ACADEMIC
PERSPECTIVE

APJESS

Journal of Engineering and Smart Systems

Volume : 13
Issue : 1
Year : 2025

Volume 13 / Issue 1
Academic Platform Journal of Engineering and Smart Systems

Correspondence Address
Academic Platform Journal of Engineering and Smart Systems
Akademik Perspektif Derneği, Tığcılar Mahallesi Kadir Sokak No:12
Kat:1 Adapazarı SAKARYA

+90 551 628 9477 (WhatsApp only)
https://dergipark.org.tr/tr/pub/apjess

Issue Link: https://dergipark.org.tr/en/pub/apjess/issue/90281

Aim and Scope

Academic Platform Journal of Engineering and Smart Systems (APJESS) is a peer reviewed open-access journal which focuses on the research and applications related to smart systems and artificial intelligence. APJESS accepts both **original research papers** and **review articles** written in **English**. It is essential that the information created in scientific study needs to be new, suggest new method or give a new dimension to an existing information. Articles submitted for publication are evaluated by at least two referees in case the editor finds potential scientific merit, and final acceptance and rejection decision are taken by editorial board. The authors are not informed about the name of referees who evaluate the papers. In similar way, the referees are not allowed to see the names of authors. The papers which do not satisfy the scientific level of the journal can be refused with unexplained reason.

There are two key principles that APJESS was founded on: Firstly, to publish the most exciting, novel, technically sound, and clearly presented researches with respect to the subjects of smart systems and artificial intelligence. Secondly, to provide a rapid turn-around time possible for reviewing and publishing, and to disseminate the articles freely for research, teaching and reference purposes.

Any information about a submitted manuscript cannot be disclosed by the editor and any other editorial staff to anyone other than the corresponding author, reviewers, potential reviewers, other editorial advisers, and the publisher. No confidential information or ideas obtained through peer review can be used for personal advantage.

Journal History

The journal was published between 2013-2021 with the title of "Academic Platform - Journal of Engineering and Science". It will be published under its new title "Academic Platform Journal of Engineering and Smart Systems" after 2022.

Former Title: Academic Platform - Journal of Engineering and Science

Years: 2013-2021

Scope

APJESS aims to publish research and review papers dealing with, but not limited to, the following research fields:

- Knowledge Representation and Reasoning,
- Data Mining & Data Science,
- Supervised, Semi-Supervised and Unsupervised Learning,
- Machine Learning (ML) and Neural Computing,
- Evolutionary Computation,
- Natural Language Processing, Internet of Things, Big Data
- Fuzzy Systems,
- Intelligent Information Processing,
- AI Powered Robotic Systems,
- Multi-agent Systems and Programming for Smart Systems

Author Guidelines

Article Types

Manuscripts submitted to APJESS should neither be published previously nor be under consideration for publication in another journal.

The main article types are as follows:

Research Articles: Original research manuscripts. The journal considers all original research manuscripts provided that the work reports scientifically sound experiments and provides a substantial amount of new information.

Review Articles: These provide concise and precise updates on the latest progress made in a given area of research.

Checklist for Submissions

Please,

• read the Aims & Scope to see if your manuscript is suitable for the journal,
• use the Microsoft Word template to prepare your manuscript;
• Download Copyright Transfer Form and signed by all authors.
• make sure that issues about Ethical Principles and Publication Policy, Copyright and Licensing, Archiving Policy, Repository Policy have been appropriately considered;
• Ensure that all authors have approved the content of the submitted manuscript.

The main text should be formed in the following order:

Manuscript: The article should start with an introduction written in scientific language, putting thoughts together from diverse disciplines combining evidence-based knowledge and logical arguments, conveying views about the aim and purpose of the article. It must address all readers in general. The technical terms, symbols, abbreviations must be defined at the first time when they are used in the article. The manuscript should be formed in the following order:

Introduction,

Material and Method,

Findings,

Discussion and Conclusion.

References: At the end of the paper provide full details of all references cited in-text. The reference list should be arranged in the order of appearance of the in-text citations, not in an alphabetical order, beginning with [1], and continuing in an ascending numerical order, from the lowest number to the highest. In the reference list, only one resource per reference number is acceptable.
References must be numbered in order of appearance in the text (including citations in tables and legends) and listed individually at the end of the manuscript. We recommend preparing the references with a bibliography software package, such as EndNote, Reference Manager or Zotero to avoid typing mistakes and duplicated references. Include the digital object identifier (DOI) for all references where available. Please use IEEE style.

IEEE Sample Reference List

[1] R. E. Ziemer and W. H. Tranter, Principles of Communications: Systems, Modulation, and Noise, 7th ed. Hoboken, NJ: Wiley, 2015.
[2] J. D. Bellamy et al., Computer Telephony Integration, New York: Wiley, 2010.

[3] C. Jacks, High Rupturing Capacity (HRC) Fuses, New York: Penguin Random House, 2013, pp. 175–225.
[4] N. B. Vargafik, J. A. Wiebelt, and J. F. Malloy, "Radiative transfer," in Convective Heat. Melbourne: Engineering Education Australia, 2011, ch. 9, pp. 379–398.
[5] H. C. Hottel and R. Siegel, "Film condensation," in Handbook of Heat Transfer, 2nd ed. W. C. McAdams, Ed. New York: McGraw-Hill, 2011, ch. 9, pp. 78–99.
[6] H. H. Gaynor, Leading and Managing Engineering and Technology, Book 2: Developing Managers and Leaders. IEEE-USA, 2011. Accessed on: Oct. 15, 2016. [Online]. Available: http://www.ieeeusa.org/communications/ebooks/files/sep14/n2n802/Leading-and-Managing-Engineering-and-Technology-Book-2.pdf
[7] G. H. Gaynor, "Dealing with the manager leader dichotomy," in Leading and Managing Engineering and Technology, Book 2, Developing Leaders and Mangers. IEEE-USA, 2011, pp. 27–28. Accessed on: Jan. 23, 2017. [Online]. Available: http://www.ieeeusa.org/communications/ebooks/files/sep14/n2n802/Leading-and-Managing-Engineering-and-Technology-Book-2.pdf
[8] M. Cvijetic, "Optical transport system engineering," in Wiley Encyclopedia of Telecommunications, vol. 4, J. G. Proakis, Ed. New York: John Wiley & Sons, 2003, pp. 1840–1849. Accessed on: Feb. 5, 2017. [Online]. Available: http://ebscohost.com
[9] T. Kaczorek, "Minimum energy control of fractional positive electrical circuits", Archives of Electrical Engineering, vol. 65, no. 2, pp.191–201, 2016.
[10] P. Harsha and M. Dahleh, "Optimal management and sizing of energy storage under dynamic pricing for the efficient integration of renewable energy", IEEE Trans. Power Sys., vol. 30, no. 3, pp. 1164–1181, May 2015.
[11] A. Vaskuri, H. Baumgartner, P. Kärhä, G. Andor, and E. Ikonen, "Modeling the spectral shape of InGaAlP-based red light-emitting diodes," Journal of Applied Physics, vol. 118, no. 20, pp. 203103-1–203103-7, Jul. 2015. Accessed on: Feb. 9, 2017. [Online]. Available: doi: 10.1063/1.4936322
[12] K. J. Krishnan, "Implementation of renewable energy to reduce carbon consumption and fuel cell as a back-up power for national broadband network (NBN) in Australia," Ph.D dissertation, College of Eng. and Sc., Victoria Univ., Melbourne, 2013.
[13] C. R. Ozansoy, "Design and implementation of a Universal Communications Processor for substation integration, automation and protection," Ph.D. dissertation, College of Eng. and Sc., Victoria Univ., Melbourne, 2006. [Online]. Accessed on: June 22, 2017. [Online]. Available: http://vuir.vu.edu.au/527/
[14] M. T. Long, "On the statistical correlation between the heave, pitch and roll motion of road transport vehicles," Research Master thesis, College of Eng. and Sc., Victoria Univ., Melb., Vic., 2016.
[15] Safe Working on or Near Low-voltage Electrical Installations and Equipment, AS/NZS 4836:2011, 2011.

Ethical Principles and Publication Policy

Peer Review Policy

Academic Platform Journal of Engineering and Smart Systems (APJESS) applies double blind peer-review process in which both the reviewer and the author are anonymous. Reviewer selection for each submitted article is up to area editors, and reviewers are selected based on the reviewer’s expertise, competence, and previous experience in reviewing papers for APJES.

Every submitted article is evaluated by area editor, at least, for an initial review. If the paper reaches minimum quality criteria, fulfills the aims, scope and policies of APJES, it is sent to at least two reviewers for evaluation.

The reviewers evaluate the paper according to the Review guidelines set by editorial board members and return it to the area editor, who conveys the reviewers' anonymous comments back to the author. Anonymity is strictly maintained.

The double-blind peer-review process is managed using “ULAKBİM Dergi Sistemleri”, namely Dergipark platform.

Open Access Policy

APJESS provides immediate open access for all users to its content on the principle that making research freely available to the public, supporting a greater global exchange of knowledge.

Archiving Policy

APJESS is accessed by Dergipark platform which utilizes the LOCKSS system to create a distributed archiving system among participating libraries and permits those libraries to create permanent archives of the journal for purposes of preservation and restoration.

Originality and Plagiarism Policy

Authors by submitting their manuscript to APJESS declare that their work is original and authored by them; has not been previously published nor submitted for evaluation; original ideas, data, findings and materials taken from other sources (including their own) are properly documented and cited; their work does not violate any rights of others, including privacy rights and intellectual property rights; provided data is their own data, true and not manipulated. Plagiarism in whole or in part without proper citation is not tolerated by APJESS. Manuscripts submitted to the journal will be checked for originality using anti-plagiarism software.

Journal Ethics and Malpractice Statement

For all parties involved in the publishing process (the author(s), the journal editor(s), the peer reviewers, the society, and the publisher) it is necessary to agree upon standards of expected ethical behavior. The ethics statements for APJESS are based on the Committee on Publication Ethics (COPE) Code of Conduct guidelines available at www.publicationethics.org.

1. Editor Responsibilities

Publication Decisions & Accountability

The editor of APJESS is responsible for deciding which articles submitted to the journal should be published, and, moreover, is accountable for everything published in the journal. In making these decisions, the editor may be guided by the journal’s editorial board and/or area editors, and considers the policies of the journal. The editor should maintain the integrity of the academic record, preclude business needs from compromising intellectual and ethical standards, and always be willing to publish corrections, clarifications, retractions, and apologies when needed.

Fair play

The editor should evaluate manuscripts for their intellectual content without regard to race, gender, sexual orientation, religious belief, ethnic origin, citizenship, or political philosophy of the author(s).

Confidentiality

The editor and any editorial staff must not disclose any information about a submitted manuscript to anyone other than the corresponding author, reviewers, potential reviewers, other editorial advisers, and the publisher, as appropriate.

Disclosure, conflicts of interest, and other issues

The editor will be guided by COPE's Guidelines for Retracting Articles when considering retracting, issuing expressions of concern about, and issuing corrections pertaining to articles that have been published in APJES.

Unpublished materials disclosed in a submitted manuscript must not be used in an editor's own research without the explicit written consent of the author(s). Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage.

The editor should seek so ensure a fair and appropriate peer-review process. The editor should recuse himself/herself from handling manuscripts (i.e. should ask a co-editor, associate editor, or other member of the editorial board instead to review and consider) in which they have conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or (possibly) institutions connected to the papers. The editor should require all contributors to disclose relevant competing interests and publish corrections if competing interests are revealed after publication. If needed, other appropriate action should be taken, such as the publication of a retraction or expression of concern.

2. Reviewer Responsibilities

Contribution to editorial decisions

Peer review assists the editor in making editorial decisions and, through the editorial communication with the author, may also assist the author in improving the manuscript.

Promptness

Any invited referee who feels unqualified to review the research reported in a manuscript or knows that its timely review will be impossible should immediately notify the editor so that alternative reviewers can be contacted.

Confidentiality

Any manuscripts received for review must be treated as confidential documents. They must not be shown to or discussed with others except if authorized by the editor.

Standards of objectivity

Reviews should be conducted objectively. Personal criticism of the author(s) is inacceptable. Referees should express their views clearly with appropriate supporting arguments.

Acknowledgement of sources

Reviewers should identify relevant published work that has not been cited by the author(s). Any statement that an observation, derivation, or argument had been previously reported should be accompanied by the relevant citation. Reviewers should also call to the editor's attention any substantial similarity or overlap between the manuscript under consideration and any other published data of which they have personal knowledge.

Disclosure and conflict of interest

Privileged information or ideas obtained through peer review must be kept confidential and not used for personal advantage. Reviewers should not consider evaluating manuscripts in which they have conflicts of interest resulting from competitive, collaborative, or other relationships or connections with any of the authors, companies, or institutions connected to the submission.

3. Author Responsibilities

Reporting standards

Authors reporting results of original research should present an accurate account of the work performed as well as an objective discussion of its significance. Underlying data should be represented accurately in the manuscript. A paper should contain sufficient detail and references to permit others to replicate the work. Fraudulent or knowingly inaccurate statements constitute unethical behavior and are unacceptable.

Originality and plagiarism

The authors should ensure that they have written entirely original works, and if the authors have used the work and/or words of others that this has been appropriately cited or quoted.

Multiple, redundant, or concurrent publication

An author should not in general publish manuscripts describing essentially the same research in more than one journal or primary publication. Parallel submission of the same manuscript to more than one journal constitutes unethical publishing behavior and is unacceptable.

Acknowledgement of sources

Proper acknowledgment of the work of others must always be given. Authors should also cite publications that have been influential in determining the nature of the reported work.

Authorship of a manuscript

Authorship should be limited to those who have made a significant contribution to the conception, design, execution, or interpretation of the reported study. All those who have made significant contributions should be listed as co-authors. Where there are others who have participated in certain substantive aspects of the research project, they should be named in an Acknowledgement section. The corresponding author should ensure that all appropriate co-authors are included in the author list of the manuscript, and that all co-authors have seen and approved the final version of the paper and have agreed to its submission for publication. All co-authors must be clearly indicated at the time of manuscript submission. Request to add co-authors, after a manuscript has been accepted will require approval of the editor.

Hazards and human or animal subjects

If the work involves chemicals, procedures, or equipment that has any unusual hazards inherent in their use, the authors must clearly identify these in the manuscript. Additionally, manuscripts should adhere to the principles of the World Medical Association (WMA) Declaration of Helsinki regarding research study involving human or animal subjects.

Disclosure and conflicts of interest

All authors should disclose in their manuscript any financial or other substantive conflict of interest that might be construed to influence the results or their interpretation in the manuscript. All sources of financial support for the project should be disclosed.

Fundamental errors in published works

In case an author discovers a significant error or inaccuracy in his/her own published work, it is the author's obligation to promptly notify the journal's editor to either retract the paper or to publish an appropriate correction statement or erratum.

4. Publisher Responsibilities

Editorial autonomy

Academic Perspective Foundation is committed to working with editors to define clearly the respective roles of publisher and of editors in order to ensure the autonomy of editorial decisions, without influence from advertisers or other commercial partners.

Intellectual property and copyright

We protect the intellectual property and copyright of Academic Perspective Foundation, its imprints, authors and publishing partners by promoting and maintaining each article's published version of record. Academic Perspective Foundation ensures the integrity and transparency of each published article with respect to: conflicts of interest, publication and research funding, publication and research ethics, cases of publication and research misconduct, confidentiality, authorship, article corrections, clarifications and retractions, and timely publication of content.

Scientific Misconduct

In cases of alleged or proven scientific misconduct, fraudulent publication, or plagiarism the publisher, in close collaboration with the editors, will take all appropriate measures to clarify the situation and to amend the article in question. This includes the prompt publication of a correction statement or erratum or, in the most severe cases, the retraction of the affected work.

Contents

Research Article
Academic Platform Journal of Engineering and Smart Systems (APJESS) 13(1), 1–6, 2025
https://dergipark.org.tr/en/pub/apjess
Received: 01-09-2024, Accepted: 01-10-2024
https://doi.org/10.21541/apjess.1541802

Implementation of EWMA Algorithm in the Analysis of Security Attacks

*1 Şükrü OKUL, 2 Fatih KELEŞ, 3 Muhammed Ali AYDIN

1 Corresponding Author, TÜBİTAK-BİLGEM, Türkiye, sukruokul@tubitak.gov.tr
*2 Department of Computer Engineering, Istanbul University - Cerrahpasa, Türkiye, fkeles@iuc.edu.tr
3 Department of Computer Engineering, Istanbul University - Cerrahpasa, Türkiye, aydinali@iuc.edu.tr

Abstract

This study analyzes the detection of security attacks on smart vehicles using the Exponentially Weighted Moving Average (EWMA) algorithm. We employed synthetically generated datasets, consisting of 80% non-attack and 20% attack scenarios. Various smoothing parameters (α\alphaα) were tested within the EWMA framework, specifically at values of 0.8, 0.7, and 0.6, with 0.7 yielding the most promising results. In our analysis, we normalized the selection function in the EWMA algorithm based on expert evaluations to establish the impact of different factors on anomaly detection. Specifically, we assigned weights of 24% to RPM, 40% to speed, and 18% each to fuel quantity and accelerator pedal position. The results demonstrate that the EWMA algorithm can effectively issue warnings for vehicles under potential attack, enabling proactive measures to mitigate security risks. This research contributes to enhancing the safety and reliability of smart vehicles by facilitating timely responses to detected security threats.

Keywords: Security Attacks; Smart Vehicles; EWMA

1. INTRODUCTION

Security attacks pose a significant threat, particularly to smart devices, which are increasingly interconnected through the Internet of Things (IoT). As the importance of security in modern applications grows, ensuring the safety of smart vehicles has become paramount. This study examines smart vehicles, focusing on their communication protocols, infrastructure, and the various attack scenarios, causes, and consequences they may encounter.

The literature on smart vehicle security highlights critical areas such as Vehicle-to-Vehicle (V2V) communication frameworks, the challenges inherent in V2V data transmission, and the cybersecurity vulnerabilities present in these systems [1-2]. Research indicates that smart vehicles can be attacked both directly and indirectly through their Control Area Network (CAN) and via radio frequencies [3]. A comprehensive understanding of these attack types, as well as the classification of cyber threats, is essential for developing effective security measures.

In this context, the Exponentially Weighted Moving Average (EWMA) algorithm has been identified as a promising tool for detecting anomalies in vehicle data. Although the EWMA algorithm has historical significance, emerging studies suggest its growing analytical value in cybersecurity applications [4-5]. This algorithm is particularly effective in identifying subtle changes in data, making it suitable for detecting security attacks in smart vehicle systems [6].

To validate the applicability of the EWMA algorithm in smart vehicle security, experiments were conducted using two synthetically generated datasets: one comprising 80% non-attack data and 20% attack data, and the other consisting of 70% non-attack and 30% attack data. The simulated datasets represented either normal operating conditions or data subjected to various attack types, as detailed in the literature [7-8].

The findings reveal that the EWMA algorithm can successfully identify security attacks by monitoring the CAN network of smart vehicles. The algorithm achieved a high success rate in detecting anomalies, but further improvements could be realized by optimizing key parameters such as rpm, speed, throttle, and fuel consumption, as well as exploring alternative algorithms for comparison.

2. LITERATURE REVIEW

Research on vehicle-to-vehicle (V2V) communication has gained significant traction in recent years, particularly in the context of transmitting vehicle information effectively [9-

10]. Methods for disseminating this information generally fall into two categories: centralized and decentralized systems. Centralized systems involve infrastructure-to-vehicle (I2V) communication or mobile communications, where vehicles collect and relay information through roadside units or mobile terminals, respectively [11].

Conversely, decentralized V2V communication allows for direct information exchange between vehicles, which is particularly beneficial in emergency situations, eliminating the need for additional infrastructure like roadside units and base stations [12]. Traditional centralized systems often impose significant burdens on communication infrastructure and data centers, prompting a shift toward decentralized models. Vehicle identification data obtained through these mechanisms can be leveraged to support Driving Safety Support Systems, potentially alleviating congestion and enhancing road safety. However, existing identification distribution systems face challenges such as limited-service areas, low delivery efficiency, and delays in data transmission [13].

In high-traffic environments, V2V communication facilitates efficient information exchange among vehicles. For instance, when the number of vehicles falls within a specified range, V2V communication is employed using Geocast techniques. Geocast refers to location-based data transmission in an ad-hoc network, replacing traditional node IDs with geographic information [14]. Key factors influencing communication between nodes in such networks include the target node's location and the selected transmission path.

I2V communication is particularly useful in densely populated areas or at traffic intersections, where roadside units are deployed. When a vehicle is within a predetermined distance from a roadside unit, I2V communication is activated. The roadside unit's location information is derived from digital maps, allowing the ego vehicle to assess its position relative to the roadside unit to determine the appropriate communication mode [15].

Mobile communication serves in scenarios with low vehicle density or where direct V2V communication may lead to network congestion. In cases where the number of nearby vehicles is below a specified threshold or exceeds a certain limit, mobile communication becomes the preferred option. This mode is particularly suitable for delivering non-urgent information and operates over 3G networks, enabling extensive coverage and the flexibility of pull-type communication based on driver needs [16].

3. MATERIALS AND METHODS

The Exponentially Weighted Moving Average (EWMA) algorithm was first introduced under the name Geometric Moving Average (GMA) [17]. Initially, it saw limited application outside a few studies [18-19]. However, its analytical significance began to grow in the latter half of the 1980s, leading to its adoption in various fields [20-21]. EWMA has proven effective in detecting changes of varying magnitudes in diverse processes, functioning as a smoothing technique to mitigate noise in time series data [22].

For the implementation of EWMA, an initial target value is selected, typically calculated as the average of the observations [18]. The formula for EWMA can be expressed as formula 1.

$$E(t) = \alpha \cdot X(t) + (1-\alpha) \cdot E(t-1) \qquad (1)$$

where E(t) represents the EWMA value at time t, X(t) is the observed value at time t, and α is the smoothing parameter ($0 < \alpha \leq 1$). This formulation illustrates how the influence of the initial observation E(0) diminishes exponentially over time, with its effect approaching zero as α dictates the rate of decay [23].

In anomaly detection, if the calculated EWMA value deviates from the target value by k times, it exceeds a predefined threshold, indicating an outlier [24]. In the context of this study, we focus exclusively on upward deviations within the scope of bio surveillance, monitoring only increases. If downward changes were to be considered, the following equation would also require evaluation:

$$E(t) - k\sigma \qquad (2)$$

where σ represents the standard deviation. For a comprehensive exploration of selecting the threshold k, refer to Lucas's seminal work [25].

When using EWMA, a data set was first created regarding normal vehicle movements in the test data and vehicles that may have been attacked, in order to understand whether there was an attack on the CAN Network. There are 25 cases in this data set and 6 cycle logs in each case. Each of these examined logs consists of 4 lines. The information examined and its log equivalent are as follows:

- 410D40 = 410D makes it clear that this data is the current speed data. 40 gives the numerical value of the speed as hexadecimal. 4*16+0=64 km.
- 410C0A20 = 410C indicates that this data is the current rpm data. 0A20 gives the rpm value of the engine in hexadecimal. 0*16^3+10*16^2+16*2+0 =2592.
- 412FC8 = 412F makes it clear that this data is the current percentage fuel amount data. Multiplying the hexadecimal equivalent of C8 by 100/255 gives the percentage value.
- 411195 = 4111 makes it clear that this data is the amount of pressing the accelerator pedal as a percentage at that moment. Multiplying the hexadecimal equivalent of 95 by 100/255 gives the percentage value.

With this formula, the average value is found and values that are not within the specified range are considered anomaly. In other words, those that are not within the appropriate range can be said to be an attack. Studies on the data were carried out by using the α value as 0.7 in this formula. This α value was chosen this way because it was the value that gave the best results in the tests. In addition, the value specified as X is expressed as sign value, and that value consists of the ratios of the 4 elements mentioned above and examined in CAN logs. Those ratios were taken into account as 24 percent for rpm, 40 percent for speed, and 18 percent each for fuel amount and accelerator pedal pressing. The results according to the data sets to which the EWMA algorithm is applied are included in the following headings. While choosing these values, the decision was made by testing the ratios given as a result of interviews with experts.

The flow diagram of the application of this algorithm is given below. As can be seen here, the values calculated in EWMA are calculated as a lambda ratio with the previous EWMA value and it is stated that if they exceed the standard values by 3 times, they are considered an error. These errors constitute an attack for this system.

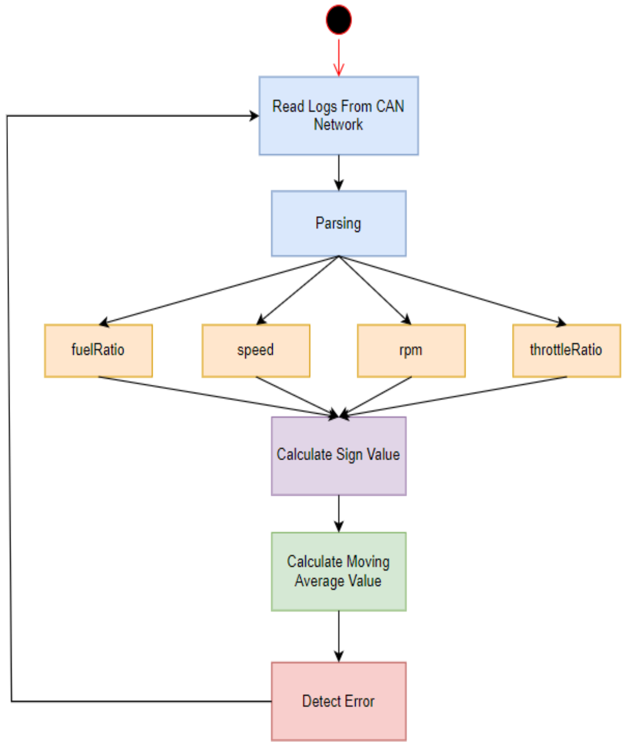

Figure 1. EWMA algorithm flow diagram

4. RESULTS

EWMA algorithm: Data set 1, which contains 80% non-attack and 20% attack; The results obtained with data set 2, which includes 70% non-attack and 30% attack situations, are included in this section. In addition, the results with the values of α in EWMA selected as 0.6 and 0.8 are also included in this section.

Data Set 1: This data set was examined on 80% normal data, 20% of which was attack.

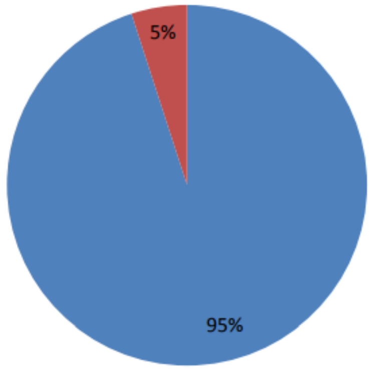

Figure 2. EWMA no-attack plot data set 1

The graph above shows that the EWMA algorithm makes the correct decision by detecting that there is no attack in 95% of cases, and detects that it is under attack in 5% of cases, even if there is no attack. Here it can be seen that the EWMA algorithm is the situation it detects in a certain period with the value of 0.7 α. In this case, the α value was determined according to the best result of the tests. The EWMA algorithm, with a value of 0.8 α, indicates that it makes the correct decision by detecting that there is no attack in 91% of the cases where there is no attack, and that it detects that it is under attack even if there is no attack in 9% of the cases. The EWMA algorithm, with a value of 0.6 α, indicates that it makes the correct decision by detecting that there is no attack in 87% of cases, and 13% of the time it detects that it is under attack even if there is no attack.

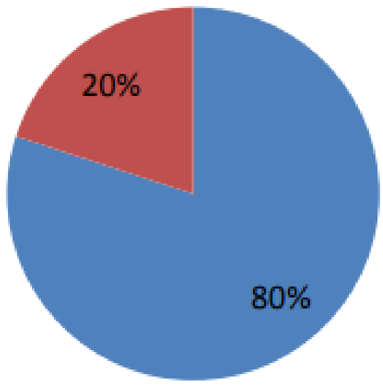

Figure 3. EWMA attack states graph data set 1

The graph above shows that the EWMA algorithm makes the correct decision by detecting an attack in 80% of cases, and detects that there is no attack in 20% of cases, even if there is an attack. Here it can be seen that the EWMA algorithm is the situation it detects in a certain period with the value of 0.7 α. In this case, the α value was determined according to the best result of the tests. The EWMA algorithm, with a value of 0.8 α, indicates that it makes the correct decision by detecting that there is an attack in 73% of cases, and that it detects that there is no attack even if there is an attack in 27% of cases. The EWMA algorithm, with a value of 0.6 α, indicates that it makes the correct decision by detecting that there is an attack in 70% of cases, and that it detects that there is no attack even if there is an attack in 30% of the cases.

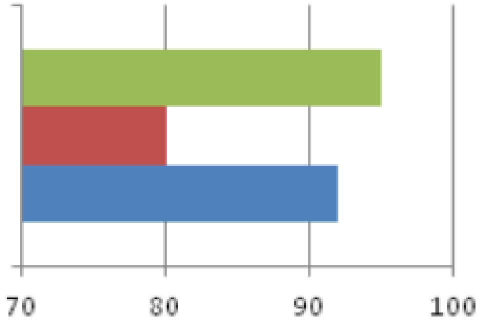

Figure 4. EWMA overall success rate chart data set 1

As can be seen in the graph above, for the EWMA algorithm, the attack detection success rate was found to be 80%, the success rate to detect non-attack situations was 95%, and in the light of all these, the overall success rate was found to be 92%. The actual result and produced result rates as a result of testing 6 cycles of test steps with the EWMA algorithm in each test step with the produced data set are as follows.

Table 1. EWMA algorithm results for data set 1

	Real Positive	Real Negative
Test Result Positive	19	1
Test Result Negative	1	4

Results details:

- Sensitivity: 19/20 = 95%,
- Specificity: 4/5 = 80%,
- Positive Predictive Value: 19/20 = 95%,
- Negative Predictive Value: 4/5 = 80%,
- Success Rate: 23/25 = 92%.

Data Set 2: This data set was examined on 70% normal data, 30% of which was attack.

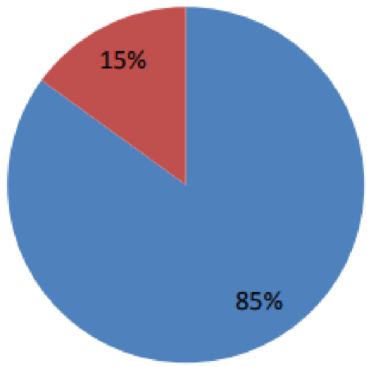

Figure 5. EWMA no-attack plot data set 2

The graph above shows that the EWMA algorithm makes the correct decision by detecting that there is no attack in 85% of the cases where there is no attack, and detects that it is under attack in 15% of the cases, even if there is no attack.

Here it can be seen that the EWMA algorithm is the situation it detects in a certain period with the value of 0.7 α. In this case, the α value was determined according to the best result of the tests. The EWMA algorithm, with a value of 0.8 α, indicates that it makes the correct decision by detecting that there is no attack in 82% of the cases, and 18% of the time it detects that it is under attack even if there is no attack. The EWMA algorithm, with a value of 0.6 α, indicates that it makes the correct decision by detecting that there is no attack 79% of the time, and 21% of the time it detects that it is under attack even if there is no attack.

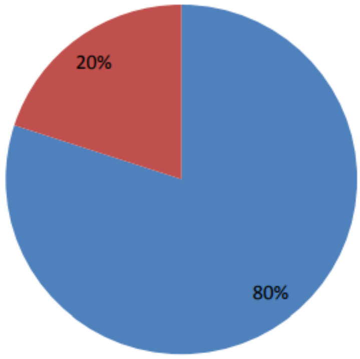

Figure 6. EWMA attack states graph data set 2

The graph above shows that the EWMA algorithm makes the correct decision by detecting an attack in 80% of cases, and detects that there is no attack in 20% of cases, even if there is an attack. Here it can be seen that the EWMA algorithm is the situation it detects in a certain period with the value of 0.7 α. In this case, the α value was determined according to the best result of the tests. The EWMA algorithm, with a value of 0.8 α, indicates that it makes the correct decision by detecting that there is an attack in 75% of the cases, and that it detects that there is no attack even if there is an attack in 25% of the cases. The EWMA algorithm, with a value of 0.6 α, indicates that it makes the correct decision by detecting that there is an attack in 73% of cases, and that it detects that there is no attack even if there is an attack in 27% of the cases.

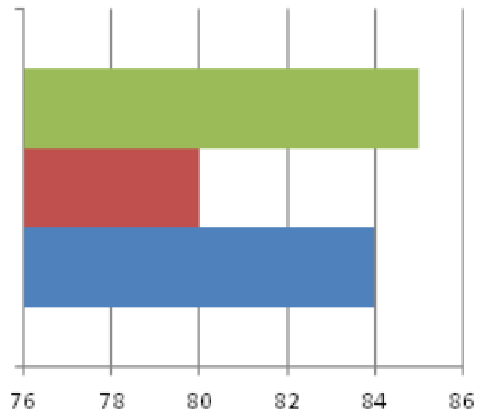

Figure 7. EWMA overall success rate chart data set 2

As seen in the graph above, for the EWMA algorithm, the attack detection success rate was found to be 80%, the success rate to detect non-attack situations was 85%, and in the light of all these, the overall success rate was found to be 84%. The actual result and produced result rates as a result of testing 6 cycles of test steps with the EWMA algorithm in each test step with the produced data set are as follows.

Table 2. EWMA algorithm results for data set 2

	Real Positive	Real Negative
Test Result Positive	17	3
Test Result Negative	1	4

Results details:

- Sensitivity: 17/20 = 85%,
- Specificity: 4/5 = 80%,
- Positive Predictive Value: 17/20 = 85%,
- Negative Predictive Value: 4/5 = 80%,
- Success Rate: 21/25 = 84%.

5. CONCLUSIONS

In this study, primarily the information regarding inter-vehicle communication in the literature is discussed. Additionally, the commands used in the CAN network and the values corresponding to these commands were examined. These commands used in the CAN network are tested with the algorithm determined in the light of this information. Test data was produced by outputting the hexadecimal values of attack and non-attack situations in the CAN network. There are two data sets used in this study. In each of these data sets, there is a moment when the 6-cycle vehicle is running, and there are 5 of these 6 cycles in each test step. In this way, there are 25 test cases in each data set. Out of these 25 data sets, 80% of them are non-attack and 20% are attack data. Data set 2 includes 70% non-attack and 30% attack cases. These data sets were tested in the EWMA algorithm and the results were evaluated.

As a result, when analyzing security attacks in smart vehicles, it can be determined whether there is an attack on the vehicle by listening to the CAN Network using the EWMA algorithm. In the tests performed, it is seen that the EWMA algorithm can achieve successful results in this regard. The ratios found can be further improved by changing the effect and calculation logic of the 4 elements mentioned above, rpm, speed, throttle and fuel, and by changing the α values in this algorithm, or better results can be found by testing with other algorithms.

Author contributions: All authors have contributed equally to the work.
Conflict of Interest: No conflict of interest was declared by the authors.
Financial Disclosure: The authors declared that this study has received no financial support.

REFERENCES

[1] Zhang, Y., Wang, Z., & Liu, X. (2022). "A Survey on Security and Privacy Issues in Smart Vehicles." IEEE Internet of Things Journal, 9(3), 1965-1981.

[2] Hussain, A., & Kim, S. (2023). "Mobile Communication in Smart Vehicle Networks: An Overview." Computer Networks, 229, 109537.

[3] Alazab, M., & Gupta, B. B. (2022). "Cybersecurity Challenges in Autonomous Vehicles: A Review." Computers & Security, 112, 102506.

[4] Bocca, F., & Barletta, G. (2021). "Analyzing Vulnerabilities in CAN Protocol for Smart Vehicle Security." Future Generation Computer Systems, 117, 365-375.

[5] Khan, M. A., & Rehman, A. (2023). "Artificial Intelligence in Vehicle Cybersecurity: A Comprehensive Review." Journal of Network and Computer Applications, 220, 103433.

[6] Mao, Y., & Zhou, Y. (2022). "Deep Learning for Anomaly Detection in Vehicle Networks." ACM Transactions on Internet Technology, 22(3), 1-30.

[7] Patel, S., & Singh, R. (2021). "Challenges in Vehicle Identification Information Distribution Systems." International Journal of Automotive Technology, 22(3), 613-620.

[8] Zhang, H., & Li, X. (2023). "The Role of Roadside Units in Enhancing Vehicle-to-Infrastructure Communication." Transportation Research Part A: Policy and Practice, 169, 209-224.

[9] Khan, M., et al. (2023). "Advancements in Vehicle-to-Vehicle Communication: A Review." Journal of Transportation Safety & Security, 15(2), 203-220.

[10] Liu, Y., & Zhang, Q. (2022). "Decentralized Communication Systems for Smart Vehicles." IEEE Transactions on Intelligent Transportation Systems, 24(4), 1085-1095.

[11] Smith, J., & Jones, A. (2023). "Infrastructure-to-Vehicle Communication: Challenges and Opportunities." Transport Research Part C: Emerging Technologies, 140, 103699.

[12] Chen, L., et al. (2023). "Direct Vehicle-to-Vehicle Communication: An Emerging Paradigm." Sensors, 23(7), 1235.

[13] Patel, M., & Singh, D. (2021). "A Comprehensive Study of Cybersecurity Measures for Smart Vehicles." Sensors, 21(15), 5150.

[14] Wang, F., et al. (2022). "Geocast Communication in Ad-Hoc Networks for Smart Vehicles." Journal of Network and Computer Applications, 193, 103303.

[15] Zhang, Z., & Li, H. (2023). "Emerging Trends in Smart Vehicle Security: Algorithmic Approaches." IEEE Access, 11, 12345-12358.

[16] Hussain, M., & Kim, S. (2023). "Recent Advances in Cybersecurity for Intelligent Transportation Systems: Challenges and Future Directions." IEEE Transactions on Intelligent Transportation Systems, 24(1), 12-25.

[17] Hyndman, R. J., & Athanasopoulos, G. (2021). Forecasting: Principles and Practice. 3rd ed. OTexts.

[18] Montgomery, D. C., Jennings, C. L., & Kulahci, M. (2008). Introduction to Time Series Analysis and Forecasting. John Wiley & Sons.

[19] Box, G. E. P., & Jenkins, G. M. (2015). Time Series Analysis: Forecasting and Control. 5th ed. Wiley.

[20] Tukey, J. W. (1985). "The Philosophy of Exploratory Data Analysis." American Statistician, 39(2), 94-98.

[21] West, M., & Harrison, J. (1997). Bayesian Forecasting and Dynamic Models. 2nd ed. Springer.

[22] Davis, R. A., & others. (2022). "Statistical Methods for Time Series Analysis." Annual Review of Statistics and Its Application, 9, 173-196.

[23] Tsai, C. H., & Wu, Y. L. (2022). "Adaptive Exponential Smoothing for Time Series Forecasting." Applied Mathematical Modelling, 103, 154-169.

[24] Iglewicz, B., & Hoaglin, D. C. (1993). How to Detect and Handle Outliers. Sage Publications.

[25] Lucas, J. M. (1985). "Monitoring for Outliers in Quality Control." Journal of Quality Technology, 17(1), 75-80.

Research Article
Academic Platform Journal of Engineering and Smart Systems (APJESS) 13(1), 7–16, 2025
https://dergipark.org.tr/en/pub/apjess
Received: 03-09-2024, Accepted: 24-10-2024
https://doi.org/10.21541/apjess.1542797

Determining International Irregularity Index (IRI) Values Through Artificial Neural Network (ANN) Modelling

[1] Hakan ASLAN, *[2] Recep Koray KIYILDI, [3] Kemal ERMİŞ

[1] Department of Civil Engineering, Sakarya University, Türkiye, haslan@sakarya.edu.tr
*[2] Corresponding Author, Department of Civil Engineering, Nigde Omer Halisdemir University, Türkiye, rkoray@ohu.edu.tr
[3] Department of Mechanical Engineering, Sakarya University of Applied Sciences, Türkiye, ermis@subu.edu.tr

Abstract

The quality of a pavement's level of service is generally determined by measuring the combinations of some important factors which affect the speed, travel time, freedom to maneuver, user comfort and convenience. In this study, a feed-forward back-propagation artificial neural network (ANN) algorithm is proposed based on the acquired International Irregularity Index (IRI) data for the highway structures, bridges and culverts, obtained through laser profilometer measurements on the surface irregularity of the bituminous hot mix roads. Analysis of ANN results were carried out through training various hidden number of neural networks for the output prediction, which is the best estimation of the surface irregularity of the roads. Results produced by artificial neural network have been compared with experimental and numerical results through extensive sets of non-training experimental data. As the comparison of results with ANN study having average absolute mean relative errors as 12.68% for bridges and 12.90% for culverts provided very accurate results, the model proposed could be used to obtain the surface irregularity of the roads by avoiding heavy duty of collecting numerous field data. The results obtained through ANN model were found more accurate than the results produced by numerical models.

Keywords: International Irregularity Index; Laser Profilometer; Artificial Neural Networks; Numerical Analysis

1. INTRODUCTION

The road network is known as an indicator of the level of development among countries. The project of a road network starts from planning and covers the design, construction and maintenance of the road throughout its service life. The pavement management system is a systematic approach that realizes these processes in the broadest sense. The performance of the highways put into service is quite high in the early days. However, it decreases due to factors such as traffic and climate conditions. These deteriorated roads affect the economy of the countries directly or indirectly. That is, if maintenance and repair are carried out before the pavement performance decreases to a certain level, the performance can be brought and kept to the desired level at a low cost. However, if no maintenance and repair work are carried out, the life of the road will end in a relatively short period of time [1].

As the budget allocated for the maintenance and repair of roads in many countries is quite limited, maintenance work should be carried out in a timely manner by determining the priority within the existing budget. In this way the pavement performance might be kept at a reasonable low cost and possible short time ending of road life is prevented. From this point of view, selection of improvement strategies is a crucial necessity to determine the most appropriate work program for the analyzed roads.

This obviously requires the resulting superstructure system to be applicable and stable at every stage with regard to economical, accurate and precise determining of the surface irregularities, slip resistance, and driving comfort [2]. The quality of a pavement's level of service, in this sense, is generally determined by measuring the combinations of some important factors which affect the speed, travel time, freedom of maneuver, and convenience [3].

For this purpose, performance prediction models have been developed to plan the required resource needs for the coming years by analyzing the deterioration level of the road surface. Solor̀zano et.al. showed that it is possible to develop IRI performance models using the IRI data of the main network of Spain, the RCE (State Road Network), even if the pavement structure is completely unknown and information about the time of the maintenance and rehabilitation activities were conducted is not provided. They, with this type of data, employed probabilistic models, more specifically, Markov chains, by means of transition probability matrices to provide an adequate solution for modelling the IRI evolution of the roads [4].

As many observations have shown, the lifespan of a superstructure designed to be 20 years can only be 10-12 years, and sometimes less, without maintenance and repair [5]. Accordingly, it is necessary to carry out planned and programmed maintenance and repairs in certain periods in order to benefit from a superstructure as it should.

A pavement management system is carried out in stages. Proper evaluation of road networks to be investigated should be evaluated at the first stage of the pavement management system. Following, the obtained data should be analyzed to determine the current condition of the road based on the factors affecting the performance of the road surface. As the final stage, the work program must be determined and selected as the most convenient strategy of the pavement management system. Through all these processes, the main objective is to acquire the improvement program that reveals when involvement should be made to make sure that the pavement performance will be kept at the desired level as much as possible in a most economical and sustainable way [6].

While the Superstructure Management System (MSM) did not include any performance prediction factor at the beginning for the initial condition assessments, later, on the other hand, a simple performance prediction model was developed based only on one factor, such as the age of the pavement. Different performance predictions are carried out using some combined data on variables such as climate conditions and traffic load in the currently implemented models [7].

Highway and transportation engineers study and investigate the surface irregularity of the roads for the different highways leading to many experimental studies [8]. In addition of the fact that it is not easy to obtain data from the field, experimental studies are costly. Therefore, numerical and different approximation methods are alternative methods for further analyses as they are less costly than the other methods. Pérez-Acebo et all developed deterministic IRI performance model based on the data available regarding the variables of thickness of bituminous materials, age of the pavement, the Annual Average Daily Traffic and type of the pavement. Their study revealed the fact that flexible and semi-rigid pavements have completely different behavior and they must be considered separately as their behavior depending on the distinguishing variables they have [9].

Zeng at. all [10] suggested an imaging-based DNN (Deep Neural Network) model through 2-dimensional pavement images as an alternative to vibration-based models for the identification of IRI values of the pavement.

Some of the research focused on limited experimental measurements to show the capability of the neural network technique in modelling surface irregularity phenomena of the roads [11]. Some research presented that the number and distribution of the training data are linked to the performance of the network when estimating the surface irregularity of the roads under different conditions [12].

Erkmen et al. [13] investigated the effect of engineering structures on surface irregularity by examining the interaction of the surface irregularity of the highway superstructure during and after the approaches to the engineering structures. In this context, International Irregularity Index (IRI) data obtained within the borders of the General Directorate of Highways in Turkey (KGM)-18th Regional (Kars) Directorate were used. They compared and assessed the effect of roadway structures on the irregularity of the asphalt structure through the analytical and statistical evaluation.

This study focuses on the prediction of the surface irregularity of the roads through experimental data and numerical model approach. Hence, an Artificial Neural Network (ANN) model was developed for the prediction of the surface irregularity of the roads with the data obtained from General Directorate of Highways in Turkey. Similar data used by Erkmen at all (2023) for analytical calculations were employed to set up the ANN model for the predictions of IRI values. The measurements were carried out and averaged for every 10m-long of the related highway sections by using Dynatest brand laser profilometer measurement device with serial number of 5051-4-278. It should be pointed out that the readings are obtained for the road sections before and after the engineering structures of bridges and culverts for the intervals of two sections of 150 meters up to 300 meters. In other words, roads were divided into 150m-long 4 different parts before and after the engineering structures, 26 bridges and 177 culverts, so that up to 300m road sections, hence 600m in total, were taken into consideration to collect the data. Furthermore, the IRI values for bridges and culverts were also obtained and averaged.

Artificial neural networks (ANN) are nonlinear mapping systems whose structure is based on principles inspired by the biological nervous systems of humans. An artificial neural network consists of large number of simple processors linked by weighted connections and provides a fundamentally different approach to forecasting modelling than numerical solution methods. This technique has been applied in many disciplines of science and has produced preliminary results in the many areas of modelling and investigations. Some of the authors considered the problem of accuracy in the surface irregularity of the roads by employing artificial neural network (ANN) models [14], [15], [16], [17].

Wu et al. [18] provides a comprehensive analysis of the patterns in predicting pavement roughness using artificial intelligence algorithms categorized into machine learning and deep learning by emphasizing the similarities and differences among them. They state that the influence of different maintenance behaviors on the long-term performance of pavement should be studied to clarify the pertinence of maintenance measures as far as the maintenance data is concerned.

Fakhri and Dezfoulian [19] suggested a method for pavement structural evaluation to assess pavement layers condition and identify needed rehabilitations. They developed a relationship between deflection bowl parameters derived from Falling Weight Deflectometer (FWD) and two pavement performance indices, International Roughness Index (IRI) and Pavement Surface Evaluation and Rating index (PASER). Artificial Neural Network (ANN) and regression models are used for this purpose. Their study revealed the fact that ANN models had superiority over non-intelligent regression models.

2. MATERIALS AND METHODS

Neuron is a basic processor in artificial neural networks. Each neuron has one output that is based on the situation of the neuron activation, and can receive many inputs from other neurons. With this sense, artificial neurons can be modelled as a multi-input nonlinear process with weighted interconnections.

The back-propagation algorithm the focus of the recent studies on modelling, is the most suitable method for training multi-layer feed-forward networks. The algorithm of training a back-propagation network is developed by using different literatures [20], [21], [22], [23], [24], [25], [26] and summarized as follows:

1. *Present a training pattern and propagate it through the network to obtain the outputs*

2. *Initialization:* Initialize all weights to small random values and threshold values: set all weights and threshold to small random values. Usually, the training sets are normalized to values between –0.1 and 0.9 during processing.

3. *The net input to the j^{th} node in the hidden layer*

$$net_j = \sum_{i=1}^{n} w_{ij} x_i - \theta_j \tag{1}$$

where *"i"* is the input node, *"j"* is the hidden layer node, *"x"* is the input, *"w_{ij}"* is the weights value connection from the *"i^{th}"* input node to the *"j^{th}"* hidden layer node and *"θ_j"* the threshold between the input and hidden layers.

4. *The output of the "j^{th}" node in the hidden layer:*

$$h_j = f_h\left(\sum_{i=1}^{n} w_{ij} x_i - \theta_j\right) \tag{2}$$

$$f_h\,(x) = \frac{1}{1+e^{-\lambda_h x}} \tag{3}$$

where *"h_j"* is the vector of hidden-layer neurons, *"$f_h(x)$"* is a logistic sigmoid activation function from input layer to hidden layer, *"λ_h"* is the variable which controls the slope of the sigmoidal function.

5. *The net input to the "k^{th}" node in the hidden layer*

$$net_k = \sum_{j} w_{kj} x_j - \theta_k \tag{4}$$

where k represents the output layer, w_{kj} is the weights connection from the *"j^{th}"* hidden layer node to the k^{th} output layer, *"θ_k"* is the threshold connecting the hidden and output layers.

6. *The output of the "k^{th}" node in the output layer:*

$$y_k = f_k\left(\sum_{j} w_{kj} x_j - \theta_k\right) \tag{5}$$

$$f_k\,(x) = \frac{1}{1+e^{-\lambda_k x}} \tag{6}$$

where *"y_k"* is the output of output-layer neurons, *"$f_k(x)$"* is a logistic sigmoid activation function from hidden layer to output layer, λ_k variable which controls the slope of the sigmoid functional.

7. *Compute errors:* The output layer error between the target and the observed output:

$$\begin{aligned} \delta_k &= -\left(d_k - y_k\right) f_k' \\ f_k' &= y_k(1-y_k) \quad \text{for sigmoid function} \end{aligned} \tag{7}$$

where *"δ_k"* is the vector of errors for each output neuron and *"d_k" is* the target activation of output layer. *"δ_k"* depends only on the error *(d_k-y_k)* and " f_k' " is the local slope of the node activation function for output nodes.

The hidden layer error:

$$\begin{aligned} \delta_j &= f_h' \sum_{k=1}^{n} w_{kj} \delta_k \\ f_h' &= h_j(1-h_j) \quad \text{for sigmoid function} \end{aligned} \tag{8}$$

where *"δ_j"* is the vector of errors for each hidden layer neuron. *"δ_j"* is a weighted sum of all nodes and the local slope " f_h' " of the node activation function for hidden nodes.

8. *Adjust the weights and thresholds in the output layer:*

$$w_{kj}^{(t+1)} = w_{kj}^{(t)} + \alpha \delta_k h_j + \eta\left(w_{kj}^{(t)} - w_{kj}^{(t-1)}\right) \tag{9}$$

$$\theta_k^{(t+1)} = \theta_k^{(t)} + \alpha \delta_k \tag{10}$$

where *"α"* is the learning rate, *"η"* is the momentum factor and *"t"* is time period.

It should be noted that the learning rate and the momentum factor are used to allow the previous weight change to influence the weight change in this time period, *"t"*. These calculation steps repeat until the output layer error is within desired tolerance for each pattern and neuron.

The feed-forward neural network has become the most popular among the various types of neural network in different applications. The back-propagation network is most commonly used for feed forward neural network as there is a mathematically strict learning scheme to train the network and guarantee mapping between inputs and outputs. In this study, an artificial neural network modelling for prediction of the surface irregularity of the roads is performed. In addition, a feed-forward back-propagation ANN approach is used for the training and learning processes. For the solution of the

ANN algorithm, a computer program has been developed in the C language. As neural networks need a range of input and output values to be between 0.1 and 0.9 to the restriction of sigmoid function, experimental field data and required data are both normalized in order to use the values. The equation of normalization is given as follows:

$$\frac{Act.data.-Min.data}{Max.data-Min.data} \times (High\ dat\ - Low\ dat\ ) + Low\ dat \qquad (11)$$

In this formula, minimum, maximum, high and low data refer to the annual minimum data value, the annual maximum data value, the maximum normalized data value (0.9), and the minimum normalized data value (0.1), respectively [27]. A three-layer feed-forward back-propagation neural network for the surface irregularity of the culverts of highways is performed as shown Figure 1. A three-layer feed-forward back-propagation neural network for the surface irregularity of the bridges of highways is performed as shown Figure 2.

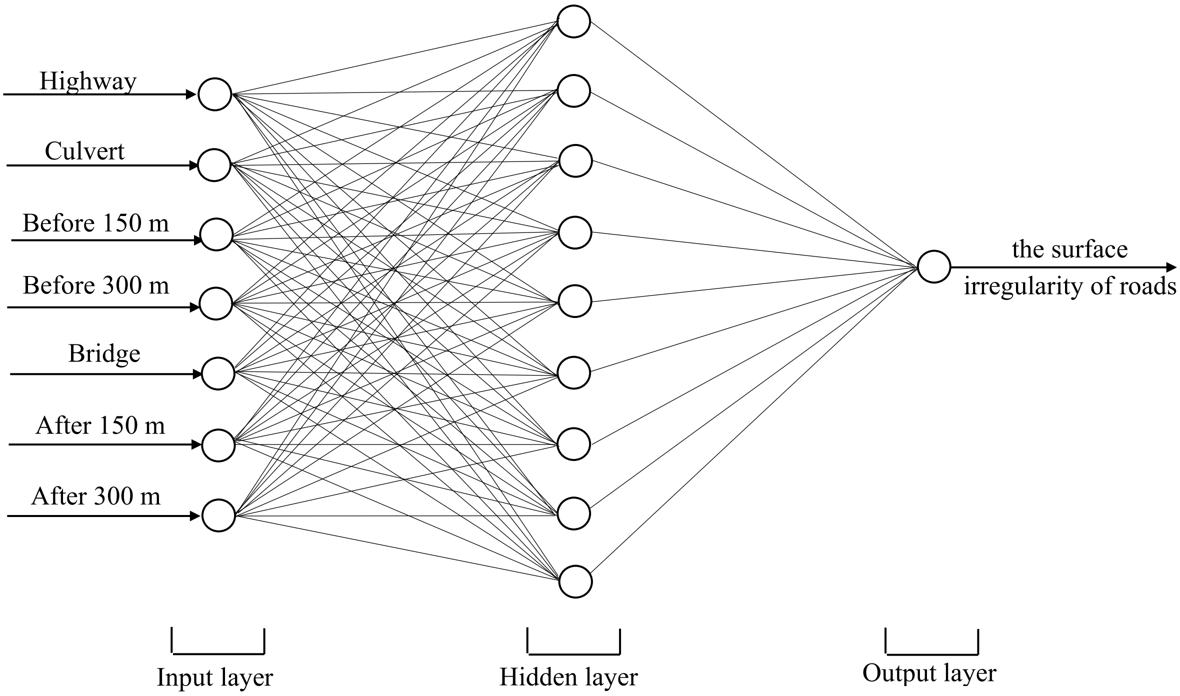

Figure 1. A three-layer feed-forward back-propagation neural network for the surface irregularity of the culverts of highways.

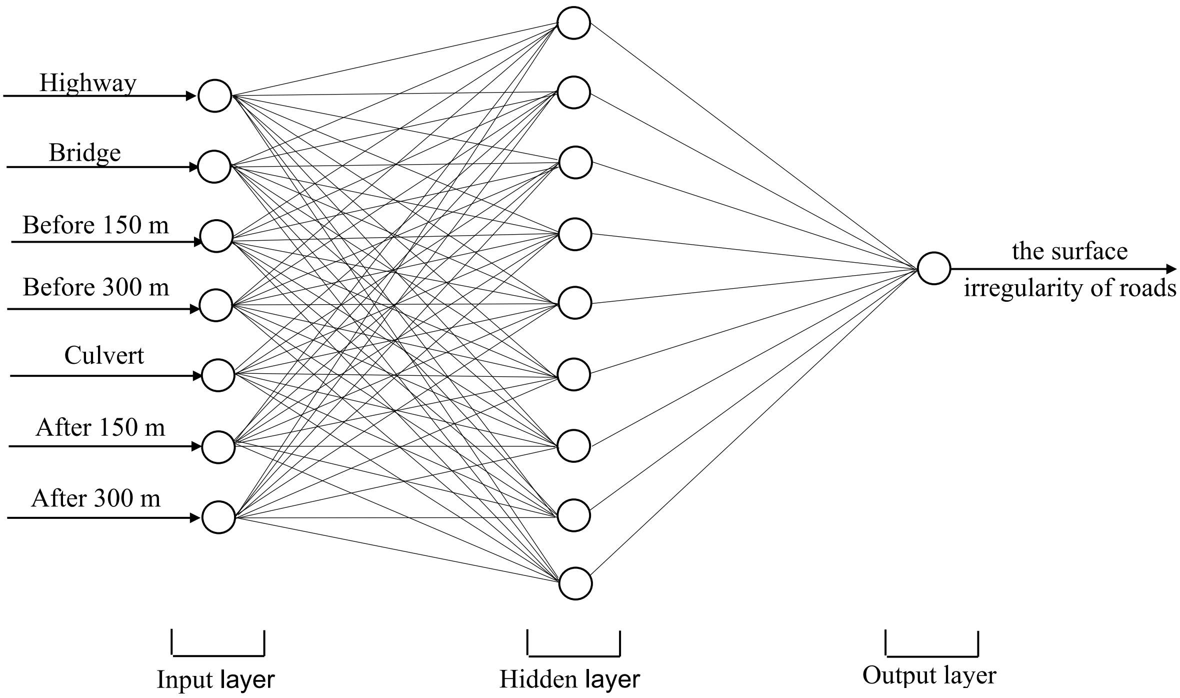

Figure 2. A three-layer feed-forward back-propagation neural network for the surface irregularity of the bridges of highways.

As far as the ANN analyses are concerned the network parameters were taken as the averaged IRI measurements taken along the two separate 150m long road sections of the highways both before and after the bridges and culverts for the highways. The lengths of the highways were also used as an input for the model. The outputs are the surface irregularity of the bridges and culverts respectively as illustrated in Figure 1 and Figure 2. The weights, biases and hidden node numbers are altered to minimize the error between the output values and the current data. In order to obtain the least error convergence, the configurations of the ANN are set by selecting the number of hidden layers and nodes along with the learning rate and momentum coefficient. The 745 cases of real measurements of data set related to culverts are divided into two sections. First 708 data groups (95% of all data) were used for trainings of the network and the remaining data group representing 37 cases were used for the verification of the ANN model. It should be noted that these data were randomly selected. The 130 cases of field measured data sets for bridges are also divided into two data sets. The first group consisting of 115 data set to be used for trainings of the network (88% of all data) and the other data group with 15 cases were used to validate the ANN model.

Table 1. The ANN model results for the surface irregularity of the culverts on 080-05 coded highway.

Location of the culverts on 080-05 coded highway (m)	Measured IRI Data-Averaged	ANN Model			
		ANN results	AMRE (%)	R^2	STD (%)
504	2.39	2.85	19.41	0.9623	0.03480
1440	2.25	2.33	3.64	0.9987	0.00955
2055	3.31	2.68	19.14	0.9634	0.02693
2549	1.48	1.22	17.25	0.9702	0.02391
3160	2.13	2.12	0.34	1.0000	0.00318
3537	1.56	1.80	15.50	0.9760	0.02854
3819	1.81	2.07	14.44	0.9792	0.02683
4081	1.66	1.98	19.55	0.9618	0.03501
4431	2.44	2.38	2.29	0.9995	0.00006
5088	2.15	2.54	17.95	0.9678	0.03246
5827	2.20	2.57	16.64	0.9723	0.03036
8100	5.81	4.68	19.44	0.9622	0.02741
10036	4.85	4.09	15.64	0.9755	0.02132
10472	3.58	3.94	10.07	0.9899	0.01985
11995	2.81	2.67	4.85	0.9976	0.00406
13449	1.02	0.83	18.19	0.9669	0.02542
15335	1.12	1.09	2.69	0.9993	0.00059
15645	1.18	1.07	9.13	0.9917	0.01091
15989	1.03	1.06	3.03	0.9991	0.00856
16338	1.42	1.15	19.31	0.9627	0.02720
16635	0.71	0.84	18.04	0.9674	0.03261
17058	1.41	1.14	19.20	0.9631	0.02703
17128	1.53	1.29	15.82	0.9750	0.02162
17841	1.29	1.09	15.63	0.9756	0.02131
19206	1.38	1.14	17.13	0.9707	0.02371
19843	1.08	1.17	8.42	0.9929	0.01719
20388	1.54	1.27	17.85	0.9681	0.02487
22087	0.94	1.12	19.16	0.9633	0.03439
22249	0.91	1.05	15.89	0.9748	0.02915
22973	1.10	1.30	18.56	0.9656	0.03343
24226	1.15	1.35	17.76	0.9685	0.03215
24447	1.38	1.36	1.23	0.9998	0.00175
28432	1.43	1.51	5.26	0.9972	0.01213
28669	1.64	1.51	7.77	0.9940	0.00873
28716	1.82	1.51	16.81	0.9717	0.02321
28827	2.05	1.81	11.60	0.9865	0.01486
29493	1.50	1.54	2.65	0.9993	0.00796
Average			12.90	0.9792	0.02062

Table 2. The ANN model results for the surface irregularity of the bridges on 080-03 coded highway.

Location of the bridges on 080-03 coded highway (m)	Location of the measurements on bridges	Measured IRI data-Averaged	ANN Model			
			ANN results	AMRE (%)	R^2	STD (%)
9487	after 300 m	2.32	2.78	19.65	0.9614	0.03518
20192	after 300 m	2.82	3.13	11.02	0.9879	0.02136
4691	after 300 m	1.44	1.72	19.27	0.9629	0.03458
9487	after 150 m	4.30	3.88	9.87	0.9903	0.01209
20192	after 150 m	3.36	3.82	13.84	0.9808	0.02587
4691	after 150 m	4.29	3.95	8.00	0.9936	0.00910
9487	over the bridge	4.17	4.57	9.62	0.9907	0.01912
20192	over the bridge	4.12	4.55	10.36	0.9893	0.02031
4691	over the bridge	3.80	4.48	18.01	0.9676	0.03255
9487	before 150 m	4.47	4.56	1.99	0.9996	0.00690
20192	before 150 m	4.05	4.73	16.78	0.9718	0.03059
4691	before 150 m	3.57	3.93	10.11	0.9898	0.01991
9487	before 300 m	3.52	3.15	10.49	0.9890	0.01308
20192	before 300 m	3.80	3.28	13.62	0.9814	0.01810
4691	before 300 m	3.46	2.85	17.51	0.9693	0.02432
	Average			12.68	0.9817	0.02154

The neural network model is basically formed for the surface irregularity of the culverts and bridges by using seven inputs (highways, the IRI values for culverts/bridges and the five 150m-long intervals of the highways defined before). The output on the other hand is the surface irregularity values of the culverts and bridges. As far as the hidden numbers are concerned, 5, 6 and 7 were tested. The most appropriate hidden number was found as 6 and this value was used in the analysis. In the algorithm, learning rates and momentum coefficients are taken as 0.6 for learning processes, in which 500,000 iterations were carried to obtain good fits. Furthermore, the three error measuring parameters were used to compare the performance of the various ANN configurations [28].

The performance of various ANN configurations was compared using the absolute mean relative error (AMRE), the standard deviations in the relative (STD) errors and the absolute fraction of variance (R^2). The following equations are used to acquire the related values for the assessment of the results.

$$\text{AMRE} = \frac{1}{\text{n}} \sum_{i=1}^{n} ABS(B) \tag{12}$$

$$\text{STD} = \sqrt{\frac{\sum_{i=1}^{n} \left(B - \bar{B}\right)^2}{n-1}} \tag{13}$$

$$\text{R}^2 = 1 - \left[\frac{\sum_{i=1}^{n} (a_i - y_i)^2}{\sum_{i=1}^{n} (y_i)^2} \right] \tag{14}$$

where B= $(y_i - a_i)/a_i$. "y_i" is the prediction value, "a_i" is the measurement value, and "n" is the number of data available.

Table 1 and Table 2 illustrate associated prediction errors, the absolute mean relative error (AMRE), the standard deviations in the relative (STD) errors and the absolute fraction of variance (R^2) with ANN configurations for the surface irregularity of the culverts and bridges in the learning process, respectively. In calculating the roughness of the surface of bridges and culverts, the hidden layer with 6 nodes in the ANN structure gave the best results in obtaining the prediction results in Table 1 and Table 2.

Comparison of the results obtained from the ANN analysis and the real field data was carried out through employing the absolute mean relative error (AMRE), the standard deviations in the relative errors (STD) and the absolute fraction of variance (R^2). The ANN model has 12.90% of average AMRE, 0.02062 of the STD and 0.9792 of R^2 for the surface irregularity of the culverts on 080-05 coded highway for the sections of 150m length after the culverts as shown in Table 1. As for the bridges, because of the limitation on the number of available data, the ANN model is developed and tested for the whole section of the highway with 080-03 code. The ANN model, in this case, resulted in 12.68% of average the AMRE, 0.02154 of the STD and 0.9817 of R^2 for the surface irregularity of the bridges as shown in Table 2.

Comparison of the results produced by the ANN model and the field data for the surface irregularity of the culverts on highway with 080-05 code for the road sections after 150m from the culverts are given in Figure 3. In similar way, Figure 4 illustrates the comparison of the ANN model results and the measured data for the surface irregularity of the bridges of 080-03 coded highway.

As can be seen from the tables above the developed ANN model produced satisfactory results in terms of evaluation criteria for the calculation of the surface irregularity of the culverts and bridges.

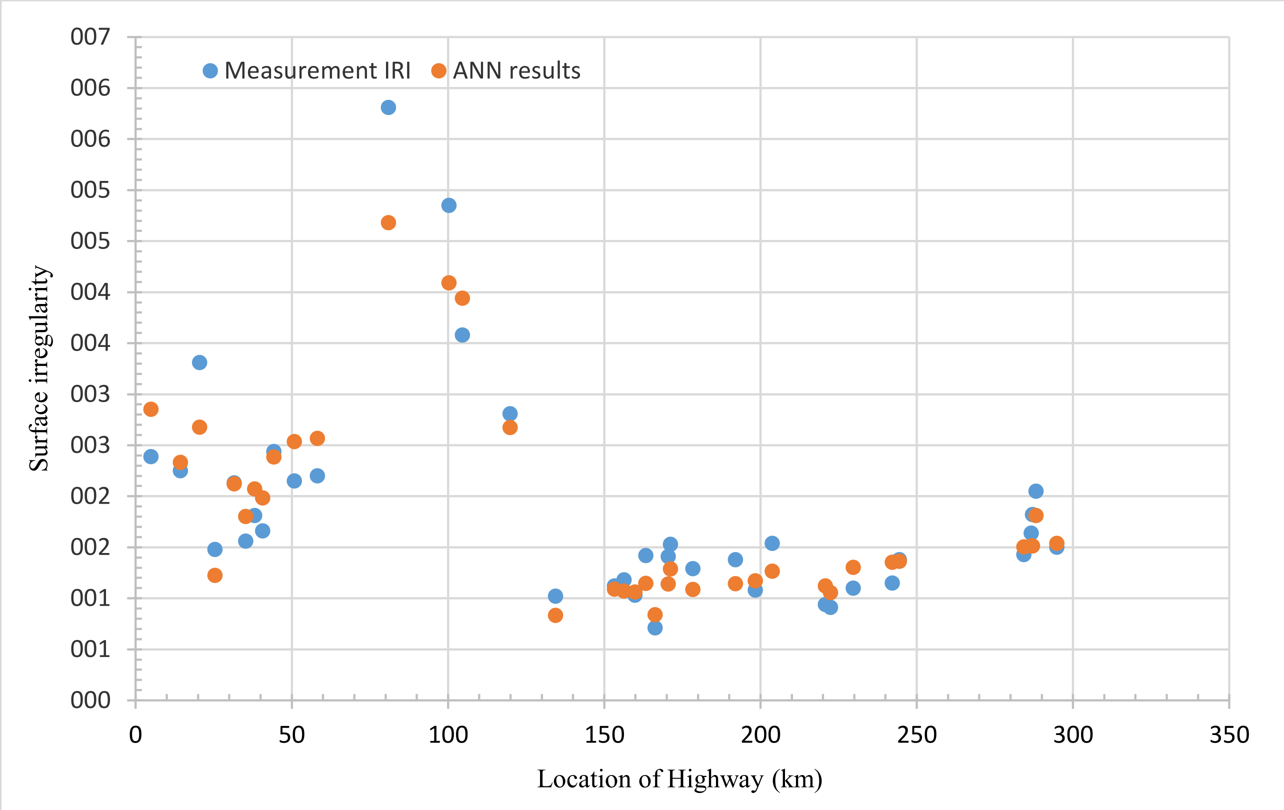

Figure 3. Comparison of the ANN model results and the measured data for the surface irregularity of the culverts on highway with the 080-05 code after 150 m on culverts.

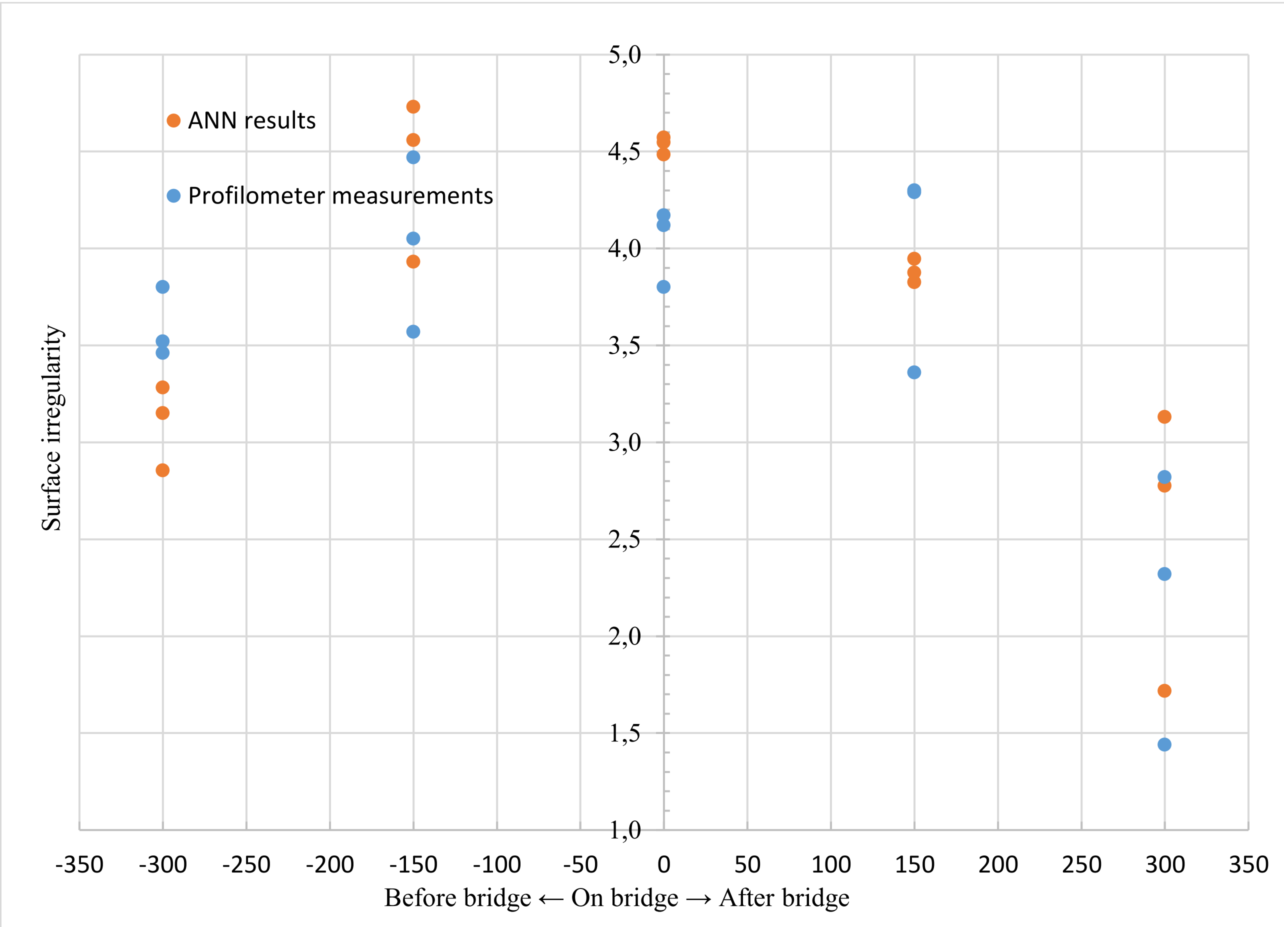

Figure 4. Comparison of the ANN model results and the measured data for the surface irregularity of the bridges for the highway with 080-03 code.

3. CONCLUSIONS

This study proposed an innovative ANN model for the calculation of surface irregularities for the bridges and culverts located in different highways based on the data obtained from General Directorate of Highways in Turkey. The findings of this study through developed ANN model led to the following concluding remarks.

- The ANN results indicate that the proposed model can be effectively used for the prediction of the surface irregularity of the bridges and culverts. The ANN approach is rather suitable for the prediction of surface irregularities of the bridges and culverts. As the proposed ANN model is based on a 6-hidden layer approach, the model effectively evaluates the importance levels of the factors and sets up the model accordingly to obtain reasonable and accurate results. Non-linear or Regression models do not provide the results with this accuracy.

- The ANN model has an average percentage value of 12.90 for AMRE, 0.02062 for STD and 0.9792 as R^2 for the surface irregularity of the culverts on highway with 080-05 code for 150m-length of the road sections from the culverts.

- The ANN model has average percentage values of 12.68 for AMRE, 0.02154 for STD and 0.9817 as R^2 for the surface irregularity of the bridges on 080-03 coded highway investigated.

- This research pointed out that ANN approach is an applicable and suitable method to predict the surface irregularities of the bridges and culverts when the related data cannot be obtained by field studies due to some physical, financial or time, professional staff and equipment related difficulties.

- This study was carried out to illustrate that artificial intelligence modelling is an effective and applicable approach to estimate the values of the highway surface irregularities based on the field data related to culverts and bridges. In this way, the effects of bridges and culverts on the IRI values of the asphalt structure of the highways to be constructed can be calculated and evaluated so that the time related applications may be put into practice as far as the maintenance programs are concerned.

- The next step of this research will be setting up new ANN models considering some important highway usage and construction parameters, such as annual average daily traffic, temperatures, heavy vehicle compositions, type of aggregates, available Marshall test results, to obtain the IRI values of the asphalt. In addition, the effect of the length and width of these constructional structures on IRI values will be investigated and modelled based on the nationwide data to be obtained from General Directorate of Highways in Turkey.

- The effectiveness of the model will also be tested by acquiring data from different regions.

NOMENCLATURE

a_i	experimental value
ANN	Artificial Neural Network
AMRE	Absolute Mean Relative Error
d_k	target activation of output layer.
h	vector of hidden-layer neurons
R^2	absolute fraction of variance
STD	Standard Deviation
t	time period
w_{ij}	weights connecting the i^{th} input node to the j^{th} hidden layer node
w_{kj}	weights connecting the j^{th} hidden layer node to the k^{th} output layer
x	multiple inputs
y	output
y_i	output value

Greek Letters

θ	external threshold,
θ_j	threshold between the input and hidden layers.
$f()$	logistic sigmoid activation function
$f_h()$	logistic sigmoid activation function from input layer to hidden layer
λ	variable which controls the slope of the sigmoid functional
θ_k	threshold connecting the hidden and output layers.
$f_k()$	logistic sigmoid activation function from hidden layer to output layer
f_k'	local slope of the node activation function for output nodes
δ_k	vector of errors for each output neuron
δ_j	vector of errors for each hidden layer neuron.
f_h'	local slope of the node activation function for hidden nodes
α	learning rate
η	momentum factor

Subscripts

h	hidden layer
i	input node, or initial condition
j	hidden layer node
k	output layer node
n	number of the data

Author contributions: All authors have contributed equally to the work.
Conflict of Interest: The authors declared that there is no conflict of interest.
Financial Disclosure: All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

REFERENCES

[1] Wen, T., Ding, S., Lang, H., Lu, J.J., Yuan, Y., Peng, Y., Chen, J., Wang, A., "Automated pavement distress segmentation on asphalt surfaces using a deep learning network". International Journal of Pavement Engineering,2022,doi:10.1080/10298436.2022.2027414.

[2] Kırbas, U, System Establishment of Superstructure Maintenance Management on Urban Roads, The case study of Turkey, 2013, PhD thesis, Istanbul University

[3] AASHTO, Pavement Management Guide, 2nd ed. American Association of State Highway and Transportation Officials; Washington, DC, USA, 2012.

[4] Ángela Alonso Solórzano, Heriberto Pérez Acebo, Alaitz Linares Unamunzaga, Hernán Gonzalo Orden., "Probabilistic International Roughness Index (IRI) prediction model for a climate homogeneous region".. Transportation Research Procedia 71, 46–52, 2023.

[5] Haas, R., & Hudson, W. R. "Pavement asset management". John Wiley & Sons, 2015.

[6] Siper. M., "Superstructure Performance Estimation with Artificial Intelligence Methods", MSc Thesis, Necmettin Erbakan University, Department of Industrial Engineering, 2021.

[7] Kulkarni, R. B., & Miller, R. W. "Pavement management systems: Past, present, and Future". Transportation Research Record, 1853(1), 65-71, 2003.

[8] G. Valdés-Vidal, A. Calabi-Floody , E. Sanchez-Alonso , C. Díaz , C. Fonseca, "Highway trial sections: Performance evaluation of warm mix asphalt and recycled warm mix asphalt", Construction and Building Materials Volume 262, 120069, 30 November 2020.

[9] Heriberto Pérez-Aceboa, Miren Isasab, Itziar Gurrutxagab, Harkaitz Garcíab, Aimar Insaustib, "International Roughness Index (IRI) prediction models for freeways", XV Conference on Transport Engineering, CIT2023, Transportation Research Procedia 71, 292–299, 2023.

[10] Jiangyu Zeng, Mustafa Gül, Qipei Mei, "A computer vision-based method to identify the international roughness index of highway pavements", Journal of Infrastructure Intelligence and Resilience 1, 100004, 2022.

[11] Jian Liu, Fangyu Liu, Chuanfeng Zheng, Ebenezer O. Fanijo, , Linbing Wang., " Improving asphalt mix design considering international roughness index of asphalt pavement predicted using autoencoders and machine learning" Construction and Building Materials Volume 360, 129439, 19 December 2022.

[12] G. Sollazzo, T.F. Fwa, G. Bosurgi, "An ANN model to correlate roughness and structural performance in asphalt pavements", Construction and Building Materials Volume 134, 1 March 2017, Pages 684-693.

[13] Erkmen ,F., Akdas,M.Emrah., Ruzgar, Y., Komut, M., and Altıok, S., "The surface irregularity analysis of the road sections approaching to the constructional structures in highways",The 5th highway national congress and exhibition", Ankara-Turkey, pp.365-379, 2023.

[14] Abdualmtalab Abdualaziz Ali, Abdalrhman Milad, Amgad Hussein, Nur Izzi Md Yusoff, Usama Heneash "Predicting pavement condition index based on the utilization of machine learning techniques: A case study", Journal of Road Engineering Volume 3, Issue 3, Pages 266-278, September 2023.

[15] Nima Sholevar, Amir Golroo, Sahand Roghani Esfahani "Machine learning techniques for pavement condition evaluation", Automation in Construction, Volume 136, 104190, April 2022.

[16] Muhammad Imran Khan, Nasir Khan, Syed Roshan Zamir Hashmi, Muhamad Razuhanafi Mat Yazid, Nur Izzi Md Yusoff, Rai Waqas Azfar, Mujahid Ali, Roman Fediuk, "Prediction of compressive strength of cementitious grouts for semi-flexible pavement application using machine learning approach", Case Studies in Construction Materials, Volume 19, e02370, December 2023.

[17] Mosbeh R. Kaloop, Sherif M. El-Badawy , Jong Wan Hu, Ragaa T. Abd El-Hakim, "International Roughness Index prediction for flexible pavements using novel machine learning techniques", Engineering Applications of Artificial Intelligence Volume 122, 106007, June 2023.

[18] Yanan Wu., Yafeng Pang., Xingyi Zhu, "Evolution of prediction models for road surface irregularity: Trends, methods and future", Construction and Building Materials, Volume 449, 138316, 2024.

[19] Mansour Fakhri., Reza Shahni Dezfoulian., "Pavement structural evaluation based on roughness and surface distress survey using neural network model", Construction and Building Materials, Volume 204, Pages 768-780, 2023.

[20] Ermis, K., Erek, A., and Dincer, I., "Heat transfer analysis of phase change process in a finned-tube thermal energy storage system using Artificial Neural Network," International Journal of Heat and Mass Transfer, 50, 3163-3175, 2007.

[21] Ermis, K., A. Midilli, I. Dincer ve M. A. Rosen, "Artificial Neural Network analysis of world green energy use," Energy Policy, 35, 1731-1743, 2007.

[22] Ermis, K., "ANN Modeling of compact heat exchangers,", International Journal of Energy Research, 32, 581-594, 2008.

[23] Reed R.D., Marks R.J., Neural Smithing: Supervised Learning in Feedforward Artificial Neural Networks, MIT Press, London, 1999.

[24] Rojas R., Neural Networks, Springer-Verlag, Berlin, 1996.

[25] Haykin S., Neural Networks: A Comprehensive Foundation, Prentice Hall, New Jersey, 1999.

[26] Fausett L., Fundamentals of Neural Networks: Architecture Algorithms and Applications, Prentice Hall, Englewood Cliffs, N.J., 1994.

[27] Nasr G.E., Badr E.A. and Joun C., "Backpropagation neural networks for modeling gasoline consumption", Energy Conversion and Management, 44, 893–905, 2003.

[28] Sablani S.S., Kacimov A., Perret J., Mujumdar A.S. and Campo A., "Non-iterative estimation of heat transfer coefficients using artificial neural network models", International Journal of Heat and Mass Transfer 48, 665–679, 2005.

Research Article
Academic Platform Journal of Engineering and Smart Systems (APJESS) 13(1), 17–21, 2025
https://dergipark.org.tr/en/pub/apjess
Received: 03-09-2024, Accepted: 28-12-2024
https://doi.org/10.21541/apjess.1542885

Modeling Objects with Artificial Intelligence Based Image Processing Techniques: Object Detection with Mask R-CNN

[1] Ömer Faruk EREKEN, [*2] Çiğdem TARHAN

[1] Department of Management Information Systems, Dokuz Eylul University, Türkiye, omerfarukereken@gmail.com
[*2] Corresponding Author, Department of Management Information Systems & BİMER, Dokuz Eylul University, Türkiye, cigdem.tarhan@deu.edu.tr

Abstract

Object detection and classification on digital images is an area of great importance in the digitalizing world. After deep learning methods started being implemented for object detection, classification and segmentation a rapid development has been observed in the field. Mask R-CNN is one of the most successful methods in the field and can be used for detection and segmentation purposes for many different objects. Our study focuses on the use of Mask R-CNN for weapon detection, specifically handguns. Today, there are many cameras in public areas and detecting weapons through these cameras before a forensic incident can provide great advantages. Our model achieved a mean average precision (mAP) of 0.78 in the detection of handguns on test data. Our findings demonstrate the potential of deep learning in security by detecting threats in images and live videos.

Keywords: Mask R-CNN; Deep Learning; Handgun Detection; Object Detection; Instance Segmentation

1. INTRODUCTION

In the digital world that we are living in today, digital images hold a very important position. Defining these images in a way that computers can understand has become increasingly valuable and recent advancements in deep learning, especially Convolutional Neural Networks (CNN), have made this process easier.

Making digital images understandable by machines is part of 'image processing'. If we set aside conceptual discussions, we can define image processing as a set of methods for analyzing, enhancing, and editing digital images [1].

While image processing consists of a broad area, our study specifically focuses on image classification, object detection and image segmentation, which are part of this field. Image classification is the process of classifying the images into what they represent. For example, if an image represents a class or not.

Object detection is the process of determining if there is a specific object on an image and the position of it. Image segmentation takes this one step further and does a pixel level classification and highlights the objects on the image. Image segmentation divides into two types; semantic segmentation which does an object category level segmentation and instance segmentation where a segmentation for every single object is conducted [2].

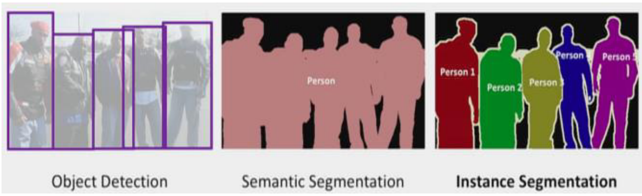

Figure 1. Detection and Segmentation [3].

The history of object detection can be divided into two main stages, with the critical point being the introduction of deep learning to the field. After the entrance of deep learning, everything changed drastically. In the first stage, we observed object detection algorithms that relied on handcrafted features. However, as the field became stagnant with handcrafted algorithms in the 2010s, a revolutionary approach was about to emerge. In 2014, R. Girshick et al. proposed their study on Regions with CNN features (R-CNN), which marked the beginning of a new era in object detection [4].

R-CNN is made from three components, category-independent region proposal generator (utilizing selective search), CNN which is extracting fixed-length feature vectors from every region, class-specific linear Support Vector Machine (SVM) [5]. R-CNN was a great breakthrough for its time, but it had its downsides like; a complex multi-stage pipeline, training being expensive, object detection and the whole process being too slow [6].

Aware of the weaknesses of R-CNN, R. Girshick proposed Fast R-CNN, which solved the drawbacks of R-CNN and enhanced its speed and accuracy. Fast R-CNN is a single-stage method where an image and a set of object proposals are taken as input. First, the whole image is passed into a CNN and a feature map is achieved. After that, every object proposal is processed with a Region of Interest pooling layer and a fixed-length feature vector is extracted from the feature map from the first stage. At the end, these feature vectors are sent to a SoftMax probability classifier and a bounding box regressor [6].

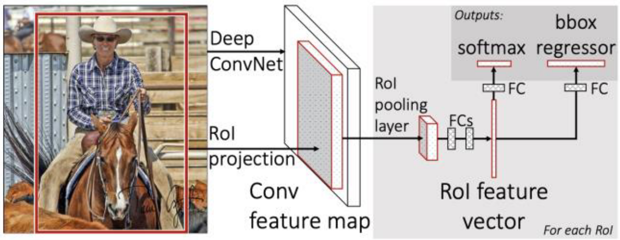

Figure 2. Fast R-CNN Architecture [6].

R-CNN and Fast R-CNN use selective search as a region proposal algorithm. Even though ROIs were introduced by Fast R-CNN, the computation of region proposals remained a bottleneck for object detection. To solve this Ren S. et.al. introduced the Region Proposal Network (RPN) with Faster R-CNN. In their study, they discovered that the convolutional feature maps employed by region-based detectors could also be utilized to generate region proposals. Briefly, RPN generates region proposals, which are subsequently passed to the ROI module. The cost-effectiveness of RPN was a significant advancement in object detection algorithms [7].

And the final algorithm we will mention, which we are using in this study, is Mask R-CNN. Mask R-CNN is a network that integrates instance segmentation capabilities into Faster R-CNN. Mask R-CNN has small differences compared to Faster R-CNN, but these small differences matter a lot. The first critical difference is the use of a new layer called ROI Align instead of ROI pooling, which enables pixel-to-pixel alignment between the network's input and outputs. Secondly, the mask and class prediction are separated [8].

Mask R-CNN can be used for a wide range of instance segmentation and object detection tasks. This versatility can be found through a simple academic search. Our focus in this study is weapon detection, specifically handguns for security purposes. With the increasing use of security cameras in public areas, the ability to detect weapons before they are used for criminal activities can be highly beneficial.

In this study we are using Mask R-CNN, which is the latest and most improved version of the R-CNN versions, thus our focus will be on this algorithm and its evolution. However, we do find value in briefly mentioning the You Only Look Once (YOLO) algorithm, which is one of the competing and popular algorithms in object detection and instance segmentation.

YOLO was introduced in 2016 as a fast (when compared to other algorithms), single step object detection model. The study aimed to build a model which works like a human glance, in other words to look at an image and directly detect objects. Other object detection systems use multiple components and complex pipelines which make the process slow and hard to optimize. In contrast, YOLO is rather simple, using a single convolutional network which predicts bounding boxes and class probabilities, and then filters the detections based on the model's confidence [9]. Over time, YOLO received a lot of interest and made big progress in accuracy and capabilities, including instance segmentation. Many different variants have been published and the model continues to be improved by researchers [10]. YOLOv8 model was shown to outperform Mask R-CNN, with higher precision and recall in less time [11].

2. LITERATURE REVIEW

There have been many studies using different methods to detect weapons in images. One of them is referenced in our dataset source, which focuses on an automatic handgun detection alarm system using CNN. The results of the study indicate that Faster R-CNN has shown the most promising outcomes. In this study, the training set is initially constructed using the outcomes from a VGG-16 based classifier to minimize the number of false positives. The study reports a recall rate of 100% and a precision rate of 84.21% [12].

Another similar study applied three CNN based models; YOLOv3, RetinaNet and Faster R-CNN to detect handguns in images. To reduce the number of false positives, they incorporated pose information on how handguns are held, which proved to be effective for one model. While YOLOv3 achieved the best precision and F1 scores without the added pose information, Faster R-CNN received lower results compared to RetinaNet and YOLOv3. With the inclusion of pose-related information, Faster R-CNN and RetinaNet showed decreased performance, whereas YOLOv3 displayed improvement. Overall, the highest rates were achieved with a 97.23% recall rate for RetinaNet without pose information and a 96.23% precision rate for YOLOv3 with pose information [13].

One study utilizes Mask R-CNN in their threat detection system, designed to detect suspicious objects in the images captured through cameras. They primarily employ CNN for classification on live camera images and subsequently use Mask R-CNN for instance segmentation on the cloud side. Regarding Mask R-CNN, they have provided only the overall average classification accuracy for classification purposes, which stands at 93.09% [14].

With the aim of preventing crimes before they happen, a study has utilized Mask R-CNN to detect guns in surveillance images. Their system takes an input image, applies preprocessing techniques like resizing, flipping etc. then they apply image sharpening with Gaussian Deblur technique and finally detect the mask with their trained model. Contrary to the popular evaluation techniques of Mask R-CNN, this study utilizes classical evaluation techniques. They achieved an F1 score of 84.69% with Mask R-CNN [15].

In a recent study called "Weapon detection system for surveillance and security" Yolo V5 is used for weapon detection and Mask R-CNN is used for instance segmentation. Before proceeding with the model training, various data augmentation and prepossessing methods are being applied. The study achieves 90.66% detection accuracy (DC) and 88.74% mean intersection over union (mIoU) [16].

All studies expressed above are focused on detecting weapons through normal camera images but there are also studies which focus on finding concealed weapons which are also very critical to detect forensic incidents. One of these studies tries to detect pistols from thermal images using deep learning. They have evaluated several deep learning algorithms for classification and segmentation. While the best result for detecting the pistols was achieved using a VGG 19-based convolutional neural network with an F1 score of 84%, for the second module which consisted of classification and bounding box detection, Yolo-V3 achieved the highest mean average precision of 95% [17].

Another area where deep learning is used for weapon detection is in X-ray images. One of the studies we examined introduced an anchor-free convolutional neural network (CNN) approach to detect weapons in X-ray baggage images. By eliminating the need for preset anchor box sizes and thus reducing computational complexity, the method demonstrates robust performance in detecting knives and handguns. By comparing different mainstream anchor-free and anchor-based methods the study has revealed that anchor-free methods YOLOx, Objects as Points and ExtremeNet have great performance in weapon detection on X-ray images [18].

All in all, there is continuous development in the use of deep learning techniques for security and surveillance. As seen in studies [12], [13], [14], [15], [16], [17] and [18], the aim is to build a system that will enhance public safety and prevent crimes through image processing techniques. The increasing number of studies suggest that there will be rapid progress in the field, and soon, using deep learning for safety will become common.

Another valuable point to mention is the new, popular Large Language Model (LLM) based tools. Even though LLMs are text-based and don't have a direct impact on object detection, as AI systems that understand user inputs, these models will undoubtedly enhance the user input/request in image processing.

3. MATERIALS AND METHODS

The first stage of our work was to create a comprehensive dataset that includes both labeled data for classification and segmentation purposes. To accomplish this, we utilized a pre-labeled dataset consisting of 3000 handgun images. These images were selected from the internet, representing at least one handgun in diverse situations [12]. The only problem about this dataset was that it only had bounding box annotations which can be used for object detection but not for instance segmentation. To solve this, we created a new dataset out of the mentioned dataset, containing 700 images (500 training, 100 validation, 100 test), annotated in COCO-style format.

Figure 3. Dataset Image Examples

The data set used for this study contains images from various conditions, however, for a real-world project the training set would need to be expanded to contain images from all types of possible conditions with objects which might resemble a gun but are not. Since this study was for educational purpose with limited resources we focused on training a prototype model.

In the original paper of Mask R-CNN it's stated that the code is made available on GitHub [5]. This code is written in python, and it's powered by the deep learning framework Caffe2 which is now deprecated and transferred to PyTorch repository. In this study we are using Mask R-CNN's deployment through Python 3, TensorFlow and Keras which can be found on a different GitHub repository [19]. The model is based on Feature Pyramid Network (FPN) and a ResNet101 backbone.

Data is crucial for training successful deep learning models, but sometimes obtaining sufficient amount of data can be challenging. To solve this issue, scientists have built a solution known as transfer learning. In transfer learning, you can access the learned weights from previous deep learning studies and enable your model to start training on your data after gaining knowledge about other classes. In our study we used the weights of Microsoft Common Objects in Context (Coco) dataset trained model for Mask R-CNN. Microsoft Coco is a data set which contains images from 91 different objects [20].

The evaluation of Mask R-CNN is different than standard deep learning algorithms. In Mask R-CNN we have object classification and segmentation predictions to evaluate. As stated in [13], popular object detection competitions have used mean average precision (mAP) as the primary evaluation metric for the models. We can briefly say that mAP is the mean of estimated area under the precision-recall curve. mAP value is used in multiclass detection problems where the Average precision (AP) value is averaged for all the classes. AP is an approximation of the area under precision-recall curve and it's obtained from the equation (1) by interpolating the curve values. $P(\tilde{r})$ in (2) represents the precision where the recall is $\tilde{r}$.

$$AP = \sum_{n=0}(r_{(n+1)} - r_n)P_{interp}(r_{(n+1)}) \quad (1)$$

in which:

$$P_{interp}(r_{(n+1)}) = \max_{\tilde{r}:\tilde{r}\geq r_{n+1}} P(\tilde{r}) \quad (2)$$

To determine if a prediction is True Positive (correct), False Negative (undetected) or False Positive (incorrect) confidence score and Intersection Over Union (IoU) values are used. Details for the evaluation of a Mask R-CNN model can be found in [21], [22] and [13]. We used the functions from [19] to calculate the mAP.

In order to enhance our handgun detection system, we used the python OpenCV library to conduct real-time predictions on streaming videos. This approach enabled generations of predictions directly from the video captured by our laptop camera. If this system gets implemented on security cameras it can provide efficient and prompt analysis to detect handguns.

4. FINDINGS

Our model trained on the coco-style formatted dataset gave us 0.81 mAP on training data, 0.78 mAP on validation and test data in 25 epochs. The instance segmentation was satisfying. You can find some examples of our predictions on the test data below.

Figure 4. Model Prediction Examples

The examples above are from the predictions made on images. Then we ran tests on live video. The results were also satisfying as seen on the screenshots below.

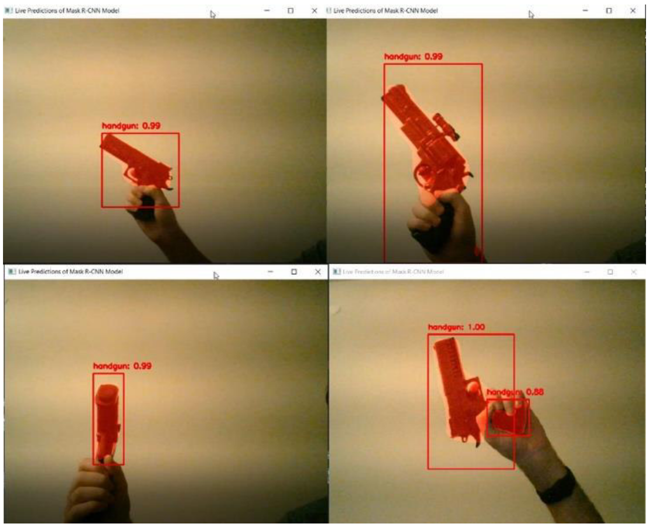

Figure 5. Predictions on Real-Time Video (With Toy Guns)

5. DISCUSSION AND CONCLUSIONS

It is obvious that deep learning is going to be used even more extensively in security issues in the future. A successfully trained AI system can detect security problems in seconds, which is usually not feasible for a person monitoring dozens of cameras, often becoming fatigued after hours of surveillance. The aim of Management Information Systems (MIS) is to help people and managers make decisions using the correct technologies. Using Mask R-CNN for security purposes is a great example of helping people through technology.

It's important to note that, although AI seems to bring great value for security, it may raise concerns regarding human rights. Continuous surveillance by AI will need strict regulations to prevent it from being controlled or used by wrong hands for improper purposes.

In this study, we aimed to demonstrate an example of how security threats can be detected both from images and live videos. In future studies our aim is to enhance our system's ability to detect a wide range of weapons in challenging environments and generate alarm signals for security forces through real-time video analysis.

Author contributions: Ömer Faruk EREKEN: Methodology, data processing, writing-original draft preparation; Çiğdem TARHAN: Conceptualization, methodology, writing-reviewing and editing.
Conflicts of interest: The authors declare no conflicts of interest.
Ethical Statement: This article is an expanded version of the paper titled 'Modeling Objects With Artificial Intelligence Based Image Processing Techniques: Handgun Detection With MASK R-CNN' presented at the 10th International Conference on Management Information Systems (IMISC 2023) held on 18-20 October 2023.
Financial Disclosure: The authors declared that this study has received no financial support.

REFERENCES

[1] The Editors of Encyclopedia Britannica, “Image processing”, Encyclopedia Britannica, Accessed on: Feb. 27, 2023. [Online]. Available: https://www.britannica.com/technology/image-processing

[2] S. Minaee, Y. Boykov, F. Porikli, A. Plaza, N. Kehtarnavaz, and D. Terzopoulos, "Image segmentation using deep learning: A survey," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 7, pp. 3523-3542, 2021. [Online]. Available: https://arxiv.org/pdf/2001.05566.pdf

[3] Computer Vision Foundation Videos, "Mask R-CNN," YouTube, Nov. 17, 2017. [Online]. Available: https://www.youtube.com/watch?v=g7z4mkfRjI4

[4] Z. Zou, K. Chen, Z. Shi, Y. Guo, and J. Ye, "Object Detection in 20 Years: A Survey," 2023. [Online]. Available: https://arxiv.org/abs/1905.05055v3

[5] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," 2014. [Online]. Available: https://arxiv.org/abs/1311.2524

[6] R. Girshick, "Fast R-CNN," 2015. [Online]. Available: https://arxiv.org/abs/1504.08083v2

[7] S. Ren, K. He, R. Girshick, and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," 2016. [Online]. Available: https://arxiv.org/abs/1506.01497v3

[8] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," 2018. [Online]. Available: https://arxiv.org/abs/1703.06870v3

[9] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 779–788.

[10] M. Hussain, "YOLO-v1 to YOLO-v8, the Rise of YOLO and Its Complementary Nature toward Digital Manufacturing and Industrial Defect Detection," Machines, vol. 11, 2023, Art. no. 677. [Online]. Available: https://doi.org/10.3390/machines11070677

[11] R. Sapkota, D. Ahmed, and M. Karkee, "Comparing YOLOv8 and Mask R-CNN for instance segmentation in complex orchard environments," Artificial Intelligence in Agriculture, vol. 13, pp. 84–99, 2024. [Online]. Available: https://doi.org/10.1016/j.aiia.2024.07.001

[12] R. Olmos, S. Tabik, and F. Herrera, "Automatic handgun detection alarm in videos using deep learning," Neurocomputing, vol. 275, pp. 66-72, 2018. [Online]. Available: doi: 10.1016/j.neucom.2017.05.012

[13] J. Salido, V. Lomas, J. Ruiz-Santaquiteria, and O. Deniz, "Automatic handgun detection with deep learning in video surveillance images," Applied Sciences, vol. 11, no. 13, p. 6085, 2021. [Online]. Available: doi: 10.3390/app11136085

[14] A. A. Ahmed and M. Echi, "Hawk-eye: An AI-powered threat detector for intelligent surveillance cameras," IEEE Access, vol. 9, pp. 63283-63293, 2021.

[15] A. Goenka and K. Sitara, "Weapon Detection from Surveillance Images using Deep Learning," in 3rd International Conference for Emerging Technology (INCET), 2022. pp. 1-6. [Online]. Available: doi: 10.1109/INCET54531.2022.9824281

[16] S. Khalid, A. Waqar, H. U. Ain Tahir, O. C. Edo, and I. T. Tenebe, "Weapon detection system for surveillance and security," in 2023 International Conference on IT Innovation and Knowledge Discovery (ITIKD), Manama, Bahrain, 2023. pp. 1-7. [Online]. Available: doi: 10.1109/ITIKD56332.2023.10099733

[17] O. Veranyurt and C. O. Sakar, "Concealed pistol detection from thermal images with deep neural networks," Multimed Tools Appl, vol. 82, pp. 44259–44275, 2023. [Online]. Available: doi: 10.1007/s11042-023-15358-1

[18] Y. Huang, X. Fu, and Y. Zeng, "Anchor-Free Weapon Detection for X-Ray Baggage Security Images," IEEE Access, vol. 10, pp. 97843-97855, 2022.

[19] W. Abdulla, "Mask R-CNN for object detection and instance segmentation on Keras and TensorFlow," GitHub, 2017. [Online]. Available: https://github.com/matterport/Mask_RCNN

[20] T.-Y. Lin, M. Maire, S. Belongie, L. Bourdev, R. Girshick, J. Hays, P. Perona, D. Ramanan, C. L. Zitnick, and P. Dollár, "Microsoft COCO: Common Objects in Context," 2015. [Online]. Available: https://arxiv.org/abs/1405.0312v3

[21] R. Padilla, S. L. Netto, and E. A. B. da Silva, "A Survey on Performance Metrics for Object-Detection Algorithms," in Proceedings of the 2020 International Conference on Systems, Signals and Image Processing (IWSSIP), Niteroi, Brazil, 2020.

[22] R. Padilla, W. L. Passos, T. L. B. Dias, S. L. Netto, and E. A. B. da Silva, "A Comparative Analysis of Object Detection Metrics with a Companion Open-Source Toolkit," Electronics, vol. 10, p. 279, 2021.