

Counselling Code : MTEC

Estd : 1999

JNTUH College Code : 86



MOTHER THERESSA COLLEGE OF ENGINEERING & TECHNOLOGY

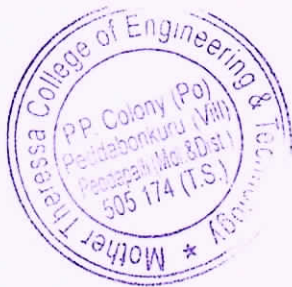
(Approved by A.I.C.T.E, New Delhi & Affiliated to J.N.T.U Hyderabad)

P.P.Colony (Po.), Peddabonkuru (Vill), PEDDAPALLI (Mdl. & Dist.) - 505174, Telangana State.

Website : www.mtec86.ac.in E-mail: mtec.86@gmail.com Contact : +91 9849472523, +91 9542709545, +91 9989959556.

Consolidate list of Patents : Granted/Published in the last Five years

S.No.	Title of the Patent	Name of the Inventor	Application No.	Granted/ Published/ Filed	Date
1	ARTIFICIAL INTELLIGENCE AND DEEP LEARNING ALGORITHMS TO DETECT AND PREVENT MALWARE IN CYBER SECURITY	1)Nidhi Sharma 2)Dr. Rashel Sarkar 3)Dr. Dushyantsinh B. Rathod 4)Dr. Ramesh T. Prajapati 5)Dr. Vijaykumar Bhikhudan Gadhavi 6)Dr. A. S Aneetha 7) <u>Kishor Kumar Gajula</u> 8)Dr. M. Anjankumar 9)Dr. Gurjinder Singh 10)Mr. Keerthipati Kumar	202211063681	Published	11/18/2022
2	DEEP LEARNING APPROACHES TO DETECT IMAGE FORGERY USING PYTHON	1)Dr. Ashwini Kumar Srivastava 2)Dr. S. Revathi 3) <u>Dr. Kishor Kumar Gajula</u> 4)Saqib Qamar 5)Janaranjani. V 6)Naveeth Kumar R 7)Dr. Gurjinder Singh 8)Mr. Saravanan R 9)Javed Akhtar Khan 10)Dr. RenukaSnehalNifadkar	202211067420	Published	12/9/2022



Yaceel
PRINCIPAL
MOTHER THERESSA
College of Engineering & Technology
PEDDAPALLI - 505174.

पेटेंट कार्यालय
शासकीय जर्नल

OFFICIAL JOURNAL
OF
THE PATENT OFFICE

निर्गमन सं. 46/2022
ISSUE NO. 46/2022

शुक्रवार
FRIDAY

दिनांक: 18/11/2022
DATE: 18/11/2022

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE



grecer
PRINCIPAL
MOTHER THERESSA
College of Engineering & Technology
PEDDAPALLI-505 174.

The Patent Office Journal No. 46/2022 Dated 18/11/2022

72338

(54) Title of the invention : ARTIFICIAL INTELLIGENCE AND DEEP LEARNING ALGORITHMS TO DETECT AND PREVENT MALWARE IN CYBER SECURITY

(51) International classification :G06N002000000, G06F002156000, G06F002157000, G06F002155000, G06N0003080000

(86) International Application No :NA
Filing Date :NA

(87) International Publication No : NA

(61) Patent of Addition to Application Number :NA
Filing Date :NA

(62) Divisional to Application Number :NA
Filing Date :NA

(71)Name of Applicant :
1)Nidhi Sharma
 Address of Applicant :Assistant Professor, Department of MMICTBM, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana- 133207, India -----

2)Dr. Rashel Sarkar
3)Dr. Dushyantsinh B. Rathod
4)Dr. Ramesh T. Prajapati
5)Dr. Vijaykumar Bhikhudan Gadhavi
6)Dr. A. S Aneetha
7)Kishor Kumar Gajula
8)Dr. M. Anjankumar
9)Dr. Gurjinder Singh
10)Mr. Keerthipati Kumar

Name of Applicant : NA
 Address of Applicant : NA

(72)Name of Inventor :
1)Nidhi Sharma
 Address of Applicant :Assistant Professor, Department of MMICTBM, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana- 133207, India -----

2)Dr. Rashel Sarkar
 Address of Applicant :Associate Professor, Department of Computer Science, University of Science and Technology (USTM), Meghalaya, Techno City, Kling Road, Baridua, 9th Mile, RI-Bhoi, Meghalaya- 783101 -----

3)Dr. Dushyantsinh B. Rathod
 Address of Applicant :Professor & HOD, Department of Computer Engineering, Ahmedabad Institute Of Technology, Ahmedabad - 380061 -----

4)Dr. Ramesh T. Prajapati
 Address of Applicant :HoD & Associate Professor, Department of CE/IT, Shree Swaminarayan Institute Of Technology, Bhat, Gandhinagar - 382428 -----

5)Dr. Vijaykumar Bhikhudan Gadhavi
 Address of Applicant :Assistant Professor & Head of Department, Department of Computer Engineering, Shree Swaminarayan Institute of Technology, Near EDI, Bhat, Gandhinagar - 382330 -----

6)Dr. A. S Aneetha
 Address of Applicant :Associate Professor, Department of Computer Science , Vels Institute of Science, Technology and Advanced Studies, Pallavaram, Chennai-600117 -----

7)Kishor Kumar Gajula
 Address of Applicant :Assistant Professor & HOD, Department of CSE(AI& ML), Mother Theresa College of Engineering & Technology, Peddapalli - 505174, Telangana -----

8)Dr. M. Anjankumar
 Address of Applicant :Professor, Department of CSE, Vivekananda Institute of Technology & Science, Housing board colony, Karimnagar - 505001, Telangana -----

9)Dr. Gurjinder Singh
 Address of Applicant :Former Assistant Professor, Department of Electronics Engineering, Sri Guru Granth Sahib World University, Fatehgarh Sahib - 140406, Punjab -----

10)Mr. Keerthipati Kumar
 Address of Applicant :Lecturer, Department of Information Technology, University of Technology and Applied Sciences, Muladdah, Mussanah - 191 -----

(57) Abstract :
 The attack surface of an organisation is vast, increasing at an alarming rate, and changing at an alarming rate. To quantify risk effectively, it may be necessary to examine hundreds of billions of data points that evolve over time. Depending on the size of your business, there may be a few or a large number of signals. In response to this unprecedented threat, cybersecurity approaches based on artificial intelligence have been created. These methods aid information security teams in defending against breaches and enhancing their security posture. AI and deep learning are crucial to the information security business because they can analyse millions of events in real time and identify a variety of dangers. These threats come in a variety of ways, including as phishing assaults, malware downloads, and malware that exploits zero-day vulnerabilities. In the future, these systems will be able to learn from their mistakes and identify new forms of dangers. AI can recognise and respond to departures from the norm by developing profiles of individuals, assets, and networks based on their prior behaviour. The phrase artificial intelligence (AI) is currently popular, yet it is occasionally abused. As is the case with other next big things such as big data, the cloud, and the Internet of Things, a growing number of firms are studying ways to implement artificial intelligence. However, the majority of AI systems now available on the market fall short. Even while it incorporates technologies that analyse data and allow the results to determine what should be done, this is not artificial intelligence. Artificial intelligence in its purest form aims to emulate human intelligence in order to execute mechanical tasks.

No. of Pages : 9 No. of Claims : 8



Y. Ceel
 PRINCIPAL
 MOTHER THERESSA
 College of Engineering & Technology
 PEDDAPALLI-505 174.

पेटेंट कार्यालय
शासकीय जर्नल

**OFFICIAL JOURNAL
OF
THE PATENT OFFICE**

निर्गमन सं. 49/2022
ISSUE NO. 49/2022

शुक्रवार
FRIDAY

दिनांक: 09/12/2022
DATE: 09/12/2022

पेटेंट कार्यालय का एक प्रकाशन
PUBLICATION OF THE PATENT OFFICE



Yeeell
PRINCIPAL
MOTHER TERESSA
College of Engineering & Technology
PEDDAPALLI-505 174.

The Patent Office Journal No. 49/2022 Dated 09/12/2022

77489

(12) PATENT APPLICATION PUBLICATION

(21) Application No.202211067420 A

(19) INDIA

(22) Date of filing of Application :23/11/2022

(43) Publication Date : 09/12/2022

(54) Title of the invention : DEEP LEARNING APPROACHES TO DETECT IMAGE FORGERY USING PYTHON

(51) International classification :G06T0001000000, G06Q0050000000, G06N0020000000, G06T0011600000, H04N0001000000

(86) International Application No :NA
Filing Date :NA

(87) International Publication No : NA

(61) Patent of Addition to Application Number :NA
Filing Date :NA

(62) Divisional to Application Number :NA
Filing Date :NA

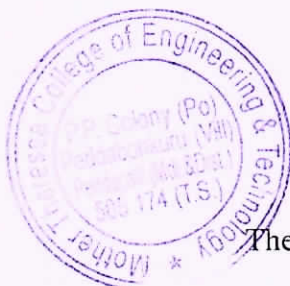
(71)Name of Applicant :
1)Dr. Ashwini Kumar Srivastava
 Address of Applicant :Assistant Professor, Department of Computer Application, Shivharsh Kisan P.G. College, Basti - 272001, Uttar Pradesh -----
2)Dr. S. Revathi
3)Dr. Kishor Kumar Gajula
4)Saqib Qamar
5)Janaranjani. V
6)Naveeth Kumar R
7)Dr. Gurjinder Singh
8)Mr. Saravanan R
9)Javed Akhtar Khan
10)Dr. RenukaSnehalNifadkar
 Name of Applicant : NA
 Address of Applicant : NA

(72)Name of Inventor :
1)Dr. Ashwini Kumar Srivastava
 Address of Applicant :Assistant Professor, Department of Computer Application, Shivharsh Kisan P.G. College, Basti - 272001, Uttar Pradesh -----
2)Dr. S. Revathi
 Address of Applicant :Assistant Professor, Department of English, Srinivasan College of Arts and Science, Perambalur District, Tamil Nadu -----
3)Dr. Kishor Kumar Gajula
 Address of Applicant :Assistant Professor & HOD, Department of CSF (AI& ML), Mother Theresa College of Engineering & Technology, Peddapalli - 505174. -----
4)Saqib Qamar
 Address of Applicant :Postdoctoral Fellow, Integrated Science Lab, Umea University, 901 87 Umeå, Sweden - 90734. -----
5)Janaranjani. V
 Address of Applicant :Assistant Professor, Department of Biomedical Engineering, Rathinam Technical Campus, Pollachi main road, Coimbatore - 641023 -----
6)Naveeth Kumar R
 Address of Applicant :Assistant Professor, Department of Biomedical Engineering, Rathinam Technical Campus, Pollachi main road, Coimbatore - 641021 -----
7)Dr. Gurjinder Singh
 Address of Applicant :Former Assistant Professor, Department of Electronics Engg, Sri Guru Granth Sahib World University, Fatehgarh Sahib - 140406 -----
8)Mr. Saravanan R
 Address of Applicant :Assistant Professor, Department of Aeronautical Engineering, Hindusthan College of Engineering and Technology, Valley Campus, Pollachi Highway, Coimbatore -32 -----
9)Javed Akhtar Khan
 Address of Applicant :Associate Professor, Department of Computer Science and Engineering, Indur Institute of Engineering and Technology, Siddipet, Telangana - 502277 -----
10)Dr. RenukaSnehalNifadkar
 Address of Applicant :Assistant Professor, School of Management (PG), Dr VishwanathKarad MIT World Peace University, Survey No, 124, Paud Road, Kothrud, Pune, Maharashtra - 411038 -----

(57) Abstract :

As social networking sites like as Facebook and Instagram have increased in popularity over the past decade, more image data has been generated. Facebook is extremely concerned about image and video editing software such as GNU Gimp and Adobe Photoshop. These photos are commonly exploited in bad ways, such as to provoke riots, and are one of the most common methods for spreading fake news. Before taking any action based on the photo in question, we must first confirm its authenticity. Fake photographs are a global issue that are routinely circulated through social media. Due to the ease with which digital pictures can be forged, Internet users no longer have faith in them. In recent years, there has been a great deal of research and development into innovative methods to prevent the duplication of photographs. If individuals learned how to identify forgeries, they could never be used to deceive or hurt others. In this work, we examine how an error level analysis method can be utilised to provide individuals with new ways to identify altered images. In this research, we illustrate how picture preprocessing and machine learning methods can be combined to detect image forgery attempts.

No. of Pages : 11 No. of Claims : 8



Handwritten signature and official stamp of the Principal, Mother Theresa College of Engineering & Technology, Peddapalli-505174.