY2.

ABSTRACT In healthcare services, telecare medicine information systems (TMIS) is the viable solution offered currently. Moreover, to provide best security to the TMIS, it attracted the various researchers to investigate the security challenges in TMIS. Subsequently, the security of TMIS is improving but the application becoming widespread hence needs robust security technique. An efficient verifier-based 3-party authentication technique in telecare medicine information systems for data exchange, which permits only two users/patients to store their verifier in the database of an authentication server, computed using own password. The authentication system will then validate the user's verifier and help them safely and easily share electronic medical records. In this work, we present an efficient provably secure verifier-based 3-party authentication technique using partial discrete logarithm (PDL) for exchanging data in TMIS. The presented technique not utilizing any public keys of the server, and does not require additional messages and number for key confirmation rounds. The proposed technique has higher security compared to the related verifier-based methods, has lower computational costs and fewer communications, and is therefore ideal for TMIS.

INDEX TERMS TMIS, partial discrete logarithm, data exchange, authentication, entropy smoothing hash function.

I. INTRODUCTION

With the rapid advancement of the internet and information technology, facilitates the development of telecare medicine information systems (TMIS). TMISs are generally utilized to provide healthcare delivery of Medical services. TMIS offers the storage and maintenance of medical information which is highly sensitive and belongs to the registered users; specifically it stores electronic medical records (EMR) conveniently and efficiently. These sensitive information are accessed and shared through public communication channel by the medical institutes, hospitals, academia, and doctors to enhance decision capability. It supports telecare medicine services directly delivered to the patients at home via public networks. Further, gradual development of e-healthcare systems also provides medical services directly at a doorstep of patient which is an economical alternative for patients and healthcare service suppliers with decrease travel expenses. TMIS require a powerful secured and efficient authentication mechanism for protecting patient's private information such as EMR, healthcare information, etc.

Subsequently, many authentication schemes or methods were developed in the recent times for TMIS. Mostly, it used for data exchange in TMIS that enables two users can share a

The associate editor coordinating the review of this manuscript and approving it for publication was Yanjiao Chen.

Name of Faculty: Dr. Chandrashekhar Meshram

An Efficient, Robust, and Lightweight Subtree-Based Three-Factor Authentication Procedure for Large-Scale DWSN in Random Oracle

Chandrashekhar Meshram, Mohammad S. Obaidat, *Fellow, IEEE*, Cheng-Chi Lee, and Sarita Gajbhiye Meshram

***Abstract*—Wireless sensor networks (WSNs) are the backbones of numerous real-time monitoring systems that are applied to serve many different parts of our everyday lives including traffic management, telecare, pollution control, military application, among others. In most cases, WSN systems involve exchanges of sensitive/private data between the sensor nodes and the outside world. In order to preserve data privacy, illegal data access must be denied, and so the remote client has to be properly authorized by both the base station and the sensor node in order to ensure data access legitimacy. Many authentication procedures have been projected by researchers based on various frameworks of parameters such as (two-factor authentication (2-FA) = Smart card + Password) and (three-factor authentication (3-FA) = Biometric + Smart card + Password) in the literature. Das *et al.* (2015) projected a three-factor technique for resource-constrained distributed WSN to address the existing pitfalls. In this article, we present an analysis of Das *et al.*'s technique and point out some inconsistencies in the technique; demonstrating that the system is vulnerable against a known session-specific particular information attack, which thus prompts leakage of the client identity. We offer a robust subtree-based 3-FA procedure to fix the problem. In addition, we show the security strengths of our devised approach which have been established both informally and formally using the random oracle model and AVISPA tool.**

***Index Terms*—Authentication, biometrics, fuzzy extractor, hash function, random oracle, security attacks, smart cards, subtree, wireless sensor networks.**

Manuscript received April 25, 2020; revised August 20, 2020, November 29, 2020, and December 28, 2020; accepted December 29, 2020. The work of Mohammad S. Obaidat was supported by PR of China Ministry of Education Distinguished Possessor under Grant MS2017BJKJ003. *(Corresponding author: Chandrashekhar Meshram; Cheng-Chi Lee.)*

Chandrashekhar Meshram is with the Department of Postgraduate Studies and Research in Mathematics, Jaywanti Haksar Government Postgraduation College, College of Chhindwara University, Betul 480001, India (e-mail: csmeshram84pdf@gmail.com).

Mohammad S. Obaidat is with the Founding Dean and Professor of College of Computing and Informatics, University of Sharjah, Sharjah 27272, UAE with the King Abdullah II School of Information Technology Department, The University of Jordan, Amman 11942, Jordan, and also with the University of Science and Technology Bejing, Beijing 100083, China (e-mail: msobaidat@gmail.comm.s.obaidat@ieee.org).

Cheng-Chi Lee is with the Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei 24205, R.O.C., and also with the Department of Photonics and Communication Engineering Asia University, Wufeng Shiang, Taiwan 413, R.O.C. (e-mail: cclee@mail.fju.edu.tw).

Sarita Gajbhiye Meshram is with the Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam, and also with the Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam (e-mail: saritagmeshram@tdtu.edu.vn).

Digital Object Identifier 10.1109/JSYST.2021.3049163

I. Introduction

THE distributed wireless sensor network (DWSN) is a dynamic infrastructure that consists of lightweight, resource constrained, battery-backup sensor nodes, or motes where communication is performed wirelessly in a smaller scope [1]. In DWSN, sensor nodes are normally randomly located everywhere throughout the objective field to form a multihop wireless communication environment among clients, the base station (BS)/sink node, and sensors. In such a network, as shown in Fig. 1, the BS has unlimited storage capacity and computational resources, and it communicates with the external world over a wireless ad hoc network. The BS monitors and controls the whole network and therefore has the authority to read data from sensors. It is assumed to be trustworthy and not subject to compromise by an attacker.

For the BS to do the job, the most convenient design would be one where the BS serves as a gateway to the WSN with all the client queries routed through it, so that it would be the easiest for the BS to monitor and control the whole system. However, when an emergency case occurs in a system for healthcare monitoring such as forest fire detection or natural disaster prevention, the clients would typically want to have direct access to local sensors rather than getting routed through the BS. To offer a design where direct communication is allowed between clients/users and sensor nodes, there are security issues to take care of regarding the authorization of clients before they connect to the network so as to maintain data privacy, especially in a wireless environment where security threats and possible attackers can be anywhere. To us, the greatest challenge is to design a DWSN system that offers optimum security protection with the least overhead.

In the literature, many remote client authentication procedures have been proposed that use various factors such as two factor authentication (2-FA) [2]–[4], elliptic curve cryptography (ECC) [5], [6], and bilinear pairing [7], [8]. However, some latest research proved that for WSN, biometric-based client authentication is more dependable and secure than conventional password-based client authentication procedures [9]–[14]. Inherent advantages of biometric-based methods include the following statements.

1) Biometric values or keys cannot be forgotten or lost; 2) Biometric values or keys are very difficult to share or copy;

IEEE SYSTEMS JOURNAL 1

A Lightweight Provably Secure Digital Short-Signature Technique Using Extended Chaotic Maps for Human-Centered IoT Systems

Chandrashekhar Meshram, Mohammad S. Obaidat, *Fellow, IEEE*, Jitendra V. Tembhurne, Shailendra W. Shende, Kailash W. Kalare, and Sarita Gajbhiye Meshram

***Abstract*—Internet of Things (IoT) consists of numerous smart devices for sharing sensed data through the availability of online services. Direct communication by smart devices with people to identify parameters of healthcare and send them to a central repository is crucial. There is a need to secure messages among the sender and recipient during data exchange in order to tackle the malicious attacks by human. To provide secure communication, various signature-based schemes are presented in the literature. However, smart devices require lightweight tasks by guaranteeing essential security strengths. The main difficulty in signature-based methods is more computational cost incurred for signature and verification stages involving large numbers. This article introduces a lightweight provably secure short digital signature technique for safe communication amongst smart devices in human-centered IoT (HCIoT), the security of which is closely related to an extended chaotic maps assumption in a random oracle model (ROM). Moreover, we used less comprehensive operations to accomplish processes of verification and signing, similar to human signing on legitimate documents and then check as per witness. The proposed technique provides a stronger guarantee of protection than existing signature techniques. The key advantage of the presented technique over the DSA techniques is that it takes less computation in the verification stage and signing length; it retains the degree of protection. The presented short signature takes less bandwidth for communication, storage, and computing resources.**

***Index Terms*—Confidentiality, digital signatures, extended chaotic maps and probability security analysis systems, Internet of Things (IoT) complex systems.**

List of Notations

u	Private key.
v	Public key.
$\mathcal{T}$	Chebyshev chaotic maps.
r	Random number per message.
h_1, h_2	One Way Hash Functions.
$\mathcal{M}$	Message.
$\mathcal{B}$	First parameter of signature.
s	Second parameter of signature.
σ	Digital signature.
q	Large prime number of bit length.
p	Large prime factors of $q-1$.

I. Introduction

TODAY is the era of Internet of Things (IoT) wherein different types of devices are connected to the Internet. These devices can be home appliances, agricultural equipment, manufacturing devices, industry tools, energy meter, mining sensors, healthcare monitoring instruments, environment equipment, surveillance systems, smart homes, smart cities, and smart grids among others, which comprise the machine-to-machine (M2M) model. With the advent of IoT-enabled devices, it is very easy to monitor or control various kinds of systems on the finger tips. IoT devices are smart enough to share and exchange data over public Internet to store on cloud. IoT is a powerful tool to apply on varieties of domains and proves the vital role by providing significant advantages. Ashton presented the notion of "*IoT*" and IoT devices came into existence in 2005. Since then tremendous evolution in IoTs has been reported; starting from the invention of basic smart devices to human centered sophisticated devices [1]. Thus, IoT devices received wide acceptance to use in various areas such as smart environment and human-centered design. The different methodologies have been adopted by the researchers to develop and experiment with IoT-enabled systems in a wide range of applications [2]. In addition, the architectures presented to investigate real-world problems are developed using the notion of IoT [3]. This motivates the research in IoTs to explore more possibilities in order to utilize the tremendous power of IoTs.

Manuscript received May 16, 2020; revised September 6, 2020; accepted November 16, 2020. *(Corresponding author: Chandrashekhar Meshram.)*

Chandrashekhar Meshram is with the Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul 480001, India (e-mail: csmeshram84pdf@gmail.com, cs_meshram@rediffmail.com).

Mohammad S. Obaidat is with the College of Computing and Informatics, University of Sharjah, Sharjah 27272, UAE, with KAST, The University of Jordan, Amman 11942, Jordan, and also with the University of Science and Technology Bejing, Bejing 100083, China (e-mail: msobaidat@gmail.com, m.s.obaidat@ieee.org).

Jitendra V. Tembhurne is with the Computer Science and Engineering Department, Indian Institute of Information Technology, Nagpur 440006, India (e-mail: jitendra.tembhurne@cse.iiitn.ac.in).

Shailendra W. Shende is with the Information Technology Department, Yeshwantrao Chavan College of Engineering, Nagpur 441110, India (e-mail: shailendra.shende@gmail.com).

Kailash W. Kalare is with the Computer Science and Engineering Department, PDPM Indian Institute of Information Technology, Design, and Manufacturing, Jabalpur 482005, India (e-mail: kailashkalare.kk2612@gmail.com).

Sarita Gajbhiye Meshram is with the Department for Management of Science and Technology Development, Ton Duc Thang University, HoChi Minh City 758307, Vietnam, and also with the Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City 758307, Vietnam (e-mail: saritagmeshram@tdtu.edu.vn).

Digital Object Identifier 10.1109/JSYST.2020.3043358

Name of Faculty: Dr. Chandrashekhar Meshram

The Journal of Supercomputing (2021) 77:8281–8304
https://doi.org/10.1007/s11227-020-03553-y

Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function

Vishesh P. Gaikwad[1] · Jitendra V. Tembhurne[1] · Chandrashekhar Meshram[2] · Cheng-Chi Lee[3,4]

Accepted: 28 November 2020 / Published online: 19 January 2021

Abstract

Telecare medicine information system (TMIS) is recognized as an important tool for improving the quality and protection of healthcare services. In addition to protecting the privacy of patients, many authentication techniques are being introduced in TMIS. After investigations, it is observed that many authentication techniques have security breaches. In this article, we propose an efficient, secure and lightweight authentication scheme for TMIS using chaotic hash function to achieve user anonymity. Chaotic hash function constitutes potential security a set in modern cryptography with its random behavior. Also, we provide the security proof in the random oracle (RO) model and proof of correctness of algorithm is presented using (Burrows–Abadi–Needham) BAN logic for proposed scheme. The comprehensive formal and informal security review demonstrate that the security of our scheme is resistive against known potential attacks. Additionally, our presented authentication scheme performs significantly better as compared to other existing schemes in the literature and also it is efficient on the basis on high security and low cost for computational and communication.

Keywords Telecare medical information system · Authentication · Smart card · Password-based remote authentication · Chaotic hash function · Subtree · Fuzzy user · Random oracle

1 Introduction

With the advent of various computing resources and storage media, the large amount of data is generated by the different applications over the public communication network. Today, variety of data is available on our finger tips such as social media, stock market, finance, medical and healthcare, etc. All these data are very crucial and vital

✉ Cheng-Chi Lee
cclee@mail.fju.edu.tw

Extended author information available on the last page of the article

Name of Faculty: Dr. Chandrashekhar Meshram

47. Liu W, Liu J, Wu Q, Qin B, Naccache D, Ferradi H (2018) Efficient subtree-based encryption for fuzzy-entity data sharing. Soft Comput 22(23):7961–7976
48. Meshram C, Lee CC, Meshram SG, Meshram A (2020) OOS-SSS: an efficient online/offline subtree-based short signature scheme using Chebyshev chaotic maps for wireless sensor network. IEEE Access 8(1):80063–80073
49. Meshram C, Lee CC, Ranadive AS, Li CT, Meshram SG, Tembhurne JV (2020) A subtree-based transformation model for cryptosystem using chaotic maps under cloud computing environment for fuzzy user data sharing. Int J Commun Syst 33(7):e4307
50. Meshram C, Lee CC, Meshram SG, Khan MK (2019) An identity-based encryption technique using subtree for fuzzy user data sharing under cloud computing environment. Soft Comput 23(24):13127–13138
51. Xiao D, Liao X, Deng S (2005) One-way hash function construction based on the chaotic map with changeable-parameter. Chaos Solitons Fract 241:65–71
52. Das AK, Goswami A (2014) An enhanced biometric authentication scheme for telecare medicine information systems with nonce using chaotic hash function. J Med Syst 38:27
53. Messerges TS, Dabbish EA, Sloan RH (2002) Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput 51(5):541–552
54. Witteman M (2002) Advances in smartcard security. Inf Secur Bull 7:11–22
55. Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36
56. Sarkar P (2010) A simple and generic construction of authenticated encryption with associated data. ACM Trans Inf Syst Secur 13(4):33
57. Chang YF, Yu SH, Shiao DR (2013) An uniqueness-andanonymitypreserving remote user authentication scheme for connected health care. J Med Syst 37:9902
58. Li CT, Lee CC, Weng CY, Fan CI (2013) An extended multi-server-based user authentication and key agreement scheme with user anonymity. KSII Trans Int Inform Syst 7:119–131
59. Li CT (2013) A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card. IET Inform Secur 7:3–10
60. Shin-Yan C, Ying Z, Liu J (2016) Improvement of a privacy authentication scheme based on cloud for medical environment. J Med Syst 40:101
61. Niloofar R, Nazari M (2018) An efficient improvement remote user mutual authentication and session key agreement scheme for E-health care systems. Multimed Tools Appl 77:55–88
62. Arezou O-S, Abbasinezhad-Mood D, Nikooghadam M (2019) An enhanced anonymous and unlinkable user authentication and key agreement protocol for TMIS by utilization of ECC. Int J Commun Syst 32:e3913
63. He D, Kumar N, Lee JH, Sherratt RS (2014) Enhanced three-factor security protocol for consumer USB mass storage devices. IEEE Trans Consum Electron 60(1):30–37

Authors and Affiliations

Vishesh P. Gaikwad[1] · Jitendra V. Tembhurne[1] · Chandrashekhar Meshram[2] · Cheng-Chi Lee[3,4]

Vishesh P. Gaikwad
gaikwad.vishesh@cse.iiitn.ac.in

Jitendra V. Tembhurne
jtembhurne@iiitn.ac.in

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Name of Faculty: Dr. Chandrashekhar Meshram

[1] Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur, India

[2] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, M.P 460001, India

[3] Department of Library and Information Science, Research and Development Center for Physical Education, Health, and Information Technology, Fu Jen Catholic University, New Taipei 24205, Taiwan, ROC

[4] Department of Photonics and Communication Engineering, Asia University, Wufeng Shiang, Taichung 413, Taiwan, ROC

Name of Faculty: Dr. Chandrashekhar Meshram

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received November 15, 2020, accepted December 11, 2020, date of publication December 21, 2020, date of current version January 7, 2021.

Digital Object Identifier 10.1109/ACCESS.2020.3046367

A Provably Secure Lightweight Subtree-Based Short Signature Scheme With Fuzzy User Data Sharing for Human-Centered IoT

CHANDRASHEKHAR MESHRAM[1], AHMED ALSANAD[2], JITENDRA V. TEMBHURNE[3], SHAILENDRA W. SHENDE[4], KAILASH WAMANRAO KALARE[5], SARITA GAJBHIYE MESHRAM[6,7], MUHAMMAD AZEEM AKBAR[8], AND ABDU GUMAEI[2]

[1]Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College of Chhindwara University, Betul 460001, India
[2]STC's Artificial Intelligence Chair, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11451, Saudi Arabia
[3]Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur 440006, India
[4]Department of Information Technology, Yeshwantrao Chavan College of Engineering, Nagpur 441110, India
[5]Department of Computer Science and Engineering, PDPM Indian Institute of Information Technology, Design, and Manufacturing, Jabalpur 482005, India
[6]Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[7]Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City 700000, Vietnam
[8]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 210023, China

Corresponding authors: Chandrashekhar Meshram (cs_meshram@rediffmail.com) and Ahmed Alsanad (aasanad@ksu.edu.sa)

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

ABSTRACT Internet of Things (IoT) is made up of various smart devices for the exchange of sensed data through online services. Direct contact with people through smart devices to define parameters for healthcare and send them to a centralized repository. At the time of data exchange, messages need to be secure between a source (sender) and target (receiver) in order to confront human malicious attacks. Various signature-based schemes are presented in the literature to provide secure communication. Smart apps, however, require lightweight activities by maintaining critical security strengths. The key challenge in signature-based methods is more incurred computational expense for signing and checking process involving large numbers. In this article, a new lightweight provably secure partial discrete logarithm (DL) based subtree-based short signature with fuzzy user data sharing for human-centered IoT systems is introduced and it's security analysis is demonstrated on random oracle (RO) model. The presented scheme provides assurance of better security than other standing short-signature schemes. For low-storage, low-computation environments and low-bandwidth communication, the presented new provably secure and lightweight subtree-based short-signature scheme is needed. The results demonstrate the strength of proposed scheme, as opposed to existing works.

INDEX TERMS Fuzzy user data sharing, IoT, identity-based signature scheme, partial discrete logarithm, probability security analysis, subtree.

I. INTRODUCTION

In the past, we had witnessed so much development in the security aspects related to numerous domains such as e-commerce, healthcare, IoT, industrial IoT, and cloud computing, etc. Variety of cryptographic algorithms are presented in various domains to satisfy the essential security needs by the users or organizations. Initially, public-key cryptography (PKC) was adopted to offer the security wherein public-key is shared amongst all the users. The message exchange is stared after the generation of key pairs (*encryption, signature*), the certificate request is submitted with identity proof to CA (certificate authority), and hence receive certificates signed by CA for authentication to exchange messages in

The associate editor coordinating the review of this manuscript and approving it for publication was Constantinos Marios Angelopoulos.

Name of Faculty: Dr. Chandrashekhar Meshram

Soft Computing
https://doi.org/10.1007/s00500-021-05781-7

METHODOLOGIES AND APPLICATION

An effective mobile-healthcare emerging emergency medical system using conformable chaotic maps

Chandrashekhar Meshram[1] · Rabha W. Ibrahim[2] · Mohammad S. Obaidat[3,4,5] · Balqies Sadoun[6,7] · Sarita Gajbhiye Meshram[8] · Jitendra V. Tembhurne[9]

Accepted: 30 March 2021

Abstract
The developments in telecommunication and online facility resolutions help to connect the digital divide among urban and rural healthcare services administrations, empowering arrangement of appropriate medicinal finding and treatment discussions. Mobile-healthcare (*m*-Healthcare) systems can be used for quality improvement of healthcare and monitoring individuals with chronic diseases like heart disease and diabetes under medical affair. Wireless body area networks are installed in the human body, which transmit the information via Bluetooth or other means to the smartphone. In this study, we introduce a new efficient mobile-healthcare emerging emergency medical system using conformable chaotic maps under cloud computing environment.

Keywords Mobile-healthcare emerging emergency · Smart health homes · Anonymity · Fractional calculus · Conformable chaotic maps · Mutual authentication · Opportunistic computing

1 Introduction

In cloud computing, Internet-based resources such as hardware/software are available for access and sharing. Nowadays, this is used to decrease paper work and manpower in every sector. Cloud computing's general objective is to handle complexity in an efficient manner where simplification is adopted to accelerate the utilization of capacities. Moreover, smartphones and tablet computers are becoming progressively important components of human life. They are most efficient and expedient communication instruments, which do not bound by moment

✉ Chandrashekhar Meshram
cs_meshram@rediffmail.com

Rabha W. Ibrahim
rabhaibrahim@yahoo.com

Mohammad S. Obaidat
msobaidat@gmail.com; m.s.obaidat@ieee.org

Balqies Sadoun
sadounbalqies@gmail.com

Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Jitendra V. Tembhurne
jtembhurne@iiitn.ac.in

[1] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Chhindwara University, Betul, M.P. 460001, India

[2] IEEE: 94086547, Kuala Lumpur 59200, Malaysia

[3] College of Computing and Informatics, University of Sharjah, Sharjah, UAE

[4] King Abdullah II School of Information Technology, The University of Jordan, Amman, Jordan

[5] University of Science and Technology Bejing, Beijing, China

[6] College of Engineering, University of Sharjah, Sharjah, UAE

[7] College of Engineering, Al-Balqa' Applied University, Al-Salt, Jordan

[8] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[9] Department of Computer Science and Engineering, Indian Institute of Information Technology, Nagpur 440006, India

Published online: 26 May 2021

Soft Computing
https://doi.org/10.1007/s00500-021-05834-x

APPLICATION OF SOFT COMPUTING

A comparative study between dynamic and soft computing models for sediment forecasting

Sarita Gajbhiye Meshram[1] · Hamid Reza Pourghasemi[2] · S. I. Abba[3] · Ehsan Alvandi[4] · Chandrashekhar Meshram[5] · Khaled Mohamed Khedher[6,7]

Accepted: 20 April 2021

Abstract
Runoff–sediment process modeling is highly variable and nonlinear in nature. For sediment yield prediction, the difficulty of rainfall–runoff–sediment yield hydrological processes remains challenging. The present study uses a simple nonlinear dynamic (NLD) model to predict daily sediment yields, taking into account the degree of daily–sediment yield in catchment areas, and its findings were compared to three widely used models including artificial neural networks (ANN), support vector machine (SVM), and gene expression programming (GEP). The daily measured discharge–sediment data for 25 years were obtained from Shakkar Watershed; Central India as in the current study. The coefficient of correlation (CC), Nash-Sutcliff (NS), and root-mean-square error (RMSE) were employed to assess the performance of the models. The results show that the NLD model was found better than ANN, SVM, and GEP model. These models had correlation coefficient (CC = 0.975, 0.887, 0.843, and 0.901), root-mean-square error (RMSE = 0.748, 1.751, 1.961, and 1.545), and Nash–Sutcliffe efficiency (0.952, 0.784, 0.673, and 0.814) correspondingly. Hence, the NLD model can be used for predicting sediment. In order to implement appropriate measures of soil conservation in the watershed to reduce the sediment load in the river, predicting the sediment yield is very necessary to maximize the life of the structure.

Keywords Sediment yield · Runoff · Dynamic model · ANN · SVM · Gene expression programming

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Department of Natural Resources and Environmental Engineering, College of Agriculture, Shiraz University, Shiraz, Iran

[3] Faculty of Engineering Department of Civil Engineering, Baze University, Abuja, Nigeria

[4] Department of Watershed Management, Gorgan University of Agricultural Sciences and Natural Resources, Gorgan, Iran

[5] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College of Chhindwara University, Betul, India

[6] Department of Civil Engineering, College of Engineering, King Khalid University, Abha, Saudi Arabia

[7] Department of Civil Engineering, High Institute of Technological Studies, Mrezgua University Campus, 8000 Nabeul, Tunisia

Published online: 22 May 2021

1 Introduction

Research on rainfall and runoff produced sediment-based problems would be very helpful in knowing the broad issue of soil degradation and soil erosion in an agricultural area like India, where there are growing pressures on soil and water resources from the inhabitants (Meshram et al. 2019a,b). The planning, designing, and evaluation of land conservation projects, reservoir design and management, environmental and water-pollution measures, and drought and flood control programs are mostly required in the case of information about a suspended sediment yield (wash load) (Meshram et al. 2018a). Information on suspended catchment sediment yields (wash load) is required on several occasions in order to schedule, plan and review land management systems, park design and operation, environmental and water pollution strategies, as well as drought and water control programs.

Various approaches have been proposed to predict soil loss and sediment transport under current and alternate

Name of Faculty: Dr. Chandrashekhar Meshram

Natural Hazards (2021) 108:2701–2719
https://doi.org/10.1007/s11069-021-04796-5

ORIGINAL PAPER

Soil erosion modeling of watershed using cubic, quadratic and quintic splines

Sarita Gajbhiye Meshram[1] · Vijay P. Singh[2,3] · Ozgur Kisi[4] · Chandrashekhar Meshram[5]

Received: 27 November 2019 / Accepted: 10 May 2021 / Published online: 27 May 2021

Abstract

Soil erosion is widespread with spatio-temporal variability and is central to the determination of sediment yield, which is vital to proper management of watersheds. We propose a relation between the Curve Number (SCS 1956) and the Sediment Yield Index (SYI) using cubic, quadratic and quintic splines in this research. Using Mohgaon watershed (part of Narmada Basin) data, the relation between observed and computed SYI is found to have a coefficient of determination (R^2) value of 0.87, 0.40 and 0.10 corresponding cubic, quadratic and quintic splines suggesting that such a relation can be used to determine SYI from the available CN value. The cubic spline was found to be the best method with respect to Absolute Prediction Error (*APE*), Integral Square Error (*ISE*), Coefficient of Efficiency (*CE*), Coefficient of Correlation (*CC*) and degree of agreement (*d*) (i.e., APE = 1.35, ISE = 3.09, CE = 62.08, CC = 79.60 and $d = 0.99$). The quintic spline (with an average value of APE = 19.59, ISE = 7.84, CE = − 165.73, CC = 19.30 and $d = 0.26$) and the quadratic spline (with an average value of APE = 20.99, ISE = 8.92, CE = − 199.90, CC = 8.95 and $d = 0.15$) ranked as the 2nd and the 3rd best methods, respectively.

Keywords Sediment yield index · Cubic/quadratic/quintic spline · Mohgaon watershed · Soil erosion

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Department of Biological and Agricultural Engineering, Texas A & M University, College Station, TX 77843-2117, USA

[3] Zachry Department of Civil Engineering, Texas A & M University, College Station, TX 77843-2117, USA

[4] Department of Civil Engineering, School of Technology, Ilia State University, Tbilisi, Georgia

[5] Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Govt. Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India

Environmental Science and Pollution Research
https://doi.org/10.1007/s11356-020-11335-5

RESEARCH ARTICLE

Iterative classifier optimizer-based pace regression and random forest hybrid models for suspended sediment load prediction

Sarita Gajbhiye Meshram[1,2] · Mir Jafar Sadegh Safari[3] · Khabat Khosravi[4] · Chandrashekhar Meshram[5]

Received: 5 July 2020 / Accepted: 20 October 2020

Abstract
Suspended sediment load is a substantial portion of the total sediment load in rivers and plays a vital role in determination of the service life of the downstream dam. To this end, estimation models are needed to compute suspended sediment load in rivers. The application of artificial intelligence (AI) techniques has become popular in water resources engineering for solving complex problems such as sediment transport modeling. In this study, novel integrative intelligence models coupled with iterative classifier optimizer (ICO) are proposed to compute suspended sediment load in Simga station in Seonath river basin, Chhattisgarh State, India. The proposed models are hybridization of the random forest (RF) and pace regression (PR) models with the iterative classifier optimizer (ICO) algorithm to develop ICO-RF and ICO-PR hybrid models. The recommended models are established using the discharge and sediment daily data spanning a 35-year period (1980–2015). The accuracy of the developed models is examined in terms of error; by root mean square error (*RMSE*) and mean absolute error (*MAE*); and based on a correlation index of determination coefficient (R^2). The proposed novel hybrid models of ICO-RF and ICO-PR have been found to be more precise than their stand-alone counterparts of RF and PR. Overall, ICO-RF models delivered better accuracy than their alternatives. The results of this analysis tend to claim the appropriateness of the implemented methodology for precise modeling of the suspended sediment load in rivers.

Keywords Hybrid technique · Iterative classifier optimizer · Pace regression · Random forest · River · Suspended sediment load

Introduction

The hydrological modeling of sediment, river stream and rainfall–overflow connection are significant to offer a design insight for the water resources management projects in practice (Firat and Gungor 2009). Sediment transport modeling is required for issues in the outline of transport of sediment in channels, ponds and bays, stable stations and dams, repositories of dams, protection of fish, effect of watershed administration, and ecological effect valuation (Cigizoglu 2004). In the field of computational hydrology, sediment and water quality modeling is a challenging task (Kisi et al. 2009). Sediment load has been estimated using traditionally method such as experimental relations, numerical reproductions, materially grounded models, remote sensing (RS) and geographic information systems (GIS) practices (Gajbhiye et al. 2015).

Responsible Editor: Marcus Schulz

✉ Sarita Gajbhiye Meshram
saritagmeshram@tdtu.edu.vn

Mir Jafar Sadegh Safari
jafar.safari@yasar.edu.tr

Khabat Khosravi
Khabat.Khosravi@gmail.com

Chandrashekhar Meshram
cs_meshram@rediffmail.com

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[3] Department of Civil Engineering, Yaşar University, Izmir, Turkey

[4] Department of Watershed Management Engineering, Sari Agricultural Science and Natural Resources University, Sari, Iran

[5] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Chhindwara University, Chhindwara, Betul, India

Published online: 30 October 2020

Name of Faculty: Dr. Chandrashekhar Meshram

ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal **10** (2021), no.2, 1131–1139
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.10.2.39

AN EFFICIENT KEY EXCHANGE SCHEME USING SANTILLI'S ISOFIELDS SECOND-KIND FOR SECURE COMMUNICATION

Mamta S. Dani, Akshaykumar Meshram[1], Chandrashekhar Meshram, and N. M. Wazalwar

ABSTRACT. We intend to bring out a unique method for constructing key exchange scheme (KES) using Santilli's isofields second kind for safe transmission. The substantial idea of our offer KES is to utilized isopolynomials with general isonumber coefficient. Suggested KES is an unusual advantage for afore application as Santilli's isofields second kind framework permutable permutation of isocongruence and isoarirthmetic progressions.

1. INTRODUCTION, MOTIVATIONS AND ORGANIZATION

The framework for KES introduced by Diffie–Hellman, permits two users to simultaneously build a mutual private key over an unconfident mechanism [1]. At present, most of KES build on the number theory. The primary concerns on that the public key cryptography is design are discrete logarithm problem (DLP) [2, 3] along with the elliptic curve DLP [4, 5]. The methodically enumerable groups in which DLP structure plays are a fundamental part in cryptosystem [6]. Various implementations of the Diffie-Hellman procedure in matrix rings and diversity of matrices are suggested in [7, 8]. Various cryptographic schemes constructed on DLP and double DLP proposed in [9–12,

[1]*corresponding author*
2020 *Mathematics Subject Classification.* 16L30, 94A60.
Key words and phrases. Isopolynomials, isoproduct, isofields and diffie-hellman problem.
Submitted: 01.02.2021; *Accepted:* 20.02.2021; *Published:* 27.02.2021.

Name of Faculty: Dr. Chandrashekhar Meshram

EFFICIENT KEY EXCHANGE SCHEME USING S.I. 2ND-KIND FOR SECURE COMMUNICATION 1139

DEPARTMENT OF APPLIED MATHEMATICS,
YESHWANTRAO CHAVAN COLLEGE OF ENGINEERING,
NAGPUR, M.S. 441110, INDIA.
Email address: milinddandale@gmail.com

DEPARTMENT OF APPLIED MATHEMATICS,
YESHWANTRAO CHAVAN COLLEGE OF ENGINEERING,
NAGPUR, M.S. 441110, INDIA.
Email address: akshaykjmeshram@gmail.com

DEPARTMENT OF POST GRADUATE STUDIES AND RESEARCH IN MATHEMATICS,
JAYAWANTI HAKSAR GOVERNMENT POST GRADUATION COLLEGE,
COLLEGE OF CHHINDWARA UNIVERSITY, BETUL, M.P. 460001, INDIA
Email address: cs_meshram@rediffmail.com

DEPARTMENT OF STATISTICS,
RASHTRASANT TUKADOJI MAHARAJ NAGPUR UNIVERSITY,
NAGPUR, M.S., INDIA.
Email address: neha-wazalwar@yahoo.co.in

INTERNATIONAL JOURNAL OF CIRCUITS, SYSTEMS AND SIGNAL PROCESSING
DOI: 10.46300/9106.2021.15.11 Volume 15, 2021

A New Remote Fuzzy User Password Authentication Scheme Using Sub-tree for Cloud Computing

Chandrashekhar Meshram
Department of Post Graduate Studies and Research in Mathematics,
Jaywanti Haksar Govt. Post-Graduation College,
College of Chhindwara University, Betul, M.P.,
India.

Cheng-Chi Lee
Department of Photonics and Communication Engineering,
Asia University, Taichung 41354, Taiwan, R.O.C.

Muhammad Khurram Khan
Center of Excellence in Information Assurance,
King Saud University, Riyadh, Saudi Arabia

Kailash Kalare
PDPM Indian Institute of Information Technology,
Design, and Manufacturing, Jabalpur, Madhya Pradesh, India

Sarita Gajbhiye Meshram
Faculty of Environment and Labour Safety,
Ton Duc Thang University, Ho Chi Minh City, Vietnam.

Received: December 18, 2020. Revised: January 27, 2021. Accepted: February 10, 2021. Published: February 11, 2021.

Abstract—Recent advancements in internet technology and the infrastructure have attracted more people and organizations to do everything online. Internet technologies have provided amazing and smooth ease for electronic sales and purchases. However, many people have refused to use these internet technologies in electronic purchases because of unstable and insecure forms. New hacking techniques and new types of attacks have been tackled to make these internet technologies better and safer. Smartcard-based password authentication schemes have been the mainstream in recent years, featuring their highly lightweight, easy-to-use equipment and low-cost apps. Various secure and faster authentication schemes have been proposed in the literature. However, most of the existing authentication schemes have found vulnerable to recent attacks and have security flaws. This paper provides and efficient way for authentication using the partial discrete logarithm and sub-tree structure. The proposed scheme has seen effective and more useful in cloud computing environment. The analysis based on the security and the computational cost shows that the proposed authentication scheme proves to be more secure and efficient compared to other protocols that serve the same purposes.

Keywords— Mutual authentication; session key; smartcard; sub-tree; partial discrete logarithm, cloud computing.

I. Introduction

SMARTCARD-based remote user authentication schemes allow a server to authenticate a remote user over public, insecure networks. The systems for authentication typically follow some of the two methods below to identify a user:

- Using something only known to the user, such as a password.
- Using something only the user has legal access to, such as a smart card.

The technology that uses both methods is sometimes referred to as two factor authentications. A smartcard-based password authentication system includes an authentication server AS and a user U. Usually there is three basic phases to the system: registration, login and authentication. However, sometimes an extra phase may also be included for user password change using

Name of Faculty: Dr. Chandrashekhar Meshram

Water Resources Management (2021) 35:3105–3120
https://doi.org/10.1007/s11269-021-02856-w

Identification of Critical Watershed for Soil Conservation Using Game Theory-Based Approaches

Sarita Gajbhiye Meshram[1] · Maryam Adhami[2] · Ozgur Kisi[3] · Chandrashekhar Meshram[4] · Pham Anh Duc[5] · Khaled Mohamed Khedher[6,7]

Received: 4 January 2021 / Accepted: 16 May 2021/ Published online: 20 July 2021

Abstract
Soil erosion causes significant damage to humans by reducing soil productivity and filling reservoirs from sediment deposition in Narmada Basin, India; hence, it is important to recognize soil erosion prone areas for preventive steps in this basin. In this research, prioritization of sub-watersheds of Narmada Basin has been done using game theory-based approaches such as Condorcet and Fallback bargaining. For this purpose, Digital Elevation Model (DEM) generated by Shuttle Radar Topography Mission (SRTM) was used to extract and analyze 12 morphometric parameters including linear, aerial, and relief parameters. Based on the Condorcet and Fallback bargaining methods, the Mohgaon watershed came at the first priority ranking, that means it's the most vulnerable watershed from the point of soil erosion (SE). Game theory was successfully implemented for prioritizing watersheds in term of SE. The findings showed that morphometric parameters and game theory approach have a high efficiency in recognizing areas that are vulnerable to erosion.

Keywords Game theory · Prioritization technique · Soil conservation · Watershed management

1 Introduction

Soil erosion is one of the major land loss problems in agricultural land and is regarded as a serious environmental hazard (Lu et al. 2003; Kim et al. 2005; Srinivasan et al. 2019). Water erosion risk is an environmental, economic and social issue that affects all countries (Meena et al. 2017). India's regions are not resistant to this type of natural hazards, whose soil loss is estimated at 147 M ha (Bhattacharyya et al. 2015).The average annual soil erosion for Narmada basin watershed (Shakkar River watershed) was estimated to be 10.04 t/ha/ year (Patil et al. 2015). Therefore, the problem needs to be addressed prudently and a systematic solution to reduce the extent of the problem needs to be pursued. To exploit land and water

✉ Sarita Gajbhiye Meshram
gajbhiyesarita@gmail.com

Extended author information available on the last page of the article

Name of Faculty: Dr. Chandrashekhar Meshram

Mulliner E, Malys N, Maliene V (2016) Comparative analysis of MCDM methods for the assessment of sustainable housing affordability. Omega 59:146–156
Patil RJ, Sharma SK, Tignath S (2015) Remote sensing and GIS based soil erosion assessment from an agricultural watershed. Arab J Geosci 8:6967–6984. https://doi.org/10.1007/s12517-014-1718-y
Raju KS, Kumar DN, Jalali A (2017) Prioritization of sub-catchments of a river basin using DEM and fuzzy VIKOR. H2 Open J 1:1–11. https://doi.org/10.2166/h2oj.2017.001
Salehi A, Izadikhah M (2014) A novel method to extend SAW for decision-making problems with interval data. Decision Sci Lett 3:225–236
Sheikhmohammady M, Kilgour DM, Hipel KW (2010) Modeling the Caspian Sea negotiations. Group Decis Negot 19(2):149–168
Shi GM, Wang JN, Zhang B, Zhang Z, Zhang YL (2016) Pollution control costs of a transboundary river basin: empirical tests of the fairness and stability of cost allocation mechanisms using game theory. J Environ Manag 177:145–152. https://doi.org/10.1016/j.jenvman.2016.04.015
Shih HS, Shyur HJ, Lee ES (2007) An extension of TOPSIS for group decision making. Math Comput Model 45:801–813. https://doi.org/10.1016/j.mcm.2006.03.023
Shojaie AB, Babaie S, Sayah E, Mohammaditabar D (2017) Analysis and prioritization of green health suppliers using fuzzy ELECTRE method with a case study. Glob J Flex Syst Manag 19:39–52. https://doi.org/10.1007/s40171-017-0168-2
Srinivasan R, Singh SK, Nayak DC, Hegde R, Ramesh M (2019) Estimation of soil loss by USLE model using remote sensing and GIS techniques - a case study of coastal Odisha, India. Eurasian J Soil Sci 8(4):321–328
Strahler AN (1957) Quantitative analysis of watershed geomorphology. Trans Am Geophys Union 38:913–920. https://doi.org/10.1029/TR038i006p00913
Su BB, Chang H, Chen YZ, He DR (2007) A game theory model of urban public traffic networks. Phys Stat Mech Appl 379(1):291–297. https://doi.org/10.1029/TR038i006p00913
Sun LJ, Gao ZY (2007) An equilibrium model for urban transit assignment based on game theory. Eur J Oper Res 181(1):305–314. https://doi.org/10.1016/j.ejor.2006.05.028
Teasley RL, McKinney DC (2011) Calculating the benefits of trans boundary river basin cooperation: the Syr Darya Basin. J Water Resour Plan Manag 137(6):481–490. https://doi.org/10.1061/(ASCE)WR.1943-5452.0000141
Thakker AK, Dhiman SD (2007) Morphometric analysis and prioritization of miniwatersheds in Mohr watershed, Gujarat using remote sensing and GIS techniques. J Indian Soc Remote Sens 35(4):313–321
Üçler N, Engin GO, Köçken HG, Öncel MS (2015) Game theory and fuzzy programming approaches for bi-objective optimization of reservoir watershed management: a case study in Namazgah reservoir. Environ Sci Pollut Res 22(9):6546–6558. https://doi.org/10.1007/s11356-015-4181-8
UNEP (1997) World atlas of desertification. 2nd edition Arnold London. 77
Wang LZ, Fang L, Hipel KW (2003) Water resources allocation: a cooperative game theoretic approach. J Environ Informatics 2(2):11–22
Yalcin A (2008) GIS-based landslide susceptibility mapping using analytical hierarchy process and bivariate statistics in Ardesen (Turkey): comparison of results and confirmations. Catena 72:1–12. https://doi.org/10.1016/j.catena.2007.01.003
Yu X, Zhang S, Liao X, Qi X (2017) ELECTRE methods in prioritized MCDM environment. Inf Sci 424:301–316
Zavadskas EK, Peldschus F, Ustinovičius L, Turskis Z (2004) Game theory in building technology and management. Technika, Vilnius 195 p. ISBN 9986-05-700-0 (in Lithuanian)

Affiliations

Sarita Gajbhiye Meshram[1] · Maryam Adhami[2] · Ozgur Kisi[3] · Chandrashekhar Meshram[4] · Pham Anh Duc[5] · Khaled Mohamed Khedher[6,7]

Maryam Adhami
m.adhami66@yahoo.com

Ozgur Kisi
ozgur.kisi@iliauni.edu.ge

Name of Faculty: Dr. Chandrashekhar Meshram

Chandrashekhar Meshram
cs_meshram@rediffmail.com

Pham Anh Duc
phamanhduc@tdtu.edu.vn

Khaled Mohamed Khedher
kkhedher@kku.edu.sa

1 Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

2 Department of Watershed Management Engineering, Faculty of Natural Resources, Tarbiat Modares University, International Campus, Noor, Mazandaran 46417-76489, Iran

3 Department of Civil Engineering, School of Technology, Ilia State University, Tbilisi, Georgia

4 Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Govt. Post Graduation College, College of Chhindwara University, Betul, MP, India

5 Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam

6 Department of Civil Engineering, College of Engineering, King Khalid University, Abha 61421, Saudi Arabia

7 Department of Civil Engineering, High Institute of Technological Studies, Mrezgua University Campus, 8000 Nabeul, Tunisia

Name of Faculty: Dr. Manoj Ughade

South East Asian J. of Mathematics and Mathematical Sciences
Vol. 17, No. 1 (2021), pp. 383-396

ISSN (Online): 2582-0850
ISSN (Print): 0972-7752

COINCIDENCE POINTS AND COMMON FIXED POINTS OF EXPANSIVE MAPPINGS IN A_b-METRIC SPACES

Anil Bakhru, Richa Gupta* and Manoj Ughade**

Department of Mathematics,
S.V. Polytechnic College, Bhopal - 462002, Madhya Pradesh, INDIA

E-mail : anilbakhru@gmail.com

*Department of Mathematics,
Sarvepalli Radhakrishnan University,
Bhopal - 462047, Madhya Pradesh, INDIA

**Department of Mathematics,
Government J. H. Post Graduate College,
Betul - 460001, Madhya Pradesh, INDIA

(**Received:** *Jun. 29, 2020* **Accepted:** *Jan. 06, 2021* **Published:** *Apr. 30, 2021*)

Abstract: In this study, we prove some fixed point theorems for expansive mappings on A_b-metric spaces. Finally, the example is presented to support the new theorem proved. Our results extend/generalize many pre-existing results in literature.

Keywords and Phrases: A_b-metric space, expansive mapping, fixed point.

2020 Mathematics Subject Classification: 47H09, 47H10.

1. Introduction

Fixed point theory has great importance in science and mathematics. Since this area has been developed very fast over the past two decades due to huge applications in various fields such as nonlinear analysis, topology and engineering problems, it has attracted considerable attention from researchers. The study of expansive mappings is a very interesting research area in the fixed point theory. Wang et al. [37] proved some fixed point theorems for expansion mappings, which

Available online at http://scik.org
J. Math. Comput. Sci. 11 (2021), No. 4, 4631-4639
https://doi.org/10.28919/jmcs/5844
ISSN: 1927-5307

RATIONAL TYPE CONTRACTION IN CONTROLLED METRIC SPACES

BABITA PANDEY[1,*], AMIT KUMAR PANDEY[1], MANOJ UGHADE[2]
[1]Department of Engineering Mathematics and Research Center, Sarvepalli Radhakrishanan University, Bhopal 462026, India
[2]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, College of Chhindawara University Betul, 460001, India

Abstract: The aim of this paper is to establish a fixed point theorem for rational type contraction in a complete controlled metric space. Our results extend/generalize many pre-existing results in literature. We also provide example which show the usefulness of these results.

Keywords: fixed point theory; rational type contraction; controlled metric space.
2010 AMS Subject Classification: 47H10, 54H25.

1. INTRODUCTION AND PRELIMINARIES

Dass and Gupta [26] established first fixed point theorem for rational contractive type conditions in metric space.

Theorem 1.1 (see [26]). Let (X,d) be a complete metric space, and let $\mathcal{T}: X \to X$ be a self-mapping. If there exist $\alpha, \beta \in [0,1)$ with $\alpha + \beta < 1$ such that

$$d(\mathcal{T}x, \mathcal{T}y) \leq \alpha d(x,y) + \beta \frac{[1 + d(x,\mathcal{T}x)]d(y,\mathcal{T}y)}{1 + d(x,y)} \qquad (1.1)$$

for all $x, y \in X$, then $\mathcal{T}$ has a unique fixed point $x^* \in X$.

*Corresponding author
E-mail address: babita.pandey829@gmail.com
Received April 11, 2021

Name of Faculty: Dr. Manoj Ughade

Zeichen Journal ISSN No: 0932-4747

Study of all Subgroups of the Symmetric Group S_6

Ram Milan Singh[1], **Manoj Ughade**[2]
[1]Govt. P. G. College, Tikamgarh
[2]Jaywanti Haskar Government Post Graduate College, Betul

Abstract: In this paper, we aimed at determining all subgroups of the Symmetric group S_6 up to Automorphism class using Sylows theorem and Lagranges theorem. This is achieved by finding all subgroups of order m for which $\frac{m}{O(S_6)}$ and are subsets of S_6. Further, the Symmetric group S6 is centerless and every automorphism of it is inner. Also, every natural homomorphism to the automorphism group is an isomorphism.

Keywords: Symmetric group, Conjugacy class, Isomorphism, Automorphism, Complete group

1.Introduction

In mathematics, the notion of permutation is used with several slightly different meanings, all related to the act of permuting (rearranging in an ordered fashion) objects or values. Informally, a permutation of a set of values is an arrangement of those values into a particular order. Thus there are six permutations of the set 1,2,3, namely, (1,2,3), (1,3,2), (2,1,3), (2,3,1), (3,1,2), and (3,2,1). In algebra and particularly in group theory, a permutation of a set S is defined as a bijection from S to itself . To such a map f is associated with the rearrangement of S in which each element s takes the place of its image f(s). Given any non empty set S, define A(S) to be the set of all bijections mapping of the set S onto itself. The set A(S) is a group with respect to composition of function. If the set S is finite with n elements, then the group A(S) is denoted by Sn. The order of Sn is n! And will be called Symmetric group. Any subset of S_n which is itself a group is called a subgroup of Sn. There are many references on subgroups of S_2, S_3, S_4 and S_5 ([2], [7], [8] and [10]). Our aim in this paper is to critically examine all subgroups of S6 up to automorphism class and their conjugacy class size. The set of all symmetry operations on all objects in the set S, can be modeled as a group action g : G × S → S, where the image of g in G and x in S is written as gx. If, for some g, gx = y then x and y are said to be symmetrical to each other. For each object x, operations g for which gx = x is the symmetry group of the object, a subgroup of G. If the symmetry group of x is the trivial group then x is said to be asymmetric, otherwise symmetric.

1

Zeichen Journal ISSN No: 0932-4747

COINCIDENCE AND COMMON FIXED POINT THEOREMS FOR EXPANSIVE MAPPINGS IN *A*-METRIC SPACES

SACHIN DEV KUSHWAHA[1], PANNALAL SANODIA[2], MANOJ UGHADE[3], RAM MILAN SINGH[4]

[1]Department of Mathematics, IES College of Technology, College of University of Technology of Madhya Pradesh, Bhopal, Madhya Pradesh 462010, India

[2]Department of Mathematics and Research Center, Institute for Excellence in Higher Education, Bhopal, Madhya Pradesh 462026, India

[3]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, College of Chhindawara University, Betul, 460001 India

[4]Department of Mathematics, Government Post Graduate College, College of Maharaja Chhatrasal Bundelkhand University, Tikamgarh, 472000, India

Correspondence should be addressed to Sachin Dev Kushwaha; kushwahsachindev15@gmail.com

ABSTRACT

In this article, we established some fixed point results for expansive mappings on *A*-metric spaces. Finally, the example is presented to support the new theorem proved. Our results extend/generalize many pre-existing results in literature.

KEYWORDS: *A*-metric space; expansive mapping; fixed point.

MSC: Primary 47H10; secondary 54H25

1. Introduction

Fixed point theory has great importance in science and mathematics. Since this area has been developed very fast over the past two decades due to huge applications in various fields such as nonlinear analysis, topology and engineering problems, it has attracted considerable attention from researchers. The study of expansive mappings is a very interesting research area in the fixed point theory. Wang et al. [36] proved some fixed point theorems for expansion mappings, which correspond to some contractive mappings in metric spaces. In 1992, Daffer and Kaneko [8] defined an expanding condition for a pair of mappings and proved some common fixed point theorems for

Journal of Xidian University https://doi.org/10.37896/jxu15.12/073 ISSN No:1001-2400

Fixed Point Results for Rational Type Contraction in *S*-Metric Spaces

JYOTI VARMA[1], MANOJ UGHADE[2], AMIT KUMAR PANDEY[3]

[1]Department of Mathematics, Government College Shahpur,College of Chhindawara University,Shahpur 460440, India
[2]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government PostGraduate College, College of Chhindawara University, Betul, 460001 India
[3]Department of Engineering Mathematics and Research Center, Sarvepalli Radhakrishanan University, Bhopal 462026, India
Correspondence should be addressed to Jyoti Varma:

ABSTRACT

The goal of this paper is to define rational contraction in the context of *S*-metric spaces and develop various fixed-point theorems in order to elaborate, generalize, and synthesize a number of previously published results. Finally, to illustrate the new theorem, an example is given.

KEYWORDS:*S*-metric space; rational contraction; fixed point.

MSC: Primary 47H10; Secondary 54H25

1. Introduction

Fixed point theory is crucial in science and mathematics. This topic has drawn a lot of interest from academics in the last two decades due to its wide range of applications in disciplines such as nonlinear analysis, topology, and engineering difficulties. The Banach contraction principle [2] is the starting point for most generalizations of metric fixed point theorems. It's difficult to enumerate all of this principle's generalizations. The Banach fixed-point theorem [2] ensures the existence and uniqueness of fixed points of particular self-maps of metric spaces, as well as a constructive approach for discovering them. The S-metric space was introduced by Sedghi et al. [9]. It's a three-dimensional space called the S-metric space. The concept of A-metric space was established by Abbas et al. [1], which is a generalization of S-metric space. Jaggi [7], Das and Gupta [3] discovered the fixed-point theorem for rational contractive type conditions in metric space. The goal of this paper is to define rational contraction in the setting of S-metric spaces, as well as to create various fixed-point theorems to elaborate, generalize, and synthesize several previously published results. Finally, an example is given to demonstrate the new theorem.

International Journal of Engineering Trends and Technology
ISSN: 2231 – 5381 /doi:10.14445/22315381/IJETT-V69I7P211
Volume 69 Issue 7, 76-79, July, 2021

SIFK based Isobeta Cryptosystem

Ajay B. Thatere[1], AkshaykumarMeshram[*2], Chandrashekhar Meshram[3] and N. M. Wazalwar[4]

[1]*Department of Electronics Engineering, YeshwantraoChavan College of Engineering, Nagpur-441110, M.S., India.*

[2]*Department of Applied Mathematics, YeshwantraoChavan College of Engineering, Nagpur-441110, M.S., India.*

[3]*Department of Post Graduate Studies and Research in Mathematics, JayawantiHaksar Government Post-Graduation College, College of Chhindwara University, Betul, M.P, 460001, India.*

[4]*Department of Statistics, RashtrasantTukadojiMaharaj Nagpur University, Nagpur-440033, M.S., India.*

[1]ajay.thatere@yahoo.co.in,[*2]akshaykjmeshram@gmail.com, [3]cs_meshram@rediffmail.com

Abstract *— The current effort takes the unique technique to construct is beta cryptosystem, whose security is established on santilli'sisofields first-kind (𝑆𝐼𝐹𝐾), generalized discrete logarithm problem (𝐺𝐷𝐿𝑃) and integer factorization problem (𝐼𝐹𝑃) in the isomultiplicative isogroup of finite 𝑆𝐼𝐹𝐾. The attacker have to find isoelement from 𝑆𝐼𝐹𝐾 and simplify both distinct 𝐺𝐷𝐿𝑃 and 𝐼𝐹𝑃 together in the isomultiplicativeisogroup of finite 𝑆𝐼𝐹𝐾 in order to get back comparable massage from the secured cipertext and so this technique is probable to achieve a higher level of security.*

Keywords — *Public Key Cryptosystem (**𝑷𝑲𝑪**), **𝑺𝑰𝑭𝑲**, **𝑮𝑫𝑳𝑷** and **𝑰𝑭𝑷**.*

I. INTRODUCTION

The technique of $\mathcal{PKC}$ suggested in article "New Directions in Cryptography" by Diffie-Hellman [1]. After that several $\mathcal{PKC}$ were suggested. Among these $\mathcal{PKC}$ techniques based on hard mathematical problems, which security be dependent on the impracticable of factoring a large integer. Among these $\mathcal{PKC}$ techniques based on hard mathematical problems, which security be dependent on the impracticable of factoring a large integer [2] and the complexity of derive the square root modulo a massive composite integer [3]. ElGamal offered an efficient $\mathcal{PKC}$ based on $\mathcal{DLP}$, which is too hard to simplify as deal with prime field or elliptic curve defined over a finite field [4]. All $\mathcal{PKC}$ based on $\mathcal{DLP}$ and $\mathcal{IFP}$ are not reliable if mathematical structure for $\mathcal{DLP}$ and $\mathcal{IFP}$ are solved. The techniques build on a single mathematical structure have security issues, so researchers proposed $\mathcal{PKC}$ based on multiple hard mathematical structure. Various $\mathcal{PKC}$ have been built on together $\mathcal{DLP}$ and $\mathcal{IFP}$ [5-22]. Some $\mathcal{PKC}$ have been built on dihedral group and suzuki-2 group [23-25]. At the latest, Meshram A. suggested key exchange protocol based on ring isopolynomials with isointeger coefficient [26]. Dani M. offered santilli'sisofields second-kind based key exchange protocol for secure communication[27]and key exchange protocol based on $\mathcal{SIFK}$[28].

Regrettably, we observed that $\mathcal{DLP}$ and $\mathcal{IFP}$ based unified presented $\mathcal{PKC}$ cannot be considered as secure. Hence, we construct a unique beta cryptosystem based on $\mathcal{SIFK}$, $\mathcal{GDLP}$ and $\mathcal{IFP}$ along its assured security, we additionally demonstrated that it is extremely capable to be enforce in the physical world applications.

The rest of this article summarize as below; in section-II, we explained $\mathcal{SIFK}$, offered beta cryptosystem based on $\mathcal{SIFK}$ in section-III, supporting example for confirmation of suggested cryptosystem in section-IV, security investigation and efficiency performance examine in section-V and in final section-VI we conclude the article.

II. $\mathcal{SIFK}$

Santilli [29] offered the generalization of arithmetic operations $\langle +, -, \times, \div \rangle$ termed as isomathematics. $\mathcal{SIFK}$ is the ring $\hat{\mathfrak{F}} = \hat{\mathfrak{F}}(\hat{y}, +, \hat{\times})$ along with isonumbers $\hat{y} = y\hat{I}, y \in \mathfrak{F}, \hat{I} = \frac{1}{\hat{T}} \notin \mathfrak{F}$ along with arithmetic operations $\langle \hat{+}, \hat{-}, \hat{\times}, \hat{\div} \rangle$, $\hat{y} + \hat{x} = (y + x)\hat{I}$an isosum, with additive unit $0 = 0\hat{I} = 0$, $\hat{y} + 0 = 0 + \hat{y} = \hat{y}$ and isoproduct $\hat{y} \hat{\times} \hat{x} = \hat{y}\hat{T}\hat{x} = y\hat{I}\hat{T}x\hat{I} = (yx)\hat{I}$, where, the left and right new unit $\hat{I}$, $\hat{I} \hat{\times} \hat{y} = \hat{y} \hat{\times} \hat{I} = \hat{y}$ is called isounit and $\hat{T}\hat{I} = 1, \hat{T}$ is called inverse of isounit $\hat{I} \neq 1$.

III. ISOBETA CRYPTOSYSTEM BASED ON$\mathcal{SIFK}$

The mechanism for isobeta cryptosystem involves three steps;

Step-A: Key Formation Algorithm

Client-1 runs following algorithm for key formation;

i. Select two large isoprimeisonumbers$\hat{\mathcal{A}}$ and $\hat{\mathcal{B}}$ of the same size.

ii. Numerate the IsoEulerphi function $\varphi(\hat{\mathcal{N}}) = (\hat{\mathcal{A}} - 1)(\hat{\mathcal{B}} - 1)$ for isointeger $\hat{\mathcal{N}} = \hat{\mathcal{A}} * \hat{\mathcal{B}}$.

iii. Pick an arbitrary isointeger $\hat{q}$, $1 \leq \hat{q} \leq \varphi(\hat{\mathcal{N}})$ such that, $\gcd\left(\hat{q}, \varphi(\hat{\mathcal{N}})\right) = 1$.

iv. Pick an arbitrary isointeger $\hat{w}$ such that $2 \leq \hat{w} \leq \varphi(\hat{\mathcal{N}}) - 1$.

Name of Faculty: Dr. Chandrashekhar Meshram

Journal of Interdisciplinary Mathematics
ISSN: 0972-0502 (Print), ISSN: 2169-012X (Online)
Vol. 24 (2021), No. 5, pp. 1163–1173
DOI : 10.1080/09720502.2021.1885811

Taylor & Francis
Taylor & Francis Group

New decomposition of soft supra locally α-closed sets applied to soft supra continuity

Alaa M. Abd El-Latif *
Department of Mathematics
Faculty of Arts and Science
Northern Border University
Rafha
Saudi Arabia

and

Department of Mathematics
Faculty of Education
Ain Shams University
Roxy 11341
Cairo
Egypt

Shaaban M. Shaaban
Department of Engineering Basic Science
Faculty of Engineering
Menofiya University
Menofiya 32511
Egypt

and

Department of Electrical Engineering
Northern Border University
Arar 1321
Saudi Arabia

E-mail: alaa_8560@yahoo.com, alaa.ali@nbu.edu.sa

Name of Faculty: Dr. Chandrashekhar Meshram

Chandrashekhar Meshram
Department of Mathematics and Computer Science
Rani Durgawati University
Jabalpur 482001
Madhya Pradesh
India

and

Department of Post Graduate Studies and Research in Mathematics
Jayawanti Haksar Government Post Graduate College
College of Chhindwara University
Betul 460001
Madhya Pradesh
India

Abstract

In this paper, firstly we introduce the notions of soft supra locally α -closed sets in soft supra topological spaces. We investigate the relationships with different types of subsets of soft supra topological spaces. Secondly, we introduce the notion of SSL- α C-continuous functions and a decomposition of soft supra continuity is obtained.

Subject Classification: *(2010) 54A05, 54A40, 54B05, 06D72.*

Keywords: *Soft supra topological spaces, SSL-α-closed sets, SSL-α C-continuous functions.*

1. Introduction

Since soft set theory [13, 14] has rich potential for practical applications in several domains, it has been studied by many authors [5, 6, 8, 11, 13, 15]. In 2011, Shabir et al. [16] initiated the notions of soft topological spaces (sts's). The notions of soft supra topological spaces (ssts's) were first introduced by El-Sheikh et al. [7] which generalized in [2]. A new concept of supra open soft sets, named soft supra strongly generalized closed sets was initiated by Abd El-latif in [3]. In 2018, Abd El-latif [1] introduced the concepts of soft supra locally closed sets and SSLC-continuous functions in ssts's. The notion of supra soft pre-locally closed sets was introduced in [9] as a generalization to that's in [1].

Our purpose of this paper, is to use the notion of soft supra α -open sets with a different manner of [9] to investigate new notions named,

Name of Faculty: Dr. Manoj Ughade

Malaya Journal of Matematik, Vol. 9, No. 1, 1035-1039, 2021
https://doi.org/10.26637/MJM0901/0181

Common fixed-point theorem for a sequence of fuzzy mappings satisfying a rational contractive condition involving non-expansive mapping

Sachin Dev Kushwaha[1*], Pannalal Sanodia[2], Ram Milan Singh[3] and Manoj Ughade[4]

Abstract
In this article, we establish a common fixed-point theorem for a sequence of fuzzy mappings satisfying a rational contractive condition involving non-expansive mapping.

Keywords
Fuzzy sets, common fixed point, fuzzy mapping, non-expansive mapping.

[1] *Department of Mathematics, IES College of Technology, College of University of Technology of Madhya Pradesh, Bhopal, Madhya Pradesh 462010, India.*
[2] *Department of Mathematics and Research Center, Institute for Excellence in Higher Education, Bhopal, Madhya Pradesh 462026, India.*
[3] *Department of Post Graduate Studies and Research in Mathematics, Government Post Graduate College, College of Maharaja Chhatrasal Bundelkh and University, Tikamgarh, 472000, India*
[4] *Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, College of Chhindawara University, Betul-460001, India.*
***Corresponding author**: [1] kushwahsachindev15@gmail.com
Article History: Received **19** December **2020**; Accepted **24** February **2021**

Contents

1. Introduction

The first important result on fixed points for contractive type mappings was the well-known Banach contraction principle [1] appeared in explicit form in Banach's thesis in 1922, where it was used and established the existence of a solution for an integral equation. Zadeh[2] familiarized the idea of a fuzzy set as a new way to represent vagueness in everyday life. The study of fixed point theorems in fuzzy mathematics was investigated by Weiss [3], Butnariu [4], Singh and Talwar [5], Mihet [6], Qiu et al. [7], and Beg and Abbas [8] and many others. Heilpern [9] first used the concept of fuzzy mappings to prove the Banach contraction principle for fuzzy mappings on a complete metric linear space. The result obtained by Heilpern [9] is a fuzzy analogue of the fixed point theorem for multivalued mappings of Nadler et al. [10]. Bose and Sahani [11], Vijayaraju and Marudai [12], improved the result of Heilpern. In some earlier work, Watson and Rhoades [13],[14] proved several fixed-point theorems involving a very general contractive definition. In this paper, we prove a common fixed point theorem for sequence of fuzzy mappings satisfyinga rational contractive condition involving nonexpansive mapping.Our results extend and generalized the correspondingresults of Bose and Sahani [11], Vijayaraju and Mohanraj [12] and Rhoades [15],[16], Salujaet al. [18] and Das and Gupta [19].

2. Preliminaries

We recall some mathematical basics and definitions to make this paper self-sufficient (see [9]).

Definition 2.1. *Let (M,m) be a complete linear metric space and $\mathcal{F}(M)$, the collection of all fuzzy sets in M. A fuzzy set in Mis a function with domain M and values in $[0,1]$. If Ais a fuzzy set and $\sigma \in M$, then the function value $A(\sigma)$ is called the grade of membership of σ in A. The α -level set of Ais denoted by*

$$A_\alpha = \{\sigma : A(\sigma) \geq \alpha\} \text{ if } \alpha \in (0,1]$$
$$A_0 = \overline{\{\sigma : A(\sigma) > 0\}}$$

where $\bar{B}$ stands for the (non-fuzzy) closure of a set B.

Name of Faculty: Dr. Manoj Ughade

The International journal of analytical and experimental modal analysis ISSN NO:0886-9367

Dass and Gupta Rational Type Contraction in Controlled Metric Spaces

SACHIN DEV KUSHWAHA[1], PANNALAL SANODIA[2], RAM MILAN SINGH[3], MANOJ UGHADE[4]

[1]Department of Mathematics, IES College of Technology, College of University of Technology of Madhya Pradesh, Bhopal, Madhya Pradesh 462010, India
[2]Department of Mathematics and Research Center, Institute for Excellence in Higher Education, Bhopal, Madhya Pradesh 462026, India
[3]Department of Post Graduate Studies and Research in Mathematics, Government Post Graduate College, College of Maharaja Chhatrasal Bundelkhand University, Tikamgarh, 472000, India
[4]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, College of Chhindawara University, Betul, 460001 India

Abstract

The aim of this paper is to establish a fixed point theorem for rational type contraction in a complete controlled metric space. Our results extend/generalize many pre-existing results in literature. We also provide example which show the usefulness of these results.

Keywords: Fixed point theory; Rational type contraction; Controlled metric space.

MSC: 47H10; 54H25

1. Introduction and Preliminaries

Dass and Gupta [26] established first fixed point theorem for rational contractive type conditions in metric space.

Theorem 1.1 (see [26]). Let (X, d) be a complete metric space, and let $\mathcal{T}: X \to X$ be a self-mapping. If there exist $\alpha, \beta \in [0, 1)$ with $\alpha + \beta < 1$ such that

$$d(\mathcal{T}x, \mathcal{T}y) \leq \alpha d(x, y) + \beta \frac{[1 + d(x,\mathcal{T}x)]d(y,\mathcal{T}y)}{1 + d(x,y)} \quad (1.1)$$

for all $x, y \in X$, then $\mathcal{T}$ has a unique fixed point $x^* \in X$.

Nazam *et al.* [27] proved a real generalization of Dass-Gupta fixed point theorem in the frame work of dualistic partial metric spaces.

Czerwik [1] reintroduced a new class of generalized metric spaces, called as b-metric spaces, as generalizations of metric spaces.

Definition 1 ([1]). Let X be a nonempty set and $s \geq 1$. A function $d_b: X \times X \longrightarrow [0, \infty)$ is said to be a b -metric if for all $x, y, \omega \in X$,

(b1). $d_b(x, y) = 0$ iff $x = y$
(b2). $d_b(x, y) = d_b(y, x)$ for all $x, y \in X$
(b3). $d_b(x, \omega) \leq s[d_b(x, y) + d_b(y, \omega)]$

Name of Faculty: Mr. Manoj Kumar Ghorase

Journal of Cardiovascular Disease Research

ISSN:0975-3583,0976-2833 VOL12,ISSUE06,2021

SCREENING OF PHYTOCHEMICAL CONTANTS OF LINUM USITATISSIMUM PLANT EXTRACTED BY DIFFERENT SOLVENT

Manoj Kumar Ghorase*, Parasnath Bele, S.K.Udaipure

*Govt. J.H P.G.College,

Betul, Govt. N.M.V., Hoshangabad

Abstract:

Many plant species that have reportedly been used in the treatment of different diseases. Plant derived compound have played an important role in the development of several clinically useful agents. *Linum usitatissimum* plant seeds are used for many diseases treatment. Aim of the present study is to investigate the phytochemical analysis of Petrolium Ether, Chloroform, Acetone, and Methanol extracts of *Linum usitatissimum plant*. Qualitative analysis of phytochemical screening reveals the presence of Alkaloids, Phenol, Saponins and Protein.

Keywords: Medicinal Plants, Phytochemical analysis, *Linum usitatissimum*is, Antioxidant activity.

Introduction:

Plants chiefly used for form of sickness relating to bacterium treatment. Plants turn out many secondary metabolites together with alkaloids, flavonoids, saponins, steroids, glycosides and terpenoids to safeguard themselves from the attack of present infectious agent, insects' pests and environmental stresses. on top of activity of these compounds ought to depend upon the ways and solvent used for extraction (Verma, S *et al.*, 2021; Shalini and Prema, 2012).

Most probably plants utilized in ancient medication include big selection of bioactive compounds which will be used as different therapeutic tools for the hindrance or treatment of the many contagious diseases. medicative plants ar thought of as clinically effective and safer alternatives to the artificial antibiotic (Govindasamy and Srinivasan, 2012; Kaur and Mondal, 2014)

*Linum usitatissimum*is associate plant growing to one m tall. The seeds are oval, 2.5- 9.5 cm. long and 1-3.5 cm. thin shiny inexperienced depilatory with a black and a brief stalk regarding one- 1.8 cm. long. *Linum usitatissimum*is a very important medicative plant that contains quite seventy completely different sort of alkaloids and therapy agents that ar effective in treating varied sort of cancers-breast cancer, carcinoma, ulterine cancer, melanomas, Hodgkin's and nonhodgkin's cancer (Govindaraji, 2007)12. Generally, it's referred to as Cape periwinkle, *Linum usitatissimum*

Academic Session 2019-2020

Name of Faculty: Dr. Chandrashekhar Meshram

Water Resources Management
https://doi.org/10.1007/s11269-020-02672-8

Check for updates

Application of Artificial Neural Networks, Support Vector Machine and Multiple Model-ANN to Sediment Yield Prediction

Sarita Gajbhiye Meshram[1,2] · Vijay P. Singh[3,4] · Ozgur Kisi[5,6] · Vahid Karimi[7] · Chandrashekhar Meshram[8]

Received: 26 November 2019 / Accepted: 15 September 2020/Published online: 20 October 2020

Abstract
Sediment yield is important for maintaining soil health, reservoir sustainability, environmental pollution, and conservation of natural resources. The main aim of the present work is to develop four machine learning models, artificial neural networks (ANNs), radial basis function (RBF), support vector machine (SVM) and multiple model (MM)-ANNs for forecasting daily sediment yield. These models were applied to the Shakkar and Manot watersheds covering 25 years (1990–2015) and 10 years (2000–2010) of rainfall and discharge data, respectively. Results showed that the MM-ANNs model satisfactorily predicted sediment yield and outperformed the other models providing the highest correlation coefficient (0.921, 0.883) and Nash-Sutcliffe efficiency (0.744, 0.763) and the lowest relative absolute error (0.360, 0.344) and root mean square error (23,609.5, 269,671.5) for the Shakkar and Manot during the test period, respectively. Hence, the MM-ANNs model can be successfully used for sediment prediction.

Keywords Machine learning models · Sediment yield · ANN · RBF · SVM · Multiple model

1 Introduction

Watershed sediment load is an ecological hazard and its estimation is needed for developing measures for environmental protection, sustainability of reservoirs and hydropower generation, avoiding blockage of water supply systems, flood control, and maintaining soil fertility (Lin et al. 2006; Xu et al. 2012; Men et al. 2012).

In many waterways, sediment is transported in suspension and estimation of suspended sediment (SS) is basic for designing channels, dams, and culverts (Targhi et al. 2017). Awareness of potential sediment loads is important for programmes for water resource

✉ Sarita Gajbhiye Meshram
saritagmeshram@tdtu.edu.vn

Extended author information available on the last page of the article

Name of Faculty: Dr. Chandrashekhar Meshram

Targhi AT, Abbaszadeh S, Arabasadi Z (2017) A hybrid method for forecasting river-suspended sediments in Iran. Int J of River Basin Manage Volume 15, Issue 4: Advances and Approaches in River Sediment Research
Tayfur G, Singh VP (2006) ANN and Fuzzy logic models for simulating event-based rainfall-runoff. J Hydraul Eng 132(12):1321–1330. https://doi.org/10.1061/(ASCE)0733-9429(2006)132:12(1321)
Tfwala SS, Wang YM, Lin YC (2013) Prediction of missing flow records using multilayer perceptron and coactive neuro fuzzy inference system. Sci World J 584516:1–7. https://doi.org/10.1155/2013/584516
Vapnik V (1998) Statistical learning theory. Wiley, New York
Vapnik V (1995) The nature of statistical learning theory. Springer, New York
Vapnik V (1999) An overview of statistical learning theory. IEEE Transac on Neur Net 5:988–999
Wang C, Kim D, Ekman MLA, Barth MC, Rasch PJ (2009) Impact of anthropogenic aerosols on Indian summer monsoon. Geophys Res Lett 36:L21704. https://doi.org/10.1029/2009GL040114
Wei S, Song J, Khan NI (2012) Simulating and predicting river discharge time series using a wavelet-neural network hybrid modelling approach. Hydrol Process 26(2):281–296. https://doi.org/10.1002/hyp.8227
Xu J, Zhang W, Zheng Z, Jiao M, Chen J (2012) Early flood warning for Linyi watershed by the GRAPES/XXT model using TIGGE data. Acta Meteorol Sin 26:103–111. https://doi.org/10.1007/s13351-012-0110-7
Yoon H, Jun SC, Hyun Y (2011) A comparative study of artificial neural networks and support vector machines for predicting groundwater levels in a coastal aquifer. J Hydrol 396:128–138. https://doi.org/10.1016/j.jhydrol.2010.11.002

Affiliations

Sarita Gajbhiye Meshram[1,2] · Vijay P. Singh[3,4] · Ozgur Kisi[5,6] · Vahid Karimi[7] · Chandrashekhar Meshram[8]

1 Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam
2 Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam
3 Department of Biological and Agricultural Engineering, Texas A & M University, College Station, TX 77843-2117, USA
4 Zachry Department of Civil Engineering, Texas A & M University, College Station, TX 77843-2117, USA
5 School of Technology, Ilia State University, Tbilisi, Georgia
6 Institute of Research and Development, Duy Tan University, Da Nang 550000, Vietnam
7 Department of Water Engineering, University of Tabriz, Tabriz, Iran
8 Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Chhindwara University, Chhindwara, Betul, M.P, India

Name of Faculty: Dr. Chandrashekhar Meshram

Water Resources Management
https://doi.org/10.1007/s11269-020-02681-7

The Feasibility of Multi-Criteria Decision Making Approach for Prioritization of Sensitive Area at Risk of Water Erosion

Sarita Gajbhiye Meshram[1,2] · Vijay P. Singh[3,4] · Ercan Kahya[5] · Ehsan Alvandi[6] · Chandrashekhar Meshram[7] · Shailesh Kumar Sharma[8]

Received: 1 April 2020 / Accepted: 21 September 2020/Published online: 08 October 2020

Abstract
Morphometric analysis is not only important for a hydrological analysis, but also necessary in the management and development of a basin. In this study, we attempted to prioritize twenty sub-watersheds of Bamhani watershed considering the linear, aerial and relief aspects of the watershed that will be further used in the multi-criterion decision making (MCDM) analysis. ELECTRE, Vlsekriterijumskaoptimizacija I kompromisno resenje (VIKOR), and aggregate method. Remote sensing and GIS approach were employed in the morphometric analysis. Percentage of changes and intensity of change indices were used in the MCDM model validation. Based on the range of Borda/Copland model values, the sub-watershed 11 took place at the first rank, while the Compound Factor (CF) model placed in the second rank, implying to be the most susceptible sub-watersheds for erosion. Vulnerability of sub-watersheds to soil loss (erosion), the VIKOR models showed four vulnerability classifications as very high, high, moderate and low. In conclusion, our results of the morphometric studies appeared to be effective in estimating the erosion status and prioritization of the watershed concerned for the purpose of easy and early development and management of natural resources. A high reductive accuracy was observed by VIKOR in comparison to CF and ELECTRE models.

Keywords Watershed · Prioritization · Morphometric parameters · Soil erosion · Geographic information system · Multi-criteria decision making (MCDM)

1 Introduction

For sustainable development of natural resources to reduce impact of natural calamities, watershed is taken as developmental unit (UNEP 1997). Watershed management planning is

✉ Sarita Gajbhiye Meshram
saritagmeshram@tdtu.edu.vn

Extended author information available on the last page of the article

Name of Faculty: Dr. Chandrashekhar Meshram

Schumm SA (1956) The evolution of drainage systems and slopes in bad lands at Perth, Amboi, New Jersey. Geol Soc Ame Bull 67(5):597–646
Shih HS, Shyur HJ, Lee ES (2007) An extension of TOPSIS for group decision making. Math Comput Model 45:801–813. https://doi.org/10.1016/j.mcm.2006.03.023
Shojaie AB, Babaie S, Sayah E, Mohammaditabar D (2017) Analysis and prioritization of green health suppliers using fuzzy ELECTRE method with a case study. Glob J Flex Syst Manag 19:39–52. https://doi.org/10.1007/s40171-017-0168-2
Strahler AN (1964) Quantitative geomorphology of drainage basins and channel networks. Section 4-II. In: Chow VT (ed) Handbook of applied hydrology. McGraw-Hill, PP, pp 4–39
Thakker AK, Dhiman SD (2007) Morphometric analysis and prioritization of mini-watersheds in Mohr watershed, Gujarat using remote sensing and GIS techniques. J Indian Soc Remote Sens 35(4):313–321. https://doi.org/10.1007/BF02990787
UNEP (1997) World atlas of desertification. 2nd edition Arnold London. 77
Yu X, Zhang S, Liao X, Qi X (2017) ELECTRE methods in prioritized MCDM environment. Inf Sci 424:301–316. https://doi.org/10.1016/j.ins.2017.09.061
Zanakis SH, Solomon A, Wishart N, Dublish S (1998) Multi-attribute decision making: a simulation comparison of select methods. European journal of. Oper Res 107:507–529. https://doi.org/10.1016/S0377-2217(97)00147-1
Zavadskas EK, Turskis Z, Kildienė S (2014) State of art surveys of overviews on MCDM/MADM. Technol Econ Dev Econ 20:165–179. https://doi.org/10.3846/20294913.2014.892037

Affiliations

Sarita Gajbhiye Meshram[1,2] · Vijay P. Singh[3,4] · Ercan Kahya[5] · Ehsan Alvandi[6] · Chandrashekhar Meshram[7] · Shailesh Kumar Sharma[8]

1 Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam
2 Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam
3 Department of Biological and Agricultural Engineering, Texas A&M, University, College Station, TX 77843-2117, USA
4 Zachry Department of Civil Engineering, Texas A&M University, College Station, TX 77843-2117, USA
5 Civil Engineering Department, Istanbul Technical University (ITU), 34469 İstanbul, Türkiye
6 Department of Watershed Management, Gorgan University of Agricultural Sciences and Natural Resources, Gorgan, Iran
7 Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar, Government Post Graduation College, College of Barkatullah Vishwavidyalaya, Betul, M.P., India
8 Department of Soil & Water Engineering, Jawaharlal Nehru Krishi Vishwa Vidyalaya Jabalpur, Jabalpur, India

Name of Faculty: Dr. Chandrashekhar Meshram

Water Resources Management
https://doi.org/10.1007/s11269-019-02470-x

Application of SAW and TOPSIS in Prioritizing Watersheds

Sarita Gajbhiye Meshram[1,2] · Ehsan Alvandi[3] · Chandrashekhar Meshram[4] · Ercan Kahya[5] · Ayad M. Fadhil Al-Quraishi[6]

Received: 27 July 2018 / Accepted: 22 December 2019/Published online: 02 January 2020

Abstract
Prioritization of watersheds for conservation measures is essential for a variety of functions, such as flood control projects in which the determination of top priority areas is an important management decision. The purpose of this study is to examine watershed morphological characteristics and identify critical sub-watersheds, which are prone to be damaged, using Remote Sensing/Geographical Information Systems (GIS) and SAW/ TOPSIS (Simple Additive Weighting/ Technique for Order of Preference by Similarity to Ideal Solution). Fourteen morphometric parameters were chosen to organize sub-watersheds using SAW/TOPSIS, which examines sub-watersheds (as susceptible zones) from the perspective of classification in four priority levels (namely, low, moderate, high and very high levels). The SAW/TOPSIS approach is a useful strategy to find out potential zones provided that the ultimate goal is to achieve successful management strategies, particularly in particular zones where information accessibility is limited and soil assorted variety is high. Without facing with high cost and exercises in futility, sub-watersheds could be organized through morphometric parameters in executing conservational measures to save soil and the earth at the same time. In short, our results showed that morphometric parameters are highly efficient in identifying erosion-prone areas.

Keywords SAW · TOPSIS · RS and GIS · Morphometric parameters · Prioritization

1 Introduction

The total geographical area of India is 328 Mha (million hectares), of which 69 Mha area are critically degraded, and another 106 Mha area are seriously eroded. This endless soil erosion by numerous agents is a serious issue all around the world (Gajbhiye and Sharma 2017). It has been assessed that a total of 16.4 tones/ha of soil has been detached yearly in India due to

✉ Sarita Gajbhiye Meshram
saritagmeshram@tdtu.edu.vn

Extended author information available on the last page of the article

Name of Faculty: Dr. Chandrashekhar Meshram

Tarboton DG (1997) A new method for the determination of flow directions and upslope areas in grid digital elevation models. Water Resour Res 33(2):309–319
Vivien YC, Hui PL, Chui HL, James JHL, Gwo HT, Lung SY (2011) Fuzzy MCDM approach for selecting the best environment-watershed plan. J Appl Soft Comput 11:265–275
Wang M, Hjlmfelt AT (1998) DEM based overland flow routing. J Hydrol Eng 3(1):1–8
Wang YM, Yanga JB, Xu DL (2005) A preference aggregation method through the estimation of utility intervals. Computers & Operations Research, 32:2027–2049

Affiliations

Sarita Gajbhiye Meshram[1,2] · Ehsan Alvandi[3] · Chandrashekhar Meshram[4] · Ercan Kahya[5] · Ayad M. Fadhil Al-Quraishi[6]

1 Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam
2 Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam
3 Department of Watershed and Arid Zone Management, Gorgan University of Agricultural Sciences and Natural Resources, Gorgan, Iran
4 Department of Mathematics, Govt. Jaywanti Haksar P.G. College, Betul, Madhya Pradesh, India
5 Department of Civil Engineering, Istanbul Technical University (ITU), 34469 İstanbul, Türkiye
6 Environmental Engineering Department, College of Engineering, Knowledge University, Erbil, Kurdistan Region 44001, Iraq

Arabian Journal of Geosciences (2020) 13:1248
https://doi.org/10.1007/s12517-020-06162-4

ORIGINAL PAPER

An effective dynamic runoff-sediment yield modeling for Shakkar watershed, Central India

Sarita Gajbhiye Meshram [1,2] · Chandrashekhar Meshram [3]

Received: 1 August 2019 / Accepted: 26 October 2020

Abstract
Modeling of the watershed runoff and sediment yield method is very variable and nonlinear in nature. The Shakkar watershed of the Narmada river basin, Central India, has been taken under the study. The linear dynamic (LD), nonlinear dynamic (NLD), and logarithm dynamic (LogD) sediment yield prediction models based on the concept of determining and assigning the varying weightings to the antecedent events for the runoff-sediment process were developed for the watershed. The data set (1990–2005) model was developed only by using active daily runoff data, together with the antecedent runoff index (AQI) and antecedent sediment yield index (ASYI). Due to the high value of R^2 (over 60%), the linear, nonlinear, and logarithm dynamic model was discovered to be appropriate for the field of research. The Nash-Sutcliff efficiency (NSE), mean absolute error (MAE), and Willmott's index (WI) were employed to assess the performance of the models. The results showed that the NLD model was found better than linear and logarithm models. These models had Nash-Sutcliff efficiency (NSE = 92.69, 64.93, 79.66), mean absolute error (MAE = 5744.20, 12,618.83, 0.02), and Willmott's index (WI = 0.98, 0.88, 0.95) correspondingly. Hence, the NLD model can be used for predicting sediment. In order to take the right conservation steps in the watershed to minimize the sediment load in the reservoir to boost the lives of the structure, the forecast for the sediment yield is of great importance.

Keywords Sediment yield · Runoff · AQI · ASYI · Daily dynamic model

Abbreviations

LD	Linear dynamic
NLD	Nonlinear dynamic
LogD	Logarithm dynamic
AQI	Antecedent runoff index
ASYI	Antecedent sediment yield index
NSE	Nash-Sutcliff efficiency
MAE	Mean absolute error
WI	Willmott's index
Q	Runoff
S	Sediment
SY	Sediment yield
MT	Metric Tonne
m^3/s	Meter cube per second
k_0, k_1, k_2, k_3	Regression coefficient
R^2	Correlation coefficient

Responsible Editor: Broder J. Merkel

✉ Sarita Gajbhiye Meshram
saritagmeshram@tdtu.edu.vn

Chandrashekhar Meshram
cs_meshram@rediffmail.com

[1] Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[2] Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam

[3] Department of Post Graduate Studies and Research in Mathematics, Jayawanti Haksar Government Post Graduation College, College of Chhindwara University, Chhindwara, Betul, India

Published online: 23 November 2020

Introduction

Research on rainfall and runoff produced sediment-based problems would be very helpful in knowing the broad issue of soil degradation and soil erosion in an agricultural nation like India, where there are growing pressures on soil and water resources from the inhabitants (Renard 1980; Dhruv Narayana and Babu 1983; Meshram et al. 2019a, b). The need for accurate information on watershed runoff and sediment yield has grown rapidly during the past decades because of various watershed management programs for conservation,

Name of Faculty: Dr. Chandrashekhar Meshram

Theoretical and Applied Climatology
https://doi.org/10.1007/s00704-020-03137-z

ORIGINAL PAPER

Check for updates

Long-term temperature trend analysis associated with agriculture crops

Sarita Gajbhiye Meshram[1,2] · Ercan Kahya[3] · Chandrashekhar Meshram[4] · Mohammad Ali Ghorbani[5] · Balram Ambade[6] · Rasoul Mirabbasi[7]

Received: 8 July 2019 / Accepted: 7 February 2020

Abstract
Temperature is one of the most significant elements in climate and weather forecasting. There was an increase in the earth's surface (land and ocean) temperature by 0.6 ± 0.2 °C during 1901–2000 (NOAA, Global Climate Report 2017). In evaluating the effects of climate change, the spatiotemporal variability of temperature was examined in the Chhattisgarh State, India, using monthly data at 16 stations over the period 1901–2016 with a length of 116 years. The standard normal homogeneity test was used to evaluate the homogeneity of temperature data. Linear regression analysis and four altered versions of the Mann-Kendall (MK) method were utilized to analyze the existence of trends in temperature series. These four versions of the MK tests include the conventional Mann-Kendall method (MK1), the removed influence of noteworthy lag-1 autocorrelation (MK2), the removed influence of all noteworthy autocorrelation coefficients (MK3) and the considered Hurst coefficient (MK4). The results of both parametric and non-parametric tests indicated an increase in the annual and seasonal temperature in the Chhattisgarh State over the period 1901–2016. The most likely change year in the state was 1950. There was a decreasing trend at some stations during the period 1901–1950, which reversed in the following period 1951–2016. Overall, annual and seasonal temperature time series showed increasing trends in all stations over the course of the long-term period. Our results confirmed a fact that the agriculture crop production has been decreased due to climate change.

1 Introduction

Environment variations and its effects on temperature vary across global spatiotemporal scales, which has resulted in unexpected impacts and changes in regions around the world. As many regions on the earth normally experience both short- and long-term climatic variability (Houghton 1994; Gardner et al. 1996), its understanding is so critical in exploring not only present and future climatic conditions due to climate change but also its effects on water resources to support the implementation of suitable adaptation strategies. Temperature patterns provide basic evidence when assessing claims with respect to anthropogenic environmental change (Nazeri Tahroudi et al. 2019). An important change in temperature can also impact soil quality since temperature and water are vital physical elements for plant growth. Non-ideal levels of water and temperature conditions can unequivocally hinder plant growth, particularly at the early phases of development, such as during seed germination and rise (Helms et al. 1996), which has major implications for future food production.

The Intergovernmental Panel on Climate Change (IPCC) reported that over the course of the twentieth century, there was an increase in the earth's surface temperature by 0.6 ± 0.2 °C (Obiekezie et al. 2010). Likewise, the temperature has been increasing by 0.13 ± 0.07 °C every decade in the past

✉ Sarita Gajbhiye Meshram
saritagmeshram@tdtu.edu.vn

1 Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam
2 Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam
3 Civil Engineering Department, Istanbul Technical University (ITU), 34469 Istanbul, Turkey
4 Department of Mathematics, Govt. Jaywanti Haksar P.G. College, Betul, Madhya Pradesh, India
5 Department of Water Engineering, University of Tabriz, Tabriz, Iran
6 Department of Chemistry, National Institute of Technology, Jamshedpur, Jharkhand, India
7 Department of Water Engineering, Faculty of Agriculture, Shahrekord University, Shahrekord, Iran

Published online: 27 February 2020

Name of Faculty: Dr. Manoj Ughade

Available online at http://scik.org
J. Math. Comput. Sci. 10 (2020), No. 5, 1687-1696
https://doi.org/10.28919/jmcs/4724
ISSN: 1927-5307

COMMON FIXED POINTS OF FUZZY MAPS UNDER NONEXPANSIVE TYPE CONDITION

ANIL BAKHRU[1,*], MANOJ UGHADE[2], RICHA GUPTA[3]

[1]Department of Mathematics, Sardar Vallabhbhai Polytechnic College, College of University of Technology of Madhya Pradesh, Bhopal 462002, India

[2]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, College of Chhindawara University, Betul, 460001 India

[3]Department of Engineering Mathematics and Research Center, Sarvepalli Radhakrishanan University, Bhopal 462026, India

Abstract: In this paper, we obtain a common fixed-point theorem for a sequence of fuzzy mappings satisfying a rational contractive condition involving nonexpansive mapping.

Keywords: fuzzy sets; common fixed point; fuzzy mapping; nonexpansive mapping.

1. INTRODUCTION

Fixed point theory plays a basic role in applications of many branches of mathematics. The term metric fixed point theory refers to those fixed point theoretic results in which geometric conditions on the underlying spaces and/or mappings play a crucial role. For the past twenty five years metric fixed point theory has been a flourishing area of research for many mathematicians. Although a substantial number of definitive results now has been discussed, a few questions

*Corresponding author
E-mail address: anilbakhru@gmail.com
Received May 24, 2020

Name of Faculty: Dr. Manoj Ughade

Available online at http://scik.org
J. Math. Comput. Sci. 10 (2020), No. 5, 1891-1910
https://doi.org/10.28919/jmcs/4757
ISSN: 1927-5307

FIXED POINT THEOREMS FOR DUALISTIC CONTRACTIONS OF RATIONAL TYPE IN PARTIALLY ORDERED DUALISTIC PARTIAL METRIC SPACES

AMIT KUMAR PANDEY[1], MANOJ UGHADE[2], JYOTI VARMA[3,*], RAM MILAN SINGH[4]
[1]Department of Engineering Mathematics and Research Center, Sarvepalli Radhakrishanan University, Bhopal 462026, India
[2]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post Graduate College, College of Chhindawara University, Betul, 460001 India
[3]Department of Mathematics, Government College Shahpur, College of Chhindawara University, Shahpur 460440, India
[4]Department of Post Graduate Studies and Research in Mathematics, Government Post Graduate College, College of Maharaja Chhatrasal Bundelkhand University, Tikamgarh, 472000, India

Abstract. The purpose of this paper is to establish some fixed point theorems for mappings involving rational expressions in the frame work of complete ordered dualistic partial metric spaces using a class of pairs of functions satisfying certain assumptions. These results unify, extend and generalize most of the existing relevant fixed point theorems from the literature. We give examples to explain our findings.

Keywords: fixed point; dualistic partial metric; dualistic contractions.
2010 AMS Subject Classification: 47H09, 47H10, 54H25.

1. INTRODUCTION

The Banach contraction principle is a classical and powerful tool in nonlinear analysis. Banach contraction principle has been generalized in various ways either by using contractive conditions or by imposing some additional conditions on the ambient spaces. Das and Gupta [7] were the pioneers in proving fixed point theorems using contractive conditions involving rational expressions. Following Das and Gupta [7], Cabrera *et al.* [5] proved a fixed point

*Corresponding author
E-mail address: jyoti.varma2504@gmail.com
Received June 6, 2020

Name of Faculty: Dr. Sonali Saini Sahu

Solid State Technology
Volume: 63 Issue: 6
Publication Year: 2020

Numerical Treatment of Fourth Order Self-Adjoint Singularly Perturbed Boundary Value Problems via Septic B-Spline Method

Ram Kishun Lodhi[a], Sonali Saini Sahu[b]
[a]Department of Applied Sciences, SymbiosisInstitute of Technology, Symbiosis International (Deemed University), Pune-412115, Maharashtra (India).
Email: ramkishun.lodhi@gmail.com
[b]Department of Post Graduate Studies andResearch in Mathematics,
Jaywanti Haksar Government Post GraduateCollege, College of ChindwaraUniversity, Betul-460001, M.P. (India)
Email: sonali.saini1386@gmail.com

Abstract- In this communication, A septic B-spline method (SBSM) is descrived for numerical treatment of fourth order self adjoint (FOSA) singularly perturbed boundary value problems (SPBVPs) and method is directly implemented on the problems without decreasing the order of the original differential equations. Convergence of the SBSM is proved and found that it gives 4th order convergence results. The present technique is applied on two numerical problems which supports the theoretical proofs .

***Keywords*:** Septic B-spline method, Singularly perturbed boundary value problems, Fourth order self-adjoint, Uniform Convergence.

Mathematics Subject Classification (MSC)2010: 65L11

1. Introduction

We consider the following fourth order self adjoint SPBVPs:

$$-\varepsilon u^{iv}(y)+a(y)u(y)=r(y), \qquad y\in[p,\ q] \tag{1}$$

with the boundary condition (BC):

$$\begin{aligned} y(p)&=\alpha_1, & y(q)&=\beta_1,\\ y'(p)&=\alpha_2, & y'(q)&=\beta_2. \end{aligned} \tag{2}$$

where α_1, α_2, β_1 and β_2 are constants and perturbation parameter ε is $0<\varepsilon\ll 1$. We suppose that the functions $a(y)$ and $r(y)$ are smooth functions in $[p, q]$. A singular perturbation problems (SPPs) is arise in nuomarus regions of mathematical and engineering science for instant fluid dynamics, optimal control theory, chemistry, hydrodynamics, quantum physics, chemical reactor theory and reaction-diffusion process etc.

Name of Faculty: Dr. Chandrashekhar Meshram

IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received September 12, 2020, accepted October 8, 2020, date of publication October 12, 2020, date of current version October 21, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3030124

Multicriteria Decision Making Taxonomy of Cloud-Based Global Software Development Motivators

MUHAMMAD AZEEM AKBAR[1], HUSSAIN ALSALMAN[2,3], ARIF ALI KHAN[1], SAJJAD MAHMOOD[4], CHANDRASHEKHAR MESHRAM[5], ABDU GUMAEI[2], AND MUHAMMAD TANVEER RIAZ[6]

[1]College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing, China
[2]Research Chair of Pervasive and Mobile Computing, Department of Information Systems, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[3]Department of Computer Science, College of Computer and Information Sciences, King Saud University, Riyadh 11543, Saudi Arabia
[4]Information and Computer Science Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
[5]Department of Post Graduate Studies and Research in Mathematics, JayawantiHaksar Government Post Graduation College, College of Chhindwara University, Betul 460001, India
[6]Department of Mechatronics and Control Engineering, University of Engineering and Technology Lahore, Faisalabad Campus, Punjab, Pakistan

Corresponding authors: Muhammad Azeem Akbar (azeem.akbar@ymail.com) and Abdu Gumaei (abdugumaei@gmail.com)

The authors are grateful to the Deanship of Scientific Research, King Saud University for funding through Vice Deanship of Scientific Research Chairs.

ABSTRACT The software organizations widely consider the cloud based global software development (CGSD) as it offer the quality projects with low cast. The adoption of CGSD is challenging due to the geographical distance between practitioners. This study aims to identify and analyses the motivators that could positively impact the implementation of CGSD paradigm. The systematic literature review approach was applied to identify the CGSD motivators reported in the literature, and were further validated with industry experts using questionnaire survey study. Moreover, the fuzzy-AHP approach was applied to prioritize the investigated motivators concerning their significance for the successful adoption of CGSD. The findings of the study provide the prioritization-based taxonomy of the investigated motivators that assists the software organizations to develop and revise their strategies for the successful implementation of CGSD.

INDEX TERMS Cloud-based global software development, motivators, systematic literature review, fuzzy-AHP.

I. INTRODUCTION

The cloud computing is increasingly adopted in the geographically distributed software development environment as it provides significant opportunities to execute and manage the software development process. The availability, scalability and the dynamic attracted th e software firms to consider the cloud based global software development (CGSD). Dhar [1]stated that in software industry the outsources includes the development practices, process and decision management and the services were transformed in different geographical location across the globe.

Currently, the adoption of CGSD paradigm is significantly increased [1]. Fan *et al.* [2] mention that the CGSD paradigm educate the software development organization in terms of marked demand and the future trends.

Clemons and Chen [3] argued that it is necessary to take the rite decision and rite time for development of quality projects. They also mentions that CGSD assists to make the right decisions considering the trend and demand of international market. Chang and Gurbaxani [4] mention that it is important to make the right decision at right time contributed to develop the quality projects within time and budget. In this study, the definition of Leimeister *et al.* [5] is used i.e. ''an IT deployment model based on virtualization, where resources in terms of infrastructure, applications and data are deployed via the internet as a distributed service by one or several service providers. Services are scalable on-demand and can be priced on a pay-per-use basis.''

The development of good quality projects with low cost and time is always the priority of every software development organization. Though, the CGSD provides the opportunity to achieve to software organization to achieve such objective by hiring the skilled human resource from developing countries and by arranging the development activities round

The associate editor coordinating the review of this manuscript and approving it for publication was Yang Liu.

Name of Faculty: Dr. Chandrashekhar Meshram

Received: 12 May 2020 | Revised: 22 May 2020 | Accepted: 30 May 2020
DOI: 10.1002/spy2.119

Check for updates

RESEARCH ARTICLE

WILEY

An efficient ID-based cryptographic technique using IFP and GDLP

Chandrashekhar Meshram[1] | Rabha W. Ibrahim[2,3] | Sarita Gajbhiye Meshram[4,5] | Kailash W. Kalare[6] | Sunil D. Bagde[7]

[1]Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India
[2]Informetrics Research Group, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[3]Faculty of Mathematics & Statistics, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[4]Department for Management of Science and Technology Development, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[5]Faculty of Environment and Labour Safety, Ton Duc Thang University, Ho Chi Minh City, Vietnam
[6]Department of Computer Science and Engineering, Visvesvaraya National Institute of Technology, Nagpur, India
[7]Department of Mathematics, Gondwana University, Gadchiroli, India

Correspondence
Chandrashekhar Meshram, Department of Post Graduate Studies and Research in Mathematics, Jaywanti Haksar Government Post-Graduation College, College of Chhindwara University, Betul, Madhya Pradesh, India.
Email: cs_meshram@rediffmail.com

Abstract
Implementing an improved ID-based cryptographic mechanism is the main objective of the proposed work. In this article, an ID-based cryptographic (IBC) technique using generalized discrete logarithm problem (GDLP) and the integer factorization problem (IFP) presented by Meshram et al have improved. Meshram et al have given IBC technique without using the bilinear pair and also, reveal that their technique can attain data protection and security objectives. Besides, their technique will deter the adversary from eavesdropping the encrypted information or the secret key of the user. However, it has found that their system carries a deadlock problem. Encryption process, as expected by the user, is not guaranteed to be secure. It is because the user may require private information about key authentication center (KAC), which has kept secret from users. Pang et al have proposed an improved technique that overcomes the deadlock problem. It has found that Pang et al have not discussed the analysis and proofs of security. In this article, generalized discrete logarithms in multiplicative group over finite fields and IFP have used to improve the technique and also a key distribution system has discussed. It has analyzed that the proposed strategy is safer than the technique described by Pang et al. Also, it has found that the proposed technique addresses the deadlock problem.

KEYWORDS
cryptography, GDLP, ID-based cryptosystem, IFP, security proof

1 | INTRODUCTION

Nowadays, computer technologies and use of the internet has evolved in the daily life of every individual. The internet of things (IoT) has changed the way of living daily life as well as business life. Secrecy over the internet has become the prime concern of every individual. Secrecy has become essential for the data, that is, transferred over insecure public channels. Before establishing secure communication, secrete session keys to be shared between the communicating parties in an

Signature Not Verified
RAKESH KUMAR TIWARI
e verified
Principal JH Govt. PG College
Betul, MP
09.08.2023 12:19:32

Name of Faculty: Dr. Chandrashekhar Meshram

ADV MATH SCI JOURNAL
Advances in Mathematics: Scientific Journal 9 (2020), no.12, 11169–11177
ISSN: 1857-8365 (printed); 1857-8438 (electronic)
https://doi.org/10.37418/amsj.9.12.97

RIPIC BASED KEY EXCHANGE PROTOCOL

AKSHAYKUMAR J. MESHRAM[1], CHANDRASHEKHAR MESHRAM, SUNIL D. BAGDE, AND RUPALI R. MESHRAM

ABSTRACT. In this article, we intend to bring out a unique system of designing key exchange protocol (KEP) based on isomathematics. The significant concept of our proposal is to use ring isopolynomials with the usage of general isointegral coefficient. This class of KEP is an interesting asset for further study because of isomathematical structure permutable permutation of ring isopolynomials with isointeger coefficient (RIPIC).

1. INTRODUCTION

A KEP is a key formation technique where a common secret key is determined by more than two users as a component of data deliberated by, or connected with each of these users, in an ideal situation in such a way that no user can foreordain the subsequent value [1, 2]. In a symmetric key cryptography based protocols, two conveying users use a commonly identified algorithm and a secret key that is shared by the users. Secret key exchange can be made possible by employing few ways like- utilizing out-of-band correspondence, (for example, by telephone, via mail, manual entry etc.), utilizing a trusted third party key distribution center, and so forth. The greater parts of these techniques require approximately from the earlier secret key creation between the protocol and single users. Secret key

[1]*corresponding author*
2020 *Mathematics Subject Classification.* 16L30, 94A60.
Key words and phrases. Iso-mathematics, iso-zero, iso-unit, RIPIC and Diffie-Hellman Problem.

Name of Faculty: Dr. Chandrashekhar Meshram

DEPARTMENT OF APPLIED MATHEMATICS, YESHWANTRAO CHAVAN COLLEGE OF ENGINEERING
NAGPUR, M.S. 441110, INDIA
Email address: akshaykjmeshram@gmail.com

DEPARTMENT OF POST GRADUATE STUDIES AND RESEARCH IN MATHEMATICS
JAYAWANTI HAKSAR GOVERNMENT POST GRADUATION COLLEGE
COLLEGE OF CHHINDWARA UNIVERSITY, BETUL, M.P. 460001, INDIA
Email address: cs_meshram@rediffmail.com

DEPARTMENT OF MATHEMATICS, GONDWANA UNIVERSITY
GADCHIROLI MIDC ROAD COMPLEX, GADCHIROLI-442605
Email address: sunilkumarbagde@rediffmail.com

DEPARTMENT OF MATHEMATICS, KAMLA NEHRU MAHAVIDYALAYA NAGPUR
M.S. 440024, INDIA
Email address: rupa.meshram15@gmail.com

Academic Session 2018-2019

Signature Not Verified
RAKESH KUMAR TIWARI
e verified
Principal JH Govt. PG College
Betul, MP
09.08.2023 12:19:32

Academic Session 2017-2018